ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ СЕМЕНА КУЗНЕЦЯ
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Кваліфікаційна наукова
праця на правах рукопису

Євсеєв Сергій Петрович

УДК 004.056:336.71

ДИСЕРТАЦІЯ

МЕТОДОЛОГІЯ ПОБУДОВИ СИСТЕМИ БЕЗПЕКИ БАНКІВСЬКИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ

21.05.01 – Інформаційна безпека держави
Галузь знань – Інформаційні технології

Подається на здобуття наукового ступеня доктора технічних наук

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ С. П. Євсеєв

Науковий консультант:
Грищук Руслан Валентинович,
доктор технічних наук,
старший науковий співробітник

Київ – 2018

АНОТАЦІЯ

Євсеєв С.П. Методологія побудови системи безпеки банківських інформаційних ресурсів. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора технічних наук (доктора наук) за спеціальністю 21.05.01 – інформаційна безпека держави (125 Кібербезпека). – Харківський національний економічний університет імені Семена Кузнеця, Національний авіаційний університет, м. Київ, 2018.

У сучасних умовах, як показала практика, важлива роль у забезпеченні національної безпеки України та особливо її економічної складової належить процесам забезпечення інформаційної безпеки держави в банківському секторі. Ключову роль при побудові систем безпеки банківських інформаційних ресурсів як складових національних інформаційних ресурсів держави, відіграє теорія та практика, в якій науково-методологічна база є основою для прийняття обґрунтованих та ефективних управлінських рішень суб'єктами забезпечення інформаційної безпеки держави на усіх рівнях.

Революційні зміни останнього десятиліття, що відбулися в банківському секторі, зумовили об'єднання інформаційних та комп'ютерних мереж в єдиний інформаційний та кібернетичний простір, що спонукало до створення автоматизованих банківських систем, які істотно розширили спектр електронних послуг державних і комерційних банків світу та України. Як наслідок, суттєво трансформувалися і загрози такому національному інформаційному ресурсу держави, як банківські інформаційні ресурси під якими в роботі розуміється банківська інформація. Загрози безпеці банківських інформаційних ресурсів набули ознак гібридності. Прояви ознак гібридності внаслідок одночасного впливу загроз інформаційній безпеці, кібернетичній безпеці та безпеці інформації на банківські інформаційні ресурси призвели до виникнення явища синергізму, негативні прояви якого потребують кардинального перегляду концепцій побудови діючих систем безпеки. Як показує світовий досвід, прояви гібридних загроз безпеці банківських інформаційних ресурсів мали місце, наприклад, під час блокування роботи автоматизованих банківських систем організацій банківського

сектору в США (вересень, 2011 р.), що призвело виникнення масової акції непокори під назвою “Захопи Уолл-Стрітт”, яка ланцюговою реакцією поширилася на найбільші міста згаданої держави та ряду найбільш економічно розвинених держав Європейського Союзу та зрештою спровокувала світовий економічний колапс. Прояви гібридних загроз безпеці банківських інформаційних ресурсів мали місце і в Україні. Наприклад, розпочавшись з кібератаки за допомогою шкідливого програмного забезпечення “Petya.A”, “Petya.B” (червень–липень, 2017 р.) було скомпрометовано процес надання банківських послуг, що викликало невдоволення клієнтів банків – громадян, які є суб’єктами інформаційної безпеки держави. Ланцюгова реакція після України поширилася на банківські сектори Італії, Ізраїлю, Сербії, Румунії, Угорщини, Аргентини, Чехії, Німеччини та інших розвинених держав світу. Таким чином, проблема забезпечення інформаційної безпеки держави для інфраструктур критичного застосування, до яких належить і банківський сектор, стоїть дуже гостро. Отже, стає зрозуміло, що потребують кардинального перегляду діючі методологічні засади побудови системи безпеки банківських інформаційних ресурсів як України зокрема, так і світу в цілому.

Перспективним підходом до безпеки банківських інформаційних ресурсів є одночасне та раціональне поєднання організаційних і технічних зусиль банку, спрямованих на забезпечення інформаційної безпеки, кібербезпеки та безпеки інформації, що зрештою позначиться на інвестиціях банку, вкладених у безпеку. При цьому комплексування сил і засобів безпеки у кожному окремому випадку не можна вважати ефективним та таким, що гарантує досягнення очікуваного безпекового синергетичного ефекту.

Таким чином, дисертація присвячена вирішенню об’єктивного протиріччя між зростаючими на практиці вимогами до безпеки банківських інформаційних ресурсів при одночасному збільшені кількості та технологічній складності загроз безпеці і набутті ними ознак гібридності та недосконалістю, а подекуди й відсутністю методології побудови системи безпеки банківських інформаційних ресурсів від таких загроз, що є актуальною науково-прикладною проблемою не тільки для України, а й для світу в цілому.

На основі проведеного дослідження було одержано такі основні наукові результати, що виносяться на захист:

1. *Вперше розроблено* концепцію побудови синергетичної моделі загроз безпеки банківських інформаційних ресурсів, базис якої становить трирівнева модель стратегічного управління безпекою банківських інформаційних технологій. Розроблена на основі концепції модель за рахунок комплексування складових інформаційної безпеки, кібербезпеки та безпеки інформації відкриває новий напрямок у забезпеченні безпеки банківських інформаційних ресурсів на основі моделі стратегічного управління банком з урахуванням величини ризику на кожному рівні та дієвого контролю за виконанням функцій системи управління інформаційною безпекою організацій банківського сектору.

2. *Удосконалено* класифікатор загроз безпеці банківських інформаційних ресурсів, який, на відміну від відомих, ґрунтується на синергетичній моделі загроз, що дозволяє класифікувати загрози за складовими безпеки, видами послуг та рівнями ієрархії інфраструктури автоматизованих банківських систем, оцінювати синергію та гібридність загроз інформаційній безпеці, кібербезпеці, безпеці інформації, ймовірність їх впливу на безпеку банківських інформаційних ресурсів.

3. *Вперше розроблено* метод оцінювання узагальненого показника рівня захищеності банківських інформаційних ресурсів на основі синергетичної моделі загроз, удосконалених класифікатора та моделі зловмисника, моделі оцінки захищеності банківських інформаційних ресурсів, та моделі інфраструктури автоматизованої банківської системи, що надає можливість встановлення взаємозв’язків між елементами ієрархічної структури автоматизованої банківської системи, каналами зв’язку, інформаційними активами банківських інформаційних ресурсів та загрозами інформаційній безпеці, кібербезпеці, безпеці інформації для досягнення синергетичного ефекту та визначення рівня захищеності банківських інформаційних ресурсів.

4. *Вперше розроблено* метод забезпечення конфіденційності та цілісності банківських інформаційних ресурсів, який ґрунтується на гібридних крипто-кодових конструкціях зі збитковими кодами на основі модифікованої крипто-

кодової системи Мак-Еліса на модифікованих алгеброгеометричних кодах, що дозволяє підвищити рівень інформаційної прихованості та достовірності банківських інформаційних ресурсів в умовах дії гібридних загроз.

5. *Вперше розроблено* метод забезпечення автентичності банківських інформаційних ресурсів, який ґрунтується на гібридних крипто-кодових конструкціях зі збитковими кодами на основі модифікованих несиметричних крипто-кодових системах Мак-Еліса і Нідеррайтера на модифікованих алгеброгеометричних кодах, що дозволяє підвищити рівень інформаційної прихованості та достовірності *OTP*-паролів в протоколі двофакторної автентифікації.

6. *Набув подальшого розвитку* метод оцінювання безпеки банківських інформаційних ресурсів, що, на відміну від відомих, враховує комплексний показник ефективності інвестицій, які виділяються на забезпечення безпеки банківських інформаційних ресурсів, що дозволяє оптимізувати витрати коштів на її побудову в умовах впливу гібридних загроз при одночасному забезпеченні заданого рівня їх безпеки.

7. *Вперше розроблено* методологію побудови системи безпеки банківських інформаційних ресурсів, в основу якої покладено концепцію побудови синергетичної моделі загроз, удосконалений класифікатор загроз, методи забезпечення конфіденційності, цілісності та автентичності банківських інформаційних ресурсів на гібридних крипто-кодових конструкціях зі збитковими кодами та удосконалений метод оцінювання безпеки банківських інформаційних ресурсів на основі комплексного показника ефективності інвестицій, що дозволяє відкрити новий (емерджентний) з позицій безпеки та ефективний з позицій витрачених коштів підхід до побудови діючих та перспективних систем безпеки банківських інформаційних ресурсів.

Наукова цінність основних положень дисертації полягає у розробленні принципово нової методології створення системи безпеки банківських інформаційних ресурсів, в основу якої покладено запропоновану концепцію побудови синергетичної моделі загроз безпеці банківських інформаційних

ресурсів, базис якої становить трирівнева модель стратегічного управління безпекою банківських інформаційних технологій, що забезпечує одержання синергетичного ефекту в умовах одночасної дії загроз інформаційної безпеки, кібербезпеки та безпеки інформації і, як наслідок, сприяє визначенню якісно нових і невідомих до цього емерджентних властивостей системи безпеки банківських інформаційних ресурсів з урахуванням коштів, витрачених на її створення.

Практична цінність роботи полягає в тому, що розроблено класифікатор загроз безпеки банківських інформаційних ресурсів (електронний доступ: *http://skl.hneu.edu.ua/*), який на відміну від відомих дозволяє в он-лайн режимі здійснювати класифікацію та оцінювати ймовірності впливу загроз інформаційної безпеці, кібербезпеці, безпеці інформації на банківські інформаційні ресурси, а також визначати рівень безпеки банківських інформаційних ресурсів на основі синергетичної моделі загроз, удосконалених моделі зловмисника, моделі інфраструктури автоматизованої банківської системи, моделі оцінки захищеності банківських інформаційних ресурсів, оптимізації витрати коштів на побудову системи безпеки банківських інформаційних ресурсів. Впровадження розроблених методів забезпечення конфіденційності, цілісності та автентичності банківських інформаційних ресурсів на гібридних крипто-кодових конструкціях забезпечує зменшення в 2 – 3 рази енергетичних витрат при використанні у складі автоматизованих банківських систем відкритих каналів зв’язку й передачі даних при одночасному забезпеченні заданих показників безпеки.

Ключові слова: безпека банківських інформаційних ресурсів, автоматизована банківська система, синергетична модель загроз безпеці БІР, класифікатор загроз безпеці БІР, інформаційна безпека, кібербезпека, безпека інформації, інвестиції, емерджентні властивості, синергетичний ефект, гібридні крипто-кодові конструкції на збиткових кодах, модифіковані еліптичні коди, методологія.

ABSTRACT

Yevseyev S.P. Methodology for building a security system for banking information resources. – Qualifying scientific work on the rights of manuscripts.

Thesis for a Doctor of Technical Science degree in specialty 21.05.01 – "Informational State Security" (125 Cybersecurity). – Simon Kuznets Kharkiv National University of Economics, National Aviation University, Kyiv, 2018.

In modern conditions, as practice has shown, the important role in ensuring the national security of Ukraine and especially its economic component belongs to the processes of ensuring information security of the state in the banking sector. A key role in the construction of security systems for banking information resources as a component of national information resources of the state is played by theory and practice, in which the scientific and methodological basis is the basis for making informed and effective management decisions by the subjects of ensuring information security of the state at all levels.

The revolutionary changes of the last decade in the banking sector have led to the integration of information and computer networks into a single information and cybernetic space, which has led to the creation of automated banking systems that have substantially expanded the spectrum of electronic services of state and commercial banks of the world and Ukraine. As a result, threats to such a national information resource of the state as the banking information resources under which the banking information refers. Threats to the security of banking information resources have become signs of hybridization. Manifestations of hybridity as a result of the simultaneous impact of threats to information security, cybernetic security and information security on banking information resources have led to the emergence of synergies, the negative manifestations of which require a radical revision of the concepts of the construction of existing security systems. As world experience shows, for example, manifestations of hybrid threats to the security of banking information resources took place while the automated banking systems of the banking sector were blocked by the banking sector organizations in the United States (Sep 2011), which led to a massive disobedience action called "Take the Wall Street". Which chain reaction spread to the largest cities of the said state and a

number of the most economically developed countries of the European Union and eventually provoked global economic collapse. Manifestations of hybrid threats to the security of banking information resources also took place in Ukraine. For example, starting with a cyberattack with the help of malicious software “Petya.A”, “Petya.B” (June-July, 2017), the process of providing banking services was compromised, which caused dissatisfaction with clients of banks – citizens who are sub The information security of the state. Chain reaction after Ukraine spread to banking sectors of Italy, Israel, Serbia, Romania, Hungary, Argentina, Czech Republic, Germany, and others main countries of the world. Thus, the problem of ensuring information security of the state for infrastructures of critical use, which includes the banking sector, is very acute. Thus, it becomes clear that there is a need for a radical revision of the current methodological principles for building a security system for banking information resources both for Ukraine and for the world as a whole.

A promising approach to the security of banking information resources is a simultaneous and rational combination of organizational and technical efforts of the bank aimed at providing information security, cyber security and security information, which ultimately affects the investments of the bank, dedicated to security. At the same time, the integration of forces and security in each individual case cannot be considered effective and one that guarantees the achievement of the expected security synergetic effect. Thus, the dissertation is devoted to the solution of the objective contradiction between the growing requirements in the security of banking information resources in practice, while increasing the quantity and technological complexity of security threats and gaining signs of hybridity and imperfection, and in some cases, and the lack of a methodology for building a security system for banking information resources from such threats, which is an actual scientific and applied problem not only for Ukraine, but also for the world as a whole.

On the basis of the conducted research the following basic scientific results, which are given for protection, were received:

1. *Developed for the first time* the concept of constructing a synergistic model of threats to the security of banking information resources, the basis of which is the three-

level model of strategic management of security of banking information technologies. The model developed on the basis of the concept, due to the integration of the components of information security, cyber security and information security, opens a new direction in ensuring the security of banking information resources based on the model of strategic management of the bank taking into account the size of risk at each level and effective control over the implementation of functions of the information security management system of banking organizations the sector.

2. *Improved* the classification of threats to the security of banking information resources, which, unlike the known ones, is based on a synergistic model of threats that allows to classify threats to security components, types of services and levels of automation banking system infrastructure hierarchy, to assess the synergy and hybridity of threats to information security, cyber security, information security, the probability of their impact on the security of banking information resources.

3. *Developed for the first time* a method for evaluating a generalized indicator of the level of security of banking information resources based on a synergistic model of threats, advanced classifier and attacker model, a model for assessing the security of banking information resources, and an infrastructure model for an automated banking system that provides opportunities for establishing interconnections between elements of the hierarchical structure of an automated banking system, communication channels, information assets of banking information resources and threats of information security, cyber security, information security to achieve a synergistic effect and determine the level of security of banking information resources.

4. *Developed for the first time* the method of securing the confidentiality and integrity of banking information resources based on hybrid crypto-code constructions with damaged codes based on the modified McEliece cryptosystem on modified algebra-geometric codes, which allows to raise the level of information hiding and reliability of banking information resources under hybrid conditions threats.

5. *Developed for the first time* a method for ensuring the authenticity of banking information resources based on hybrid crypto-code constructions with damaged codes based on modified McEliece and Niederreiter asymmetric cryptosystems on modified

algebra-geometric codes, which allows to increase the level of information hiding and authenticity of *OTP*-passwords in a two-factor protocol authentication

6. *Gained further development* a method for assessing the security of banking information resources, which, unlike the known ones, takes into account the integrated indicator of the efficiency of investments, which are allocated for ensuring the security of banking information resources, which allows to optimize the cost of funds for its construction under conditions of influence of hybrid threats while ensuring a certain level of their security.

7. *Developed for the first time* the methodology for building a security system for banking information resources, based on the concept of building a synergistic model of threats, an advanced classifier of threats, methods of securing the confidentiality, integrity and authenticity of banking information resources on hybrid crypto-code constructions with damaged codes and an improved method for assessing the security of banking information resources on based on a complex indicator of investment efficiency, which allows you to open a new (emergent) position from the position It is an effective approach from the point of view of spent money to build up operational and perspective security systems of banking information resources.

The scientific value of the main provisions of the thesis is to develop a fundamentally new methodology for creating a security system for banking information resources, based on the proposed concept of building a synergistic model of threats to security of banking information resources, which is based on a three-level model of strategic management of banking information technology security that provides synergistic effect in the conditions of simultaneous action of threats to information security, cyber security and security information AI and, consequently, contributes to the definition of quality new and unknown to this emergent properties of the security of banking information resources including funds spent on its creation.

The practical value of the work lies in the fact that the classification of threats to the security of banking information resources (e-access: http://skl.hneu.edu.ua/) has been developed, which, unlike the known ones, allows to classify and evaluate the probability of exposure in the on-line mode. threats to information security, cyber security, security of information on bank information resources, as well as to determine the level of security

of banking information resources on the basis of synergistic model of threats, improved model of the attacker, model of automation infrastructure the banking system, the model for assessing the security of banking information resources, optimizing the cost of funds for building a security system for banking information resources. Implementation of the developed methods for ensuring the confidentiality, integrity and authenticity of banking information resources on hybrid crypto-code designs provides a 2 – 3 times reduction of energy costs when using automated banking systems of open channels of communication and data transmission while providing the specified security indices.

Key words: security of banking information resources, automated banking system, synergistic model of security threats of banking information resources, classification of security threats of banking information resources, information security, cyber security, information security, investments, endangered properties, synergy effect, hybrid crypto-code constructions on damaged codes, modified elliptic codes, methodology.

Список основних публікацій здобувача:

1. О. О. Кузнецов, С. П. Євсеєв, С. В. Кавун, та О. Г. Король, *Сигнали і коди. Алгебраїчні методи синтезу*. Монографія. Харків, Україна: Вид. ХНЕУ, 2009.

2. О. О. Кузнецов, С. П. Євсеєв, та С. В. Кавун, *Захист інформації та економічна безпека підприємства*. Монографія. Харків, Україна: Вид. ХНЕУ, 2009.

3. С. П. Євсеєв, О. Ю. Йохов, та О. Г. Король, *Гешування даних в інформаційних системах*. Монографія. Харків, Україна: Вид. ХНЕУ, 2013.

4. С. П. Евсеев, и О. Г. Король, “Исследование коллизионных свойств кодов аутентификации сообщений UMAC”, *Информационные технологии и системы в управлении, образовании, науке*. Коллективная монография [под. редакцией В. С. Пономаренко]. Харків, Україна: Цифрова друкарня, с. 25 – 38, 2013.

5. С. П. Евсеев, и Т. А. Свердло, “Исследование угроз методов двухфакторной аутентификации”, *Информационные технологии и защита информации в информационно-коммуникационных системах*: Коллективная

монография [под. редакцией В. С. Пономаренка]. Харків, Україна: Вид-во ТОВ “Щедра садиба плюс”, с. 141 – 154, 2015.

6. С. П. Евсеев, та О. Г. Король, “Синергетические модели оценки безопасности в автоматизированных банковских системах”, *Інформаційні технології: проблеми та перспективи*. Колективна монографія [за заг. ред. В. С. Пономаренка]. Харків, Україна: Вид. Рожко С. Г., с. 203 – 221, 2017.

7. С. П. Евсеев, Г. П. Коц, и И. П. Отенко, “Методология построения модифицированной системы электронного документооборота в университете на основе электронной цифровой подписи стандарта X.509”, *Моделирование процессов управления в информационной экономике*. Колективна монографія [Под ред. докт. экон. наук, проф. В. С. Пономаренка, докт. экон. наук, проф. Т. С. Клебановой] – Бердянск, Україна: видавник Ткачук А. В., с. 264 – 295, 2017.

8. С. Евсеев, и А. Дорохов, “Информационные угрозы и безопасность в банковских платежных системах Украины”, *Криминологический журнал БГУЭП*, вип. 2, с. 68 – 75, 2011. *(Scopus)*

9. С. Евсеев, и В. Абдулаев, “Алгоритм мониторинга метода двухфакторной аутентификации на основе системы Passwindow”, *Восточно-европейский журнал передовых технологий*, вып. 2/2(74), с. 9 – 15, 2015. *(Scopus)*

10. С. Евсеев, О. Король, и Г. Коц, “Анализ законодательной базы к системе управления информационной безопасностью НСМЭП”, *Восточно-европейский журнал передовых технологий*, вып. 5/3(77), с. 48 – 59, 2015. *(Scopus)*

11. С. Евсеев, О. Король, Х. Рзаев, и З. Иманова, “Разработка модифицированной несимметричной крипто-кодовой системы Мак-Элиса на укороченных эллиптических кодах”, *Восточно-европейский журнал передовых технологий*. том 4, 9(82), с. 18 – 26, 2016. *(Scopus)*

12. S. Yevseiev, H. Kots, and Y. Liekariev, “Developing of multi-factor authentication method based on Niederreiter-McEliece modified crypto-code system”, *Восточно-европейский журнал передовых технологий*, 6/4(84), с. 11 – 23, 2016 *(Scopus)*

13. С. Євсеєв, С. Остапов, Х. Рзаєв, та В. Ніколаєнко, “Оцінка обміну даними в глобальних обчислювальних мережах на основі комплексного показника якості обслуговування мережі”, *Науковий журнал Радіоелектроніка, інформатика, управління*, № 1(40), с. 115 – 128, 2017. *(Web of Science)*

14. S. Yevseiev, O. Korol, and H. Kots, “Construction of hybrid security systems based on the crypto-code structures and flawed codes”, *Восточно-европейский журнал передовых технологий*, 4/9(88), с. 4 – 20, 2017. *(Scopus)*

15. S. Yevseiev, H. Kots, S. Minukhin, O. Korol, and A. Kholodkova, “The development of the method of multifactor authentication based on hybrid crypto-code constructions on defective codes”, *Восточно-европейский журнал передовых технологий*, 5/9(89), с. 19 – 35, 2017. *(Scopus)*

16. S. Yevseiev, V. Ponomarenko, and O. Rayevnyeva, “Assessment of functional effectiveness of the corporate scientific-educational network based on comprehensive indicators of service quality”, *Восточно-европейский журнал передовых технологий*, 6/2 (90), с. 4 – 15, 2017. *(Scopus)*

17. С. Евсеев, и О. Король, “Результаты статистического тестирования безопасности и продуктивности хеш-алгоритмов-претендентов конкурса по отбору стандартного алгоритма SHA-3”, *Известия Высших технических учебных заведений Азербайджана*. том.14, № 2 (78), с. 73 – 78, 2012.

18. S. Yevseiev, T. Sverdlo, and O. Korol, “Mécanismes intégrés de sécurité et de fiabilité des données dans les systèmes d’information basés sur la théorie des codes correcteurs d’erreurs”, *French Journal of Science and Education*, № 2(12), p. 358 – 368, 2014.

19. С. Евсеев, А. Сочнева, О. Король, и В. Абдулаев, “Анализ методик оценки рисков нарушения безопасности банковской информации”, *Известия Высших технических учебных заведений Азербайджана*. том.19, № 2 (106), с. 77 – 86, 2017.

20. С. Евсеев, и О. Король, “Метод каскадного формирования MAC-кодов на основе модулярных преобразований”, *Известия Высших технических учебных заведений Азербайджана*, № 1 (89), с. 71 – 78, 2014.

21. С. Евсеев, О. Король, и А. Жученко, “Защита информации в интернет-платежных системах”, *Восточно-европейский журнал передовых технологий*, 5/2(35), с. 34 – 37. 2008.

22. С. Евсеев, О. Король, и Л. Пархуць, “Разработка модели и метода каскадного формирования МАС с использованием модулярных преобразований” *Захист інформації: науково-технічний журнал*, том 15, № 3, с. 186 – 196, 2013.

23. S. Evseev, “International legislation on personal data protection”, *Системи обробки інформації*, № 9(107), с. 140 – 144, 2012.

24. S. Evseev, and B. Tomashevsky, “Two-factor authentication methods threats analysis”, *Радіоелектроніка, інформатика, управління*, вип. 1(32), с. 52 – 59, 2015.

25. С. Евсеев, “Синергетический подход к оценке безопасности банковских систем”, *Системи обробки інформації*, № 4(141), с. 90 – 103, 2016.

26. R. Hryshchuk, and S. Yevseiev, “The synergetic approach for providing bank information security: the problem formulation”, *Безпека інформації*, № 22 (1), с. 64 – 74. 2016.

27. С. Евсеев, Х. Рзаев, и А. Цыганенко, “Анализ программной реализации прямого и обратного преобразования по методу недвоичного равновесного кодирования”, *Науково-технічний журнал “Безпека інформації”*, том 22, № 2, с. 196 – 203, 2016.

28. С. Евсеев, “Методология оценивания безопасности информационных технологий автоматизированных банковских систем Украины”, *Науково-технічний журнал “Безпека інформації”*, том. 22, № 3, с. 297 – 309, 2016.

29. С. Евсеев, “Модель нарушителя прав доступа в автоматизированной банковской системе на основе синергетического подхода”, *Науково-технічний журнал “Інформаційна безпека”*, № 2 (26), с. 110 – 119, 2017.

30. С. Евсеев, “Оценка эффективности инвестиций в безопасность организаций банковского сектора на основе синергетической модели угроз”, *Системи обробки інформації*, № 2 (148), с. 88 – 94, 2017.

31. С. Євсеєв, С. Остапов, та Р. Королев, “Використання міні-версій для оцінки стійкості блоково-симетричних шифрів”, *Науково-технічний журнал “Безпека інформації”,* том 23, № 2, с. 100 – 108, 2017.

32. Р. Грищук, та С. Євсеєв, “Методологія побудови системи забезпечення інформаційної безпеки банківської інформації в автоматизованих банківських системах”, *Науково-технічний журнал “Безпека інформації”*, том 23, № 3, с. 204 – 214, 2017.

33. С. Євсеєв, “Анализ методов построения универсальных классов хеш-функций”, *Вісник Державного університету інформаційно-комунікаційних технологій*, том 7 (№ 4), с. 337 – 345, 2009.

34. С. Евсеев, О. Король, и А. Гончарова, “Построение моделей атак на внутриплатежные банковские системы”, *Радіоелектроніка, інформатика, управління*, вип. 1(22), с. 56 – 66, 2010.

35. С. Евсеев, и Б. Томашевский, “Исследование теоретико-кодовых схем для комплексного обеспечения безопасности и достоверности данных в информационных системах”, *Науковий вісник Чернівецького університету. Серія: Комп’ютерні системи та компоненти*, том 2, вип.1, с. 6 – 14, 2011.

36. А. Кузнецов, О. Король и С. Евсеев, “Исследование коллизионных свойств кодов аутентификации сообщений UMAC”, *Прикладная радиоэлектроника*, том 11, № 2, с. 171 – 183, 2012.

37. С. Евсеев, О. Король, и Н. Суханова, “Анализ угроз и механизмов защиты во внутриплатежных системах коммерческого банка”, *Науково-практичний журнал “Сучасна спеціальна техніка”*, 1(24), с. 49 – 60, 2011.

38. С. Евсеев, “Анализ защиты в национальной системе массовых электронных платежей”, *Інформаційна безпека*, № 3(15), с. 15 – 28, 2014.

39. С. Евсеев, О. Король, и А. Сочнева, “Анализ оценки рисков кибербезопасности банковской информации”, *Сборник научных трудов НАУ “Защита информации”*, вып. 23, с. 109 – 128, 2016.

40. С. Евсеев, “Синергетическая модель оценки безопасности банковской информации”, *Науково-технічний журнал “Інформаційна безпека”*, № 4 (24), с. 104 – 118, 2016.

41. С. Євсеєв, О. Андрощук, та В. Федорченко, “Побудова систем безпеки інформаційно-телекомунікаційних систем на основі комплексного крипто-графічного підходу”, *Збірник наукових праць Нац. академії Держ. прикор. служби України ім. Богдана Хмельницького. Серія : військові та технічні науки* [гол. ред. Олексієнко Б. М.], № 2 (72), с. 258 – 268, 2017.

42. С. Євсеєв, та О. Король, “Дослідження загроз методів двофакторної автентифікації”, *Вісник національного університету “Львівська політехніка”*, № 806, с. 62 – 71, 2014.

43. С. Евсеев, Ю. Хохлачева, и О. Король, “Оценка обеспечения непрерывности бизнес-процессов в организациях банковского сектора на основе синергетического подхода, ч.1”, *Сучасна спеціальна техніка. Науково-практичний журнал*, № 1(48), с. 17 – 25. 2017.

44. С. Евсеев, Ю. Хохлачева, и О. Король, “Оценка обеспечения непрерывности бизнес-процессов в организациях банковского сектора на основе синергетического подхода, ч. 2”, *Сучасна спеціальна техніка. Науково-практичний журнал*, № 2(49), с. 10 – 17, 2017.

45. С. Евсеев, Р. Грищук, и О. Король, “Анализ современных методов выявления кибератак на ресурсы коммуникационных систем”, *Науково-практична конференція “Проблеми науково-технічного та правового забезпечення кібербезпеки у сучасному світі”*, Харків, 2016, с. 9.

46. С. Евсеев, и И. Белодед, “Крипто-кодовая система на модифицированных кодах”, *V Міжнародна науково-технічна конференція “Методи та засоби кодування, захисту й ущільнення інформації”*, Вінниця, 2016, с. 47 – 50.

47. С. Евсеев, “Методология оценивания безопасности информационных технологий автоматизированных банковских систем”, *III Міжнародна науково-практична конференція “Актуальні питання забезпечення кібербезпеки та захисту інформації”*, Київ, 2017, с. 75 – 76.

48. С. Евсеев, и О. Король, “Модель нарушителя прав доступа в автоматизированной банковской системе на основе синергетического подхода”, *Друга Міжнародна науково-практична конференція “Проблеми науково-технічного та правового забезпечення кібербезпеки у сучасному світі”*, Харків, 2017, с. 23.

49. С. Євсеєв, та О. Король, “Комплексний показник ефективності інвестицій в безпеку банківської інформації на основі синергетичної моделі загроз”, *VI Міжнародна наукова конференція “Інформація, комунікація, суспільство 2017”*, Славське, 2017, с. 18 – 19.

50. С. Евсеев, и О. Король, “Классификатор угроз на основе синергетического подхода”, *VII міжнародна науково-технічна конференція “ITSEC: Безпека інформаційних технологій”*, Київ, 2017, с. 83 – 84.

51. С. Євсеєв, “Математичні моделі модифікованої несиметричної крипто-кодової системи Мак-Еліса на модифікованих еліптичних кодах”, *Міжнародна науково-практична конференція “Інформаційні технології та комп’ютерне моделювання”*, Івано-Франківськ, 2017, с. 192 – 196.

52. С. Евсеев, и О. Король, “Математическая модель протокола обмена данными на основе модифицированных несимметричных крипто-кодовых систем Мак-Элиса и Нидеррайтера на ущербных кодах”, *VII міжнародна науково-технічна конференція “Захист інформації і безпека інформаційних систем”*, Львів, 2017, с. 89 – 90.

53. С. Євсеєв, та І. Білодід, “Використання збиткових кодів в гібридних крипто-кодових конструкціях”, *П’ята міжнародна науково-технічна конференція “Проблеми інформатизації”*, Черкаси – Баку – Бельсько-Бяла – Полтава, 2017, с. 11.

54. С. Євсеєв, та О. Андрощук, “Система безпеки інформаційно-телекомунікаційних систем на основі комплексного криптографічного підходу”, *X Всеукраїнська науково-практична конференція “Освітньо-наукове забезпечення діяльності складових сектору безпеки і оборони України”,* Хмельницький, 2017, с. 268 – 269.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

АБС – автоматизована банківська система

АСОІБ – автоматизована система обробки інформації банку

БІ – безпека інформації

БІн – банківська інформація

БІР – банківські інформаційні ресурси

БнС – банківський сектор

БСШ – блоково-симетричний шифр

ГККЗК – гібридні крипто-кодові конструкції на збиткових кодах

ЗІ – захист інформації

ІБ – інформаційна безпека

ІК – інформаційний конфлікт

ІКЗ – інфраструктури критичного застосування

КБ – кібербезпека

КВО – критично важливий об’єкт

КІ – критична інфраструктура

ККІС – критична кібернетична інфраструктура системи

МКІД – метасистема критичною інфраструктури держави

МНККС – модифіковані несиметричні крипто-кодові системи

НБУ – Національний банк України

НСМЕП – національна система масових електронних платежів

НККС – несиметричні крипто-кодові системи

НСД – несанкціонований доступ

ОБС – організація банківського сектору

ОККІ – об’єкт з критичною кібернетичної інфраструктурою

ОККС – об’єкт з критичною кібернетичної структурою

ПЗ – програмний застосунок

РЗ – рівень захищеності

СВА – система виявлення атак

СЗІ – система захисту інформації

СІБ – система інформаційної безпеки

СКЗІ – система комплексного захисту інформації

СККІ – система з критичною кібернетичної інфраструктурою

ТТЗІ – технічні засоби захисту інформації

BCP – (*Business Continuity Planning*) план безперервності бізнесу

BIA – (*Business Impact Analysis*) оцінка впливу переривань на бізнес

CHD – (*damage*) збиток

$\boldsymbol{CH_D}$ – (*ciphertext of damage*) шифртекст збитку

$\boldsymbol{CHD/CH_D}$ – (*ciphertext of damage*) шифртекст збитку

$\boldsymbol{CH_{FT}}$ – (*ciphertext of flawed text*) шифртекст збиткового тексту

$\boldsymbol{CFT/\ CH_{FT}}$ (*ciphertext of the flawed text*) шифртекст збиткового тексту

CFT – (*flawed text*) збитковий текст

$\boldsymbol{DCH/D_{CH}}$ – (*damage of ciphertext*) збиток шифртексту

DRP – (*Disaster Recovery Planning*) планування аварійного відновлення

EC – алгеброгеометричний блоковий код на еліптичних кривих

MEC – модифікований (укорочений або подовжений) алгеброгеометричний блоковий код на еліптичних кривих

$\boldsymbol{FTC/FT_{CH}}$ – (*flawed ciphertext*) збитковий шифртекст

$\boldsymbol{FT_{CH}}$ – (*flawed ciphertext*) збитковий шифртекст

MAO (*Maximum Allowable Outage)* максимально допустимий час простою

MTPD – (*Maximum Tolerable Period of Disruption*) максимально прийнятний період переривання бізнесу

PDCA – (*Plan-Do-Check-Act*) модель менеджменту

RPO – (*Recovery Point Objective*) цільова точка відновлення

RTO – (*Recovery Time Objective*) цільовий час відновлення

SDO – (*Service Delivery Objective*) цільова доступність сервісу

2FA – (*multi-factor authentication*) двофакторна автентифікація

ВСТУП

Актуальність. У сучасних умовах, як показала практика, важлива роль у забезпеченні національної безпеки України та особливо її економічної складової належить процесам забезпечення інформаційної безпеки (ІБ) держави в банківському секторі (БнС). Ключову роль при побудові систем безпеки банківських інформаційних ресурсів (БІР) як складових національних інформаційних ресурсів держави, відіграє теорія та практика, в якій науково-методологічна база є основою для прийняття обґрунтованих та ефективних управлінських рішень суб'єктами забезпечення ІБ держави на усіх рівнях.

Революційні зміни останнього десятиліття, що відбулися в банківському секторі, зумовили до об'єднання інформаційних та комп'ютерних мереж в єдиний інформаційний та кібернетичний простір, що спонукало до створення автоматизованих банківських систем (АБС), які істотно розширили спектр електронних послуг державних і комерційних банків світу та України. Як наслідок, суттєво трансформувалися і загрози такому національному інформаційному ресурсу держави, як БІР під якими в роботі розуміється банківська інформація (БІн). Загрози безпеці БІР набули ознак гібридності. Прояви ознак гібридності внаслідок одночасного впливу загроз інформаційній безпеці, кібернетичній безпеці (КБ) та безпеці інформації (БІ) на БІР призвели до виникнення явища синергізму, негативні прояви якого потребують кардинального перегляду концепцій побудови діючих систем безпеки. Як показує світовий досвід, прояви гібридних загроз безпеці БІР мали місце, наприклад, під час блокування роботи АБС БнС в США (вересень, 2011 р.), що призвело виникнення масової акції непокори під назвою "Захопи Уолл-Стрітт", яка ланцюговою реакцією поширилася на найбільші міста згаданої держави та ряду найбільш економічно розвинених держав Європейського Союзу та зрештою спровокувала світовий економічний колапс. Прояви гібридних загроз безпеці БІР мали місце і в Україні. Наприклад, розпочавшись з кібератаки за допомогою шкідливого програмного забезпечення "Petya.A", "Petya.B" (червень–липень, 2017 р.) було скомпрометовано процес надання банківських послуг, що викликало невдоволення клієнтів банків – громадян, які є суб'єктами ІБ держави. Ланцюгова

реакція після України поширилася на банківські сектори Італії, Ізраїлю, Сербії, Румунії, Угорщини, Аргентини, Чехії, Німеччини та інших розвинених держав світу. Таким чином, проблема забезпечення ІБ держави для інфраструктур критичного застосування (ІКЗ), до яких належить і банківський сектор, стоїть дуже гостро. Отже, стає зрозуміло, що потребують кардинального перегляду діючі методологічні засади побудови системи безпеки БІР як України зокрема, так і світу в цілому.

Відомо, що вирішенню проблеми ІБ держави в цілому та безпеки БІР зокрема присвячено праці відомих вітчизняних і закордонних вчених та їх наукових шкіл: І. Горбенка, В. Задіраки, О. Кузнецова, С. Ленкова, О. Молдовяна, В. Мохора, В. Сідельникова, С. Тімофєєва, Б. Шнайера, В. Шокала, В. Ярочкина, А. Калашнікова та багатьох ін. Разом з тим встановлено, що невирішеними аспектами загальної проблеми забезпечення ІБ держави залишається **проблема** створення цілісної науково обґрунтованої методології побудови системи безпеки БІР, впровадження якої на практиці сприятиме стійкому та стабільному розвитку банківського сектору держави.

Отже, на сьогодні ***склалося об'єктивне протиріччя*** між зростаючими на практиці вимогами до безпеки БІР при одночасному збільшенні кількості та технологічній складності загроз безпеці і набутті ними ознак гібридності з одного боку та недосконалістю, а подекуди й відсутністю методології побудови системи безпеки БІР від таких загроз з іншого. Наявність цього протиріччя ***обумовлює актуальність теми дисертації***, а тому вирішення поставленої науково-прикладної проблеми має важливе наукове та практичне значення.

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційні дослідження проведено згідно з Доктриною інформаційної безпеки України, затвердженою указом Президента України від 25.02.2017 р. № 47/2017 та Стратегією кібербезпеки України, затвердженою указом Президента України від 15.03.2016 р. № 96/2016 у рамках НДР: № 36Б115 "Розробка методів синтезу тестових моделей поведінки програмних об'єктів, підвищення оперативності передачі та захисту інформації у телекомунікаційних системах" (д.р. № 0115U003103) – виконувалася у

Кіровоградському національному технічному університеті; “Розроблення алгоритмів несиметричного шифрування для мобільних засобів зв’язку” (д.р. № 0116U005696), “Розробка методу підвищення конфіденційності і ймовірності банківської інформації в автоматизованих банківських системах” (д.р. №. 0117U000136), № 15/2016-2017 “Методологія побудови системи забезпечення безпеки банківської інформації: аналіз проблеми та синтез нових рішень” (д.р. №. 0117U001628) – виконувалися в Харківському національному економічному університеті ім. С. Кузнеця. У згаданих НДР здобувач брав участь як виконавець, відповідальний виконавець, а в останній НДР виступав науковим керівником.

Мета і задачі дослідження. Метою дисертаційної роботи є створення науково обґрунтованої методології побудови системи безпеки банківських інформаційних ресурсів для підвищення рівня їх захищеності від загроз безпеці гібридного характеру..

Для досягнення поставленої мети **необхідно розв’язати такі основні завдання**:

– провести аналіз сутності та змісту проблеми інформаційної безпеки держави на сучасному етапі розвитку науки і техніки та дослідити роль й місце систем безпеки банківських інформаційних ресурсів при впливі на них нових загроз, які мають гібридний характер. Оцінити сучасний стан нормативно-правової бази, яка регламентує порядок побудови системи безпеки банківських інформаційних ресурсів, а також встановлює вимоги до їх захищеності;

– розробити концепцію побудови синергетичної моделі загроз безпеки банківських інформаційних ресурсів для обґрунтування та вибору найбільш ефективних напрямків досягнення цілей безпеки банківських інформаційних ресурсів на кожному з рівнів моделі управління стратегічним управлінням безпекою банківських інформаційних технологій з урахуванням величини ризику на кожному рівні та забезпеченням дієвого контролю за виконанням функцій системи управління інформаційною безпекою організацій банківського сектору;

– удосконалити класифікатор загроз безпеці банківських інформаційних ресурсів для формування експертної оцінки рівня загроз банківських

інформаційних ресурсів за складовими безпеки, видами послуг та рівнями ієрархії інфраструктури автоматизованих банківських систем, аналізу їх синергії та гібридності, оцінювання ймовірності впливу загроз інформаційній безпеці, кібербезпеці та безпеці інформації на безпеку банківських інформаційних ресурсів;

– розробити метод оцінювання узагальненого показника рівня захищеності банківських інформаційних ресурсів з урахуванням розробленої синергетичної моделі загроз та удосконаленого класифікатора для встановлення взаємозв'язків між елементами структури автоматизованих банківських систем, каналами зв'язку, активами банківських інформаційних ресурсів, та загрозами інформаційній безпеці, кібербезпеці, безпеці інформації, а також визначення рівня захищеності банківських інформаційних ресурсів;

– розробити метод забезпечення конфіденційності та цілісності банківських інформаційних ресурсів при одночасній дії на них загроз інформаційній безпеці, кібербезпеці та безпеці інформації для підвищення рівня їх інформаційної прихованості та достовірності банківських інформаційних ресурсів;

– розробити метод забезпечення автентичності банківських інформаційних ресурсів при одночасній дії на них загроз інформаційній безпеці, кібербезпеці та безпеці інформації для підвищення рівня їх інформаційної прихованості та достовірності *OTP*-паролів в протоколі двофакторної автентифікації;

– розробити метод оцінювання безпеки банківських інформаційних ресурсів, що повинен враховувати комплексний показник ефективності інвестицій, які виділяються на забезпечення безпеки банківських інформаційних ресурсів, для оптимізації витрати коштів на її побудову в умовах впливу гібридних загроз при одночасному забезпеченні заданого рівня їх безпеки;

– розробити методологію побудови системи безпеки банківських інформаційних ресурсів, яка забезпечує одержання максимальної кількості емерджентних властивостей системи безпеки банківських інформаційних ресурсів при мінімальних ресурсних витратах на її створення та функціонування в умовах впливу гібридності загроз.

Об’єктом дослідження є процеси забезпечення інформаційної безпеки держави в банківському секторі.

Предметом дослідження є методологія побудови системи безпеки банківських інформаційних ресурсів.

Методи дослідження. Проведені дослідження ґрунтуються на теоретично обґрунтованих та практично апробованих методах теорії множин (формалізовано загрози безпеки банківських інформаційних ресурсів, здійснено їх класифікацію, визначено вимоги і повноту забезпечення безпеки банківських інформаційних ресурсів), теорії криптографії, теорії кодування та теорії скінченних полів Галуа (використано при розробці гібридних крипто-кодових конструкцій на збиткових кодах (ГККЗК) та обґрунтуванні їх стійкості), теорії ймовірностей і математичної статистики (використано для розроблення методу експрес-аналізу стійкості і дослідження властивостей гібридних крипто-кодових конструкцій на збиткових кодах), експертного оцінювання (для визначення вагових коефіцієнтів загроз для формування класифікатора загроз), математичної логіки і теорії автоматів (для оцінювання енергетичних затрат при практичній реалізації гібридних крипто-кодових конструкцій на збиткових кодах), системного аналізу (для ієрархічного подання автоматизованих банківських систем), законах синергії (для побудови моделі загроз, дослідження її впливу на систему безпеки банківських інформаційних ресурсів).

Наукова новизна одержаних результатів:

– *вперше розроблено* концепцію побудови синергетичної моделі загроз безпеки банківських інформаційних ресурсів, базис якої становить трирівнева модель стратегічного управління безпекою банківських інформаційних технологій. Розроблена на основі концепції модель за рахунок комплексування складових інформаційної безпеки, кібербезпеки та безпеки інформації відкриває новий напрямок у забезпеченні безпеки банківських інформаційних ресурсів на основі моделі стратегічного управління банком з урахуванням величини ризику на кожному рівні та дієвого контролю за виконанням функцій системи управління інформаційною безпекою організацій банківського сектору;

– *удосконалено* класифікатор загроз безпеці банківських інформаційних ресурсів, який, на відміну від відомих, ґрунтується на синергетичній моделі загроз, що дозволяє класифікувати загрози за складовими безпеки, видами послуг та рівнями ієрархії інфраструктури автоматизованих банківських систем, оцінювати синергію та гібридність загроз інформаційній безпеці, кібербезпеці, безпеці інформації, ймовірність їх впливу на безпеку банківських інформаційних ресурсів;

– *вперше розроблено* метод оцінювання узагальненого показника рівня захищеності банківських інформаційних ресурсів на основі синергетичної моделі загроз, удосконалених класифікатора та моделі зловмисника, моделі оцінки захищеності банківських інформаційних ресурсів, та моделі інфраструктури автоматизованої банківської системи, що надає можливість встановлення взаємозв'язків між елементами ієрархічної структури автоматизованої банківської системи, каналами зв'язку, інформаційними активами банківських інформаційних ресурсів та загрозами інформаційній безпеці, кібербезпеці, безпеці інформації для досягнення синергетичного ефекту та визначення рівня захищеності банківських інформаційних ресурсів;

– *вперше розроблено* метод забезпечення конфіденційності та цілісності банківських інформаційних ресурсів, який ґрунтується на гібридних крипто-кодових конструкціях зі збитковими кодами на основі модифікованої крипто-кодової системи Мак-Еліса на модифікованих алгеброгеометричних кодах, що дозволяє підвищити рівень інформаційної прихованості та достовірності банківських інформаційних ресурсів в умовах дії гібридних загроз;

– *вперше розроблено* метод забезпечення автентичності банківських інформаційних ресурсів, який ґрунтується на гібридних крипто-кодових конструкціях зі збитковими кодами на основі модифікованих несиметричних крипто-кодових системах Мак-Еліса і Нідеррайтера на модифікованих алгеброгеометричних кодах, що дозволяє підвищити рівень інформаційної прихованості та достовірності *OTP*-паролів в протоколі двофакторної автентифікації;

– *набув подальшого розвитку* метод оцінювання безпеки банківських інформаційних ресурсів, що, на відміну від відомих, враховує комплексний показник ефективності інвестицій, які виділяються на забезпечення безпеки банківських інформаційних ресурсів, що дозволяє оптимізувати витрати коштів на її побудову в умовах впливу гібридних загроз при одночасному забезпеченні заданого рівня їх безпеки;

– *вперше розроблено* методологію побудови системи безпеки банківських інформаційних ресурсів, в основу якої покладено концепцію побудови синергетичної моделі загроз, удосконалений класифікатор загроз, методи забезпечення конфіденційності, цілісності та автентичності банківських інформаційних ресурсів на гібридних крипто-кодових конструкціях зі збитковими кодами та удосконалений метод оцінювання безпеки банківських інформаційних ресурсів на основі комплексного показника ефективності інвестицій, що дозволяє відкрити новий (емерджентний) з позицій безпеки, та ефективний з позицій витрачених коштів підхід до побудови діючих та перспективних систем безпеки банківських інформаційних ресурсів.

Практичне значення одержаних результатів у сукупності складає підґрунтя для практичної побудови дієвої та ефективної системи безпеки БІР.

Практична цінність одержаних результатів у такому:

1. Розроблено програмний застосунок, який реалізує удосконалений класифікатор загроз інформаційній безпеці, кібербезпеці та безпеці інформації банківських інформаційних ресурсів (електронний доступ: *http://skl.hneu.edu.ua/*), що дозволяє в он-лайн режимі здійснити класифікацію та оцінювання ймовірності впливу зазначених загроз інформаційній безпеці, кібербезпеці та безпеці інформації на безпеку банківських інформаційних ресурсів, їх синергію та гібридність.

2. Розроблено практичну методику для оцінювання рівня захищеності банківських інформаційних ресурсів на основі синергетичної моделі загроз, удосконалених класифікатора загроз та моделі зловмисника, моделі оцінки захищеності банківських інформаційних ресурсів та моделі інфраструктури автоматизованих банківських систем, що дозволяє встановити взаємозв’язки між

елементами ієрархічної структури автоматизованої банківської системи, каналами зв'язку, інформаційними активами банківських інформаційних ресурсів та загрозами інформаційній безпеці, кібербезпеці, безпеці інформації для досягнення синергетичного ефекту та визначення рівня захищеності банківських інформаційних ресурсів.

3. Розроблено методику оцінювання безпеки банківських інформаційних ресурсів на основі комплексного показника ефективності інвестицій, які виділяються на забезпечення безпеки банківських інформаційних ресурсів для оптимізації витрати коштів на її побудову в умовах впливу гібридних загроз при одночасному забезпеченні заданого рівня їх безпеки.

4. Розроблені практичні алгоритми забезпечення конфіденційності, цілісності та автентичності банківських інформаційних ресурсів на основі інтеграції криптографічних перетворень і завадостійкого та збиткового кодування, що дозволяє інтегровано (одним механізмом) забезпечувати безпеку банківських інформаційних ресурсів (безпечний час – $T_Б$ >200 р., стійкість до криптоаналізу P_K <10^{25}–10^{35} групових операцій), достовірність передачі банківських інформаційних ресурсів ($P_{пом}$ <10^{-9}) та зменшення енергетичних витрат на їх практичну реалізацію в 10 – 12 разів (шифрування, розшифрування) за рахунок зменшення порядку *GF (q)*.

5. Розроблено програмні макети криптографічних засобів захисту інформації з використанням гібридних крипто-кодових конструкціій зі збитковими кодами, які дозволяють проводити експериментальні дослідження запропонованих крипто-кодових конструкцій, оцінювати їх властивості та стійкість.

6. Результати впроваджено у діяльність ТОВ "Сайфер БІС" (акт впровадження від 18.05.2017), ТОВ "ТАНТАРІУМ" (акт впровадження від 14.06.2017), "МЕГАБАНК" Публічне акціонерне товариство (акт впровадження від 9.06.2017), ТОВ "Мікрокріпт Текнолоджіс" (акт впровадження від 30.11.2017).

Особистий внесок здобувача. Основні положення і результати дисертаційної роботи, що виносяться на захист, отримані автором самостійно. У роботах, написаних у співавторстві, автору належать: [21, 37, 38] – дослідження сучасних механізмів забезпечення ІБ в інтернет-платіжних, внутрішньо-платіжних системах;

[3, 4, 17, 33, 36] – дослідження методів побудови та властивості універсальних класів геш-функцій; [8, 34, 39, 42] – розробка моделей атак на АБС, дослідження загроз на БІР, механізмів надання послуг безпеки; [1, 2, 18, 27, 35] – розробка методів побудови несиметричних крипто-кодових систем (НККС) на основі теоретико-кодових схем (ТКС) Мак-Еліса та Нідеррайтера на еліптичних кодах (*EC*), дослідження їх властивості; [22] – розроблення вимог оцінки методу каскадного формування *MAC*-коду на основі модулярних перетворень; [5, 9, 12, 15, 24, 42] – дослідження методів 2*FA*, розробка методу моніторингу системи *PassWindow*, розробка методу 2*FA* на основі *OTP*-паролів з використанням модифікованих крипто-кодових систем Мак-Еліса і Нідеррайтера, методу 2*FA* на основі ГККККЗК; [10, 23, 47] – порівняльний аналіз законодавчої бази забезпечення безпеки БІР в національної системі масових електронних платежів; [6, 7, 25, 26, 29, 40, 48] – розробка концепції та розробка синергетичної моделі оцінки загроз; [19, 28, 45] – дослідження ризиків КБ БІР та методів їх виявлення, розробка моделі оцінки складових безпеки БІР на основі синергетичного підходу оцінки загроз; [11, 46, 51, 52] – розроблено метод побудови модифікованої крипто-кодової конструкції на модифікованих еліптичних кодах (*MEC*); [29, 50] – розробка удосконаленого класифікатора загроз безпеці БІР; [13, 16] – розробка методики оцінки функціональної ефективності комп'ютерних систем; [43, 44] – розробка методики оцінки безперервності бізнес-процесів в організаціях банківського сектору; [14, 41, 52, 53, 54] – розробка методів побудови ГККККЗК; [31] – дослідження адекватності використання міні-версій блоково-симетричних шифрів (БСШ) для оцінки їх криптостійкості, [30, 49] – методика оцінки ефективності інвестицій в безпеку ОБС на основі синергетичної моделі загроз, [20] – удосконалення методу формування *MAC*-коду на основі модулярних перетворень, [32] – методологія побудови системи безпеки БІР.

Апробація результатів дисертації. Основні положення дисертаційної роботи доповідалися та обговорювалися на понад 20 наукових конференціях серед яких: "Securitatea informaţională 2008", conf. intern. (2008; Chişinău), "Інформаційна безпека" (Київ, 2009, 2015–2016 рр.), "Проблеми й перспективи розвитку ІТ-індустрії" (Харків, 2010–2017рр.), "Сучасні проблеми і досягнення в галузі радіотехніки, телекомунікацій

та інформаційних технологій" (Запоріжжя, 2014 р.), "Проблеми науково-технічного та правового забезпечення кібербезпеки у сучасному світі" (Харків, 2016–2017 рр.), "Інформаційно-комп'ютерні технології – 2016" (Житомир, 2016 р.), "Методи та засоби кодування, захисту й ущільнення інформації" (Вінниця, 2016 р.), "Захист інформації і безпека інформаційних систем" (Львів, 2016–2017 рр.), "Економічний розвиток і спадщина Семена Кузнеця" (Харків, 2016 р.), "Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку" (Харків, 2017 р.), "Інформація, комунікація, суспільство 2017" (Славське, 2017 р.), "ITSEC: Безпека інформаційних технологій" (Київ, 2017 р.), "Інформаційні технології та комп'ютерне моделювання" (Івано-Франківськ, 2017 р.), "Проблеми інформатизації" (Черкаси, 2017 р.), "Освітньо-наукове забезпечення діяльності складових сектору безпеки і оборони України" (Хмельницький, 2017 р.).

Публікації. Основні положення дисертації опубліковано у 120 наукових працях (54 основних з яких наведено у авторефераті), у тому числі: 3 монографії (у співавторстві) [1 – 3], 4 розділи у колективних монографіях [4 – 7]; 9 наукових статей у міжнародних рецензованих виданнях, що входять до баз даних *Scopus* та *Web of Science* [8 – 16]; 16 наукових статей у закордонних [17 – 20], вітчизняних фахових наукових журналах, які входять до інших міжнародних наукометричних баз даних (*Index Copernicus, EBSCO , Inspec* тощо) [21 –32], , та 12 статей у наукових журналах та збірниках наукових праць [33 – 44], що входять до переліку фахових видань України, а також 10 матеріалів і тез доповідей на міжнародних конференціях [45 – 54]. Без співавторів – опубліковано 8 наукових статей [23, 25, 28 – 30, 33, 38, 40].

Структура роботи та її обсяг. Дисертація складається з анотації, змісту, переліку умовних позначень, вступу, п'яти розділів, загальних висновків, додатків, списку використаних джерел в кінці кожного розділу основної частини дисертації і має 289 сторінок основного тексту, 102 рисунки, 67 таблиць, 90 сторінок додатків. Список використаних джерел містить 279 найменувань і займає 41 сторінку. Загальний обсяг дисертації – 471 сторінка.

РОЗДІЛ 1
АНАЛІЗ СУЧАСНОГО СТАНУ ПРОБЛЕМИ

1.1. Огляд літератури за проблемою

1.1.1. Аналіз сутності та змісту проблеми інформаційної безпеки держави на сучасному етапі розвитку науки і техніки

Розвиток суспільства на початку XXI століття характеризується, в *першу чергу*, переходом від інформаційного суспільства до суспільства високих технологій, що забезпечують перенасиченість новітніми інформаційними та комунікаційними технологіями, подальший розвиток глобалізаційних процесів в сучасній економіці, динаміку інформатизації таких областей діяльності суспільства, як сфера зв'язку, енергетика, транспорт, система видобутку та зберігання нафти і газу, фінансова і банківська системи, оборонна та національна безпеки, структура забезпечення стабільної роботи центральних органів виконавчої влади, повсюдний перехід на методи електронного урядування та документообігу [1; 2; 3]. У *другу чергу*, інформаційні процеси, що відбуваються повсюдно в світі, висувають на перший план найважливіше завдання забезпечення безпеки інформації. Це пояснюється особливою значущістю для розвитку держави його інформаційних ресурсів, зростанням вартості інформації в умовах ринку, її високою вразливістю і нерідко значними збитками в результаті її несанкціонованого використання [1; 2; 3; 4; 5; 6; 7]. У *третю чергу*, бурхливий розвиток Інтернету та інших інформаційно-комунікаційних технологій формує глобальний інформаційний простір, що дозволяє створити нові загрози і нові форми міжнародних конфліктів, включаючи інформаційні війни, мережеві протиборства, хакерські атаки і т.п. Розвиток комп'ютерних технологій та інформаційно-телекомунікаційних мереж дають великі можливості суспільству, водночас породжуючи новий вид злочинів – кіберзлочинність [4; 6].

У 2015 році терористична організація "Ісламська держава Іраку і Леванту " (ІДІЛ) створила підрозділ, що займається проведенням комп'ютерних атак. В мережі Інтернет цей підрозділ відомий під назвою *Cyber Caliphate*, основною

метою якої є злом і розкриття конфіденційної інформації, атаки на інтернет-ресурси, в число яких входять сайти банків, наукових центрів, державних підприємств та ін. [8]. Про степінь небезпеки для суспільства електронних злочинів можна судити за тими витратами на засоби захисту, які вважаються допустимими і доцільними. За оцінками фахівців з безпеки електронного документообігу США, загальні витрати на захист банківських або інших фінансових установ можуть становити лише близько 510 тисяч доларів. Однак надійною вважається система захисту великої фінансової установи що обслуговує до 80000 клієнтів, вартість якої становить не менше 15 мільйонів доларів, причому в цю суму входять тільки вартості апаратних і програмних засобів (без урахування оплати праці найманого штату власних співробітників безпеки компанії) [7].

Інформаційні загрози можуть проявляти себе в різних формах. *Кібертероризм* характеризується прагненням до суттєвої дестабілізації громадського порядку. Це явище нерозривно пов'язане з розвитком інформаційної інфраструктури: при постійному зростанні залежності суспільства від безперебійного функціонування обчислювальних систем дії, спрямованих на їх руйнування, наносять все більш значної шкоди і викликають серйозний громадський резонанс [7]. При цьому під *кібертероризмом* розуміється цілеспрямоване залякування населення та органів влади реальними або потенційними і проголошеними (заявленими) кібернетичними впливами на соціум, соціотехнічні і технічні системи, вчинення яких призводить до виникнення (створення передумов для виникнення) небезпеки для громадян, суспільства, держави [1]. Особливе занепокоєння в останнє десятиліття викликає використання міжнародним тероризмом існуючих інформаційних ресурсів, в першу чергу, мережі Інтернет для здійснення терористичних акцій. Глобальна мережа привертає увагу терористичних груп такими своїми особливостями [1; 6; 9]:

– оперативністю, економічністю і доступністю;

– слабкою цензурою або повною відсутністю її, а також будь-якого контролю з боку держави;

– наявністю величезної потенційної аудиторії користувачів, розкиданої по

всьому світу;

– швидким і відносно дешевим поширенням спеціально підібраної інформації, комплексністю її подачі та сприйняття (розсилання електронних листів *e-mail*, організація новинних груп, створення сайтів для обміну думками, розміщення інформації на окремих сторінках або в електронних версіях періодичних видань та мережевого мовлення та ін.);

– більшість серверів комунікаційних мереж дають можливість користувачам працювати відносно конфіденційно і анонімно;

– існує можливість використання спеціальних роботів (*bots*) для зниження часу і витрат на терористичну діяльність;

– висока ефективність наслідків, які можуть мати як локальний, так і глобальний характер;

– кіберзлочини складно відстежити і зібрати докази;

– невизначеність місця, часу і процесу підготовки до здійснення кібертеракту;

– можливість організації актів кібертерору одночасно на різні об’єкти або суб’єкти з різних напрямків без необхідності порушення будь-яких кордонів;

– можливість несанкціонованого підключення до комп’ютерних мереж управління стратегічними об’єктами, в тому числі військовими;

– високий ступінь анонімності при здійсненні кібертерактів;

– просторово-часова віддаленість від об’єкта або суб’єкта кібератаки. Всі кібернетичні впливи здійснюються в кіберпросторі і безпосередньо через кіберпростір. Основні засоби кібертероризму наведені на рис. 1.1.

Аналіз рис. 1.1 показує що, тероризм все більше стає інформаційною технологією особливого типу, оскільки терористи все ширше використовують можливості сучасних інформаційно-телекомунікаційних систем для зв’язку і збору інформації, більшість терористичних актів розраховані не тільки на нанесення матеріального збитку і загрози життю і здоров’ю людей, а й на інформаційно-психологічний шок, вплив якого на великі маси людей створює сприятливу обстановку для досягнення терористами поставлених завдань.

Рисунок 1.1 – Основні засоби кібертероризму в інтернет-просторі

Таким чином, в умовах нарощування в світі процесів глобалізації та формування інформаційного суспільства тероризм став самостійним фактором, що здатний загрожувати державній цілісності країн і дестабілізувати міжнародну обстановку.

Терористичні групи все частіше використовують можливості новітніх інформаційних технологій та мережі Інтернет для поширення пропаганди і обміну інформацією, залучення нових найманців, збору фінансових коштів на свою підтримку, планування терактів, а також для здійснення контролю за їх проведенням [9].

Основні напрямки використання новітніх інформаційних технологій та мережі Інтернет з терористичною метою наведені на рис. 1.2.

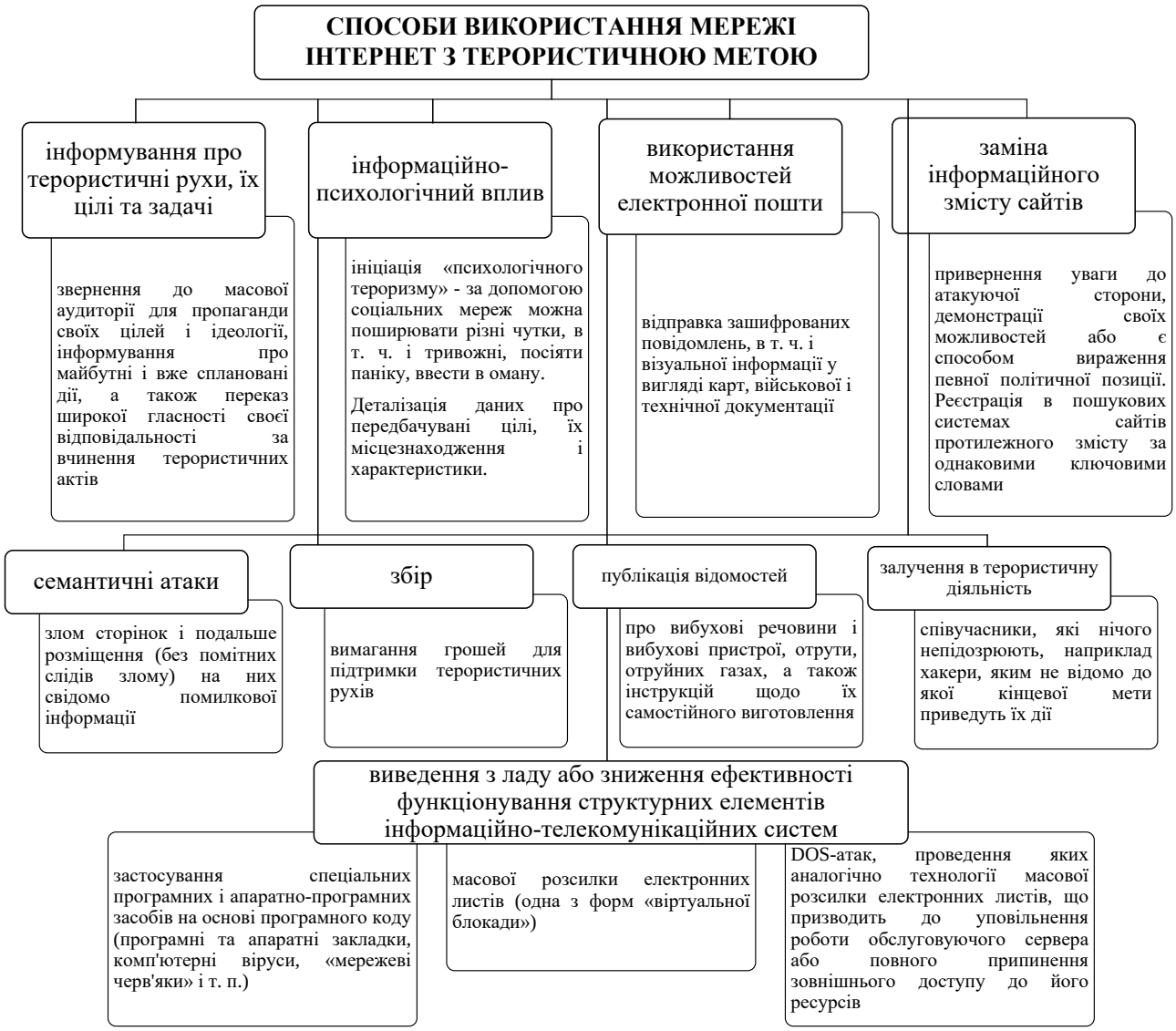


Рисунок 1.2 – Основні напрямки використання новітніх інформаційних технологій та мережі Інтернет з терористичною метою

Проведений аналіз рис. 1.2 показав, що соціальні мережі активно використовуються для пропаганди демонстрації нібито матеріального достатку бойовиків, військового способу життя і героїзму бойовиків, заклику боротися за свої ідеали зі зброєю в руках, трансляції сцен вдалих бойових дій і актів залякування. Фото та відеозвіти супроводжуються джихадистськими піснями, які посідають важливе місце в формованій культурній матриці глобального терористичного співтовариства. У них є власний мобільний застосунок і інтернет-магазин, де можна купити футболку або худі з логотипом терористів. Вся ця небезпечна для свідомості продукція поширюється на багатьох мовах світу.

Аналіз використання ІДІЛ кіберпростору в Європі показав такі результати [9]: 84 % – молодих людей прийшли до рядів терористичної організацій за допомогою мережі Інтернет; 47 % – звернули увагу на матеріали (відео, текст), розміщені онлайн; 41 % – присягнули на вірність ІДІЛ онлайн; 19 % – користувалися онлайн-інструкціями при підготовці теракту (виготовлення саморобних вибухових пристроїв і бомб). Основне завдання подібних продуктів – зацікавити користувачів, почати спілкування в форматі питання-відповідь з метою психологічного впливу для подальшої ізоляції людини від близького оточення і соціуму в цілому і залучення до рядів терористів.

Таким чином, на відміну від традиційного тероризму, що не загрожував суспільству як такому і не торкався основ його життєдіяльності, сучасний високотехнологічний тероризм здатний продукувати системну кризу в кожній державі з високорозвиненою інформаційною інфраструктурою. Розвиток соціальних мереж супроводжується все більш широким використанням їх можливостей для здійснення інформаційного протиборства, зростанням координації, масштабів і складності дій його учасників, якими найчастіше виступають як держави, так і окремі організовані групи, в т. ч. терористичні. Об’єктом кібератак все частіше стають інформаційні ресурси, виведення з ладу або “перешкоджання” функціонуванню, яких може завдати протиборчій стороні значних економічних збитків або викликати великий суспільний резонанс [9].

Зміна вектора безпеки світових лідерів розвинених країн у напрямку забезпечення кібербезпеки об’єктів з критичною кібернетичною структурою (ОККС), прийняття стратегій і концепцій з кібербезпеки провідними світовими державами, створення національних Команд реагування на комп’ютерні інциденти (*Computer Emergency Response Team, CERT*) істотно змінило в останні десятиліття погляди провідних країн світу на становлення феномену кібернетичної безпеки і свідчить, що тлумачення цієї категорії постійно еволюціонує.

На процес еволюції поглядів істотно впливають рівень економічного розвитку країни, рівень освіченості її населення, ступінь впровадження високих технологій, доступність до мережі Інтернет і т.п.

Проведений аналіз основних принципів і методів реалізації кіберзагроз дозволяє зробити висновок, що в найближчі один-два роки, різко зросте кількість і “якість” кіберзагроз на ОККС держави, які дозволяють підірвати зсередини економічний базис державної метасістеми [1; 12; 19; 20; 21; 22; 23; 25; 26; 34; 35; 36].

Проведений аналіз основних положень систем з критичною кібернетичною структурою в роботі [1] дозволяє використовувати запропоновані авторами основні поняття, пов’язані з формуванням ієрархічної структури критичної інфраструктури метасистеми держави:

Критична інфраструктура (КІ) – системи, мережі та / або окремі об’єкти, цілеспрямоване або випадкове виведення з ладу яких може потенційно призвести до непоправних наслідків, дестабілізації розвитку економіки і політичних процесів в державі, соціального благополуччя і здоров’я населення.

Система з критичною кібернетичною інфраструктурою (СККІ) – сукупність взаємопов’язаних елементів, об’єднаних в єдине ціле, правильність функціонування та взаємодії яких значно впливає на кібернетичну безпеку держави протягом певного інтервалу часу.

Об’єкт з критичною кібернетичною інфраструктурою (ОККІ) – елемент системи з критичною кібернетичною інфраструктурою, кібернетичний вплив на якого призводить до зниження рівня його кібернетичного захисту від кіберзагроз.

У табл. 1.1 наведені порівняльні результати співвідношення секторів держави до КІ [1].

Проведений аналіз табл.1.1 показав, що більшість розвинених держав світу до найбільш вразливих критичних інфраструктур відносять об’єкти, що належать банківського та фінансового сектору (сфері), енергетиці та телекомунікації.

Таблиця 1.1 – Порівняльна таблиця критичних інфраструктур

ДЕРЖАВА / СЕКТОР КРИТИЧНОЇ ІНФРАСТРУКТУРИ	Велика Вісімка																
	США	Японія	Німеччина	Великобританія	Франція	Італія	Канада	Російська федерація	Австралія	Австрія	Нідерланди	Нова Зеландія	Норвегія	Польща	Фінляндія	Швеція
Банки і фінанси	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Водопостачання	■	■	■	■	■	■	■		■	■	■		■	■	■	
Дамби	■															
Енергетика	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Комунальні мережі			■						■	■			■		■	
Національні символи	■						■			■						
Небезпечні матеріали (Х, Б, Р, Я)	■	■		■			■							■		
Оборонно-промисловий комплекс	■	■			■		■	■	■						■	
Органи виконавчої влади	■		■	■			■		■		■	■	■	■		■
Органи судової влади	■															
Охорона здоров'я	■	■	■	■	■	■	■		■	■	■		■	■		■
Паливно-енергетичний комплекс	■	■	■	■	■	■	■	■	■		■	■	■	■		
Поштові служби	■									■						
Сільське господарство	■	■	■	■			■		■		■			■	■	
Система управління повітряним рухом																■
Служби охорони громадського руху				■	■	■	■	■	■	■	■		■			
Служби екстреної допомоги та реагування на НС	■	■	■	■		■	■		■	■		■	■			
Телекомунікації	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Транспорт	■	■		■	■	■	■	■	■	■	■	■	■	■	■	
Управління відходами		■		■		■	■		■				■			

На основі ознакового підходу, запропонованого в роботі [36] пропонується ієрархічна структура критичної інфраструктури метасистеми держави яка наведена на рис. 1.3. У сучасних умовах, як показала практика, важлива роль у забезпеченні національної безпеки України та особливо її економічної складової належить процесам забезпечення інформаційної безпеки (ІБ) держави в банківському секторі (БнС). Ключову та системотвірну роль при побудові систем безпеки інформаційних ресурсів (ІР) автоматизованих банківських систем (АБС) як складової національних інформаційних ресурсів держави відіграє теорія та практика, в якій науково-методологічна база є основою для прийняття обґрунтованих та

ефективних управлінських рішень суб’єктами забезпечення ІБ держави на усіх рівнях.

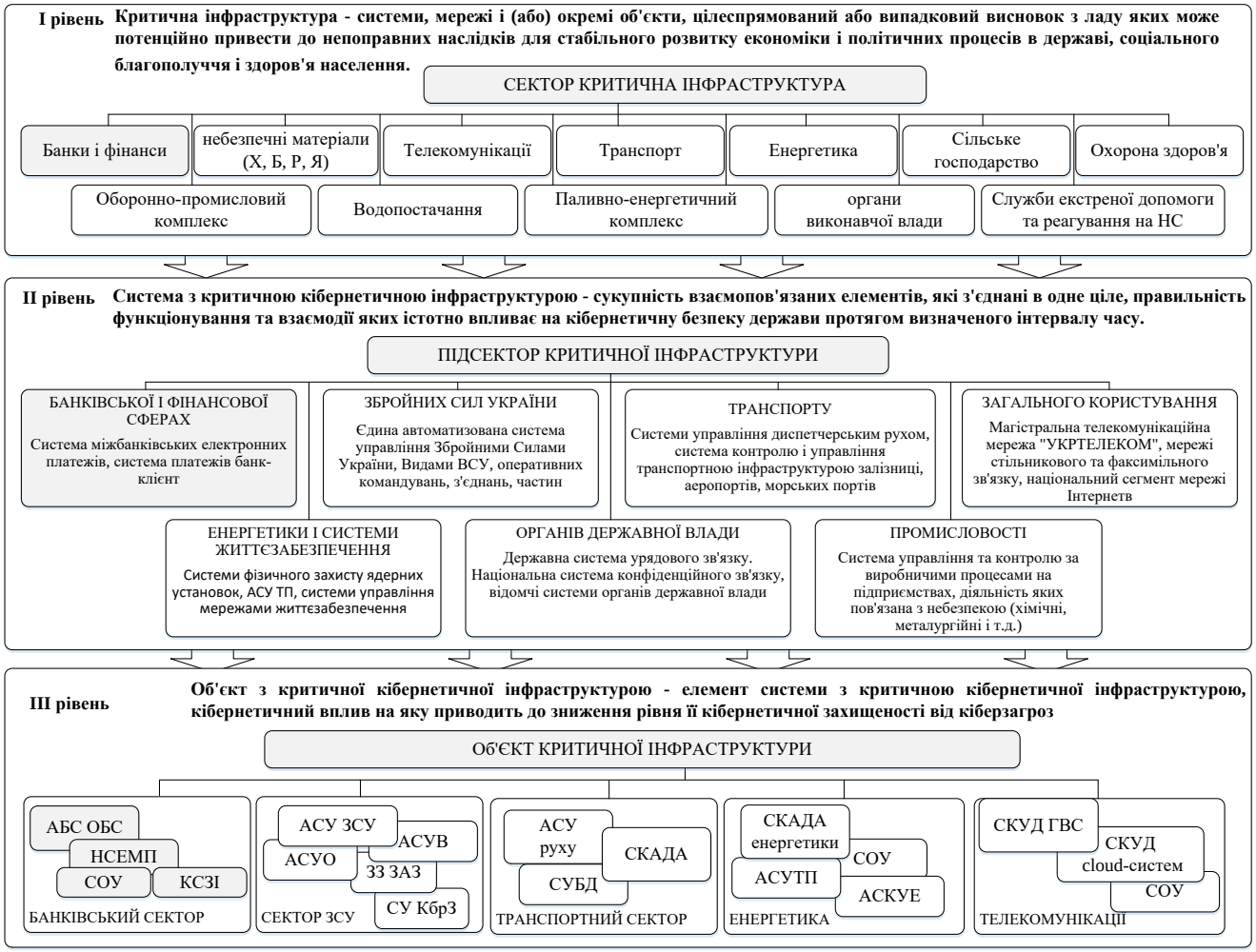


Рисунок 1.3 – Ієрархічна структура критичної інфраструктури метасистеми держави

При цьому під *метасистемою критичної інфраструктури держави* (МКІД) розуміється система стратегічного масштабу, що являє собою сукупність значної кількості різноманітних елементів, об’єднаних в рамках єдиної критичної кібернетичної архітектури в єдину систему, що володіє синергізмом і має загальну емерджентну властивість (призначення, функцію), що відрізняється від властивостей окремих елементів всієї сукупності [1].

На рис. 1.4 наведений взаємозв’язок між основними складовими інформаційної безпеки (ІБ) держави.

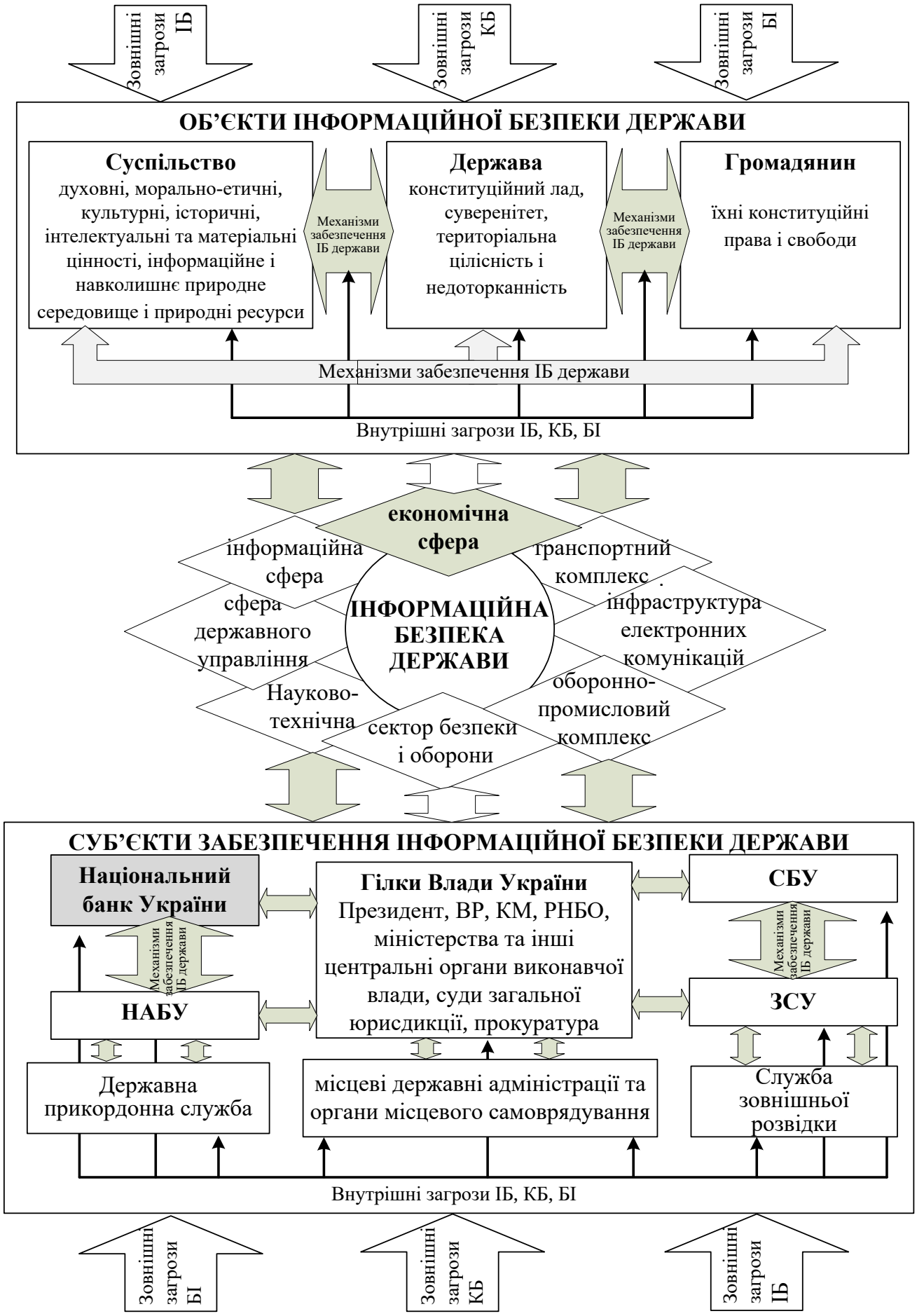


Рисунок 1.4 – Взаємозв'язок основних складових інформаційної безпеки держави

Революційні зміни останнього десятиліття, що відбулися в банківському секторі, зумовили до об’єднання інформаційних та комп’ютерних мереж в єдиний інформаційний та кібернетичний простір, що спонукало до створення автоматизованих банківських систем, які істотно розширили спектр електронних послуг державних і комерційних банків світу та України. Як наслідок, суттєво трансформувалися і загрози такому національному інформаційному ресурсу держави, як БІР під якими в роботі розуміється банківська інформація. Ключовою і найбільш потенційно небезпечною з них є загроза зриву або взяття під віддалений контроль процесів управління в АБС.

Наслідки у разі відсутності або недосконалості механізмів забезпечення безпеки АБС можуть мати колосальний і незворотній характер, що приводить в результаті до обвалу фінансово-банківської системи України, зокрема, і економічного колапсу в державі в цілому.

Аналіз рис. 1.3 та 1.4 показав, що забезпечення ІБ держави цілком залежить від забезпечення ІБ її складових, які належать до об’єктів МКІД і впливають не тільки на стан ІБ держави, а також на інші складові життєдіяльності суспільства та держави в цілому. Загрози набули ознак гібридності, отже їх необхідно розглядати як комплексовані загрози, які мають синергетичний ефект дії на все складові безпеки держави: ІБ, КБ, БІ. Підтвердженням цього підходу є останній керівний документ НБУ, який затверджує “Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України” [34], основні положення та їх взаємозв’язок наведені на рис. 1.5.

Тому вирішення всього комплексу питань, пов’язаних із забезпеченням кібербезпеки, інформаційної безпеки та безпеки інформації БІР має вирішуватися в комплексі і нерозривно один від іншого, гармонійно доповнюючи і заповнюючи, в разі необхідності, один одного. Просте комплексування сил і засобів в кожному окремому випадку для забезпечення безпеки БІР є недоцільним, як з практичної, так і наукової точок зору.

Рисунок 1.5 – Основні принципи і механізми забезпечення ІБ в ОБС України

Відсутність інших альтернативних підходів спонукає нагальну потребу у вирішенні проблеми, що склалася – підвищення захищеності БІР України на основі нових невідомих до сьогодні підходів.

Відомо, що комп'ютерні системи і телекомунікації забезпечують надійність функціонування величезної кількості інформаційних систем найрізноманітнішого призначення, в тому числі і банківського. Більшість таких систем містять інформацію з обмеженим доступом, яка має конфіденційний характер. Таким чином, рішення задачі автоматизації процесів обробки даних зумовило породження нової проблеми – **проблеми безпеки інформації** [37; 54; 55; 56; 57; 58; 59; 25; 20; 21; 19].

З часів свого виникнення банки незмінно викликали злочинний інтерес. І цей інтерес був пов'язаний не тільки зі зберіганням в кредитних організаціях грошових коштів, але і з тим, що в банках зосереджувалася важлива і часто секретна інформація про фінансову і господарську діяльність багатьох людей, компаній, організацій і навіть цілих держав.

При цьому, незалежно від застосовуваних засобів, механізмів та технологій забезпечення безпеки БІР, ще однією актуальною проблемою і, другою за загальним рахунком, є **проблема інформаційної безпеки** особистості, суспільства і держави, в якій людина – співробітник банку або його клієнт – найбільш уразлива ланка [33; 39; 40; 41; 42; 29].

Комп'ютеризація банківської діяльності дозволила значно підвищити продуктивність праці співробітників банку, впровадити нові технології в фінансові продукти. Інтернет-банкінг сьогодні є поширеним серед банків і клієнтів, використання Інтернет-ресурсів як альтернативний засіб передачі ПІН-коду клієнта в банк не тільки призводить до зниження витрат на передачу, але і дозволяє поліпшити банківську конкурентоспроможність, збільшити гнучкість роботи банку з клієнтами. Головними перешкодами на шляху інтернет-банкінгу є питання забезпечення кібербезпеки, а також відсутність довіри і правової підтримки [42].

Як приклад можна назвати той факт, що 90% всіх злочинів в банківській сфері – це кіберзлочини, пов'язані з використанням автоматизованих систем

обробки інформації банку [38]. Тому захист власне банківської системи повинен використовувати потужні засоби автентифікації і контролю дій як внутрішніх користувачів, так і клієнтів. Загальновідомо, що найбільш надійний захист можуть забезпечити засоби двофакторної автентифікації, наприклад електронні ключі (токени) або генератори одноразових паролів [45; 63; 64; 65;66]. Безпека даних при зберіганні вимагає використання засобів шифрування, які зможуть працювати або на рівні сховищ даних або на рівні окремих компонентів системи, наприклад, таблиць баз даних. Безпека банкоматів і платіжних терміналів повинна забезпечуватися з використанням засобів антивірусного захисту. Водночас специфіка таких пристроїв вимагає застосування додаткових засобів забезпечення безпеки, включаючи створення "замкнутого програмно-апаратного середовища", що повністю виключає установку будь-якого стороннього програмного застосунку (ПЗ) і підключення зовнішніх пристроїв [17; 18; 29; 31; 33; 34 39; 41]. Таким чином, **проблема кібербезпеки** також є невід'ємною третьою складовою на шляху вирішення проблеми забезпечення безпеки БІР [44; 45; 46; 47].

Для досягнення адекватності системи безпеки БІР, незалежно від того, якою її складовою є проблема безпеки інформації, проблема інформаційної безпеки або проблема кібербезпеки, так само доцільно застосовувати принципи методу Ризик-менеджменту [40]. Цей метод при грамотному підході дозволить своєчасно визначити та класифікувати загрози, і, відповідно до ймовірності настання негативних наслідків від їх можливого прояву, адекватно організувати систему безпеки БІР. Але з огляду на недосконаліть принципів методу Ризик-менеджменту в банківській сфері він ще вимагає необхідного доопрацювання з погляду піднятих раніше проблем.

У роботі [29] відзначається, що безпека інформації в тому числі і банківської може бути забезпечена лише при комплексному використанні всього арсеналу наявних засобів захисту у всіх структурних елементах виробничої системи і на всіх етапах технологічного циклу обробки інформації. Цей підхід покладений в основу забезпечення ІБ організацій банківського сектору і визначено Постановою НБУ [34].

Ігнорування методології системного аналізу щодо створення системи безпеки БІР виходячи зі складності, а іноді і з неможливості об’єктивного підтвердження ефективності створеної системи через недосконаліть нормативно-методичного забезпечення системи безпеки БІР, перш за все в області показників і критеріїв [41] так само створює перешкоди на шляху вирішення вказаної проблеми. Наприклад, Міжнародний стандарт для операцій з банківськими картами з чіпом (*EMV*), введений в 2005 році, визначає фізичну, електронну та інформаційну взаємодію між банківською картою і платіжним терміналом для фінансових операцій на основі стандартів *ISO/IEC 7816* для контактних карт, і *ISO/IEC 14443* для безконтактних карт.

Таким чином, в результаті вивчення літературних джерел можна зробити висновок про те, що принципово нового ефекту в безпеці БІР можна досягти тоді і тільки тоді, коли всі описані вище засоби, методи, заходи і технології безпеки об’єднуються в єдиний цілісний механізм, в подальшому званий *синергетичним*.

1.1.2. Дослідження ролі й місця системи безпеки банківських інформаційних ресурсів

Враховуючи стрімкий розвиток науки і техніки за останні десять років, а також інтенсивне застосування новітніх високотехнологічних розробок в банківському секторі сутність і зміст категорії БІР під якими в роботі розуміється “банківська інформація” (БІн) істотно змінилась. Сьогодні, як відомо, БІР є основою компонентою сучасних АБС. Виходячи з цього і спираючись на [43; 60], можна стверджувати, що під БІР в найширшому сенсі розуміється сукупність відомостей, пов’язаних зі Статутними документами та Керівництвом банківської установи, організаційно-правовою формою банківської установи, нинішнім виглядом банківської установи та її службовців, видами і формами банківського обслуговування, кількістю і складом клієнтів, операціями з рахунками клієнтів, наявністю кореспондентських стосунків і технічним забезпеченням банку. Враховуючи широту тлумачення категорії “банківські інформаційні ресурси” або

“банківська інформація” з метою подальшого її коректного застосування пропонується ознакова класифікація БІР (БІн) (рис. 1.6).

Рисунок 1.6 – Ознакова класифікація банківських інформаційних ресурсів

Перевагою запропонованої ознакової класифікації БІР (БІн) (див. рис. 1.6) є те, що вона на відміну від відомих класифікацій дозволяє розкрити глибину змісту суті цієї категорії. Наприклад, за видами банківська інформація буває організаційною, технологічною та параметричною.

При цьому під *організаційною банківською інформацією* слід розуміти інформацію, що відображає характер ділових зв’язків банку з клієнтами, інформацію про особливості організації та побудови системи управління банку.

Технологічна банківська інформація – це інформація про принципи управління банком при здійсненні ним усіх видів банківської діяльності, а також інформація про застосовувані в системах банківського захисту новітні високотехнологічні розробки.

Параметрична банківська інформація – це інформація, яка ілюструє кількісні показники, що відображають банківський капітал і величину його кредитного портфеля при здійсненні банком всіх видів діяльності. Ще однією перевагою запропонованої класифікації є те, що в разі появи нових ознак, які

характеризують ті чи інші аспекти категорії банківська інформація в запропонованій класифікації передбачена можливість розширення множини ознак.

Із запропонованої класифікації також випливає висновок про те, що в підсистемах АБС Банку циркулюють БІР різних рівнів конфіденційності (секретності) від відкритої інформації, до відомостей, що містять інформацію з обмеженим доступом (комерційна, банківська та службова таємниця). У документообігу АБС банку також присутні: платіжні доручення та інші розрахунково-грошові документи, звіти (фінансові, аналітичні та інші), відомості про особові рахунки, узагальнена інформація та інші конфіденційні (обмеженого доступу) документи і т.д., які також можуть бути віднесені до поняття БІР.

Таким чином, в найзагальнішому вигляді під *банківськими інформаційними ресурсами (банківською інформацією)* можна розуміти інформацію, яка виникає в результаті банківської діяльності. Це перш за все відомості, що характеризують сам банк, його фінансове становище, надійність і виконання вимог законодавства.

Таку інформацію можна почерпнути зі статуту банку, його ліцензій, бухгалтерських балансів, звітів про прибутки і збитки та інших джерел. Крім того, в більш вузькому розумінні *банківські інформаційні ресурси* – це відомості про конкретні операції банку. Така інформація характеризує не тільки банк, але і тих осіб, з якими банк вступає в правовідносини. Як приклад БІР можна навести відомості про наявність рахунків або вкладів і про операції з ними, про майно, що знаходиться на зберіганні в банку.

Незалежно від того в широкому або вузькому розумінні трактується змістовна частина категорії БІР діяльність всіх підсистем АБС, в яких вони виробляються, обробляються, зберігаються та циркулюють забезпечується і регулюється на основі законодавчих актів і рекомендацій Національного банку України. Виходячи з цього всі основні діючі нормативні акти, які регулюють описані вище процеси на державному рівні в систематизованому вигляді можуть бути представлені у вигляді структурної схеми (рис. 1.7).

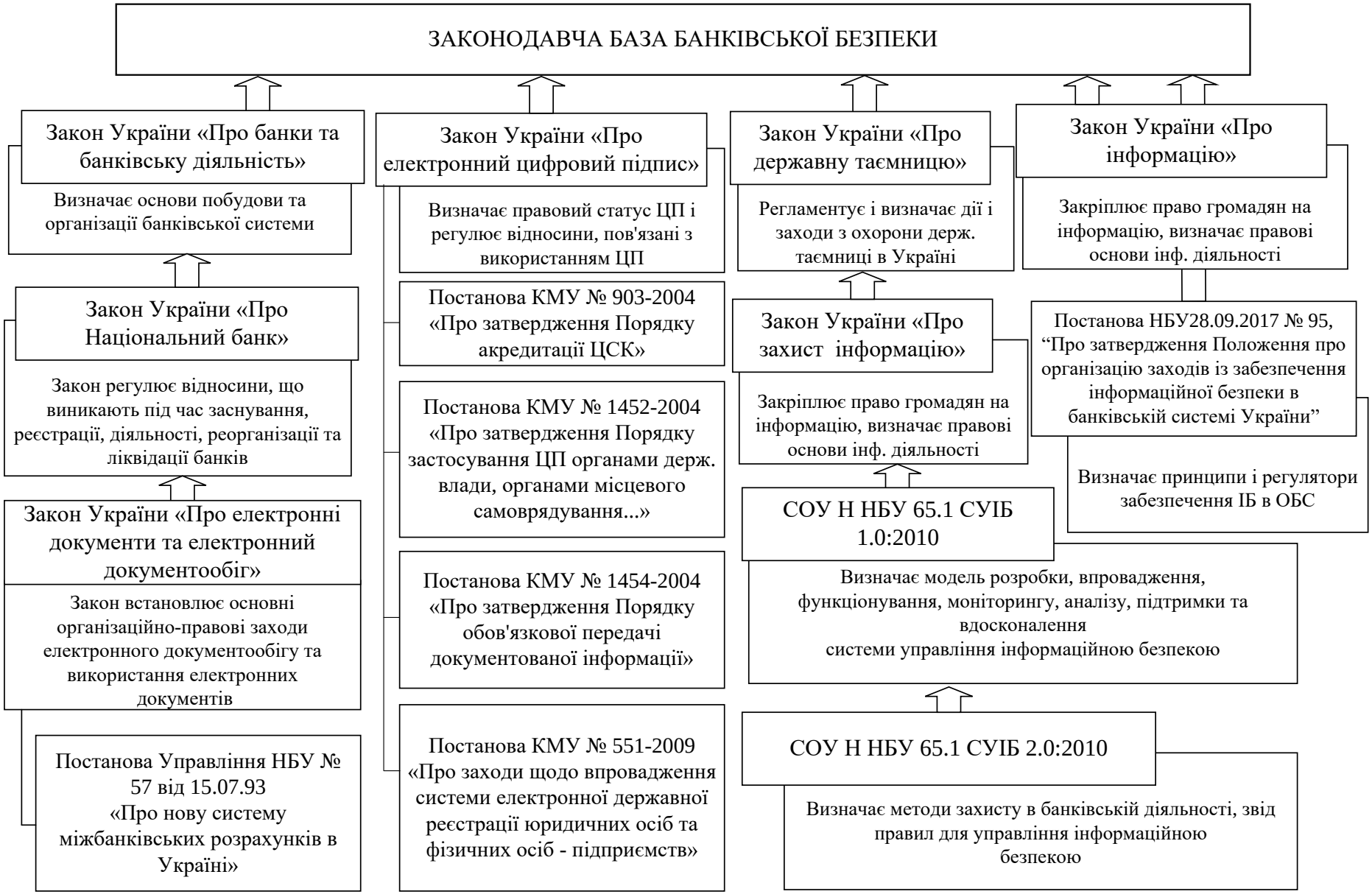


Рисунок 1.7 – Чинна нормативна база діяльності АБС в Україні та її взаємозв’язки

Проведений критичний аналіз діючої законодавчої бази України показав, що для забезпечення захисту БІР використовуються системи управління інформаційною безпекою (СУІБ), які забезпечують контроль функціонування комплексних систем захисту інформації. Таким чином, як випливає з попереднього висновку, АБС є комплексною інформаційною банківською системою, що інтегрує різні сфери діяльності банку, здатна автоматизувати і об'єднати в єдині цілі бізнес-процеси фінансової установи. Комплексна система, що підтримує централізовану обробку, мультивалютність і автоматизацію основних фінансових операцій, повинна забезпечувати ефективне управління, контроль, отримання звітів про поточну діяльність всіх філіалів банку [9, 31].

Серед функцій, властивих сучасним комплексним АБС, можна виділити наступні: операційний день; операції на фондовому ринку, робота банку з цінними паперами; внутрішньогосподарська діяльність; роздрібні банківські послуги; дистанційне банківське обслуговування; електронні банківські послуги; розрахунковий центр і платіжна система (карткові продукти); інтеграція бек-офісу банку з його зовнішніми операціями; управління діяльністю банку, реалізація бізнес-логіки, контроль, облік, в тому числі податковий, і звітність; управління ризиками та стратегічне планування; програми лояльності клієнтів, маркетингова, рекламна та *PR*-служби.

Як відомо [23; 24; 26; 28; 29; 34; 37; 38; 39; 40; 41; 42; 43; 55; 56; 57; 58; 59; 60], наведені основні функції АБС реалізуються за допомогою застосування таких технологій і засобів забезпечення безпеки БІР:

– системи управління базами даних (розподіленими базами даних);

– сховища даних, *OLAP*- і *OLTP*- технологій обробки даних (системи оперативної аналітичної обробки і системи оперативної обробки транзакцій);

– системи пошуку, вилучення та підготовки достовірних даних;

– розподіленої обчислювальної системи, організації колективної роботи користувачів, створення реального інформаційного простору банку, включаючи філіали, клієнтів і партнерів;

– безпечного підключення інформаційної системи банку до зовнішніх обчислювальних мереж (Інтернет);

– організації безпечної, достовірної передачі даних загальнодоступними каналами зв'язку (криптографія: шифрування і електронний цифровий підпис (ЕЦП), організаційні заходи), електронний документообіг;

– технічного, програмного, математичного та іншого забезпечення;

– інформаційної аналітики і системи підтримки прийняття рішень (*decision support systems, DSS*);

– захисту інформації, що зберігається і обробляється, всієї АБС в цілому;

– системи віддаленої роботи з фондовими ринками і програми передбачення поведінки курсів;

– *CRM*-системи управління відносинами з клієнтами;

– програми реалізації фронт-офісу взаємодії з клієнтами;

– системи підтримки внутрішньої організації, менеджменту і виконавчої діяльності персоналу;

– розмежування доступу до інформації різного рівня секретності;

– антивірусного захисту;

– інтернет-магазини й інтернет-картки;

–центри обробки викликів (*call*- центри) та *IP*-телефонія;

– підтримка різних каналів доступу: Інтернет, телефон, мобільна мережа, *SMS, WAP* та ін.;

– підтримка множинних стандартів обліку, включаючи управлінський облік;

– підтримка і дослідження в області планомірного інформаційного розвитку АБС.

Приклад АБС НСЕМП наведений на рис. 1.8.

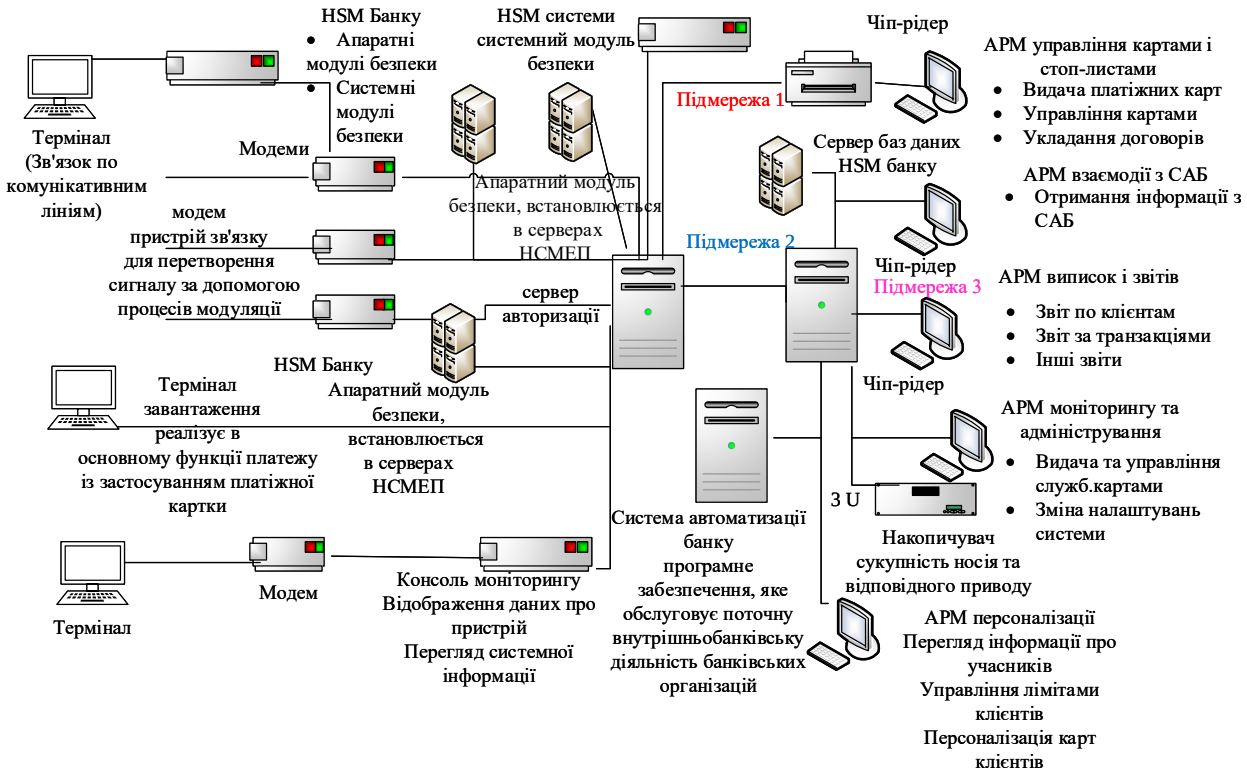


Рисунок 1.8 – Структурна схема АБС НСЕМП

Проведений аналіз організаційної структури НСМЕП показав, що в основі виконання функцій її роботи використовується *автоматизована карткова система (АКС)* – програмно-технічний комплекс, за допомогою якого забезпечується виконання функцій членом (ами) або учасником (ами) НСМЕП щодо емісії карток, обробки інформації про операції з їх застосуванням, управління терміналами і банкоматами і т.д.). Така система належить до складних багаторівневих систем управління критичного застосування (СУКЗ), в яких передача інформації вимагає контролю безпеки на кожному рівні [63].

Ця система інтегрується в банківські системи і множину типів терміналів, в тому числі переносні, які працюють в автономному режимі, і банкомати, які виконують більш широкий спектр функцій. НСМЕП управляє потоками електронних грошей, зв’язком терміналів і локальних мереж. Для забезпечення надійної роботи електронна платіжна система повинна бути надійно захищена.

З точки зору безпеки в НСМЕП існують такі вразливі місця: пересилка платіжних та інших повідомлень між банком і клієнтом або між банками; обробка

інформації всередині організацій відправника і одержувача повідомлень; доступ клієнтів до засобів, акумульованих на рахунках.

1.1.3. Дослідження об'єктів загроз на інфраструктуру автоматизованих банківських систем

Еволюційні зміни АБС істотно розширили спектр електронних послуг державних і комерційних банків світу та України. Як наслідок, суттєво трансформувалися і загрози такому національному інформаційному ресурсу держави, як БІР під якими в роботі розуміється БІн. Загрози безпеці БІР набули ознак гібридності. Прояви ознак гібридності унаслідок одночасного впливу загроз інформаційній безпеці, кібернетичній безпеці та безпеці інформації на БІР призвели до виникнення явища синергізму, негативні прояви від якого потребують кардинального перегляду концепцій побудови діючих систем безпеки. Як показує світовий досвід, наприклад, прояви гібридних загроз безпеці БІР мали місце під час блокування роботи АБС БнС в США (вересень, 2011 р.), що призвело виникнення масової акції непокори під назвою "Захопи Уолл-Стрітт", яка ланцюговою реакцією поширилася на найбільші міста згаданої держави та ряду найбільш економічно розвинених держав Європейського Союзу та зрештою спровокувала світовий економічний колапс. Прояви гібридних загроз безпеці БІР мали місце і в Україні. Наприклад, розпочавшись з кібератаки за допомогою шкідливого програмного забезпечення "*Petya.A*", "*Petya.B*" (червень–липень, 2017 р.) було скомпрометовано процес надання банківських послуг, що викликало невдоволення клієнтів банків – громадян, які є суб'єктами ІБ держави. Ланцюгова реакція після України поширилася на банківські сектори Італії, Ізраїлю, Сербії, Румунії, Угорщини, Аргентини, Чехії, Німеччини та інших розвинених держав світу. Таким чином, проблема забезпечення ІБ держави для інфраструктур критичного застосування (ІКЗ), до яких належить і банківський сектор, стоїть дуже гостро. Отже, стає зрозуміло, що потребують кардинального перегляду діючі методологічні засади побудови системи безпеки БІР як України зокрема, так і світу в цілому. Для знаходження необхідних і достатніх умов, що забезпечують досягнення

синергетичного ефекту в сфері безпеки державних і приватних систем банківського захисту, проаналізуємо і уточнимо множину актуальних загроз безпеки БІР. Але перед тим, як перейти до вирішення викладеного вище часткового завдання відзначимо, що вперше в основу безпеки БІР пропонується покласти ***принципи синергізму***. При цьому взаємодіючими профілями, які забезпечують безпеку БІР слід вважати ІБ, КБ та БІ БІР, що до сьогодні розглядалися або розрізнено, або в комплексі, що не дозволяло отримати синергетичний ефект при забезпеченні безпеки банківської інформації. Провівши декомпозицію певних профілів безпеки, розглянемо їх окремо з метою визначення найбільш актуальних загроз. Виходячи з [31] тут і надалі під *загрозою безпеці* банку будемо розуміти випадкові або цілеспрямовані, потенційні або реальні дії різної природи, які здатні завдати банку збитків.

Відомо, що для аналізу основних видів загроз безпеки інформації БІР може бути адаптована модель тріади *CIA* (*confidentiality, integrity, availability*) [38; 55]. У даній моделі під *безпекою інформації* БІР слід розуміти процес забезпечення конфіденційності, цілісності та доступності інформації клієнтами / клієнтом банку на основі сукупності колективної та індивідуальної свідомості. При цьому під *конфіденційністю* розуміється забезпечення доступу до інформації тільки авторизованим користувачам, під *цілісністю* – забезпечення достовірності та повноти інформації, і методів її обробки для авторизованих користувачів, під *доступністю* – забезпечення доступу до інформації та пов’язаних з нею активів авторизованих користувачів при необхідності.

З огляду на специфіку банківської сфери основними ***загрозами безпеці інформації БІР*** можна вважати такі [63]:

Порушення конфіденційності: виявлення паролів користувачів при негласному активному підключенні до мережі, аналіз трафіку для виявлення протоколів обміну, створення помилкових тверджень про отримання платіжних документів, несанкціоноване введення даних, вилучення інформації зі статистичних баз даних (БД) на основі семантичних зв’язків між секретною та несекретною інформацією, підключення до комп’ютерній мережі (КМ) як

активного ретранслятора (фальсифікація платіжних документів), фішинг, фармінг, претекстінг, скрімінг, віртуальне викрадення, несанкціонована передача конфіденційної інформації, встановлення прихованих передавачів з метою копіювання даних або доступу до них легальними КМ в результаті негласного відвідування в неробочий час, негласна перебудова обладнання або програмного забезпечення (ПЗ) з метою впровадження засобів несанкціонованого доступу до інформації.

Порушення цілісності: копіювання даних з магнітних носіїв, залишених на столах або в комп'ютерах, копіювання даних з устаткування і магнітних носіїв, прибраних в спеціальні сховища, використання включеного в систему терміналу, залишеного без нагляду, копіювання та викрадення ПЗ, внесення змін в дані і програми для підробки і фальсифікації фінансових документів в результаті негласного відвідування в неробочий час, зчитування інформації з жорстких і гнучких дисків, внесення змін в дані, записані на залишених без нагляду магнітних носіях, використання ПЗ для подолання захисних можливостей системи, несанкціоноване використання ресурсів комп'ютерів, знищення обладнання, магнітних носіїв або дистанційне знищення інформації, внесення змін або зчитування інформації з БД або окремих файлах через присвоєння чужих повноважень з метою модифікації фінансової інформації, підміна елементів обладнання, залишених без нагляду в робочий час.

Порушення доступності (автентичності): несанкціоноване використання інформації високого рівня секретності, несанкціоноване перевищення повноважень на доступ в обхід механізмів безпеки, відмова абонента від факту прийому (передачі) або створення помилкових відомостей про час прийому (передачі) повідомлень для зняття з себе відповідальності за виконання цих операцій, проникнення в систему через комунікаційні КМ з присвоєнням повноважень з метою підробки, копіювання або викрадення інформації, зловживання привілеями супервізора при порушенні механізмів захисту банківської інформації, виявлення паролів при викраденні або візуальному спостереженні, безпосередньо розкриття або зміна даних.

До числа ***загроз інформаційній безпеці БІР***, що впливає на банк, персонал банку і його клієнтів, а також на економічну складову національної безпеки держави належать внутрішні і зовнішні загрози. Як перші, так і другі за спрямованістю і характером впливу на діяльність певних суб'єктів і об'єктів можуть бути економічними, фізичними та інтелектуальними [25; 59].

Економічні загрози: корупція, шахрайство, недобросовісна конкуренція, використання банками неефективних технологій банківського виробництва. Реалізація таких погроз призводить до завдання збитків банкам або втрати ними прибутків.

Фізичні загрози: пограбування, викрадення майна і коштів банків, поломки, виведення з ладу обладнання банків, неефективна експлуатація сил і засобів. У результаті реалізації таких загроз завдаються збитки банкам, пов'язані з втратою своєї власності і необхідністю нести додаткові витрати на відновлення засобів виробництва та інших матеріальних засобів.

Інтелектуальні загрози: розголошення або неправомірне використання банківської інформації, дискредитація банку на ринку банківських послуг, різного роду соціальні конфлікти навколо банківських установ або в них самих. Наслідки реалізації таких загроз: збитки банків, погіршення їх іміджу, соціальна чи психологічна напруженість навколо установи банків або в їх колективах.

Третім необхідним профілем безпеки БІР пропонується вважати КБ. *Кібербезпека* – набір засобів, стратегій, принципів забезпечення безпеки, гарантій безпеки, підходів до управління ризиками, дій, професійної підготовки, страхування і технологій, які використовуються для захисту кіберпростору, ресурсів організацій та користувачів [47; 48; 58]. Відповідно до стандарту *ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cybersecurity* на кібербезпеку також покладаються завдання щодо забезпечення умов, спрямованих на досягнення і збереження властивостей безпеки у ресурсах організації або користувачів, що покликані захистити від відповідних кіберзагроз. При цьому кібербезпека охоплює таке поняття, як захист персональної інформації, та взаємодіє з мережевою безпекою, прикладною безпекою, Інтернет-безпекою та

безпекою критичних інформаційних інфраструктур (рис. 1.9).

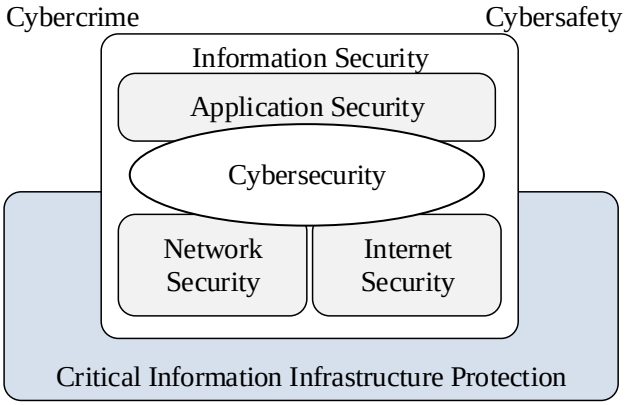


Рисунок 1.9 – Логічні взаємозв'язки кібербезпеки та інших доменів безпеки згідно зі стандартом *ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cybersecurity*

Аналіз результатів в області оцінки кількості кібератак, в тому числі і на АБС, співвідношення рівнів складності програмного забезпечення та технічної грамотності зловмисників, отриманих такими компаніями як *"Arbor Networks"* [61], *CISCO* [62] та іншими вендорами на ринку кібербезпеки і засобів мережевої периферії, дозволяє зробити висновок про те, що зі зростанням кіберзлочинності і обчислювальних можливостей в найближчому майбутньому слід очікувати зростання не тільки кількості і технічної складності кібератак, а й перенаціленння їх на периферійне мережеве обладнання.

З огляду на це, а також спираючись на результати досліджень [1; 3; 6; 12; 22; 29; 34; 38; 40; 41; 56; 57; 58; 61; 62] можна стверджувати про те, що основними загрозами кібербезпеці АБС, спрямованими на зрив процесів управління або взяття їх під контроль, будуть кібератаки, які можна об'єднати в чотири основні класи, змістовна частина яких розкрита на рис. 1.10.

Рисунок 1.10 – Класифікація кібератак на АБС з прив’язкою до моделі *OSI*

Запропонована класифікація (рис. 1.10) наочно свідчить, що кібератаки різних класів не залежно від функціонального призначення мають місце на різних рівнях моделі взаємодії відкритих систем *OSI*, а отже мають і свої конкретні завдання впливу на БІР. Наприклад, перед кіберзлочинцем через вразливість протоколів і служб нижнього рівня моделі *OSI* відкриваються можливості отримання технологічної банківської інформації, а через вразливість протоколів і служб верхніх рівнів – до організаційної та параметричної банківської інформації.

З огляду на те, що описані вище загрози в силу різних суб’єктивних і об’єктивних причин мали і надалі матимуть місце для більшості відомих і проектованих АБС, а також спираючись на тісний взаємозв’язок між ними для різних профілів безпеки, і з метою розробки ефективних систем безпеки БІР, пропонується нова модель загроз безпеці БІР, в подальшому звана **синергетичною** (рис. 1.11).

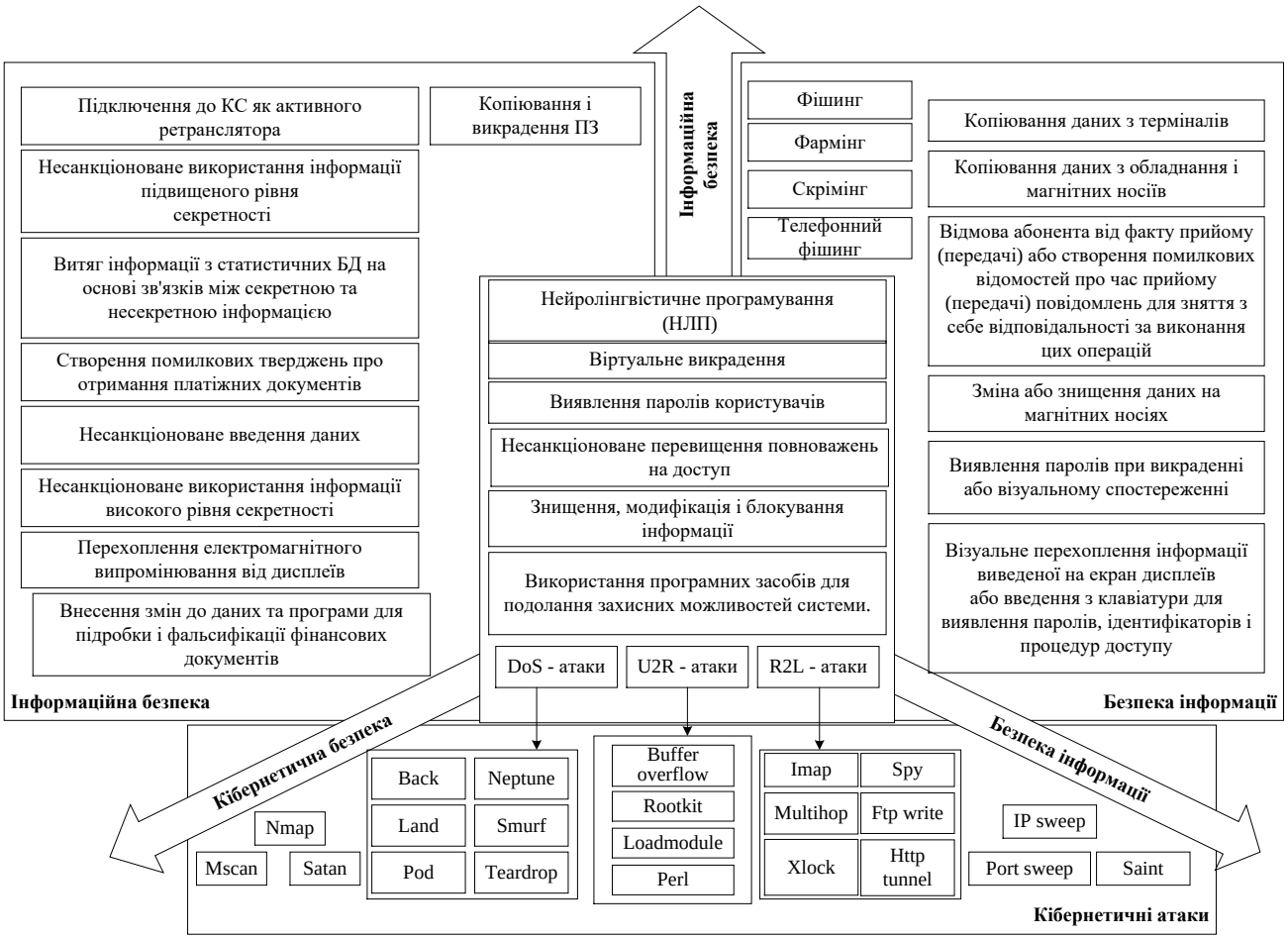


Рисунок 1.11 – Синергетична модель загроз безпеці БІР

Особливістю запропонованої моделі (рис. 1.11) є відображення на ній у вигляді логічних зв’язків взаємодії загроз для різних профілів безпеки. Тому синергетична модель загроз безпеці БІР закладає необхідні і достатні умови для розробки нового методологічного базису, спрямованого на досягнення синергетичного ефекту в сфері забезпечення безпеки державних і приватних систем банківського захисту.

Спираючись на розроблену синергетичну модель (рис. 1.11) так само стає зрозумілим механізм зародження проблем безпеки БІР в просторово-часовому континуумі: цілі кіберзлочинців (конкурентів, кібертерористів, окремих держав і т.п.) координуються за часом, місцем, завданнями, формами реалізації.

З огляду на особливості побудови засобів мережевої периферії [11; 31; 37; 39; 40; 41; 47; 49; 50; 55] і організації комунікацій в АБС будь-якого банку синергетична модель дозволяє виявити найбільш вразливі місця в їх системі

безпеки. Ними є технологічні процеси, пов'язані з пересиланнями платіжних та інших повідомлень між банками (бізнес-процеси / бізнес-продукти), між банком і банкоматом, між банком і клієнтом. Ці особливості, як наслідок, породжують ряд проблем системного характеру:

– проблеми взаємної автентичності при встановленні з'єднання (взаємне впізнання абонентів);

– проблеми забезпечення конфіденційності і цілісності документів (захист електронних документів, переданих каналами зв'язку);

– проблеми доказовості факту відправлення та доставки документа (захист процесу обміну електронними документами);

– проблеми взаємної недовіри між відправником і отримувачем через їх належність до різних організацій і взаємної незалежності (забезпечення виконання документів).

Невід'ємною частиною проблеми забезпечення безпеки БІР є проблема аналізу ризиків. Фактично *ризик* являє собою інтегральну оцінку того, наскільки ефективно існуючі засоби захисту здатні протистояти атакам на БІР.

На сьогодні чітко можна виділити дві основні групи методик оцінювання ризиків безпеки. У застосуванні до банківської сфери на підставі першої групи можливо встановити рівень ризику шляхом оцінювання ступеня відповідності визначеному набору вимог щодо забезпечення безпеки БІР. Друга група методик оцінювання ризиків зводиться до визначення ймовірності реалізації атак, а також рівнів можливих збитків. У цьому разі значення ризику оцінюється окремо для кожної атаки і у загальному випадку є добутком ймовірності проведення атаки та величини можливого збитку від цієї атаки. Значення збитку визначається власником БІР, а ймовірність атаки обчислюється групою експертів, які проводять процедуру аудиту.

У будь-якій соціальній сфері (до якої належить і область безпеки БІР ОБС) інциденти безпеки, переривання роботи (*disruptive events*) і аварії (*disasters*) неминучі. Однак їх вплив на діяльність компанії має бути мінімізовано: дані повинні бути збережені, технічні засоби знаходиться в робочому стані, репутація

врятована, люди – поза небезпекою [13; 14; 35; 36]. Рішення вказаних завдань можливо здійснити в рамках управління безперервністю бізнесу (*Business Continuity Management*) – цілісного процесу управління, в рамках якого ідентифікуються потенційні загрози діяльності організації, оцінюються можливі впливи на бізнес-операції в разі реалізації цих загроз, а також створюється система приписів для забезпечення здатності організації відновлювати свою діяльність і ефективно реагувати на інциденти, що дозволяє гарантувати дотримання інтересів зацікавлених сторін, забезпечити захист репутації, бренду. Тому в першу чергу при реалізації стратегії і циклу управління безперервністю необхідно забезпечити вирішення таких завдань [16].

Існує два основні інструменти забезпечення безперервності бізнес-процесів [13; 14; 15]:

– план безперервності бізнесу (*Business Continuity Planning*, *BCP*) – набір превентивних заходів, детальних інструкцій для дій в гострих (критичних) ситуаціях, в ОБС додатково розглядаються заходи спрямовані на відновлення БІР. Відновлення даних БІР передбачає повну ясність того, коли вони були скопійовані, що містять, який їх формат, як їх слід інтерпретувати і інше. Визначається максимальний “вік” даних, втрата яких допустима (*Recovery Point Objective*, *RPO*);

– планування аварійного відновлення (*Disaster Recovery Planning*, *DRP*) – підготовка організації до найшвидшого повного відновлення її діяльності в разі аварії, надзвичайної ситуації, лиха, кризової ситуації і т.п.

Незважаючи на відмінність, *BCP* і *DRP* є невід’ємними частинами менеджменту безперервності бізнесу і процедурно перетинаються. В цьому аспекті їх зручно розглядати за допомогою моделі менеджменту *PDCA* (*Plan-Do-Check-Act*) [13; 17; 18]. Основні завдання на етапах моделі менеджменту *PDCA* наведені на рис. 1.12.

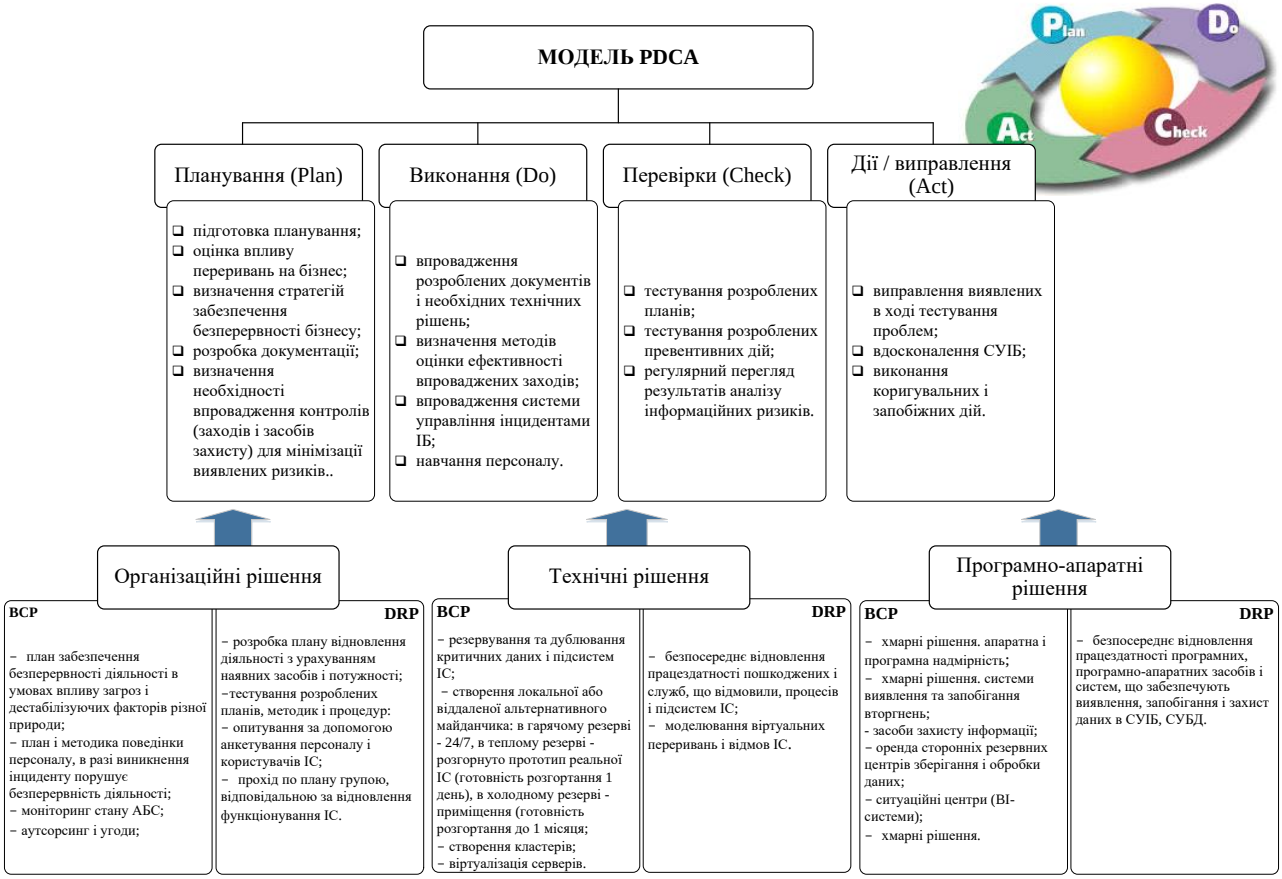


Рисунок 1.12 – Основні завдання та рішення забезпечення безперервності на етапах моделі менеджменту *PDCA*

Таким чином, запропоновані рішення мають свою вартість, сумісність, складність реалізації, час розгортання і ефективність, та можуть застосовуватися як окремо, так і у вигляді комплексу заходів, реалізованих до, під час і / або після інциденту, який викликав порушення безперервності функціонування АБС і діяльності ОБС.

Оцінка впливу переривань на бізнес (*Business Impact Analysis*, *BIA*) є ключовим питанням безперервності бізнесу і полягає у функціональному аналізі того, як переривання вплинуть на діяльність організації. До завдань *BIA* відносять [13; 14; 15; 16]: визначення цінності кожного бізнес-процесу; ідентифікацію та ранжування переривань кожного бізнес-процесу; пріоритизацію бізнес-процесів; оцінку ресурсів на забезпечення безперервності бізнес-процесів.

Підсумковим результатом *BIA* є вибір стратегій управління безперервністю бізнесу. При визначенні цінності бізнес-процесів для інформаційних систем (АБС)

можуть бути застосовані значення ряду технічних показників [13; 14; 15; 16], зв’язок між якими наведений на рис. 1.13:

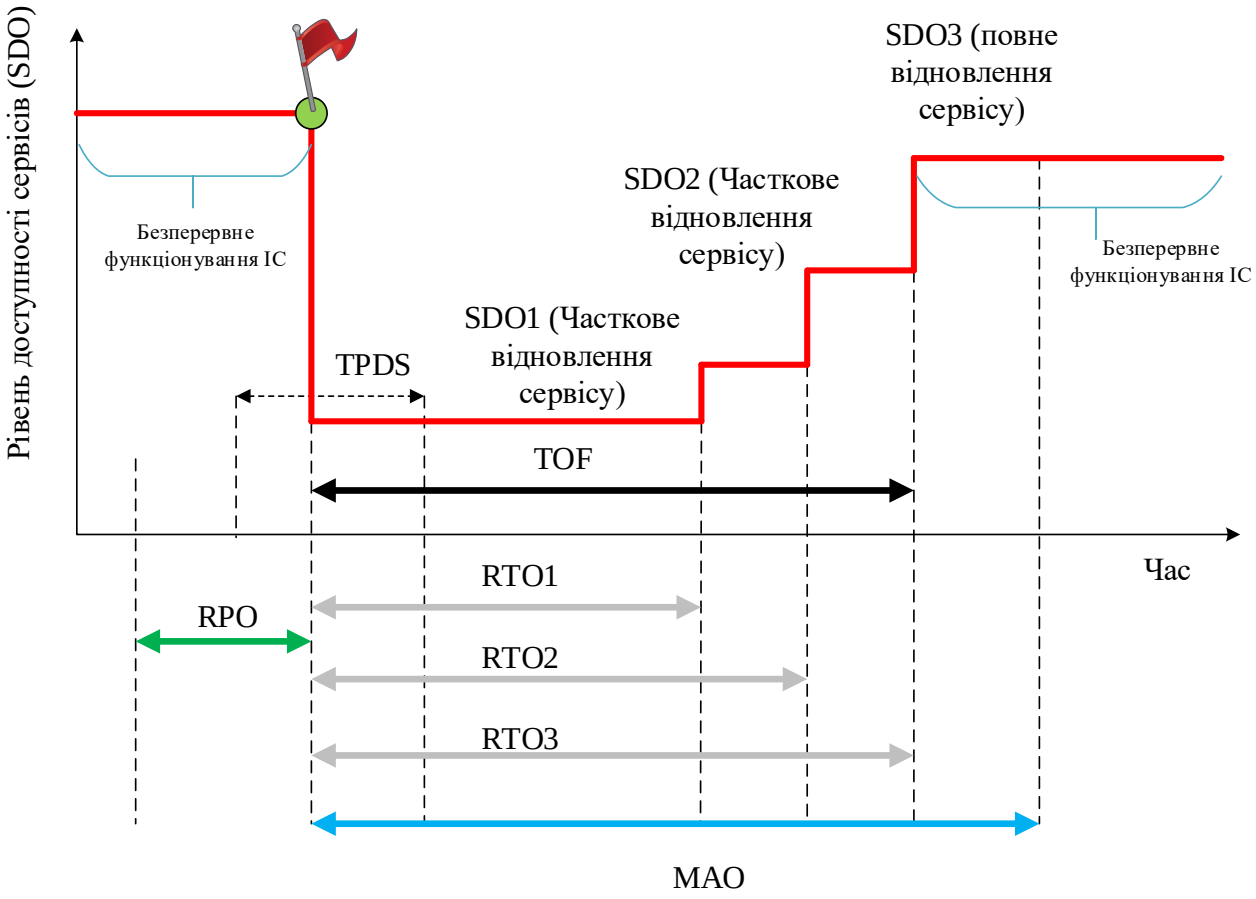


Рисунок 1.13 – Визначення показників безперервності діяльності

Основні позначення:

MTPD (*Maximum Tolerable Period of Disruption*, максимально прийнятний період переривання бізнесу) – період часу, після закінчення якого несприятливі наслідки, що виникли в результаті переривання бізнесу, стають неприйнятними;

RTO (*Recovery Time Objective*, цільовий час відновлення) – період часу після події переривання, протягом якого повинен бути відновлений мінімальний рівень діяльності організації, а також підтримуючі його системи, прикладні програми та функції. Вважається, що: *RTO* < *MTPD*;

RPO (*Recovery Point Objective*, цільова точка відновлення) – період часу, протягом якого повинні бути відновлені дані після минулого переривання;

MAO (*Maximum Allowable Outage*, максимально допустимий час простою) – період часу, після закінчення якого існує ризик остаточного припинення діяльності ОБС, в разі, якщо надання сервісів, даних, бізнес-процесів і / або послуг не будуть відновлені;

TOF (поточний час простою) – період часу, протягом якого діяльність була перервана в результаті відмови АБС або її компонентів, недоступності сервісів і даних, в прийнятному для підприємства випадку повинна бути менше максимально допустимого часу простою. Вважається, що $TOF \leq MAO$;

SDO (Service Delivery Objective, цільова доступність сервісу) – відображає рівень доступності сервісу в певний момент часу;

TPDS – час планування і розгортання рішень забезпечення та відновлення безперервності діяльності, в ідеальному випадку рішення і плани повинні бути розроблені і впроваджені до настання інциденту порушення безперервності, $TPDS << RTO$.

Аналіз рис. 1.13 показав, що для зниження *TOF* необхідний комплексний підхід до вирішення завдань *BCP* і *DRP*. Впровадження превентивних заходів захисту від кіберзагроз, спрямованих на порушення безперервності дозволить не тільки мінімізувати втрати даних БІР, а й скоротити цільовий час відновлення даних.

Подібний ефект досягається за рахунок того, що плани і засоби забезпечення безперервності діяльності розробляються і розгортаються не під час відмови, а в період штатного функціонування АБС, до реалізації загрози та виникнення лавинного ефекту. Це дозволяє відразу після настання інциденту скоординувати дії персоналу і почати відновлення або повністю уникнути простою і втрат за рахунок оперативного перемикання на резервну площу (рис. 1.14) [15; 36].

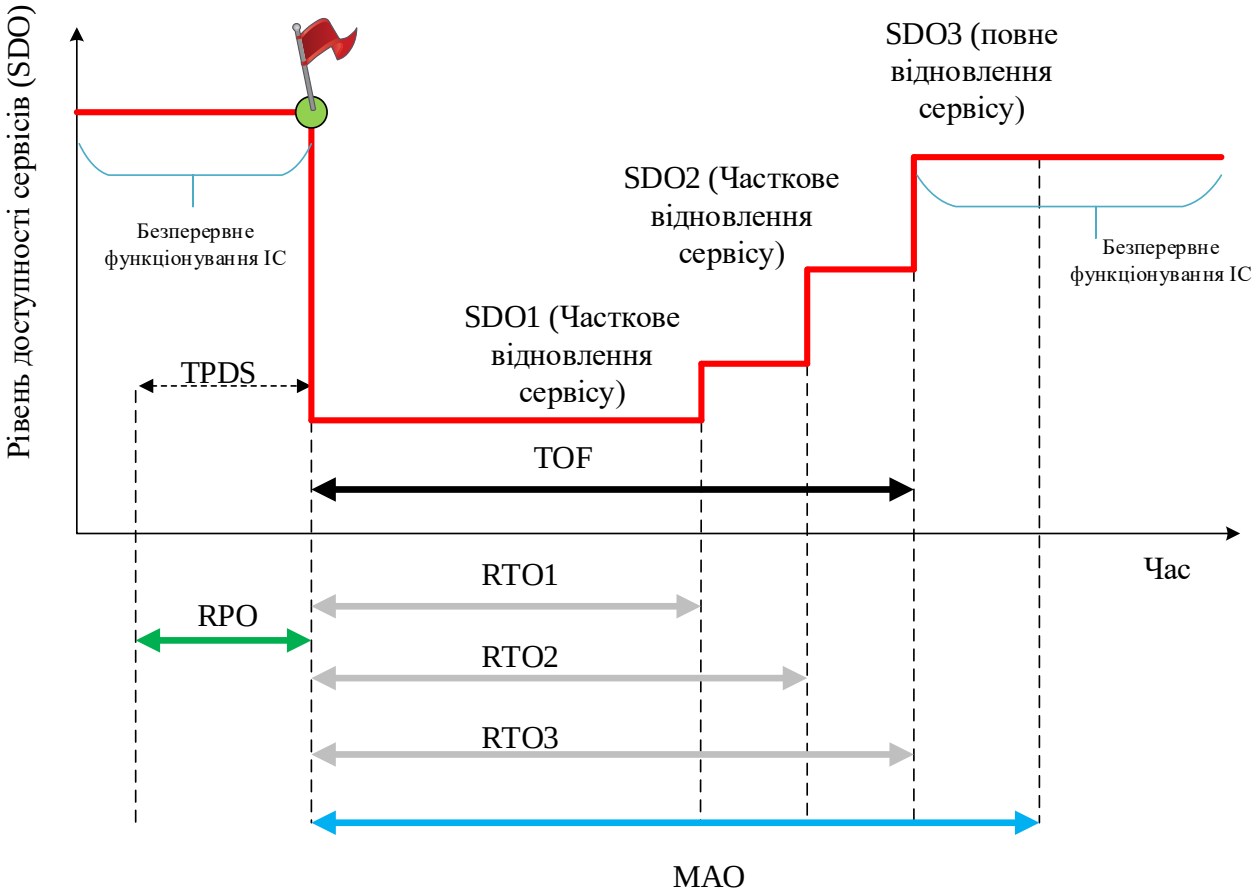


Рисунок 1.14 – Зниження часу відновлення функціонування АБС (*TOF*) за рахунок застосування превентивних планів і заходів захисту

Таким чином, для забезпечення комплексного підходу безперервності бізнес-процесів ОБС пропонується використовувати дублювання АБС на основі концепції альтернативної площини (площина у гарячому резерві (*Hot Site*), площина у теплому резерві (*Warm Site*), площина у холодному резерві (*Cold Side*) з використанням стратегій актуалізації даних – копіювання резервних даних (*electronic vaulting*, *off-site data protection*, періодична передача копій баз даних на альтернативні носії, зазвичай в пакетному режимі), віддалене відображення (*remote journaling*, періодична передача журналу виконаних транзакцій з основної площини на альтернативну), віддалене віддзеркалення (*remote mirroring*, повне дублювання у реальному часі), що забезпечує необхідні показники цінності бізнес-процесів. Запропонований підхід забезпечення безперервності бізнес-процесів в

АБС ОБС підтверджений в Постанові НБУ “Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України”. Проведемо аналіз основних механізмів криптографічного захисту БІР на прикладі АБС НСЕМП.

1.1.4. Аналіз сучасного стану послуг і механізмів криптографічного захисту банківських інформаційних ресурсів

Система захисту електронних банківських документів в обчислювальній мережі НБУ складається з комплексу апаратно-програмних засобів криптографічного захисту та ключової системи до них, технологічних і організаційних заходів, спрямованих на захист БІР в мережі НБУ. Відповідно до Концепції системи електронного грошового обігу в Україні, затвердженої Правлінням НБУ 02.10.92, розроблені і виготовлені апаратно-програмні засоби криптографічного захисту електронних банківських документів в обчислювальній мережі НБУ, в такому складі:

– апаратура захисту банківських даних (АЗБД);

– апаратура захисту електронного грошового обігу (АЗЕГО);

– ключова система з генерацією ключів в НБУ і захищеними електронними носіями ключів (шифрів);

– електронні картки (ЕК).

Апаратура захисту відповідає стандарту ГОСТ 28147-2009 на алгоритми шифрування і має сертифікат Державної служби України з питань технічного захисту інформації, задовольняє всі вимоги обчислювальної мережі “Банк”.

Якість вирішення зазначених вище проблем значною мірою визначається раціональним вибором криптографічних засобів, при реалізації механізмів захисту.

Відповідно до міжнародних стандартів *ISO 7498*, *ISO/IEC 10181* для забезпечення необхідних показників безпеки визначені п’ять базових загальноприйнятих послуг, основними з яких є тільки дві: автентичність і цілісність. Для їх забезпечення використовуються механізми безпеки, більшість з яких реалізується на основі криптографічних методів перетворення інформації.

Основні механізми забезпечення цілісності та автентичності БІР на різних рівнях засновані на використанні стандартів блочно-симетричних шифрів (3*DES*, ГОСТ 28147-2009). Структурна схема комплексної системи захисту БІР НСЕМП наведена на рис.1.15.

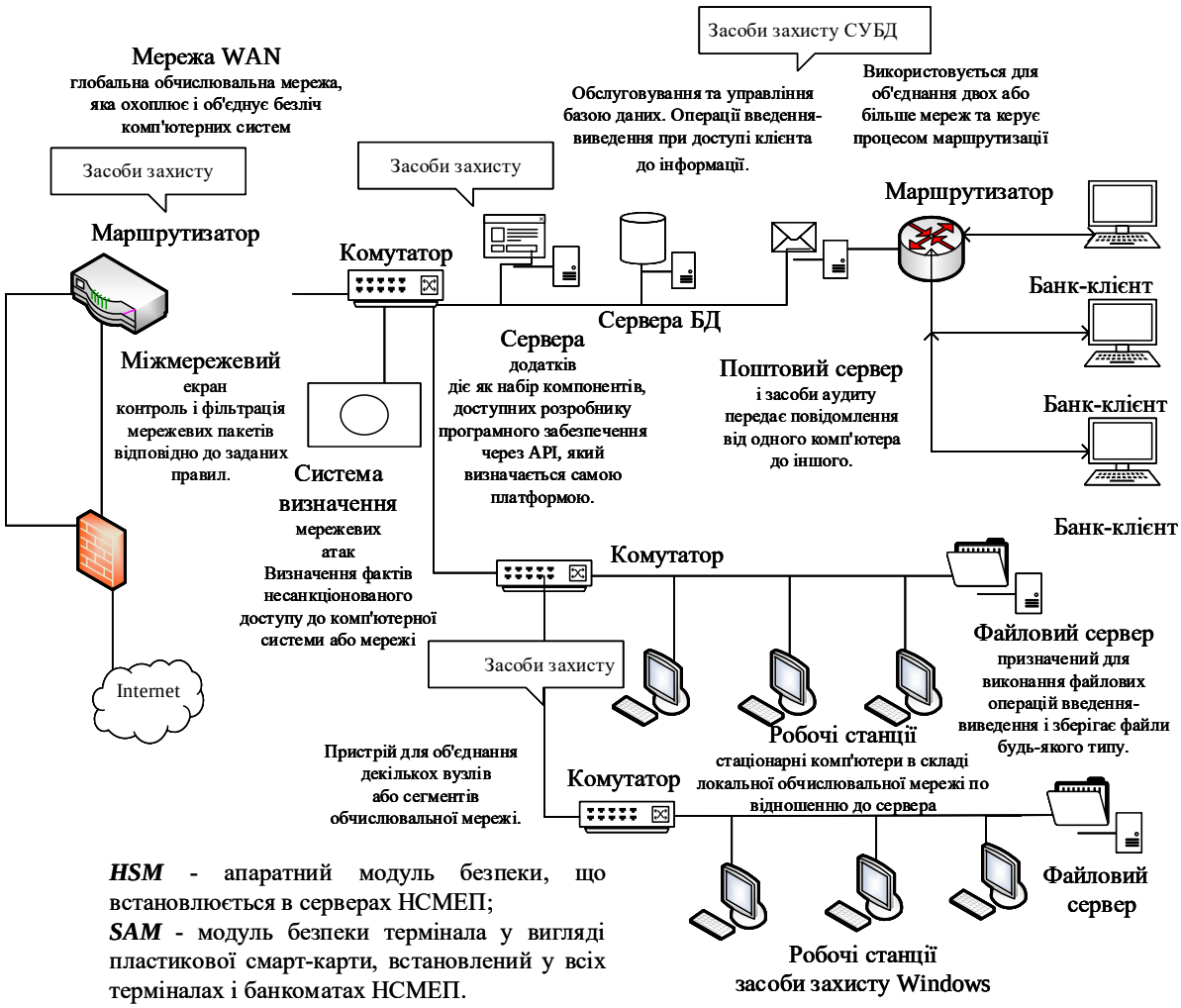


Рисунок 1.15 – Структурна схема СУІБ НСМЕП

Для забезпечення ведення електронного документообігу в АБС використовують електронні ключі (сертифікати) відповідно до стандарту ДСТУ *ISO/IEC 9594-8:2006* [67], прикладом системи комплексного захисту інформації (СКЗІ) є центр сертифікації ключів (ЦСК) “Шифр Х.509”. Система криптографічного захисту інформації “Шифр-Х.509” призначена для:

– створення інфраструктури відкритих ключів (створення ЦСК, в тому числі акредитованих, центрів реєстрації в рамках відповідальності ЦСК, надання користувачам засобів управління ключами);

– забезпечення послугами ЕЦП органів державної влади, органів місцевого самоврядування, підприємств, установ та організацій будь-якої форми власності, а також фізичних осіб.

Функціональним призначенням СКЗІ “Шифр-Х.509” є:

– забезпечення управління ключами та сертифікатами відповідно до ДСТУ *ISO/IEC 9594-8:2006*;

– забезпечення криптографічного захисту конфіденційної і відкритої інформації: обчислення і перевірка електронного цифрового підпису даних відповідно до ДСТУ 4145-2002, шифрування та імітозахист даних відповідно до ГОСТ 28147-89, формування геш-функції відповідно до ГОСТ 34.311-95.

СКЗІ “Шифр-Х.509” є програмним комплексом, засоби якого функціонують у середовищі ОС електронно-обчислювальної техніки та взаємодіють із загальним прикладним програмним забезпеченням, його загальна структура наведена на рис. 1.16.

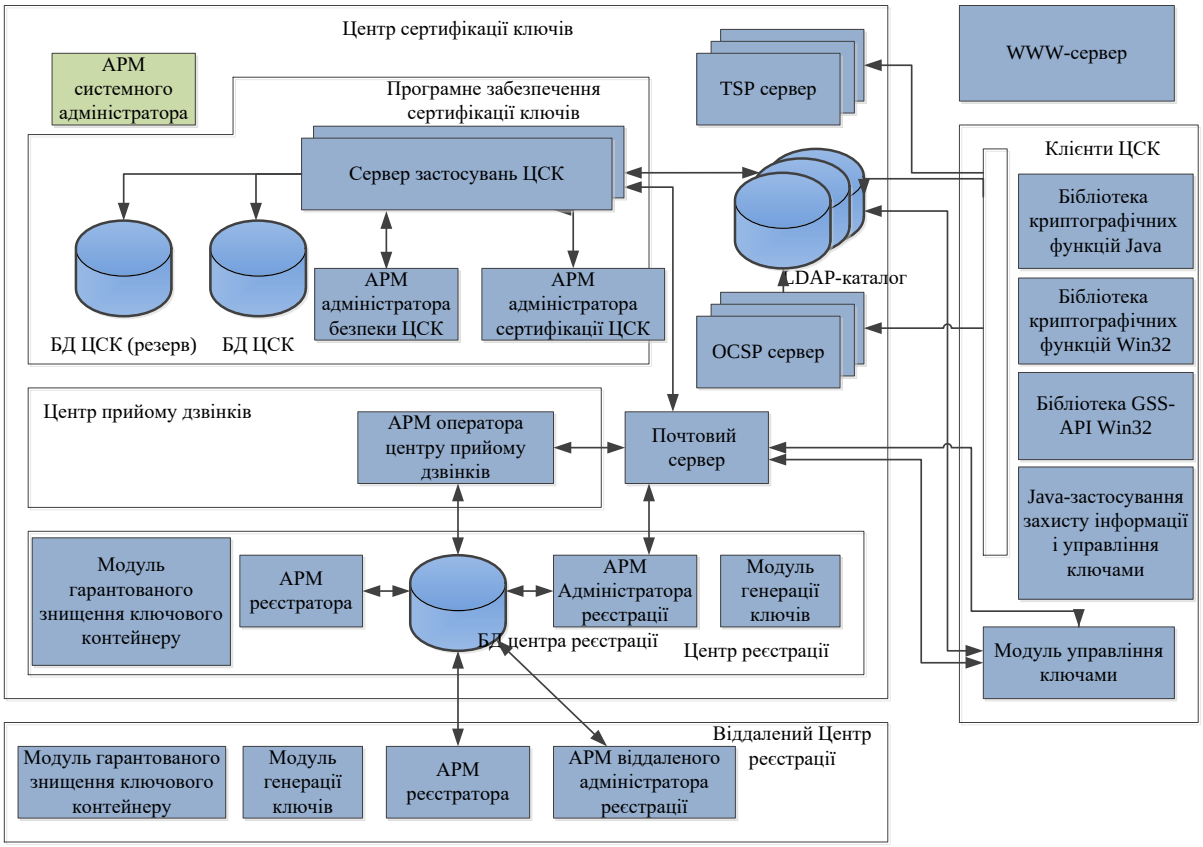


Рисунок 1.16 – Загальна структурна схема СКЗІ “Шифр-Х.509”

Організація мережевої взаємодії між компонентами СКЗІ вимагає особливої уваги. Типова топологія мережі СКЗІ “Шифр-Х.509” наведена на рис. 1.17.

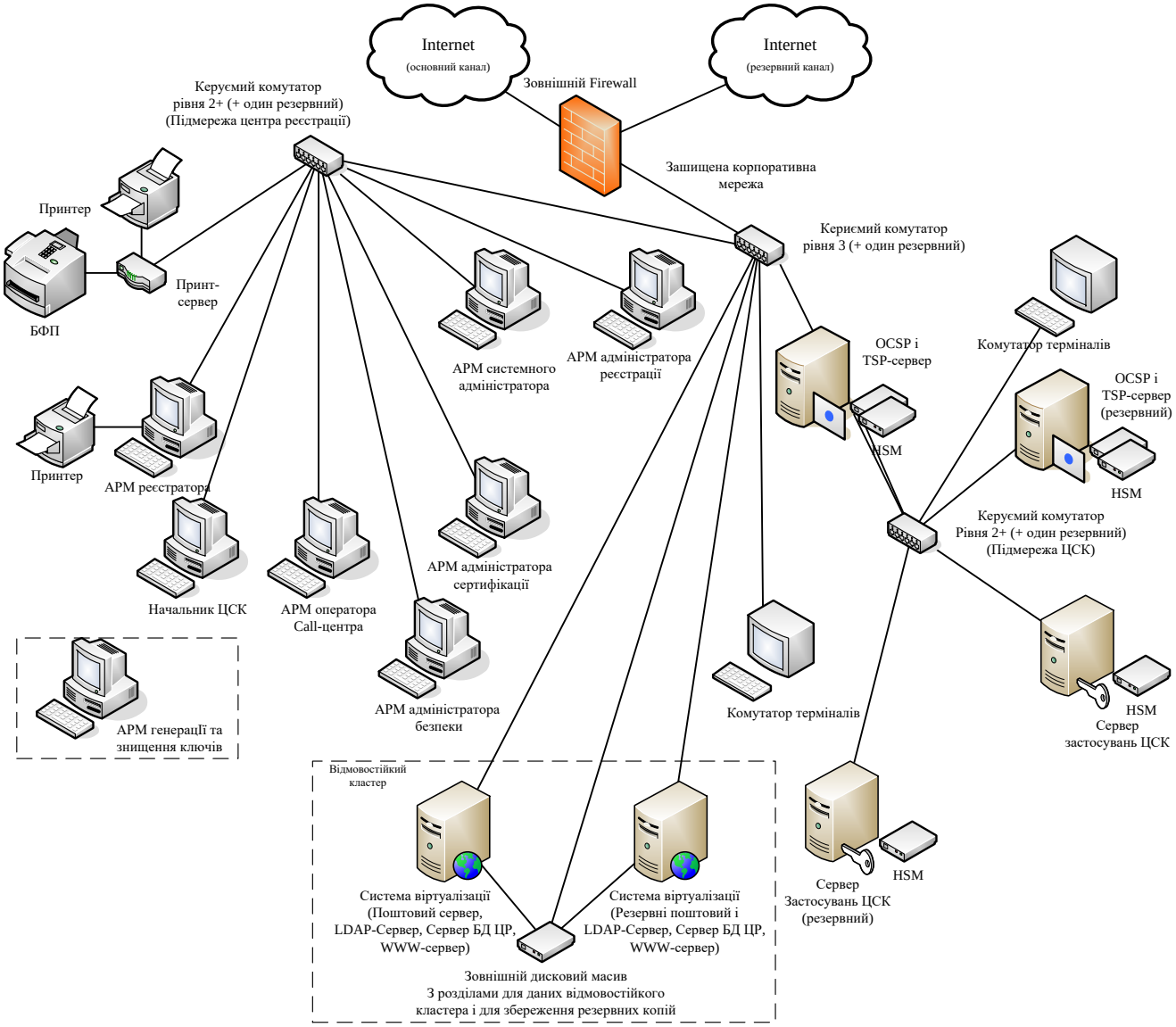


Рисунок 1.17 – Типова топологія мережі СКЗІ “Шифр-Х.509”

СКЗІ “Шифр-Х.509” підтримує такі криптографічні алгоритми:

– формування образу даних виконується за допомогою геш-функції за алгоритмом ГОСТ 34311-95;

– управління ключами шифрування забезпечується за протоколом Діффі-Геллмана відповідно до вимог п. 5.3 та п. 6.1 ДСТУ *ISO/IEC 159461-1* (в поліноміальному базисі), а також п. 8.2 ДСТУ *ISO/IEC 15946-3* (без використання множення в поліноміальному базисі). Підтримуються всі довжини ключів рекомендовані стандартами;

– шифрування / розшифрування даних та їх імітозахист виконуються за алгоритмом ГОСТ 28147-89 (ДСТУ ГОСТ 28147-2009);

– формування і перевірка ЕЦП здійснюється за алгоритмом ДСТУ 4145- 2002. Підтримуються всі довжини ключів рекомендованих стандартом.

На рис. 1.18 наведено взаємозв’язок між механізмами і застосовуваними стандартами в СУІБ НСМЕП.

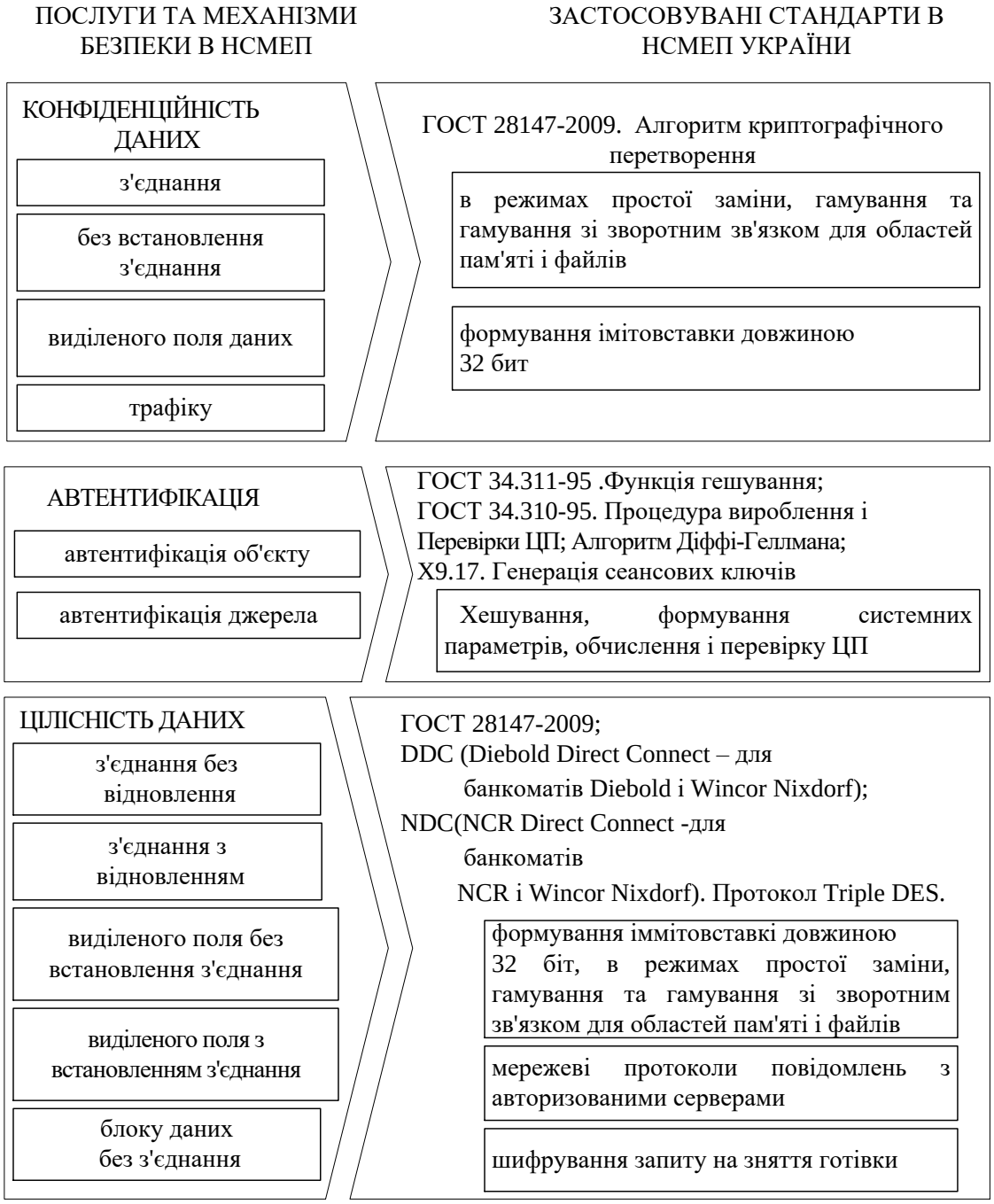


Рисунок 1.18 – Взаємозв’язок між послугами безпеки і механізмами в НСМЕП

Прикладами програмної реалізації розглянутих механізмів є програмні засоби криптографічного захисту інформації “Грифон-Б” і “Грифон-Л”, що призначені для криптографічного захисту конфіденційної інформації в автоматизованих банківських системах і застосовуються для обміну інформацією всередині корпоративної мережі банку, з клієнтами, які працюють з системою “Клиієнт-Банк”, в системах обслуговування пластикових карт [31; 68; 69]. Програмний засіб криптографічного захисту інформації “Грифон-Л” [68] призначено для використання в сфері банківської діяльності, зокрема, для обміну конфіденційною (в т.ч. фінансовою) інформацією в середині корпоративної мережі банку, з клієнтами, які працюють за системою “Клієнт-Банк”, в системах обслуговування пластикових карт і ін.

Бібліотека процедур криптографічного захисту інформації “Тайфун - *PKCS* # 11” містить процедури, призначені для забезпечення захисту цілісності та конфіденційності інформації, виконання автентифікації відправників повідомлень з використанням механізмів криптографічного захисту (електронний цифровий підпис, шифрування, формування імітовставок і геш-функцій) шляхом вбудовування в конкретні прикладні системи [59].

Процедури, що входять до складу бібліотеки реалізують:

– шифрування / розшифрування даних за алгоритмом ГОСТ 28147-2009;

– формування / перевірку імітовставки за алгоритмом ГОСТ 28147-2009;

– формування / перевірку ЕЦП за алгоритмами ДСТУ 4145-2002, ГОСТ 34.310-95, 34.311-95;

– формування ключів шифрування за схемою Діффі-Геллмана (використовується відкритий розподіл ключів відповідно до вимог *ISO 11166-94*).

Швидкісні характеристики програмних засобів, що реалізують алгоритми криптографічних перетворень (для ПК на базі *Intel Celeron* 2,4 ГГц):

– швидкість шифрування / розшифрування даних в режимі простої заміни БСШ ГОСТ 28147-2009 не менше 8 Мбайт/с;

– швидкість обчислення геш-функції даних відповідно до ГОСТ 34.311 – 95 не менше 3 Мбайт/с;

– формування ЕЦП відповідно до ГОСТ 34.310-95 при довжині ключа 512 біт не більше 0,003 с;

– час перевірки ЕЦП відповідно до ГОСТ 34.310-95 при довжині ключа 512 біт не більше 0,006 с;

– формування ЕЦП відповідно до ГОСТ 34.310-95 при довжині ключа 1024 біт не більше 0,01 с;

– час перевірки ЕЦП відповідно до ГОСТ 34.310-95 при довжині ключа 1024 біт не більше 0,02 с;

– формування ЕЦП (з обчисленням предпідпису) згідно з ДСТУ 4145-2002 для основного поля степені 163 не більше 0,0068 с;

– при перевірці ЕЦП згідно з ДСТУ 4145-2002 для основного поля степені 163 не більше 0,013 с.

Криптографічні перетворення в бібліотеці “Тайфун-*PKI PKCS#11*” реалізуються з використанням бібліотеки програмних процедур криптографічного захисту інформації “Тайфун-*W*32” версії 2.01.

Система захищеної електронної пошти “Бриз” призначена для здійснення обміну електронними повідомленнями в форматі *SMF*-70, захищеними з використанням механізмів криптографічного захисту (електронний цифровий підпис, шифрування / розшифрування, формування імітовставок), між клієнтами електронної пошти (ЕП), зареєстрованими на вузлах ЕП через мережу передачі даних вільного типу і відповідає критеріям НД ТЗІ 2.5-004-99 [70].

З метою удосконалення вимог до захисту БІР з урахуванням актуальних кіберзагроз, установлення вимог до організації заходів із забезпечення інформаційної безпеки та кіберзахисту банків, Правління Національного банку України в [34] визначило основні механізми, які можна використовувати для забезпечення послуг безпеки – криптографічні алгоритми симетричної криптографії (ГОСТ-28147-2009, “Калина-256”, *AES*, з довжиною ключа не менше 128 біт – для забезпечення конфіденційності та цілісності даних), несиметричної криптографії (алгоритми Діффі-Геллмана, алгоритм Ель-Гамаля, як звичайні, так і на еліптичних кривих, алгоритм *RSA*, з довжиною простих чисел 2048 біт –

забезпечення обміну ключами), забезпечення автентичності на основі *MAC*-кодів “Купина” (ДСТУ 7564), *SHA*-224, *SHA*-256, *SHA*-384, *SHA*-512, методів суворої автентифікації, ЕЦП ДСТУ – 4145). Аналіз запропонованих змін у ПЗ свідчіть про значне підвищення вимог до рівня криптостійкості, застосуванні державних стандартів, та алгоритмів на еліптичних кривих, які забезпечують додатковий рівень стійкості (див. рис. 1.5).

Таким чином, проведений аналіз послуг і відповідних механізмів безпеки БІР свідчить, що для їх забезпечення, як правило, застосовуються БСШ та алгоритми несиметричної криптографії. Зростання загроз, їх синергізм і гібридність на складові безпеки (ІБ, КБ, БІ) вимагають підвищення рівня їх криптостійкості, що в свою чергу приводить до зниження якості обслуговування клієнтів (суб’єктів) АБС, зниження довіри суспільства до організацій банківського сектору, виникнення елементів інформаційного хаосу серед суспільства, що веде до зниження ІБ держави.

1.2. Обґрунтування напряму дисертаційного дослідження

Проведений аналіз нормативно-правової бази, що регламентує порядок побудови системи безпеки БІР дав підстави виділити основні невирішені завдання в галузі безпеки БІР (стосується як міжнародних ОБС загалом, так і ОБС України зокрема): 1) розглядаються лише окремі складові методології оцінювання рівня безпеки інформаційних технологій, застосовуваних в ОБС; 2) відсутність синергетичного підходу до аналізу ризиків, єдиної методології оцінювання безпеки інформаційних технологій в стандартах банківського сектору, що не дозволяє своєчасно виробляти відповідні політики, нові підходи і заходи щодо безпеки БІР; 3) відсутність врахування в моделі безпеки БІР (модель *CIA*) невід’ємної складової банківських транзакцій – послуги автентичності; 4) відсутні механізми оцінювання рівня захисту БІР від гібридного нападу на основі комплексування ознак загроз ІБ, КБ, БІ на БІР, технічні об’єкти її інфраструктури; 5) для забезпечення цілісності й конфіденційності в АБС застосовуються “морально застарілі” симетричні БСШ – ГОСТ-28147, 3*DES*, та несиметричні криптосистеми *RSA, Diffie-Hellman*, у перших

механізмах існує проблема розподілу ключів шифрування, у других – низька швидкість шифрування (на 3–5 порядків нижче, ніж у БСШ), проте використання інтегрованих механізмів надає змогу забезпечити швидкість криптоперетворень, безпеку та достовірність БІР.

Таким чином, дотримуючись триєдиного правила щодо забезпечення безпеки БІР та ґрунтуючись на синергетичному підході до побудови відповідної системи безпеки в умовах дії загроз гібридного характеру, запропоновано ідею, яка розвинута в дисертації. Її загальний вигляд подано на рис. 1.19.

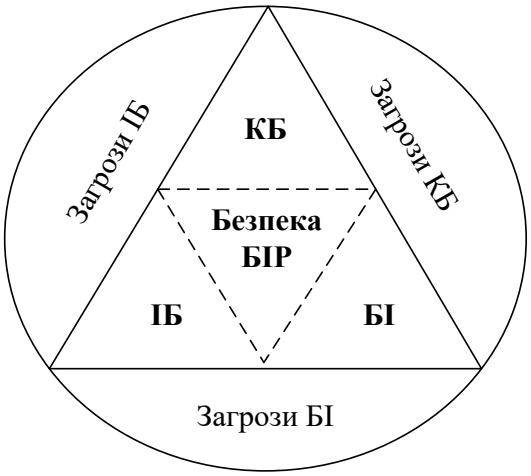


Рисунок 1.19 – Сутність синергетичного підходу до побудови системи безпеки банківських інформаційних ресурсів в умовах дії загроз гібридного характеру

Слід відзначити ключову особливість характерну тільки для пропонованого синергетичного підходу до безпеки БІР: пропонований підхід не є простим комплексуванням сил і засобів забезпечення безпеки, він так само не є суперпозицією їх властивостей. **Основна мета запропонованого підходу – це збудження в системі безпеки БІР керованих емерджентних властивостей, спрямованих на отримання синергетичного ефекту, який досягається завдяки якісно новому підходу до створення системи безпеки.** Розробка такого підходу немислима без розробки єдиної методології побудови системи безпеки БІР, що спирається на глибоку наукову проробку проблеми шляхом її всебічного критичного аналізу і, на основі отриманих висновків, синтезу нових нетривіальних рішень. Сьогодні, як показав аналіз, і в теорії, і практиці забезпечення безпеки БІР подібна методологія відсутня.

З огляду на різну природу загроз для обраних профілів безпеки БІР і в інтересах отримання в подальшому оцінювання величини ризику еквівалентного грошового капіталу, що безпосередньо відображає її захищеність, так само пропонується введення синергетичного показника безпеки БІР (рис. 1.20).

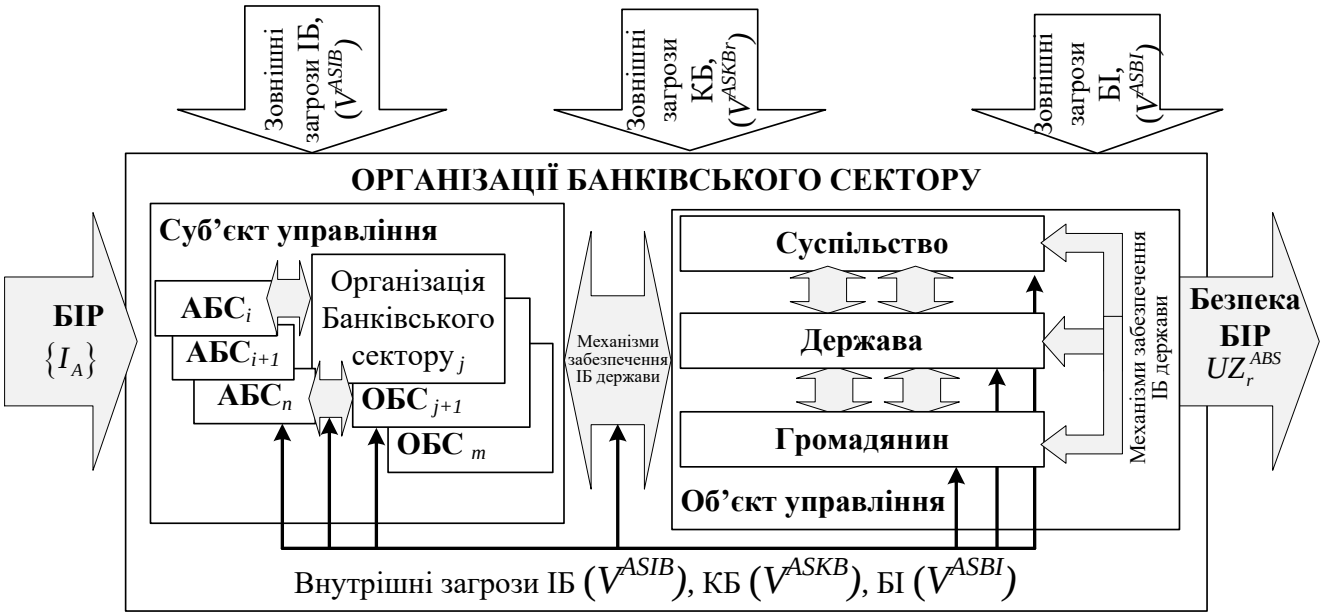


Рисунок 1.20 – Роль і місце синергетичного показника безпеки БІР в сучасних системах банківського захисту АБС

Синергетичний показник безпеки БІР – це синергетична оцінка ефективності комплексного застосування сил і засобів забезпечення безпеки БІР в умовах антагоністичної протидії системи банківського захисту випадковим і цілеспрямованим загрозам безпеки.

Відомо, що вирішенню проблеми ІБ держави в цілому та безпеці БІР зокрема присвячено праці відомих вітчизняних та закордонних вчених та їх наукових шкіл: І. Горбенка, В. Задіраки, О. Кузнецова, С. Ленкова, О. Молдовяна, В. Мохора, В. Сідельникова, С. Тімофєєва, Б. Шнайера, В. Шокала, В. Ярочкина, А. Калашнікова та багатьох ін. Разом з тим встановлено, що невирішеними аспектами загальної проблеми забезпечення ІБ держави залишається **проблема** створення цілісної науково обґрунтованої методології побудови системи безпеки

БІР, впровадження якої на практиці сприятиме стійкому та стабільному розвитку банківського сектору держави.

1.3. Постановка проблеми

Відсутність на сьогодні відповідної методології також обумовлено наявністю протиріччя, яке визначається тим, що з одного боку практика вимагає від теорії пошуку нових підходів до забезпечення безпеки БІР в умовах зростання кількості загроз їх кібернетичної та інформаційної безпеки, а також безпеки інформації при одночасному зростанні їх технологічної складності.

З іншого боку, в теорії відсутня цілісна науково обґрунтована методологія побудови на практиці системи безпеки БІР в цілому, що обумовлено недосконалістю механізмів забезпечення їх інформаційної безпеки, безпеки інформації та кібербезпеки зокрема (рис. 1.21) [46; 48; 52; 53].

Рисунок 1.21 – Сутність наукової проблеми

Формалізовано наукова проблема може бути описана виразом:

$$Emerdg = \max\left\{\prod_{synerg}{}^{M}_{N}\right\},$$

де $\prod_{synerg}{}^{M}_{N}$ – максимальна кількість емерджентних властивостей системи забезпечення банківської безпеки в цілому, що досягається при виникненні

синергетичного ефекту в результаті взаємодії обраних профілів безпеки; N – кількість станів системи безпеки БІР або кількість її емерджентних властивостей, $M \le N$. При цьому максимальну кількість емерджентних властивостей системи забезпечення банківської безпеки в цілому можна досягти при виконанні умови:

$$\prod_{synerg}{}_{N}^{M} = \sum_{m=1}^{M} C_N^m .$$

Необхідно так вирішити проблему підвищення рівня БІР при заданих умовах, щоб отримати максимальну кількість емерджентних властивостей при мінімальних ресурсних витратах, спрямованих на збудження в системі синергетичного ефекту.

Порядок проведення дисертаційного дослідження у вигляді структурно-логічної схеми подано на рис. 1.22. Таке подання дозволяє систематизувати основні етапи проведення дисертаційного дослідження, визначити їх зміст, взаємозв’язок між собою і висунути вимоги до частинних та загальних результатів досліджень. Отже, для досягнення мети дисертаційного дослідження необхідно розв’язати наступні основні задачі.

1. Провести аналіз сутності та змісту проблеми ІБ держави на сучасному етапі розвитку науки і техніки та дослідити роль й місце систем безпеки БІР при впливі на них нових загроз, які мають гібридний характер. Оцінити сучасний стан нормативно-правової бази, яка регламентує порядок побудови системи безпеки БІР, а також встановлює вимоги до їх захищеності.

2. Розробити концепцію побудови синергетичної моделі загроз безпеки БІР для обґрунтування та вибору найбільш ефективних напрямків досягнення цілей безпеки БІР на кожному з рівнів моделі управління стратегічним управлінням безпекою банківських ІТ з урахуванням величини ризику на кожному рівні та забезпеченням дієвого контролю за виконанням функцій СУІБ ОБС.

3. Удосконалити класифікатор загроз безпеці БІР для формування експертної оцінки рівня загроз БІР за складовими безпеки, видами послуг та рівнями ієрархії інфраструктури АБС, аналізу їх синергії та гібридності, оцінювання ймовірності впливу загроз ІБ, КБ, БІ на безпеку БІР.

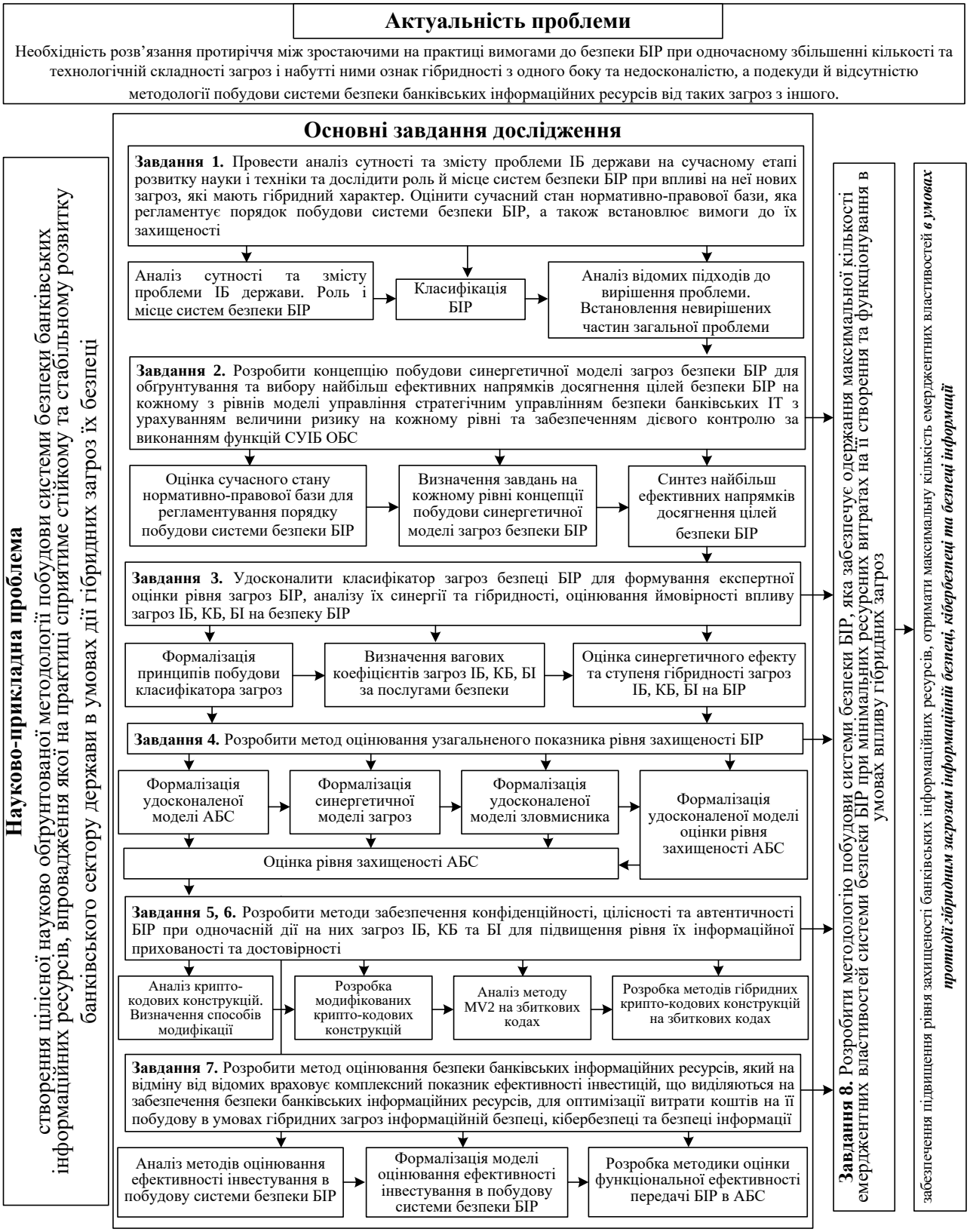


Рисунок 1.22 – Структурно-логічна схема проведення дисертаційного дослідження

4. Розробити метод оцінювання узагальненого показника рівня захищеності

БІР з урахуванням розробленої синергетичної моделі загроз та удосконаленого класифікатора для встановлення взаємозв'язків між елементами структури АБС, каналами зв'язку, активами БІР та загрозами ІБ, КБ, БІ, а також визначення рівня захищеності БІР.

5. Розробити метод забезпечення конфіденційності та цілісності БІР при одночасній дії на них загроз ІБ, КБ та БІ для підвищення рівня їх інформаційної прихованості та достовірності БІР.

6. Розробити метод забезпечення автентичності БІР при одночасній дії на них загроз ІБ, КБ та БІ для підвищення рівня їх інформаційної прихованості та достовірності *OTP*-паролів в протоколі двофакторної автентифікації.

7. Розробити метод оцінювання безпеки банківських інформаційних ресурсів, який на відміну від відомих враховує комплексний показник ефективності інвестицій, що виділяються на забезпечення безпеки банківських інформаційних ресурсів, для оптимізації витрати коштів на її побудову в умовах впливу гібридних загроз інформаційній безпеці, кібербезпеці та безпеці інформації.

8. Розробити методологію побудови системи безпеки БІР, яка забезпечує одержання максимальної кількості емерджентних властивостей системи безпеки БІР при мінімальних ресурсних витратах на її створення та функціонування в умовах впливу гібридних загроз.

Отже, на сьогодні *склалося об'єктивне протиріччя* між зростаючими на практиці вимогами до безпеки БІР при одночасному збільшенні кількості та технологічної складності загроз і набутті ними ознак гібридності з одного боку, та недосконалістю, а подекуди й відсутністю методології побудови систем безпеки БІР від таких загроз з іншого. Наявність такого протиріччя *обумовлює актуальність теми дисертації*, а тому вирішення поставленої науково-прикладної проблеми має важливе наукове та практичне значення.

1.4. Висновки до першого розділу

Таким чином, у першому розділі дисертаційної роботи було проведено аналіз наукової літератури за темою дисертації, зокрема, проаналізовано сучасні підходи

до забезпечення ІБ критичних інфраструктур держави у різних галузях, зокрема у галузі банківського сектору. У результаті досліджень було отримано такі результати:

1. Проведено аналіз сучасних моделей, методів та систем безпеки банківських інформаційних ресурсів організацій банківського сектору як складової систем з критичною кібернетичною інфраструктурою держави. Встановлено, що переважна більшість відомих досліджень орієнтована на розробку або загальних підходів до безпеки банківських інформаційних ресурсів, або створення методів, моделей та засобів забезпечення на основі моделі *CIA*, що не повною мірою враховує сучасні вимоги й підходи до побудови системи безпеки банківських інформаційних ресурсів.

2. Невирішеними аспектами загальної проблеми захисту банківських інформаційних ресурсів залишаються питання розробки цілісної науково-обґрунтованої методології побудови на практиці системи безпеки банківських інформаційних ресурсів, розробка та впровадження в комплексну систему захисту інформації інтегрованих механізмів *CIA* з забезпеченням вимог з швидкодії та достовірності циркуляції банківських інформаційних ресурсів в автоматизованих банківських системах.

3. Результати проведеного аналізу дали можливість чітко визначити завдання дисертаційного дослідження щодо розробки методології побудови системи безпеки банківських інформаційних ресурсів.

Список використаних джерел у першому розділі

1. Р. В. Грищук, та Ю. Г. Даник. *Основи кібернетичної безпеки: Монографія* /; за заг. ред. Ю. Г. Данника. Житомир: ЖНАЕУ, 2016.

2. Н. Л. Волковский, *История информационных войн*. В 2 ч. Ч. 2. – СПб.: ООО “Издательство “Полигон”, 2003.

3. Е. С. Пелевина, “Информационные угрозы кибертерроризма”, *Евразийский Союз Ученых (ЕСУ)*, № 11 (20). Политические Науки, с. 100 – 103, 2015.

4. А. А. Бок, и Д. А. Николаева, “Некоторые вопросы борьбы с киберпреступностью в Германии”, [Электронный ресурс]. Доступно: http://cj.isea.ru/pdf.asp?id=8613. Дата обращения: Дек. 11.12.2017.

5. А. В. Коротков, и Е. С. Зиновьева, “Безопасность критических информационных инфраструктур в международном гуманитарном праве”, [Электронный ресурс]. Доступно: http://cyberleninka.ru/article/n/bezopasnost-kriticheskih-informatsionnyh-infrastruktur-v-mezhdunarodnom-gumanitarnom-prave. Дата обращения: Дек. 11.12.2017.

6. Е. В. Иванченко, и В. А. Хорошко, “Тенденции развития кибертерроризма”, *МНПК “Современные информационные и электронные технологии”*, Одесса, с. 105 – 106, 2014.

7. Е. А. Маслакова, “Кибертерроризм как новая форма терроризма”, *Наука и Практика*, № 2 (63), с. 79 – 81, 2015.

8. Кибератаки исламского государства (ИГИЛ) на объекты и компании Российской Федерации, [Электронный ресурс]. Доступно: http://www.inside-zi.ru/pages/3_2015/22.html. Дата обращения: Дек. 11.12.2017.

9. А. Королев, “Киберпространство и информационный терроризм”, [Электронный ресурс]. Доступно: http://vpoanalytics.com/2016/02/15/kiberprostranstvo-i-informacionnyj-terrorizm/. Дата обращения: Дек. 11.12.2017.

10. Некоторые аспекты кибертерроризма, [Электронный ресурс]. Доступно: http://nk.org.ua/geopolitika/nekotoryie-aspektyi-kiberterrorizma-16846. Дата обращения: Дек. 11.12.2017.

11. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001. H.R. 3162.

12. Г. П. Леоненко, и А. Ю. Юдин, “Проблемы обеспечения информационной безопасности систем критически важной информационной инфраструктуры Украины”, *Information Technology and Security*, № 1(3), с. 44 – 48. 2013.

13. А. В. Дорофеев, и А. С. Марков, “Планирование обеспечения непрерывности бизнеса и восстановления”, *Вопросы кибербезопасности*, №3(11), с. 68 – 73, 2015.

14. А. В. Барабанов, А. В. Дорофеев, А. С. Марков, и В. Л. Цирлов, *Семь безопасных информационных технологий* / Под. ред. А. С. Маркова. М.: ДМК Пресс, 2017.

15. В. С. Оладько, и С. Ю. Микова, “Стратегии и показатели обеспечения непрерывности бизнеса”, *Международный научный журнал № 7. Технические науки*, с. 109 – 112, 2016.

16. А. Башнин, “Ситуативное управление и непрерывность бизнеса. Ситуационные центры”. ч.3, [Электронный ресурс]. Доступно: http://upr.ru/article/kontseptsii-i-metody-upravleniya/. Дата обращения: Дек. 11.12.2017.

17. ISO/IEC 27031:2011 Information Technology – Security Techniques – Guidelines for Information and Communication Technology Readiness for Business Continuity. [Online]. Available: http://www.iso.org/iso/ru/home/store/catalogue_tc/catalogue_detail.htm?csnumber=44374. Accessed on: Des. 09, 2017.

18. ISO/IEC 27001:2013. Information technology – Security techniques – Information security management systems – Requirements. [Online]. Available: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54534 Accessed on: Des. 09, 2017.

19. Доктрина інформаційної безпеки України, затверджено Указом Президента України від 25 лютого 2017 року № 47/2017. [Електронний ресурс]. Доступно: http://zakon3.rada.gov.ua/laws/show/47/2017/paran2#n2.

20. Указ Президента України від 15 березня 2016 року № 96 “Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року “Про Стратегію кібербезпеки України”. [Електронний ресурс]. Доступно: http://zakon3.rada.gov.ua/laws/show/96/2016/paran11#n11.

21. Указ Президента України від 12 лютого 2007 року № 105 “Про Стратегію національної безпеки України”. [Електронний ресурс]. Доступно: http://zakon3.rada.gov.ua/laws/show/105/2007.

22. Р. В. Грищук, та Ю. Г. Даник, “Синергія інформаційних та кібернетичних дій”, *Труди університету. НУОУ*, № 6 (127), с. 132–143. 2014.

23. В. Л. Бурячок, Р. В. Грищук, та В. О. Хорошко, під заг. ред. проф. В. О. Хорошка, *“Політика інформаційної безпеки”*, ПВП «Задруга»,. 2014.

24. Ю. Г. Даник та ін., “*Основи захисту інформації*” навч. пос., Житомир : ЖВІ ДУТ, 2015.

25. О. К. Юдін “*Інформаційна безпека. Нормативно-правове забезпечення*”, К. : НАУ, 2011.

26. І. С. Іванченко, В. О. Хорошко, Ю. Е.Хохлачова, та Д. В. Чирков під заг. ред. проф. В. О. Хорошка, *“Забезпечення інформаційної безпеки держави”*, К: ПВП “Задруга”, 2013.

27. О. Г. Корченко, О. Є. Архипов, та Ю. О. Дрейс, *“Оцінювання шкоди національній безпеці України у разі витоку державної таємниці”*, монографія, К: наук.-вид.центр НА СБУ України, 2014.

28. А. О. Корченко, Л. М. Скачек, та В. О. Хорошко, під заг. ред. проф. В. О. Хорошка, *“Банківська безпека”* підручник, К: ПВП “Задруга”, 2014.

29. В. И. Ярочкин, *“Безопасность банковских систем”*, М.: Издательство: Ось-89, 416 с., 2012.

30. С. Евсеев, “Анализ защиты в национальной системе масовых электронных платежей”, *Інформаційна безпека*, № 3(15), № 4 (16), с. 15 – 28, 2014.

31. С. Евсеев, О. Король, и Г. Коц, “Анализ законодательной базы к системе управления информационной безопасностью НСМЭП”, *Восточно-европейский журнал передовых технологий*, вып. 5/3(77), с. 48 – 59, 2015.

32. С. Евсеев, “Методология оценивания безопасности информационных технологий автоматизированных банковских систем Украины”, *Науково-технічний журнал “Захист інформації”*, том. 22, № 2, с. 297 – 309, 2016.

33. Р. Грищук, и С. Евсеев, “The synergetic approach for providing bank information security: the problem formulation”, *Безпека інформації*, № 22(1), с. 64 – 74, 2016.

34. Постанова НБУ28.09.2017 № 95, “Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України”, [Электроний ресурс]. Доступно : http://zakon2.rada.gov.ua/laws/show/en/v0095500-17/page. Дата звернення: Груд., 5, 2017.

35. С. Евсеев, Ю. Хохлачева, и О. Король, “Оценка обеспечения непрерывности бизнес-процессов в организациях банковского сектора на основе синергетического подхода, ч.1”, *Сучасна спеціальна техніка. Науково-практичний журнал*, № 1(48), с. 17 – 25. 2017.

36. С. Евсеев, Ю. Хохлачева, и О. Король, “Оценка обеспечения непрерывности бизнес-процессов в организациях банковского сектора на основе синергетического подхода, ч. 2”, *Сучасна спеціальна техніка. Науково-практичний журнал*, № 2(49), с. 10 – 17, 2017.

37. С. С. Химка, “Разработка моделей и методов для создания системы информационной безопасности корпоративной сети предприятия с учетом различных критериев”, [Электронный ресурс] Доступно: http://masters.donntu.org/2009/fvti/khimka/diss/index.htm. Дата обращения: Дек. 7, 2017.

38. Украинский ресурс по безопасности [Электронный ресурс]. Доступно: http://kiev-security.org.ua. Дата звернення: Груд. 7.2017.

39. Д. Слободенюк, “Банковские технологии, Средства защиты информации в банковских системах”, [Электронный ресурс] Доступно: http://www.arinteg.ru/about/publications/press/sredstva-zashchity-informatsii-v-bankovskikh-sistemakh-131107.html. Дата звернення: Груд. 7.2017.

40. М. Н. Симаков, V Съезд директоров по информационной безопасности [Электронный ресурс] Доступно: http://www.cso-

summit.ru/data/2012/presentations/cso2012_013_express-tula_simakov.pdf. Дата звернення: Груд. 7.2017.

41. П. В. Ревенков, “Защита информации в банке: основные угрозы и борьба с ними”, [Электронный ресурс] Доступно: http://www.crmdaily.ru/novosti-rynka-crm/568-zashhita-informacii-v-banke-osnovnye-ugrozy-i-borba-s-nimi.html. Дата звернення: Груд. 7.2017.

42. Security of Internet Banking – A Comparative Study of Security Risks and Legal Protection in Internet Banking in Thailand and Germany [Online].Available: http://www.thailawforum.com/articles/internet-banking-thailand.html. Acessed on: Des. 09, 2017.

43. М. В. Старинський, “Щодо визначення поняття “банківська інформація” та виділення її видів”, [Електронний ресурс]. Доступно: uabs.edu.ua/images/.../K.../Starinskii_s_015.pdf. Дата звернення: Груд. 7.2017.

44. В. А. Сердюк, *Новое в защите от взлома корпоративных систем*. Москва: Техносфера, 2007.

45. S. Evseev, and B. Tomashevsky, “Two-factor authentication methods threats analysis”, *Радіоелектроніка, інформатика, управління*, Вип. 1(32), с. 52 – 60, 2015.

46. Р. В. Грищук, “Синтез систем інформаційної безпеки за заданими властивостями”, *Вісник національного університету “Львівська політехніка”. Серія : Автоматика, вимірювання та керування : зб. наук. пр.*, ЛП, № 74, с. 271 – 276, 2012.

47.Р. В. Грищук, “Атаки на інформацію в інформаційно-комунікаційних системах”, *Сучасна спеціальна техніка*, №1(24), с.61 – 66. 2011.

48.Р. В. Грищук, і В. В. Охрімчук, “Постановка наукового завдання з розроблення шаблонів потенційно небезпечних кібератак”, *Безпека інформації*, Том 21, № 3, с. 276 – 282, 2015.

49.Ю. Г. Даник, Р. В. Грищук, “Синергетичні ефекти в площині інформаційного та кібернетичного протиборства”, *Наук.-практ. конф. “Актуальні проблеми управління інформаційною безпекою держави”*, Київ, 19 берез, 2015, с. 235 – 237.

50. Р. В. Грищук, В. В. Охрімчук, “Напрямки підвищення захищеності комп’ютерних систем та мереж від кібератак”, *ІІ Міжнар. наук.-практ. конф. “Актуальні питання забезпечення кібербезпеки та захисту інформації”* (Закарпатська область, Міжгірський район, село Верхнє Студене, 24-27 лют. 2016 р.). – К. : Видавництво Європейського університету, 2016 с. 60 – 61.

51. Роджерс, Еверетт М. *Дифузія інновацій* [пер. з англ.] Вид. дім “Києво-Могилянська академія”, 2009.

52. А. А. Колесников, *Синергетическое методы управления сложными системами : теория системного синтеза*, М. : Едиторал УРСС, 2005.

53. Г. Хакен, *Синергетика. Иерархия неустойчивостей в самоорганизующихся системах и устройствах*, М. : Мир, 1985.

54. А. В. Сериков, “Эффективность хозяйственной деятельности : определение, измерение, синергетическое управление”, *Економічний вісник Донбасу*, № 2 (24). с. 212 – 219, 2011.

55. В. Г. Олифер, Н. А. Олифер, *Безопасность компьютерных сетей*. М. : Горячая линия. Телеком, 2015.

56. Звіт CERT-UA за 2010 – 2013 роки [Електронний ресурс]. Доступно: http://cert.gov.ua/?p=316. Дата обращения: Дек. 7, 2017.

57. Киберщит Украины: кто стоит на страже кибергранниц страны, [Електронний ресурс]. Доступно: http://zillya.ua/ru/kibershchit-ukrainy-kto-stoit-na-strazhe-kibergranits-strany. Дата обращения: Дек. 7, 2017.

58. W. Ten, G. Manimaran, and C.-C. Liu, “Cybersecurity for criticalinfrastructures : Attack and defense modeling”, *IEEETrans. Syst., Man Cybern. A*, vol. 40, no. 4, pp.853 – 865, 2010.

59. С. В. Ленков, Д. А. Перегудов, и В. А. Хорошко, *Методы и средства защиты информации : монография* [в 2-х т.] Т. 2. Информационная безопасность. К. : Арий, 2008.

60. Методичні рекомендації щодо впровадження системи управління інформаційною безпекою та методики оцінки ризиків відповідно до стандартів національного банку України/ [Електронний ресурс]. Доступно:

zakon.rada.gov.ua/laws/show/v0365500-11. Дата звернення: Груд. 7, 2017.

61. Worldwide Infrastructure Security Report. 2014. Arbor Networks, Inc [Online]:
Available: https://www.google.com.ua/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CB8QFjAA&url=http%3A%2F%2Fpages.arbornetworks.com%2Frs%2Farbor%2Fimages%2FWISR2014_EN2014.pdf&ei=DyR2VfznJOPgyQOghoN4&usg=AFQjCNGP0_ZTliItqCtofJ-cXfZT9QHRiQ&sig2=4hgA_vIye1idQyQgsTIZXg&bvm=bv.95039771,d.bGQ.
Accessed on: Des. 09, 2017.

62. Безопасность IP-сетей нового поколения для провайдеров услуг, [Электронный ресурс] : Доступно : http://www.eureca.ru/edu/study/cisco/library/download.php?type=pdf&att=IP_NGN.pd. Дата звернення: Груд. 7, 2017.

63. С. П. Евсеев, "Анализ защиты в национальной системе масовых электронных платежей", *Інформаційна безпека*, № 3(15), № 4 (16), с. 15 – 28, 2014.

64. S. Yevseiev, H. Kots, and Y. Liekariev, "Developing of multi-factor authentication method based on Niederreiter-McEliece modified crypto-code system", *Восточно-европейский журнал передовых технологий*, 6/4(84), с. 11 – 23, 2016 *(Scopus)*

65. S. Yevseiev, H. Kots, S. Minukhin, O. Korol, and A. Kholodkova, "The development of the method of multifactor authentication based on hybrid crypto-code constructions on defective codes", *Восточно-европейский журнал передовых технологий*, 5/9(89), с. 19 – 35, 2017. *(Scopus)*

66. С. П. Евсеев, и Т. А. Свердло, "Исследование угроз методов двухфакторной аутентификации". *Информационные технологии и защита информации в информационно-коммуникационных системах*: Колективна монография [под. редакцией В. С. Пономаренко]. Харків, Україна: Вид-во ТОВ "Щедра садиба плюс", 2015, с. 141 – 154.

67. ДСТУ ISO/IEC 9594-8:2006 Інформаційні технології. Взаємозв'язок відкритих систем. Каталог. Частина 8. Основні положення щодо сертифікації

відкритих ключів та атрибутів, [Електронний ресурс]. Доступно: http://document.ua/informaciini-tehnologiyi_-vzaemozvE28099jazok-vidkritih-sist-std10750.html. Дата звернення: Груд. 7.2017.

68. Программное средство криптографической защиты информации “Грифон-Б”, [Электронный ресурс]. Доступно: http://www.banksoft.com.ua/index.php?id=28. Дата звернення: Груд. 7, 2017.

69. Программное средство “Библиотека функций криптографической защиты информации ""“Грифон-Л”, [Электронный ресурс]. Доступно: http://www.banksoft.com.ua/index.php?id=27. Дата звернення: Груд. 7, 2017.

70. С. П. Євсеєв, В. Е. Чевардин, С. А Радковский, “Механизмы обеспечения аутентичности банковских данных во внутриплатежных системах комерческого банка”, *Збірник наукових статей ХНЕУ*. Харків: ХНЕУ,Вип. 6, с. 40 – 44, 2008.

РОЗДІЛ 2
РОЗРОБЛЕННЯ КОНЦЕПТУАЛЬНИХ ЗАСАД ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ БАНКІВСЬКИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ

2.1. Розроблення концепції побудови синергетичної моделі загроз безпеці банківських інформаційних ресурсів

У сучасних умовах масової доступності комп'ютерних систем і телекомунікацій, збільшення обігу електронного документообігу між банками і клієнтами, переходу на електронну комерцію проблеми безпеки БІР в силу природних і штучних чинників тільки загострюються. Як наслідок, збитки від порушення безпеки БІР стають все більш дорогим як для банків, так і для їх клієнтів [1; 2; 46]. Наприклад, найбільша кількість загроз безпеки ІТ АБС України, як і в інших державах, виходить з мережі Інтернет при передачі БІР відкритими каналами зв'язку [3; 2; 32; 42; 44; 45]. Недосконаліть стратегічного управління безпекою ІТ АБС України виливається для державного банківського сектору в ряд проблем, основними з яких є безсистемність в забезпеченні безпеки, неузгодженість механізмів забезпечення безпеки ІТ АБС, особливо в міжнародному двох- і багатосторонньому форматах і т.п. [4; 41; 42].

Аналіз основних міжнародних стандартів і стандартів України [7; 8; 9; 10; 11; 12; 13; 24; 26; 28; 29; 31; 32; 33; 34; 35; 36; 37] показав, що розглянуті окремі складові методології оцінювання безпеки інформаційних технологій, застосовуваних в банківському секторі, ґрунтуються на моделі безпеки – забезпечення цілісності, конфіденційності та доступності (моделі ЦКД), при цьому не враховується невід'ємна складова банківських транзакцій – послуга автентичності – стан БІР, при якому інформація забезпечує підтвердження автентичності джерела (авторизованого користувача і / або процесу) інформації. Відсутність синергетичного підходу до аналізу ризиків, єдиної методології оцінювання безпеки інформаційних технологій в стандартах банківського сектору не дозволяє своєчасно сформувати відповідні політики, нові підходи і заходи щодо забезпечення безпеки БІР, що обумовлено недосконалістю механізмів забезпечення її ІБ, КБ, БІ. Зокрема, невід'ємною частиною

проблеми забезпечення безпеки БІР є проблема аналізу ризиків. Фактично ризик являє собою інтегральну оцінку того, наскільки ефективно існуючі засоби захисту здатні протистояти атакам на БІР [1; 2; 6; 32; 33; 44; 45; 46; 47; 48; 50]. Незважаючи на те, що нині розроблено множину механізмів і засобів захисту інформації, на сьогоднішній день одним з пріоритетних завдань залишається завдання оцінювання ефективності процесу забезпечення безпеки ІТ АБС на основі відповідних метрик. Наприклад, як показав аналіз [6; 7; 8; 9; 10; 11; 12; 13; 24], серед найпоширеніших метрик безпеки є їх такі таксономії: *Vaughn-Hennig-Siraj*, *NIST STS*822, *OCIPEP*, *OCTAVE*, *CISWG*, *Erkan Kahraman.*

У результаті вивчення наведених метрик безпеки встановлено, що їх ефективне впровадження в банківський сектор України стримує: дефініційна невизначеність – в силу недосконалості національної законодавчої бази та її розбіжності з кращими світовими практиками в цій сфері; низька об'єктивність отриманих оцінок – зважаючи на відсутність міжнародного досвіду більшості банківського персоналу, який забезпечує безпеку БІР; методологічних проблем – з огляду на проблематичність отримання гармонізованих між собою кількісних і якісних оцінок тощо. [5; 50]. При цьому остання з наведених проблем носить системотвірний ключовий характер, а тому вимагає глибокого наукового та методичного опрацювання та подальшого дослідження.

Проведений аналіз показав, що основними документами, які внесли серйозний теоретичний і практичний внесок у вирішення завдань забезпечення інформаційної безпеки [6] є: Критерії оцінювання захищеності комп'ютерних систем [7], що відомі як "Рожева книга"; Європейські критерії оцінювання безпеки ІТ [8]; Канадські критерії оцінювання безпеки надійних комп'ютерних систем [9]; Федеральні критерії США [10]; Міжнародний стандарт *ISO / IEC 15408* – "Критерії оцінювання безпеки ІТ" [11; 12; 13]; Робочий проект стандарту *CEM-97/017* – "Загальна методологія оцінювання безпеки ІТ" [34], ДСТУ *ISO / IEC TR 13335* "Інформаційні технології. Настанови з управління безпекою інформаційних технологій", ч. 1 – 5 [14; 15; 16; 17; 18], Стандарт України ДСТУ СУІБ 2.0 / *ISO / IEC 27002*: 2010 "Інформаційні технології. Методи

захисту. Звід правил для управління інформаційною безпеки" (*ISO / IEC 27002*: 2005, *MOD*) [23].

Аналіз цих документів підтверджує той факт, що для рішення завдань забезпечення ІБ, поряд з формальними методами моделювання процесів і оцінювання ефективності функціонування систем забезпечення безпеки, необхідно широко використовувати методи декомпозиції і структуризації компонентів систем і процесів, неформальні методи оцінювання ефективності функціонування та прийняття рішень. Це означає, що апарат системного аналізу необхідно використовувати на всіх етапах життєвого циклу систем захисту інформації [46; 50]. Особливе місце у розробці методології оцінювання безпеки інформаційних технологій в АБС посідає стандарт *ISO / IEC 15408* "Загальні критерії оцінювання захищеності ІТ", "Загальні критерії". Стандарт визначає загальні критерії, що є основою для оцінювання властивостей безпеки інформаційних продуктів і технологій [11; 12; 13]. Єдині критерії спрямовані на забезпечення порівнянності результатів оцінок, отриманих різними експертами, шляхом введення загальної множини вимог до функцій безпеки продуктів і систем інформаційних технологій, а також до показників цих функцій. Використовуючи стандарт, що аналізується, можна вирішити конкретне прикладне завдання вибору відповідних вимог і показників безпеки ІТ [6; 46]. Крім цього, потенційні загрози безпеки з Єдиних критеріїв, а саме цілісності, доступності, конфіденційності в подальшому пропонується покласти як складові в нову синергетичну модель загроз безпеки. Стандарти Національного банку України [22, 23] базуються на міжнародних стандартах *ISO 27001* [19] і *ISO 27002* [20] з додаванням до них вимог захисту інформації [23], обумовлені конкретними потребами сфери банківської діяльності та правовими вимогами національного законодавства [26]. Ключовим моментом розглянутих документів є те, що вони приписують принципи управління інформаційною безпекою банку, найбільш важливими з яких є оцінювання ризиків [14; 15; 16; 17; 18; 22; 23; 26]. Практика показує, що сьогодні можна чітко виділити дві основні групи методів оцінювання ризиків безпеки [19; 20; 23; 28; 29]. Перша група методів дозволяє встановити рівень ризику шляхом оцінювання ступеня відповідності визначеному набору вимог до забезпечення інформаційної безпеки.

Джерелом таких вимог у банківському секторі України можуть виступати як міжнародні, так і національні керівні документи, систематизація яких у вигляді схеми наведена на рис. 2.1.

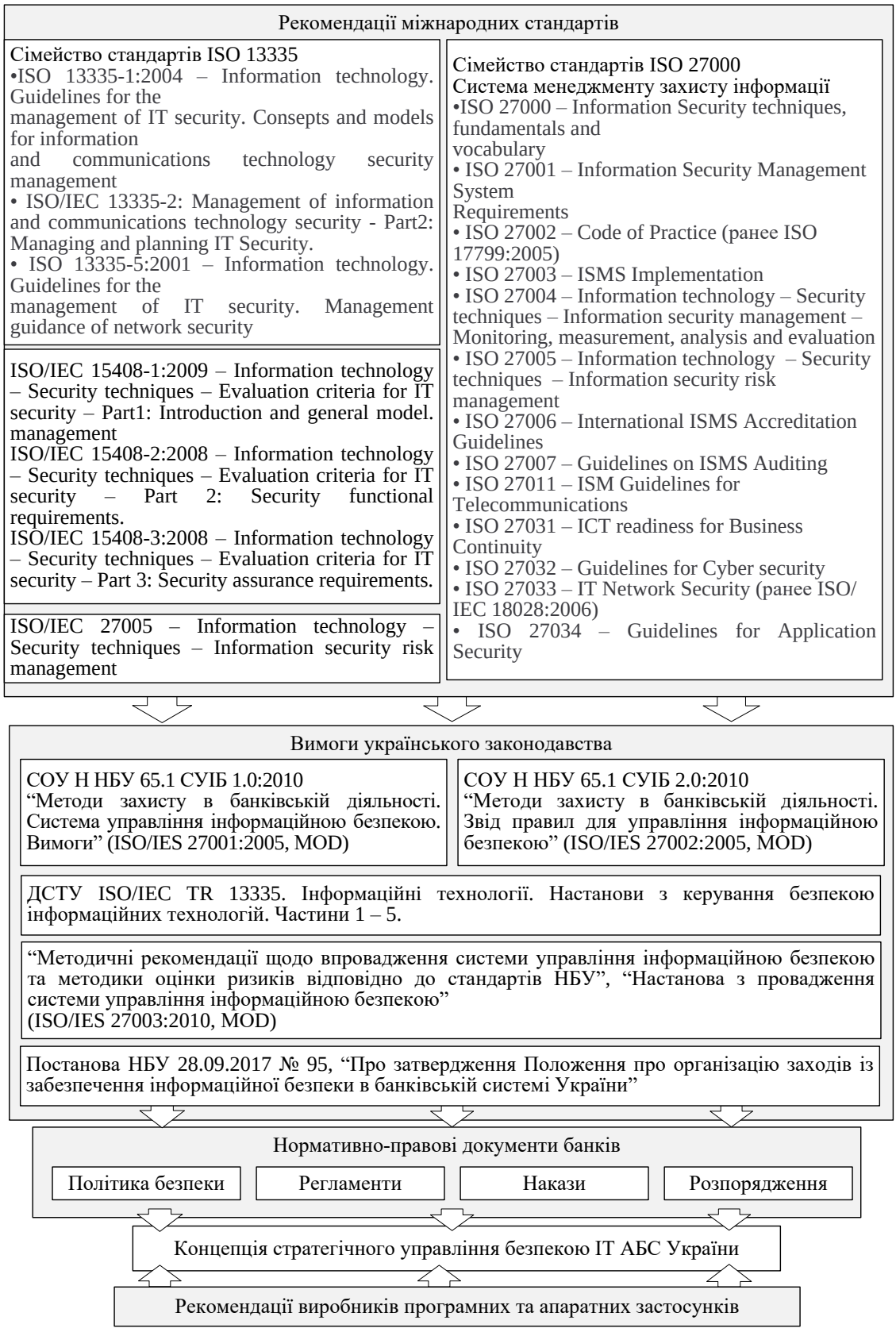


Рисунок 2.1 – Систематизація джерел вимог до безпеки ІТ АБС України

Друга група методів оцінювання ризиків безпеки БІР базується на визначенні ймовірності реалізації атак, а також рівня їх збитків. У такому разі значення ризику вираховується окремо для кожної загрози і в загальному випадку є добутком ймовірності реалізації загрози на величину потенційних збитків від цієї загрози. Значення збитків визначається власником БІР, а ймовірність реалізації загрози вираховується групою експертів, які проводять процедуру аудиту.

Відмінною рисою методів першої і другої груп є застосування різноманітних шкал для визначення величини ризику. У першому випадку ризик і всі його параметри виражаються в числових, тобто кількісних значеннях. У другому випадку використовуються якісні шкали.

Згідно з вимогами стандартів Національного банку України відповідно до запропонованої концепції стратегічного управління безпекою ІТ АБС України (див. рис. 2.1) сферою застосування системи управління ІБ (СУІБ), яка повинна бути впроваджена, в цілому є банк.

Таким чином, весь комплекс питань, пов’язаних із забезпеченням безпеки БІР України, а саме – ІБ, КБ, БІ в АБС повинен вирішуватися в комплексі і нерозривно один від іншого, гармонійно доповнюючи і заповнюючи, в разі необхідності, один одного. Просте комплексування сил і засобів у кожному окремому випадку для забезпечення безпеки БІР є недоцільним як з практичної, так і наукової точок зору. Відсутність інших альтернативних підходів обумовлює нагальну потребу у вирішенні проблеми, що склалася – підвищення захищеності БІР на основі розробки нових підходів.

Враховуючи взаємозв’язок гібридності загроз ІБ, КБ, БІ на БІР, в подальшому пропонується провести синтезування БІР з типовими загрозами згідно синергетичної моделі загроз БІР [1] (рис. 2.2). Відмінною рисою запропонованого підходу (рис. 2.2) є закладання необхідної і достатньої умови розробки нового методологічного базису, спрямованого на досягнення синергетичного ефекту у сфері забезпечення складових безпеки (ІБ, КБ, БІ) БІР в умовах дії гібридних загроз не лише України, а й інших розвинених держав.

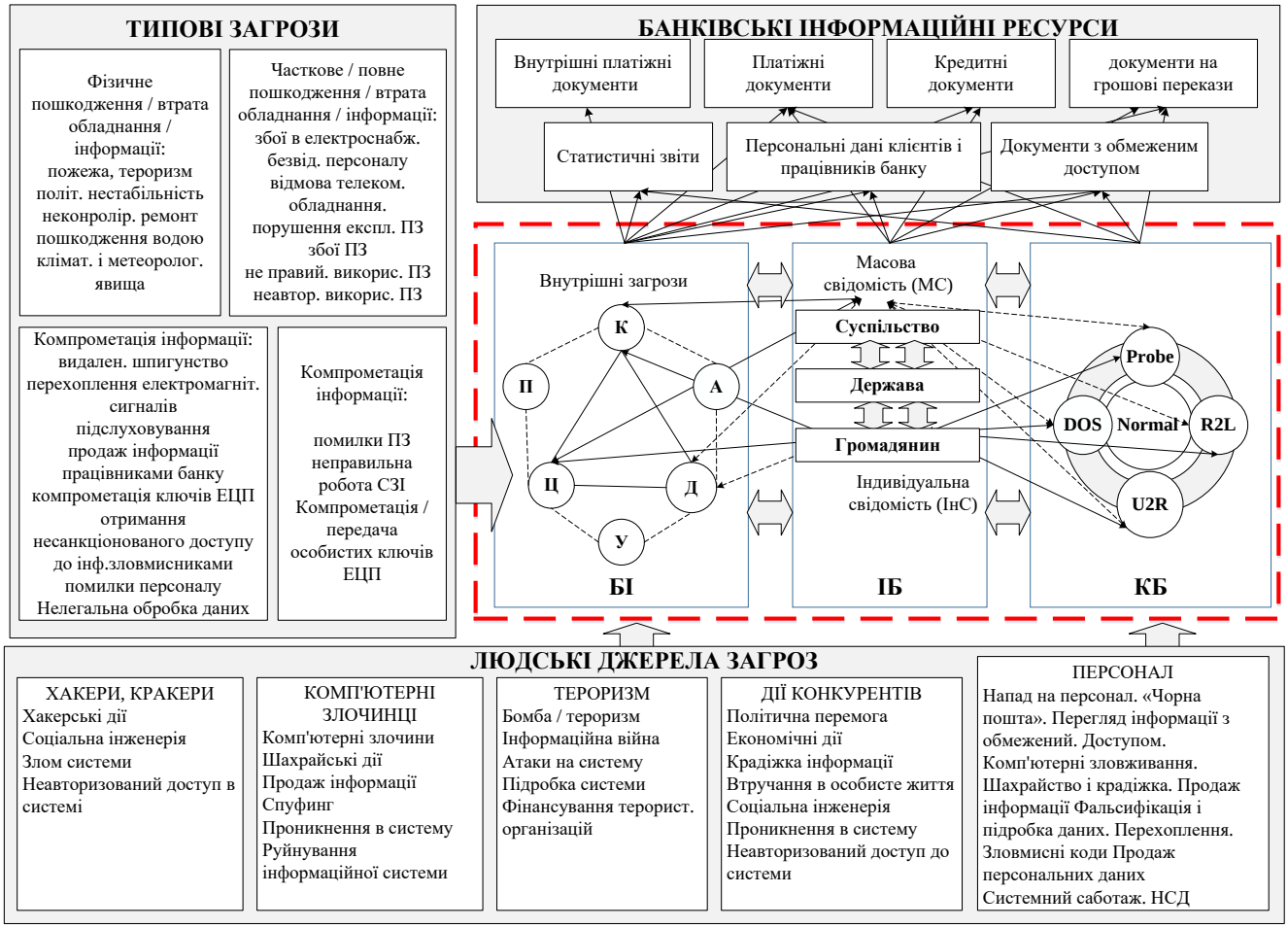


Рисунок 2.2 – Взаємозв’язок БІР з типовими джерелами загроз

Таким чином, в результаті уточнення вимог передових світових практик у питаннях методології оцінювання безпеки БІР встановлений взаємозв’язок між основними ризиками безпеки і БІР, які сьогодні і в найближчому майбутньому матимуть місце в АБС України.

Спираючись на функціонал трирівневої моделі стратегічного набору типового підприємства [4] з метою розроблення концептуальних засад забезпечення безпеки БІР запропонована концепція побудови синергетичної моделі загроз безпеці БІР, яка базується на трирівневій стратегії управління безпекою БІР (рис. 2.3, *а*, *б*, *в*).

Перший рівень описує загальну корпоративну стратегію банку та його функціональні стратегії (рис. 2.3, *а*). Корпоративна стратегія визначає перспективи розвитку та сприяє виконанню основної місії банку. На цьому рівні відповідно до синергетичного підходу розглядається загальна концепція безпеки інформаційних

технологій АБС і формуються цілі і завдання забезпечення КБ, а також визначається стан безпеки БІР:

$$S^{ABS} = \left\{ S_1^{ABS}, S_2^{ABS}, ..., S_m^{ABS} \right\},$$

де $S_i^{ABS} \in \left\{ S^{ABS} \right\}, (i = \overline{1,m})$ – стан безпеки БІР.

Функціональні стратегії одного рівня мають горизонтальні зв'язки і узгоджуються на рівні цілей, з подальшою деталізацією на наступному рівні стратегічного набору.

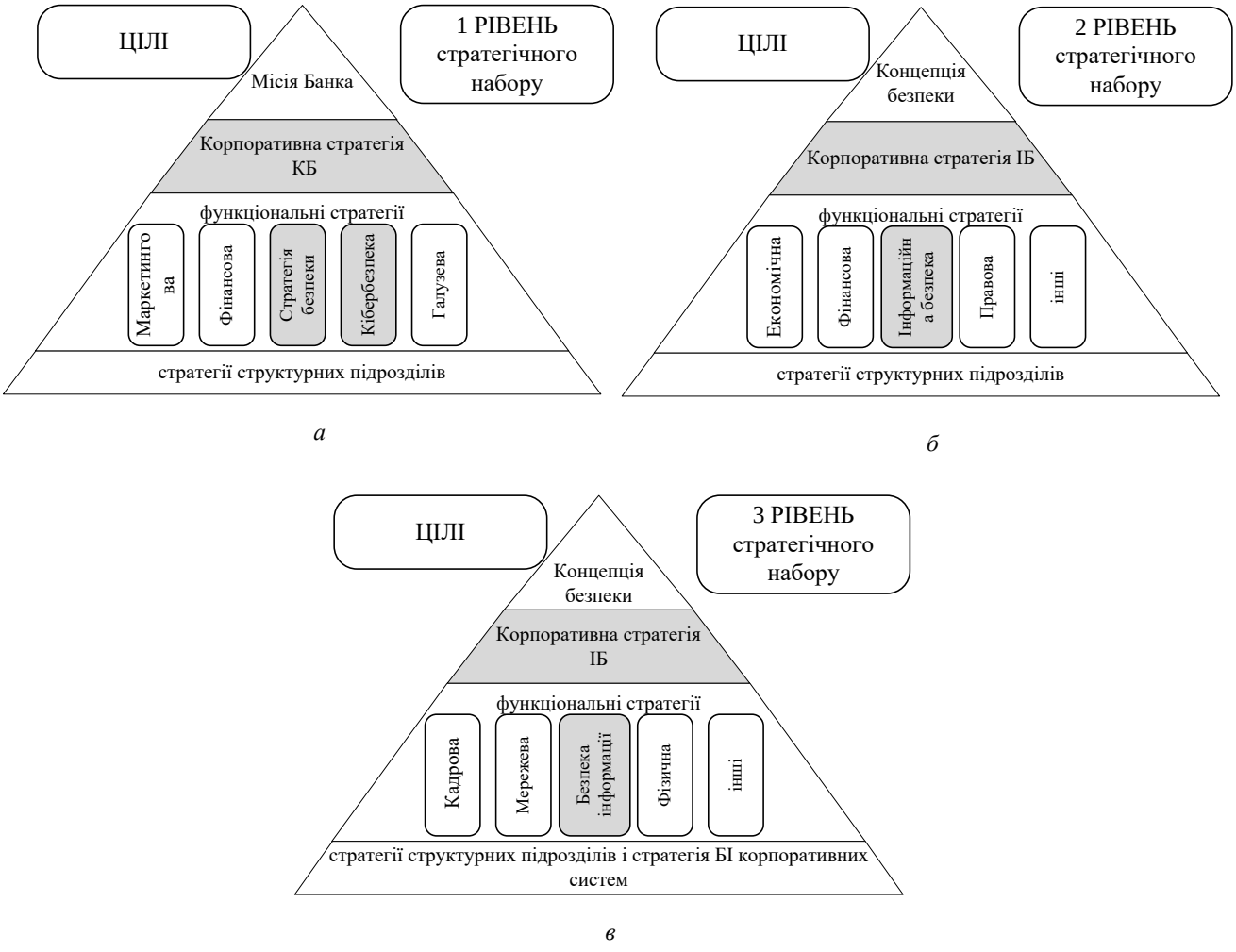


Рисунок 2.3 – Концепція побудови синергетичної моделі загроз безпеці БІР

На *другому рівні* формується корпоративна стратегія безпеки БІР (рис. 2.3, *б*):

$$\left\{ RR^{ABS} \right\} = \left\{ R_{BBI} \right\} \bigcup \left\{ OV_{BBI} \right\} \bigcup \left\{ IU_{BBI} \right\},$$

де $\{RR^{ABS}\}$ – множина вимог регуляторів, яка включає вимоги до безпеки БІР – $\{R_{BBI}\}$, що визначені у міжнародних і національних стандартах; множина оцінок ступеня виконання вимог безпеки $\{OV_{BBI}\}$ та множина попереднього підсумкового рівня відповідності безпеки БІР $\{IU_{BBI}\}$. Також визначаються цілі та завдання основних бізнес-процесів, пов'язаних із захистом персональних даних юридичних і фізичних клієнтів банку. Корпоративна стратегія безпеки описує, яким чином слід керувати і координувати зусилля за різними аспектами безпеки. Вона розвивається у формі функціональних стратегій: фінансової економічної, фізичної та ІБ.

На *третьому рівні* проводиться деталізація функціональних стратегій другого рівня стратегічного набору, формується корпоративна стратегія безпеки інформації (рис. 2.3, *в*). Серед основних напрямків захисту доцільно виділити кадрову безпеку, фізичну безпеку, мережеву та БІ. На цьому рівні визначається відповідність між застосованими технічними засобами захисту інформації (ТЗЗІ) та загрозами ІБ, КБ, БІ на безпеку БІР:

$$OPZ^{ABS} = \sum_{i=1}^{k} OPZ_i ,$$

де OPZ_i – узагальнений показник рівня захищеності АБС, що дозволяє оцінити рівень відповідності ТЗЗІ вимогам регуляторів. Стратегія безпеки БІР є важливою функцією керівництва банку і повинна формуватися його керівництвом на основі методів експертних оцінок.

Запропонована концепція ґрунтується на синергетичному підході до вибору найбільш ефективних напрямків досягнення поставлених цілей безпеки БІР з урахуванням величини ризику на кожному рівні моделі стратегічного управління банком. Описаний підхід дозволяє комплексно проводити відбір альтернативних варіантів можливих стратегічних рішень з питань безпеки та розробити методику оцінювання узагальненого показника рівня захищеності БІР, яка містить три етапи.

Перший етап передбачає визначення ймовірності впливу загроз ІБ, КБ, БІ на безпеку БІР, другий – визначення залежностей між елементами інфраструктури АБС, інформаційними активами БІР, загрозами ІБ, КБ, БІ та ТЗЗІ на основі

удосконаленої моделі інфраструктури АБС, синергетичної моделі загроз, удосконалених класифікатора загроз та моделі зловмисника. Третій, заключний етап, присвячений визначенню узагальненого показника рівня захищеності БІР на основі удосконаленої моделі оцінювання рівня захищеності БІР. Реалізацію концепції на прикладі ОБС України подано на рис. 2.4.

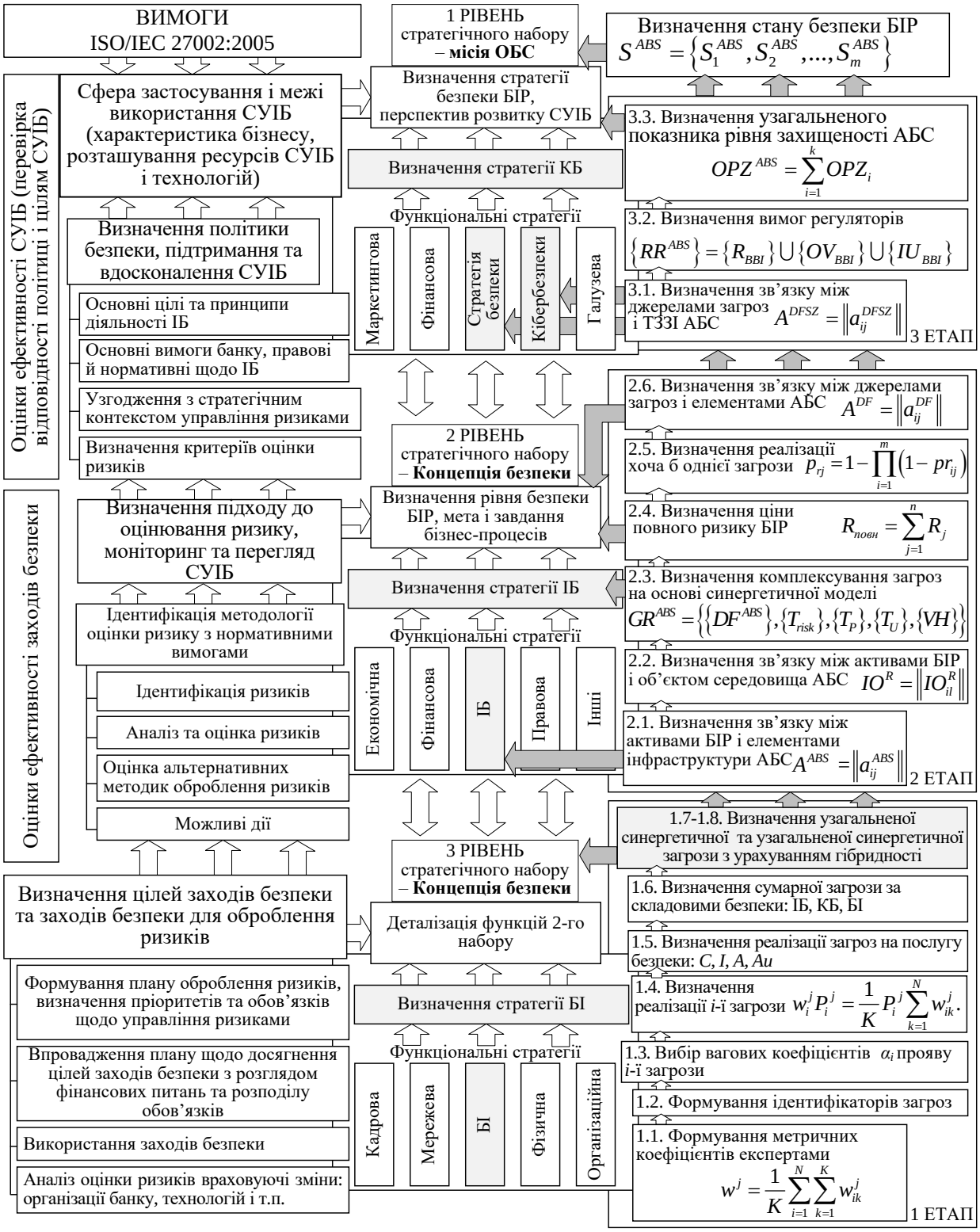


Рисунок 2.4 – Реалізація концепції на прикладі ОБС України

Розроблена на основі концепції модель за рахунок комплексування складових інформаційної безпеки, кібербезпеки та безпеки інформації відкриває новий напрямок у безпеці банківських інформаційних ресурсів на основі моделі стратегічного управління банком з урахуванням величини ризику на кожному рівні.

2.2. Формалізація принципів побудови класифікатора загроз складових безпеки банківських інформаційних ресурсів: інформаційної безпеки, кібербезпеки, безпеки інформації

Етап 1. Визначення ймовірності впливу загроз ІБ, КБ, БІ на безпеку БІР реалізується на основі запропонованого класифікатора.

Для побудови метрик загроз на основі синергетичного підходу, запропонованого в роботі [50] скористаємося підходом побудови класифікатора загроз на основі інформаційно-аналітичної моделі методу подвійних трійок, запропонованого авторами в роботах [51; 52; 53; 54]. На відміну від відомого при побудові класифікатора змістовна частина кожної з чотирьох платформ включає в себе відповідно ряд складових.

Перша платформа – класифікації загроз за складовими безпеки БІР ОБС: інформаційна безпека (ІБ) (01), безпека інформації (БІ) (02), кібербезпека (КБ) (03). Введемо такі дефініції.

Дефініція 1. *Безпека банківських інформаційних ресурсів (Б БІР)* – стан захищеності банківських інформаційних ресурсів, що характеризується здатністю користувачів, технічних засобів і інформаційних технологій забезпечити конфіденційність, цілісність автентичність і доступність банківських інформаційних ресурсів при їх обробці в АБС.

Дефініція 2. *Інформаційна безпека банківських інформаційних ресурсів (ІБ БІР)* – стан захищеності інформаційного середовища ОБС, що забезпечує її формування, використання і розвиток в інтересах громадян і ОБС.

Дефініція 3. *Кібербезпека банківських інформаційних ресурсів (КБ БІР)* – набір засобів, стратегій, принципів забезпечення безпеки, гарантій безпеки, підходів до управління ризиками, дій, професійної підготовки, страхування і

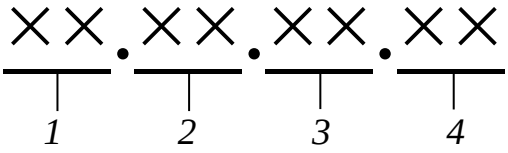
технологій, які використовуються для захисту кіберсереди АБС, ресурсів і користувачів ОБС.

Друга платформа – класифікація загроз за характером напрямків: нормативно-правовий (01), організаційний (02), інженерно-технічний (03);

Третя платформа – класифікація загроз у відповідності з основними особливостями інформації: конфіденційність (01), цілісність (02), доступність (03), автентичність (04).

Четверта платформа – класифікація загроз за рівнями ієрархії інфраструктури АБС: *FL* – фізичний рівень (01), *NL* – мережевий рівень (02), *OSL* – рівень операційних систем (ОС) (03), *DBL* – рівень систем управління базами даних (04), *BL* – рівень банківських технологічних застосунків і сервісів (05).

Частини класифікатора поділяються точкою і мають вигляд, зображений на рис. 2.5.



(*1* – синергетична складова безпеки БІР, *2* – характер напрямків;
3 – особливості інформації; *4* – рівні ієрархії інфраструктури АБС).

Рисунок 2.5 – Складові узагальненого класифікатора

На рис. 2.6 наведено взаємозв'язок структурної схеми класифікатора загроз з АБС ОБС. Множину загроз інформаційній безпеці, кібербезпеці, безпеці інформації на банківські інформаційні ресурси запропоновано використовувати з електронного ресурсу (http://bdu.fstec.ru/vul).

Крок 1.1. Формування метричних коефіцієнтів загроз експертами за послугами безпеки. Нехай *j* – послуги безпеки БІР. Основними послугами безпеки БІР є *C* –конфіденційність; *I* – цілісність; *A* – доступність; *Au* – автентичність. Тоді класифікатор за чотирма послугами безпеки описується виразом вигляду $j = \{C, I, A, Au\}$ Класифікатор містить *N* загроз. У складанні вагових коефіцієнтів прояву кожної загрози на послуги безпеки БІР брали участь *K* експертів.

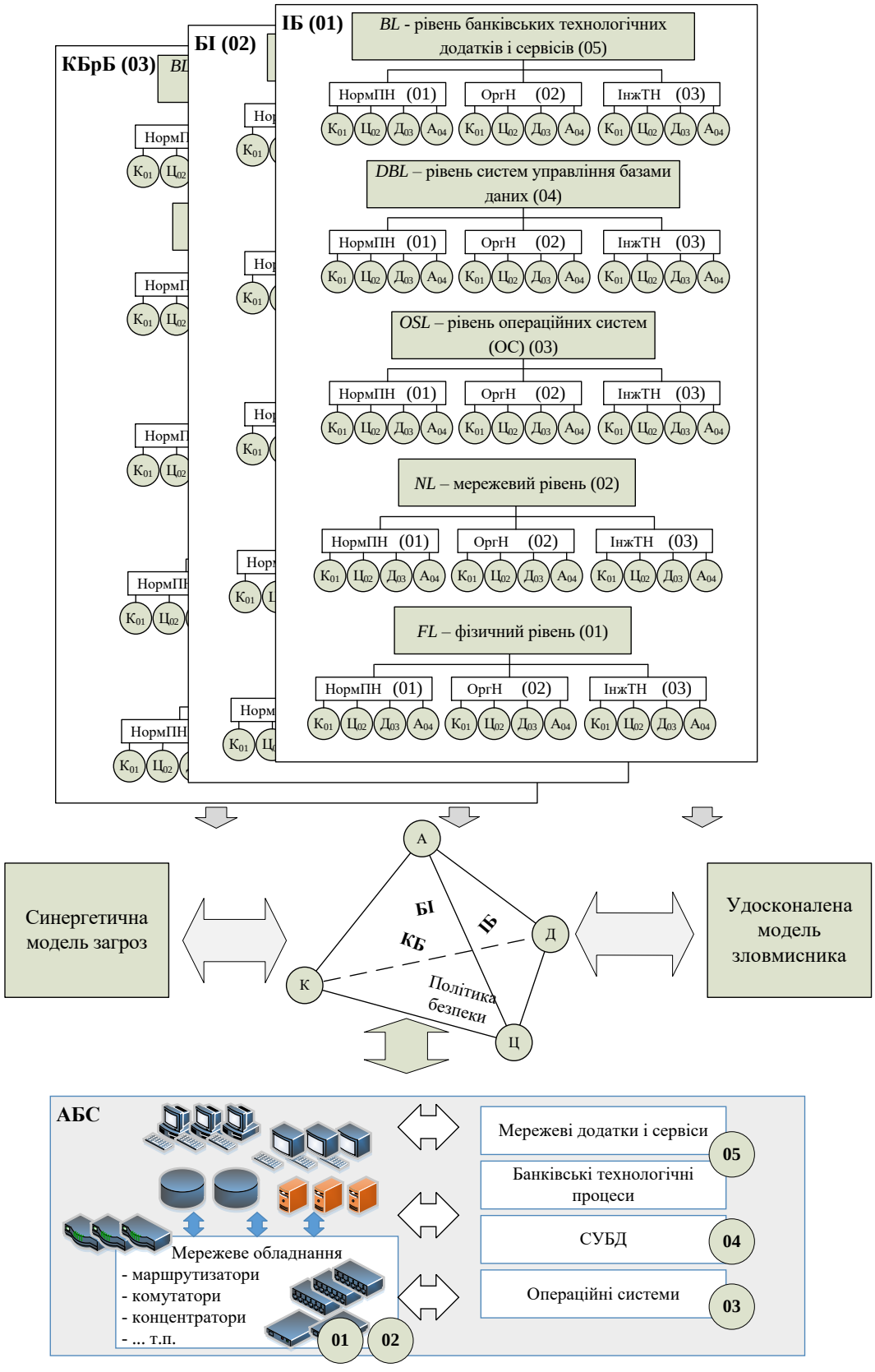


Рисунок 2.6 – Взаємозв’язок структурної схеми класифікатора загроз з АБС ОБС

Позначимо через *i* поточний номер загрози ($\{i\}_1^N$), через *k* – поточний номер експерта, який виконував оцінку ($\{k\}_1^K$). Середнє значення оцінки експертів за всіма загрозами для певної послуги безпеки може бути записане:

$$w^j = \frac{1}{K}\sum_{i=1}^{N}\sum_{k=1}^{K} w_{ik}^j , \qquad (2.1)$$

де w_{ik}^j – значення метричного коефіцієнта, виставленого *k*-м експертом для *i*-ї загрози *j*-ї послуги безпеки; *N* – кількість загроз; *K* – кількість експертів.

Крок 1.2. Формування ідентифікаторів загроз за складовими класифікатора. На цьому кроці експерти формують цифрове значення (код) ідентифікатора загрози за відповідними складовими класифікатора.

Крок 1.3. Вибір вагових коефіцієнтів α_i, що визначають умови прояву *i*-ї загрози (табл. 2.1) [76; 77].

Таблиця 2.1 – Таблиця вибору вагових коефіцієнтів α_i прояву *i*-ї загрози залежно від умови її прояву

Вагові коефіцієнти α_i	Умови прояву загрози
0,067	загроза проявляється не частіше одного разу на 5 років
0,133	загроза проявляється не частіше одного разу на рік
0,2	загроза проявляється не частіше одного разу на місяць
0,267	загроза проявляється не частіше одного разу на тиждень
0,333	загроза проявляється щодня

Крок 1.4. Визначення реалізації кожної *i*-ї загрози з урахуванням імовірності прояву атаки (її виникнення) здійснюється за виразом:

$$w_i^j P_i^j = \frac{1}{K} P_i^j \sum_{k=1}^{N} w_{ik}^j . \qquad (2.2)$$

Для кожної послуги безпеки та *i*-ї загрози:

$$w_i^C \alpha_i^C = \frac{1}{K} \alpha_i^C \sum_{k=1}^{K} w_{ik}^C \text{ – послуга конфіденційність;}$$

$$w_i^I \alpha_i^I = \frac{1}{K} \alpha_i^I \sum_{k=1}^{K} w_{ik}^I \text{ – послуга цілісність;}$$

$$w_i^A \alpha_i^A = \frac{1}{K} \alpha_i^A \sum_{k=1}^{K} w_{ik}^A \text{ – послуга доступність;}$$

$$w_i^{Au} \alpha_i^{Au} = \frac{1}{K} \alpha_i^{Au} \sum_{k=1}^{K} w_{ik}^{Au} \text{ – послуга автентичність,}$$

де $w_{ik}{}^C$, $w_{ik}{}^I$, $w_{ik}{}^A$, $w_{ik}{}^{Au}$ – експертні вагові коефіцієнти послуг безпеки: конфіденційності, цілісності, доступності, автентичності; α_i^C, α_i^I, α_i^A, α_i^{Au} – ваговий коефіцієнт послуги безпеки: конфіденційності, цілісності, доступності, автентичності прояву атаки *i*-ї загрози.

Крок 1.5. Визначення реалізації виникнення декількох загроз для обраної послуги розраховується з урахуванням виразу (2.2):

$$W_{synerg}^C = \sum_{i=1}^{M} w_i^C \alpha_i^C \text{ – послуга конфіденційність;}$$

$$W_{synerg}^I = \sum_{i=1}^{M} w_i^I \alpha_i^I \text{ – послуга цілісність;}$$

$$W_{synerg}^A = \sum_{i=1}^{M} w_i^A \alpha_i^A \text{ – послуга доступність;}$$

$$W_{synerg}^{Au} = \sum_{i=1}^{M} w_i^{Au} \alpha_i^{Au} \text{ – послуга автентичність,} \qquad (2.3)$$

де M – кількість декількох загроз, які вибрані експертом з ІБ банку з множини $\{i\}_i^M$, яка є підмножиною усієї множини загроз класифікатора, тобто $M \le N$.

При формуванні метричних коефіцієнтів уважається, що отримані результати належать до незалежних загроз, у випадку їх залежності (збіг класифікатора загроз) необхідно скористатися виразом визначення повної ймовірності залежних подій:

$$P(AB) = P(A) + P(B) - P(AB).$$

Статистична обробка результатів оцінювання можливості впливу *i*-ї загрози на послугу безпеки в АБС експертами проводиться за методикою, описаної в роботі [55]. Підсумкова оцінка *i*-ї загрозі осереднюється за кількістю експертів відповідно до виразу:

$$x_i = \frac{\sum_{k=1}^{K} x_k \times k_k}{K}, \tag{2.4}$$

де x_k– оцінка *k*-го експерта впливу *i*-ї загрози;

k_k – рівень компетентності експерта;

K– кількість експертів.

Мірою погодженості думок експертів вважається дисперсія, що обчислюється за виразом:

$$\sigma_x^2 = \frac{1}{K}\sum_{k=1}^{K} k_k \left(x_k - x_i\right)^2. \tag{2.5}$$

Статистична значимість отриманих результатів з імовірністю 1 – α_i, становить: $\left[x_i - \Delta, x_i + \Delta\right]$, де величина x_i розподілена за нормальним законом із центром у x_i і дисперсією σ_x^2 . Тоді Δ визначається за виразом:

$$\Delta = t\sqrt{\sigma_x^2 / N}, \tag{2.6}$$

де *t* – величина, що підкоряється розподілу Стьюдента для *K* – 1 ступенів свободи, *K* – кількість експертів.

Крок. 1.6. Визначення сумарної загрози за складовими безпеки з урахуванням виразу (2.3) розраховується:

$$W_{synerg}^{IB} = \sum_{i=1}^{N}\left(w_i^C \bigcap w_i^I \bigcap w_i^A \bigcap w_i^{Au}\right)\alpha_i,$$

$$W_{synerg}^{KB} = \sum_{i=1}^{N}\left(w_i^C \bigcap w_i^I \bigcap w_i^A \bigcap w_i^{Au}\right)\alpha_i,$$

$$W_{synerg}^{BI} = \sum_{i=1}^{N}\left(w_i^C \bigcap w_i^I \bigcap w_i^A \bigcap w_i^{Au}\right)\alpha_i. \tag{2.7}$$

Крок. 1.7. Визначення узагальненої синергетичної загрози на БІР:

$$W_{synerg}^{IB,KB,BI} = W_{synerg}^{IB} \bigcup W_{synerg}^{KB} \bigcup W_{synerg}^{BI}. \quad (2.8)$$

Крок 1.8. Визначення узагальненої синергетичної загрози з урахуванням її гібридності розраховується:

$$W_{synerg}^{\text{hybrid } C,I,A,Au} = W_{synerg}^{C} \bigcap W_{synerg}^{\text{I}} \bigcap W_{synerg}^{A} \bigcap W_{synerg}^{Au}. \quad (2.9)$$

Результати досліджень загроз з максимальною частотою їх прояву на БІР наведені у табл. 2.2

Таблиця 2.2 – Результати оцінювання загроз на основі синергетичного підходу

Складові безпеки	Послуги безпеки				
	C, W_{synerg}^{C}	*I*, W_{synerg}^{I}	*A*, W_{synerg}^{I}	*Au*, W_{synerg}^{Au}	Підсумок
IB, W_{synerg}^{IB}	0,023	0,223	0,193	0,207	0,0002
KB, W_{synerg}^{KB}	0,222	0,234	0,197	0,134	0,0014
BI, W_{synerg}^{BI}	0,226	0,109	0,152	0,189	0,0007
Підсумок	0,471	0,566	0,542	0,53	
$W_{synerg}^{IB,KB,BI} = W_{synerg}^{IB} \bigcup W_{synerg}^{KB} \bigcup W_{synerg}^{BI} =$ =0,0002+0,0014+0,0007=**0,0223**			$W_{synerg}^{\text{hybrid } C,I,A,Au} = W_{synerg}^{\text{C}} \bigcap W_{synerg}^{\text{I}} \bigcap W_{synerg}^{A} \bigcap W_{synerg}^{Au}$ = =0,471×0,566×0,542×0,53=**0,0766**		

Результати дослідження загроз безпеки банківських інформаційних ресурсів на основі запропонованого класифікатору наведені у додатку Е.

Розроблено програмний засіб, що реалізує удосконалений класифікатор загроз безпеці БІР, який, на відміну від відомих, ґрунтується на синергетичній моделі загроз, що дозволило класифікувати загрози за складовими безпеки, видами послуг та рівнями ієрархії інфраструктури автоматизованих банківських систем. Практична реалізація дозволяє в он-лайн режимі формувати експертну оцінку загроз БІР, аналізувати їх синергію та гібридність, оцінювати ймовірність впливу

зазначених загроз на безпеку БІР без значних витрат інвестицій та людських ресурсів (електронний доступ до ресурсу: http://skl.hneu.edu.ua/).

Для визначення залежностей між елементами інфраструктури АБС, інформаційними активами БІР, загрозами ІБ, КБ, БІ та ТЗЗІ на етапі 2 розглянемо удосконалену модель інфраструктури АБС, синергетичну модель загроз, та удосконалену модель зловмисника.

2.3. Розробка методу оцінювання узагальненого показника рівня захищеності банківських інформаційних ресурсів

2.3.1. Удосконалення інфраструктури автоматизованої банківської системи

Одним з найважливіших завдань оптимальної побудови комплексної системи захисту інформації є вибір з множини засобів такого їх набору, який дозволить забезпечити нейтралізацію всіх потенційно можливих інформаційних загроз з найкращою якістю і мінімально можливими витратами ресурсів. Найбільш ефективно завдання захисту інформації (ЗІ) вирішуються в рамках *попереджувальної стратегії захисту*, коли на етапі проектування оцінюються потенційно можливі загрози і реалізуються механізми захисту від них. При цьому в процесі проектування систем ЗІ розробник, не маючи статистичних даних про результати функціонування створюваної системи, змушений приймати рішення про склад комплексу засобів ЗІ, перебуваючи в умовах значної невизначеності [1; 48; 56; 59; 61].

Моделі безпеки відіграють важливу роль в процесах розробки і дослідження захищених комп’ютерних систем до яких належать і АБС. Моделі забезпечують системотехнічний підхід, що включає вирішення найважливіших завдань: вибору і обґрунтування базових принципів архітектури АБС, що визначають механізми реалізації засобів і методів захисту інформації; підтвердження властивостей (захищеності) розроблюваних систем шляхом формального доведення дотримання політики безпеки (вимог, умов, критеріїв); складання формальної специфікації політики безпеки як найважливішої складової частини організаційного та документаційного забезпечення розроблюваних захищених комп’ютерних систем.

Побудова моделей при проектуванні або модернізації системи захисту інформації в банках здійснюється природним шляхом вирішення задач аналізу та проектування з мінімальними витратами і високою ефективністю. Так, на етапі аналізу модель системи захисту інформації використовується для дослідження кожної виконуваної функції (операції), щоб виявити, наприклад, до якої інформації і до яких ресурсів повинен мати доступ кожен працівник при виконанні службових обов'язків [1; 48; 56; 59; 61].

Основним результатом формування методологічних основ безпеки БІР, відповідно до системного підходу [57; 59; 61; 63; 64; 65; 66; 67; 70; 74] є ідеалізована або еталонна модель (ЕМ) захищеної АБС, що реалізує принципово безпечні технології циркуляції БІР. Крім цього, ЕМ забезпечує потенційну можливість реалізації рішень стандартизації та уніфікації архітектурних підходів, шляхом розробки регламентів і стандартів в області безпеки БІР.

Для побудови моделі безпеки на основі синергетичного підходу до оцінки загроз БІР, незалежно від складової безпеки (ІБ, КБ, БІ) доцільно застосовувати принципи ризик-менеджменту, що дозволить при грамотному використанні основних його процедур своєчасно визначити та класифікувати загрози, і, відповідно до ймовірності настання негативних наслідків від їх можливого прояву, адекватно організувати систему безпеки БІР.

У роботах [1; 2; 30; 38; 39; 45; 46; 47; 48; 56; 57; 59; 60; 61; 62; 63; 64; 67; 68; 69; 70; 73] відзначається, що безпека інформації, в тому числі і банківської, може бути забезпечена лише при комплексному використанні всього арсеналу наявних засобів захисту у всіх структурних елементах виробничої системи і на всіх етапах технологічного циклу обробки інформації. Ігнорування методології системного аналізу при створенні систем безпеки БІР виходячи зі складності, а іноді і з неможливості об'єктивного підтвердження ефективності створених систем через недосконаліть нормативно-методичного забезпечення безпеки, перш за все в області показників і критеріїв [69; 72; 74], так само створює перешкоди на шляху знаходження вирішення означеної проблеми.

Розвиток теорій ІБ, КБ, БІ на сучасному етапі пов’язаний з урахуванням нових обставин, характерних для сучасного періоду розвитку інформатизації суспільства на основі високих технологій. *По-перше*, оскільки все більшої актуальності набуває не тільки захист інформації, а й захист спільноти, особи і комунікаційних систем, в першу чергу, критичного застосування від руйнівного впливу інформації в кіберпросторі, то формується завдання забезпечення безпеки як органічної сукупності задач захисту інформації і захисту від інформації.

По-друге, від початку регулярного використання автоматизованих технологій обробки інформації актуальність завдання забезпечення необхідної якості інформації зростає, а саме завдання ускладняється. Отже, еволюція обчислювальних технологій веде до виникнення емерджентних властивостей автоматизованих систем управління, а забезпечення безпеки неможливе без урахування завдань забезпечення якості інформації.

По-третє, рішення завдань захисту інформації, завдань захисту від інформації і забезпечення якості інформації обумовлює ефективність діяльності об’єктів. Виникає узагальнене поняття управління інформацією, що об’єднує вище означені поняття. У свою чергу, врахування завдань управління інформацією необхідний при формуванні, підтримці і використанні концепції інформаційного забезпечення діяльності об’єктів.

По-четверте, серйозну увагу на новому етапі розвитку теорії захисту інформації слід приділити вдосконаленню науково-методологічного базису та інструментальних засобів, що забезпечують вирішення будь-яких виникаючих завдань на регулярній основі в органічному зв’язку з вирішенням проблем інформаційної безпеки, інформаційних технологій, інформатизації суспільства. Таким чином, усе сказане дозволяє виділити такі найактуальніші проблеми розвитку теорії та практики безпеки БІР [2; 36; 37; 39; 45; 48]:

– створення теоретичних основ і формування науково-методологічного базису, що дозволяють адекватно описувати процеси в умовах значної невизначеності та непередбачуваності прояву дестабілізуючих факторів (інформаційних загроз) при

комплексованому синергетичному підході до їх оцінки в усіх складових поняття безпеки: ІБ, КБ, БІ;

– розробка науково-обґрунтованих нормативно-методичних документів у галузі безпеки БІР на основі вивчення та класифікації загроз інформації і вироблення стандартів вимог до захисту;

– стандартизація підходів до створення систем захисту інформації та раціоналізація схем і структур управління захистом на об’єктовому, регіональному та державному рівнях.

Рішення спектра перерахованих завдань має велике значення для реалізації положень Стратегії національної безпеки України та Доктрини безпеки банківської інформації. Очевидно, що одним з найважливіших завдань оптимальної побудови комплексної системи захисту інформації є вибір з множини засобів такого їх набору, який дозволить забезпечити нейтралізацію всіх потенційно можливих загроз з найкращою якістю і мінімально можливими витратами ресурсів.

З цією метою використовуються моделі безпеки, що дозволяють синтезувати налаштування параметрів безпеки АБС з метою зменшення трудовитрат і підвищення ступеня відповідності нормативних документів при проектуванні систем (підсистем) ЗІ і планування заходів захисту протягом усього циклу використання ТЗЗІ в АБС.

На рис. 2.7 наведено узагальнений підхід до побудови синергетичної моделі безпеки банківських інформаційних ресурсів. Аналіз рис. 2.7 показує, що основною відмінністю запропонованого підходу моделювання моделі безпеки від відомих є, по-перше, використання синергетичного підходу при побудові моделі загроз, що дає емерджентний ефект отримання комплексованої оцінки загроз БІР, по-друге, забезпечення успішності виконання бізнес-процесів за допомогою функцій безпеки БІР, виділених елементів АБС, заснованих на вимогах:

– забезпечення конфіденційності інформації;

– забезпечення доступності інформації, сервісів і мережевих, і апаратних підсистем;

– забезпечення цілісності інформації;

– забезпечення безперервності бізнес-процесів.

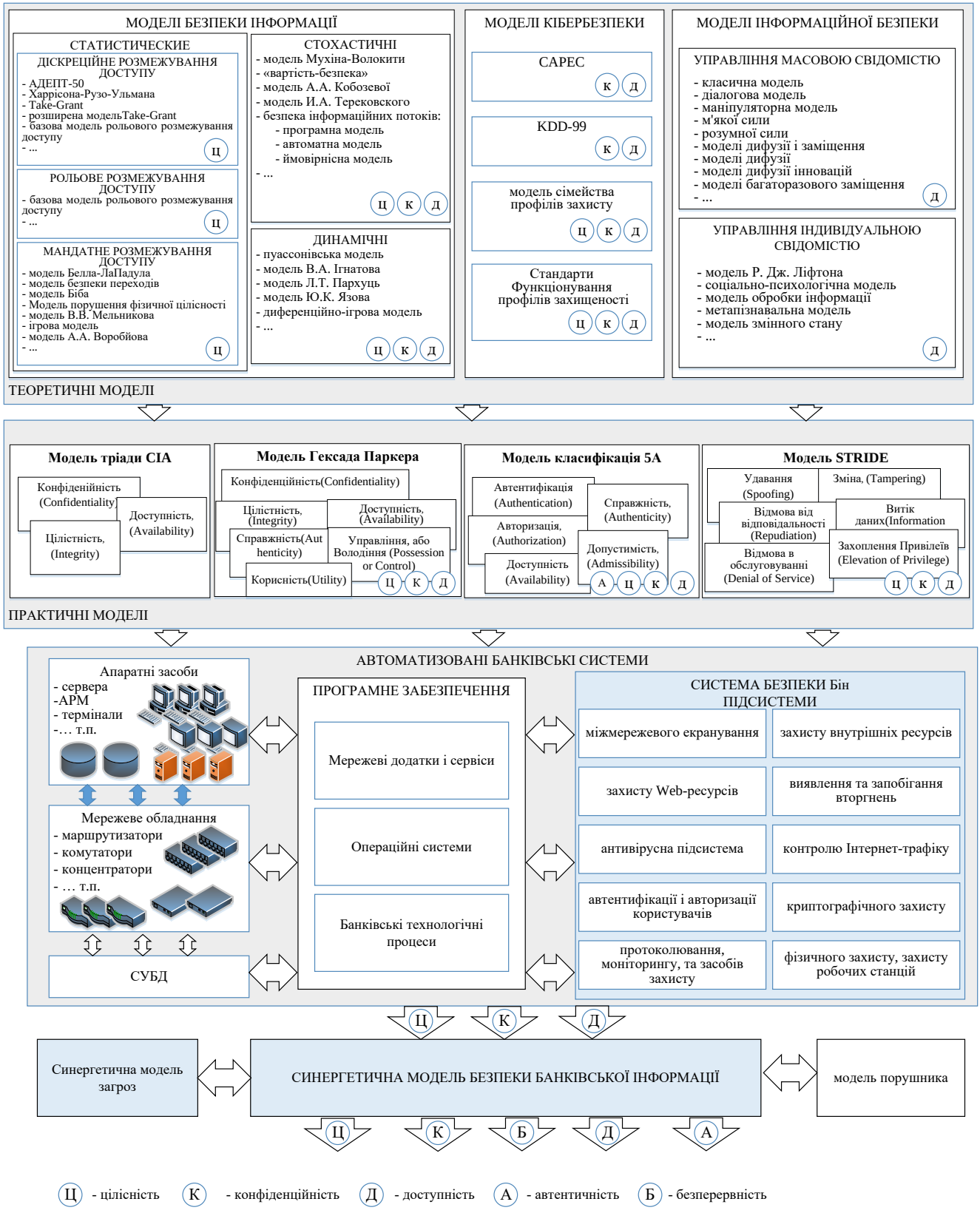


Рисунок 2.7 – Узагальнений підхід формування синергетичної моделі безпеки БІР

На практиці найбільшого поширення набули два підходи до обґрунтування проекту підсистеми забезпечення безпеки [1; 45; 57].

Перший з них заснований на перевірці відповідності рівня захищеності ІС вимогам одного зі стандартів в області інформаційної безпеки. Це може бути клас захищеності відповідно до вимог профілю захисту розроблених відповідно до стандарту *ISO-15408*, або будь-який інший набір вимог. Тоді критерій досягнення мети в області безпеки – це виконання заданого набору вимог.

Критерій ефективності – мінімальні сумарні витрати на виконання поставлених функціональних вимог: $\Sigma c_i \rightarrow min$, де c_i – витрати на i-й засіб захисту. Основний недолік цього підходу полягає в тому, що в разі, коли необхідний рівень захищеності жорстко не заданий (наприклад, через законодавчі вимоги) визначити "найбільш ефективний" рівень захищеності АБС досить складно.

Другий підхід до побудови системи безпеки БІР пов'язаний з оцінкою і управлінням ризиками на основі принципу "розумної достатності". Однак, проведений аналіз показав, що дотримання балансу між витратами на захист і одержуваним ефектом, в т.ч. і економічним, що полягає в зниженні втрат від порушень безпеки носить суб'єктивний характер, і безпосередньо залежить від оцінки ризику загроз елементам АБС.

На основі аналізу [1; 22; 23; 26; 34; 35; 36; 37; 41; 45; 47; 48; 52; 56; 57; 59; 60; 61; 62; 63; 64; 70; 71; 73] введемо дефініції безпеки інформації, основних механізмів і процедур, в рамках побудови моделі безпеки БІР на основі синергетичного підходу:

Дефініція 4. *Банківські інформаційні ресурси (БІР)* – інформація, що виникла в результаті банківської діяльності, а також відомості, що характеризують сам банк, його фінансове становище, надійність і виконання вимог законодавства.

Дефініція 5. *Конфіденційність (confidentiality)* – стан БІР, при якому інформація не може бути отримана неавторизованим користувачем і / або процесом.

Дефініція 6. *Конфіденційність системи (system confidentiality)* – властивість системи забезпечити захист БІР при передачі від пасивних атак.

Дефініція 7. *Цілісність (integrity)* – стан БІР, при якому інформація не може бути модифікована неавторизованим користувачем і / або процесом.

Дефініція 8. *Цілісність системи (system integrity)* – властивість системи забезпечити захист БІР при зберіганні, а також можливість модифікації БІР тільки авторизованим користувачем і / або процесом.

Дефініція 9. *Доступність (availability)* – стан БІР, при якому відсутні перешкоди доступу до інформації та закономірного її використання авторизованим користувачем і / або процесом.

Дефініція 10. *Доступність системи (system availability)* – властивість системи, яка полягає в тому, що авторизований користувач і / або процес, що володіє відповідними повноваженнями, може використовувати ресурс відповідно до правил, встановлених політикою безпеки, не чекаючи довше заданого (малого) проміжку часу, у вигляді, необхідному користувачеві, в місці, необхідному користувачеві, і в той час, коли вона йому необхідна.

Дефініція 11. *Автентичність (authenticity)* – стан БІР, при якому інформація забезпечує підтвердження автентичності джерела (авторизованого користувача і / або процесу) інформації.

Дефініція 12. *Автентичність системи (system authenticity)* – властивість системи, яка полягає в тому, що авторизований користувач і / або процес, що володіє відповідними повноваженнями, може підтвердити справжність джерела інформації.

Дефініція 13. *Безперервність бізнес-процесів (business continuity)* – властивість системи, яка полягає в забезпеченні безперебійної роботи внутрішніх і зовнішніх застосунків, дозволяє навантаженням і службам працювати без перерви під час запланованого простою і незапланованих збоїв, а також забезпечує резервне копіювання і зберігання критичних бізнес-даних і можливість їх відновлення протягом прийнятного періоду часу в випадку несподіваного інциденту або аварії.

Дефініція 14. *Об'єкти загроз ІБ* – відомості про склад, стан і діяльність банку (персоналу, матеріальних і фінансових цінностей, інформаційних ресурсів банку).

Дефініція 15. *Загрози безпеки БІР* – сукупність умов і факторів, що створюють загрозу несанкціонованого, в тому числі випадкового, доступу до банківських даних, результатом якого може стати знищення, зміна, блокування, копіювання, поширення БІР, а також інших НСД при їх обробці в АБС.

Загрози інформації виражаються в порушенні доступності, цілісності, автентичності та конфіденційності БІР.

Дефініція 16. *Синергетичний показник безпеки БІР* – синергетична оцінка ефективності комплексного застосування сил і засобів безпеки БІР в умовах антагоністичної протидії системи банківського захисту випадковим і цілеспрямованим загрозам безпеки.

Дефініція 17. *Рівень захищеності банківських інформаційних ресурсів* – якісний (кількісний) показник здатності системи захисту банківських інформаційних ресурсів АБС протистояти синергетичним і гібридним загрозам на складові безпеки: інформаційну безпеку, кібербезпеку, безпеку інформації.

Дефініція 18. *Гібридність загроз ІБ, КБ, БІ* – сукупність кількох загроз на банківські інформаційні ресурси за складовими безпеки: інформаційна безпека, кібербезпека, безпеку інформації, спрямованих на окрему послугу безпеки: конфіденційність, цілісність або автентичність, що дозволяє отримати максимальний ефект від їх комплексування.

Дефініція 19. *Синергізм загроз ІБ, КБ, БІ* – комбінований вплив декількох загроз на складові безпеки: інформаційну безпеку, кібербезпеку, безпеку інформації за послугами безпеки: конфіденційність, цілісність, автентичність, що характеризується тим, що їх об’єднана дія істотно перевершує ефект кожної окремо взятої загрози і їх простої суми.

Дефініція 20. *Емерджентність АБС* – сукупність особливих властивостей АБС, які не належать її підсистемам і блокам, а також сумі елементів, не пов’язаних особливими системоутворюючими зв’язками, на основі оцінювання синергізму і гібридності загроз складових безпеки (ІБ, КБ, БІ) на БІР, мінімізації витрат на інвестування в побудову системи безпеки БІР, забезпечення високої швидкості криптоперетворень та доказовий рівень стійкості в інтегрованих механізмах забезпечення цілісності, конфіденційності, автентичності і достовірності при використанні відкритих каналів зв’язку, оцінювання функціональної ефективності передачі БІР в АБС.

В узагальненому вигляді розглянуті компоненти наведені у вигляді концептуальної синергетичної моделі безпеки БІР на рис. 2.8.

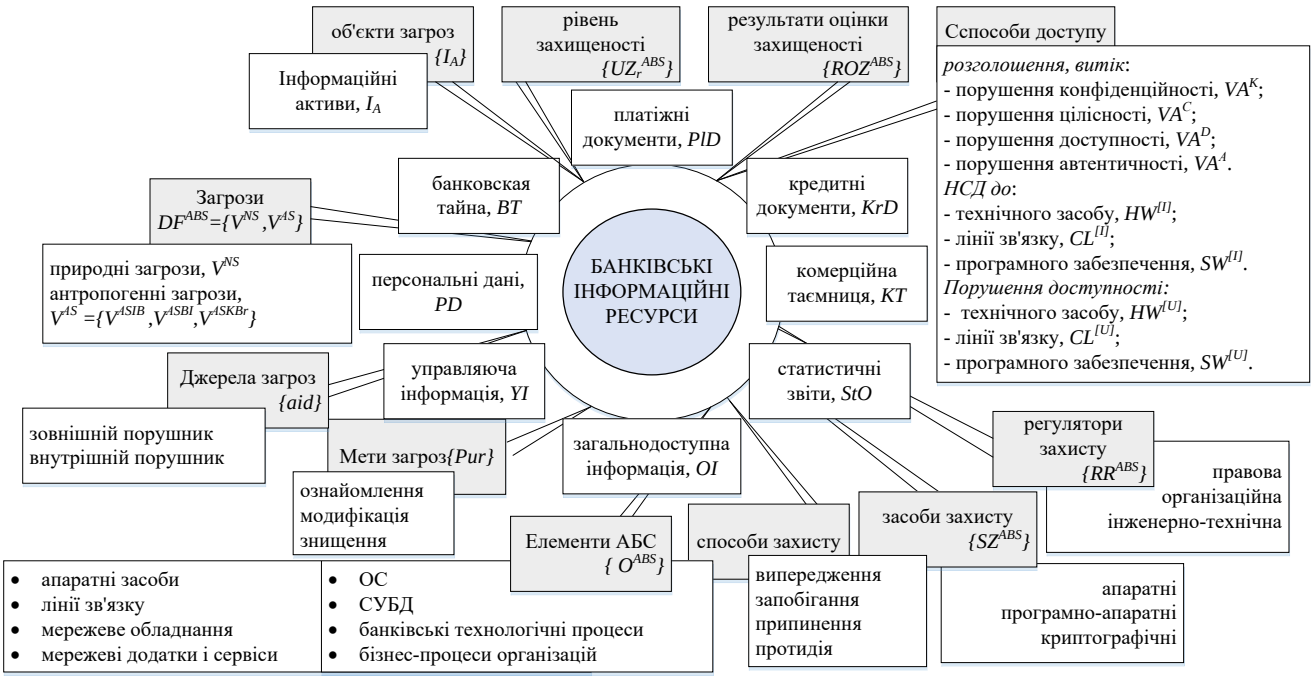


Рисунок 2.8 – Структурна схема концептуальної синергетичної моделі безпеки банківських інформаційних ресурсів

Джерелами загроз виступають *конкуренти, зловмисники-хакери, бакери, інсайдери, тощо*. *Джерела загроз* при цьому мають на меті: *ознайомлення* з БІР, їх *модифікацію* в корисних цілях і/або *знищення* для нанесення прямих матеріальних збитків.

Неправомірне заволодіння конфіденційною інформацією можливе за рахунок її *розголошення*, *витоку БІР* через технічні засоби та *несанкціонований доступ* до БІР.

Джерелами конфіденційної інформації є *персонал, банківські процеси, документи, технічні носії БІР, технічні засоби* забезпечення банківських транзакцій.

Основними *напрямками захисту* інформації є *правовий, організаційний та інженерно-технічний захисти* інформації як виразники комплексного підходу до безпеки БІР.

Засобами захисту інформації є *фізичні, апаратні, програмно-апаратні засоби і криптографічні методи*.

Як *способи захисту* виступають *організаційно-технічні заходи, способи* і *дії,* що забезпечують *упередження* протиправних дій, їх *запобігання, припинення* та *протидія* несанкціонованому доступу до БІР.

Етап 2. Визначення залежностей між елементами інфраструктури АБС, інформаційними активами БІР, загрозами ІБ, КБ, БІ та ТЗЗІ на основі удосконаленої моделі інфраструктури АБС, синергетичної моделі загроз, удосконалених класифікатора загроз та моделі зловмисника.

Концептуальна синергетична модель безпеки БІР формується на основі методології та синергетичному підході до безпеки БІР, оцінювання рівня захищеності БІР ОБС України в умовах гібридизації загроз на складові безпеки (ІБ, КБ, БІ), а також часткових моделей: удосконаленої інфраструктурної моделі АБС, синергетичної моделі загроз, удосконалених моделі зловмисника і моделі оцінювання захищеності АБС.

Удосконалена інфраструктурна модель АБС являє собою таку формальну модель:

$$G^{ABS} = \{\{O^{ABS}\}, \{L^{ABS}\}, \{I_A\}\}, \tag{2.10}$$

де O^{ABS} – множина об’єктів середовища, що описують елементи АБС та їх приналежність до рівнів ієрархії АБС; L^{ABS} – множина зв’язків між елементами, визначається матрицею суміжності:

$$A^{ABS} = \left\| a_{ij}^{ABS} \right\|; \tag{2.11}$$

$\{I_A\}$ – множина елементів інформаційних активів БІР. Кожен елемент $I_{A_i} \in \{I_A\}$ описується вектором $I_{A_i} = \left(Type, A^C, A^D, A^A, A^K, C_Y\right)$. *Type* – тип інформаційного активу, описується множиною базових значень *Type = {BT, PID, RrD, KT, StO, Ol, YI, PD}*, де *BT* – банківська таємниця; *PID* – платіжні документи; *KrD* – кредитні документи; *KT* – комерційна таємниця; *StO* – статистичні звіти; *Ol* – загальнодоступна інформація; *YI* – керівна інформація; *PD* – персональні дані. A^K – конфіденційність; A^C – цілісність; A^D – доступність; A^A – автентичність; C_Y –

безперервність – властивості інформації, які необхідно забезпечувати. Вони набувають значення 1 – якщо властивість необхідна, 0 – в іншому випадку.

Крок 2.1. Визначення зв'язку між інформаційними активами БІР $\{I_A\}$ та елементами інфраструктури АБС $A^{ABS} = \left\| a_{ij}^{ABS} \right\|$. Кожен елемент $I_{A_i} \in \{I_A\}$ описується вектором $I_{A_i} = \left(Type, A^C, A^I, A^A, A^{Au}, C_Y \right)$. *Type* – тип інформаційного активу, описується множиною базових значень *Type* = {*BT, PID, RrD, KT, StO, Ol, YI, PD*}, де *BT* – банківська таємниця; *PID* – платіжні документи; *KrD* – кредитні документи; *KT* – комерційна таємниця; *StO* – статистичні звіти; *Ol* – загальнодоступна інформація; *YI* – керівна інформація; *PD* – персональні дані. A^C – конфіденційність; A^I – цілісність; A^A – доступність; A^{Au} – автентичність; *CY* – безперервність – властивості інформації, які необхідно забезпечувати. Вони набувають значення 1 – якщо властивість необхідна, 0 – в іншому випадку.

Крок 2.2. Визначення зв'язку між інформаційними активами $\{I_A\}$ й об'єктами середовища. Кожен елемент $O_l \in \{O^{ABS}\}$ описується вектором $O_l = \{Y^{ABS}, IO\}$, де Y^{ABS} – рівень ієрархії інформаційної структури, яка визначається множиною Y^{ABS} = {*FL, NL, OSL, DBL, BL*}, де *FL* – фізичний рівень; *NL* – мережевий рівень; *OSL* – рівень операційних систем (ОС); *DBL* – рівень систем управління базами даних; *BL* – рівень банківських технологічних застосунків і сервісів. Для визначення типу зв'язку та існуючого співвідношення I^{OR} між інформаційними активами БІР і об'єктами АБС використовується правило:

$$IO^R = \left\| IO_{il}^R \right\|, \tag{2.12}$$

де IO_{il}^R – відображає наявність і тип зв'язку між *i*-м інформаційним активом та *l*-м об'єктом середовища АБС. При цьому $\forall i \in \{I_A\}$, а $\forall l \in \{O^{ABS}\}$:

$$IO_{il}^R = \begin{cases} 0 \ - \text{ зв'язок відсутній} \\ cs \ - \text{включає і зберігає} \\ pt - \text{обробляє або передає} \\ so - \text{підтримує функціонування} \end{cases}. \tag{2.13}$$

Наступний крок – визначення комплексування множини загроз на основі синергетичної моделі загроз й узагальненої моделі зловмисника.

2.3.2. Розроблення концептуальної синергетичної моделі загроз безпеки банківських інформаційних ресурсів

Крок. 2.3. Визначення комплексування множини загроз на основі синергетичної моделі загроз й удосконаленої моделі зловмисника.

Синергетична модель загроз формально описується виразом:

$$GR^{ABS} = \left\{ \left\{ DF^{ABS} \right\}, \left\{ T_{risk} \right\}, \left\{ T_P \right\}, \left\{ T_U \right\}, \left\{ VH \right\} \right\}. \quad (2.14)$$

Множина джерел загроз безпеці АБС представлена кортежем $DF^{ABS} = \left\{ V^{NS}, V^{AS} \right\}$, в якому V^{NS} – клас природних джерел загроз, $V^{AS} = \left\{ V^{ASIB}, V^{ASKB}, V^{ASBI} \right\}$ – клас антропогенних загроз, де V^{ASIB} – множина загроз інформаційній безпеці; V^{ASKB} – множина загроз кібербезпеці; V^{ASBI} – множина загроз безпеці інформації. T_{risk} – якісний показник ризику; T_p – множина базових визначень ймовірності реалізації хоча б однієї загрози *j*-му активу; T_U – множина базових визначень величини збитку від реалізації загрози u_i; *VH* – множина деструктивного стану елементів АБС, під яким розуміється небажаний і незапланований стан компонента АБС, в якому він опинився в результаті реалізації однієї або декількох загроз.

Для отримання синергетичного ефекту підвищення рівня захищеності БІР необхідно враховувати комплексування загроз:

$$DF^{ABS} = \left\{ V^{NS} \right\} \bigcup \left\{ V^{AS} \right\}, \quad (2.15)$$

де $\left\{ V^{AS} \right\} = \left\{ V^{ASBI} \right\} \bigcap \left\{ V^{ASIB} \right\} \bigcap \left\{ V^{ASKB} \right\}$.

Кожен елемент з множини загроз $DF_i \in \left\{ DF^{ABS} \right\}$, може бути представлений таким вектором значень:

$$DF_i\ (p,u,risk),$$

де p – ймовірність реалізації загрози; u – потенційний збиток; $risk$ – ризик, виражений в якісній формі, що набуває один з двох станів: T_{risk}={допустимий, недопустимий}={α_{r1},α_{r2}}.

Крок 2.4. Визначення ціни повного ризику всіх активів БІР. Ціна повного ризику дорівнює сумі цін ризику всіх активів:

$$R_{повн} = \sum_{j=1}^{n} R_j \,. \tag{2.16}$$

Крок 2.5. Визначення ймовірності реалізації хоча б однієї загрози для кожного активу БІР. Розрахунок ймовірності реалізації хоча б однієї загрози для кожного активу виконується за виразом:

$$p_{rj} = 1 - \prod_{i=1}^{m} \left(1 - pr_{ij}\right), \tag{2.17}$$

де p_{rj} – ймовірність реалізації хоча б однієї загрози j-му активу.

Передбачається, що в разі реалізації для j-го активу хоча б однієї із загроз з множини $V^{AS} = \left\{V^{ASIB}, V^{ASBI}, V^{ASKBr}\right\}$, збиток дорівнює вартості активу на основі деталізації активів і ретельного вибору актуальних загроз:

$$q_j = u_j. \tag{2.18}$$

Вважається, що загрози можуть бути реалізовані незалежно один від одного [72], тоді ціна ризику R_j для кожного j-го активу визначається за виразом:

$$R_j = pr_j \times q_j. \tag{2.19}$$

Таким чином, ймовірність реалізації середовища p_{rj}, з областю визначення P = [0, 1] задамо відповідно до [73] множиною базових визначень T_p = {нереалізована, мінімальна, середня, висока, критична } = {α_{x1}, α_{x2}, α_{x3}, α_{x4}, α_{x5}}.

Оцінка потенційно можливого збитку від реалізації загрози тісно пов’язана з капіталом (2.18) і формується на основі експертних оцінок. Величина збитку від реалізації загрози u_i задається множиною базових визначень T_U = {мінімальна, середня, висока, критична} = {α_{y1}, α_{y2}, α_{y3}, α_{y4}, α_{y5}}. Для переходу між якісними і кількісними значеннями використовуємо правило, запропоноване в [73].

Для визначення значення ризиків скористаємося правилом, запропонованим в роботі [70] на основі системи нечітких висловлювань:

$$\tilde{L}^1 = \begin{cases} \tilde{L}_1^1 : \langle E_{11} \cup E_{12} \cup E_{13} \cup E_{14} \cup E_{21} \cup E_{22} \cup E_{23} \cup E_{31} \cup E_{32} : risk_i \text{ есть } \alpha_{r1} \rangle; \\ \tilde{L}_2^1 : \langle E_{24} \cup E_{33} \cup E_{34} \cup E_{42} \cup E_{43} \cup E_{44} \cup E_{51} \cup E_{52} \cup E_{53} \cup E_{54} : risk_i \text{ есть } \alpha_{r2} \rangle \end{cases}, \quad (2.20)$$

де E_{kj}: "$p_{ri} \in \alpha_{xk}$ і $u_i \in \alpha_{yj}$"

У ході аналізу документів з моделювання загроз, оцінки ризиків та теорії надійності визначені такі деструктивні стани елементів АБС (множина $\{VH\}$, рис. 2.9):

а) *інформаційний актив*:

– недоступний (порушена доступність), $I_A^{[D]}$;

– скомпрометований (порушена конфіденційність), $IA^{[K]}$;

– змінений (порушена цілісність), $I_A^{[C]}$;

– порушена мітка безпеки (цифровий підпис) (порушена автентичність), $I_A^{[A]}$;

б) *програмне забезпечення*:

– недоступне (стався збій), $SW^{[B]}$;

– зламане (відбувся несанкціонований доступ (НСД) зловмисником або підвищені привілеї користувача), $SW^{[I]}$;

– порушення доступності, $SW^{[U]}$;

– змінене (несанкціоновано змінений код і / або конфігурація), $SW^{[M]}$;

в) *технічний засіб*:

– недоступний (стався тимчасовий збій), $HW^{[B]}$;

– порушення доступності, $HW^{[U]}$;

– непрацездатний (відбулася відмова, що вимагає ремонту або заміни), $HW^{[D]}$;

– загублено (відбулася втрата або крадіжка у законного власника), $HW^{[L]}$;

– зламано (відбувся несанкціонований доступ (НСД) зловмисником або було перевищено повноваження), $HW^{[I]}$;

г) *лінія зв'язку*:

– недоступна (відбувся збій або відмова), $CL^{[D]}$;

– порушення доступності, $CL^{[U]}$;

– зламано (відбувся НСД зловмисником), $CL^{[I]}$.

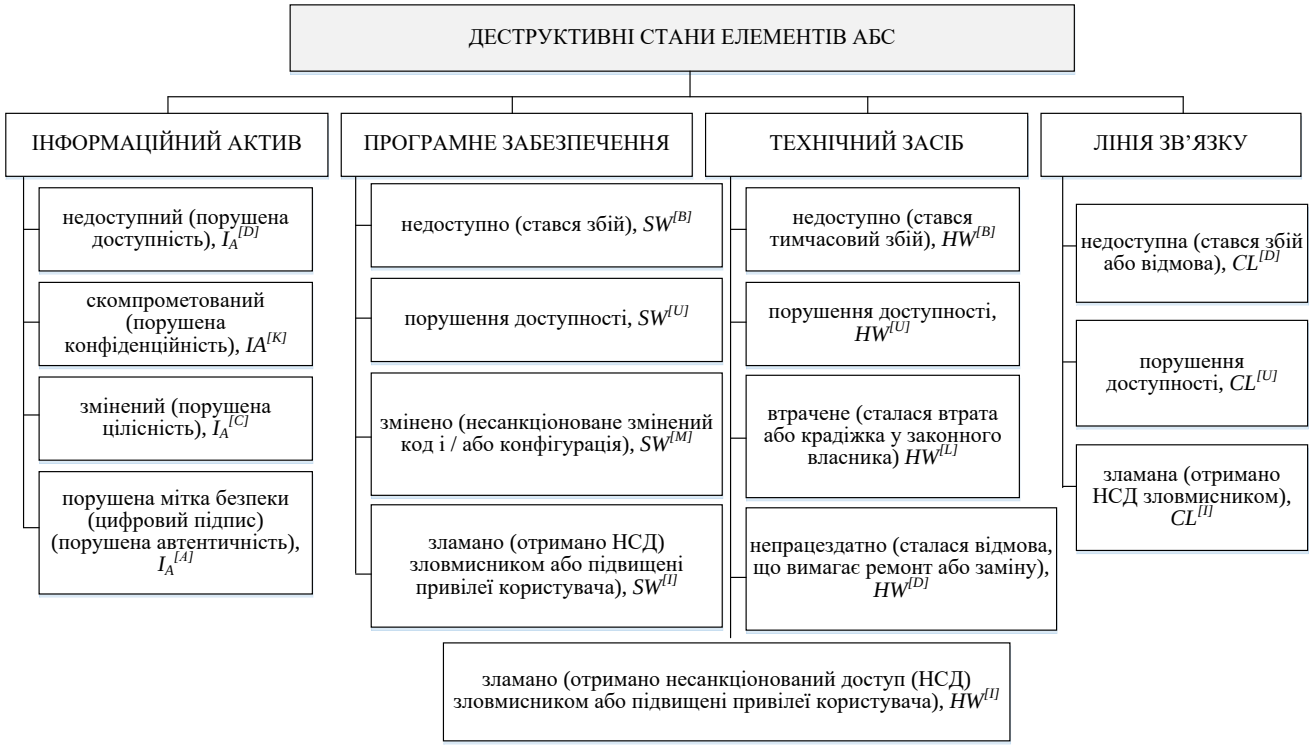


Рисунок 2.9 – Деструктивні стани елементів інфраструктури АБС

В наступному підрозділі розглядається удосконалена модель зловмисника.

2.3.3. Удосконалення моделі зловмисника на основі синергетичного підходу до оцінювання загроз інформаційній безпеці, кібербезпеці, та безпеці інформації

Однією з основних частин моделей загроз є модель зловмисника, що забезпечує смислові відносини між повним описом загроз і припущенням про можливості зловмисника, який є джерелом загроз, які він може використовувати для розробки і проведення атак, а також про обмеження на ці можливості.

Для побудови моделі зловмисника використовуються підходи, що мають спільні класифікаційні ознаки, однак не завжди корельовані в різних джерелах.

При побудові моделей зловмисника виділяють внутрішніх і зовнішніх зловмисників, а також враховують [47; 58]:

наявність у зловмисників доступу до штатних засобів (сукупність програмного, програмно-апаратного і технічного забезпечення);

– рівень знань зловмисників про об'єкти атак;

– рівень професійної підготовки зловмисників;

– можливість використання зловмисниками різних засобів для проведення атак;

– переслідувані зловмисниками мети;

– можливу змову зловмисників різних категорій.

Крім цих аспектів, при побудові моделі зловмисника в АБС слід розглядати перелік відповідності об’єктів доступу суб’єктам атак, опис каналів атак, обґрунтування виключення суб’єктів атак з числа потенційних зловмисників, а також стадії життєвого циклу і рівні АБС, на які може впливати зловмисник.

Для гарантованого вирішення завдань захисту інформації в АБС [47; 48] необхідно враховувати такі рівні впливу зловмисників: рівні технічних каналів, несанкціонованого доступу, шкідливого впливу, закладних пристроїв, системи захисту інформації. Штатні засоби, з використанням яких можливий несанкціонований доступ, можуть бути найрізноманітнішими: програмне, програмно-апаратне і технічне забезпечення засобів обчислювальної техніки (ЗОТ) або АБС. Отже, необхідно класифікувати рівень несанкціонованого доступу до БІР, а також до об’єктів і ліній зв’язку (ЛЗ) АБС. На основі запропонованих кваліфікаційних ознак модель зловмисника визначимо за п’ятьма категоріями (рис. 2.10):

Категорія 1. *Користувачі АБС і застосунків* – працівники ОБС, що мають доступ до інформації конфіденційного характеру в рамках реалізації своїх службових обов’язків. Вони можуть впливати на рівень систем управління базами даних (04), і рівень банківських технологічних застосунків і сервісів (05), з метою викрадення інформації, самоствердження або випадково.

При цьому використовують технічні засоби перехоплення без модифікації компонентів АБС, а також штатні засоби та недоліки систем захисту для її подолання.

Категорію користувачів АБС доцільно розподілити на такі групи за рівнем довіри: 1.1 – довірений користувач (наприклад, вище керівництво організації БС); 1.2 – користувач (більшість працівників ОБС); 1.3 – користувач “ в зоні ризику” (наприклад, працівники ОБС на випробувальному терміні, ті, що подали заяву на звільнення або раніше були причетні до інцидентів ІБ).

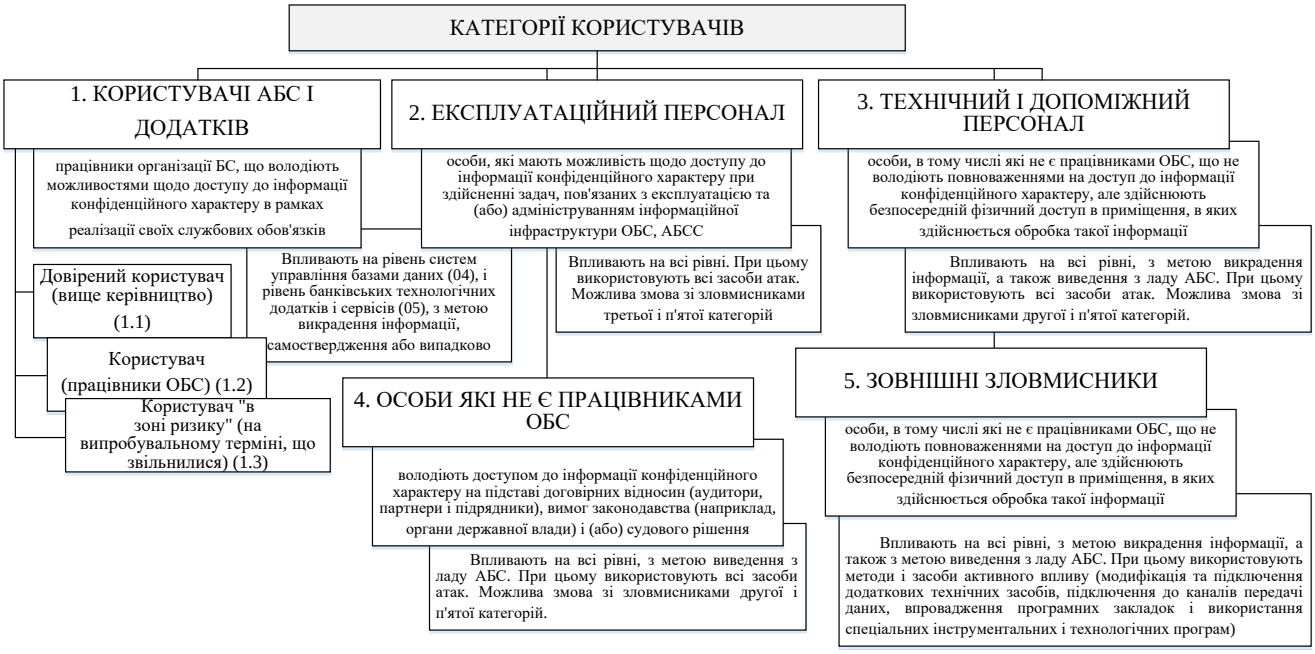


Рисунок 2.10 – Класифікація зловмисників в АБС

Категорія 2. *Експлуатаційний персонал* – особи, в тому числі які не є працівниками організації БС, що мають доступ до інформації конфіденційного характеру при реалізації завдань, пов’язаних з експлуатацією та (або) адмініструванням інформаційної інфраструктури ОБС, АБС і застосунків ОБС. Можуть впливати на всі рівні – фізичний рівень (01), мережевий рівень (02), рівень операційних систем (ОС) (03), рівень систем управління базами даних (04), рівень банківських технологічних застосунків і сервісів (05), з метою викрадення інформації, а також виведення з ладу АБС. При цьому використовують всі засоби атак. Можлива змова зі зловмисниками третьої і п’ятої категорій. Крім того до цієї категорії належать особи, що не мають прав доступу до конфігурації технічних засобів мережі, за винятком контрольних (інспекційних).

Категорія 3. *Технічний і допоміжний персонал* – особи, в тому числі які не є працівниками ОБС, що не володіють повноваженнями з доступу до інформації конфіденційного характеру, але здійснюють безпосередній фізичний доступ в приміщення, в яких здійснюється обробка такої інформації. Можуть впливати на всі рівні – фізичний рівень (01), мережевий рівень (02), рівень операційних систем (ОС) (03), рівень систем управління базами даних (04), рівень банківських технологічних додатків і сервісів (05) з метою викрадення інформації, а також

виведення з ладу АБС. При цьому використовують всі засоби атак. Можлива змова зі зловмисниками другої та п’ятої категорій.

Категорія 4. *Особи, які не є працівниками організації БС*, але володіють доступом до інформації конфіденційного характеру на основі договірних відносин (наприклад, аудитори, партнери і підрядники), вимог законодавства (наприклад, органи державної влади) і (або) судового рішення. Можуть впливати на всі рівні, з метою виведення з ладу АБС. При цьому використовують всі засоби атак. Можлива змова зі зловмисниками другої та п’ятої категорій. Не мають доступу до засобів захисту інформації та протоколювання і до частини ключових елементів АБС.

Категорія 5. *Зовнішні зловмисники* – особи, які здійснюють вплив за межами контрольованої зони ОБС. Можуть впливати на всі рівні з метою викрадення інформації, самоствердження, а також виведення з ладу АБС. При цьому використовують методи і засоби активного впливу (модифікація та підключення додаткових технічних засобів, підключення до каналів передачі даних, впровадження програмних закладок і використання спеціальних інструментальних і технологічних програм).

Ця класифікація найбільш повно охоплює аспекти, відображені в нормативно-методичній документації, а також дає змогу однозначно класифікувати зловмисника.

Формально удосконалену модель зловмисника визначимо з урахуванням пропозицій авторів [58; 68]:

$$G_{IA}^{ABS} = \left\{ aid_i, pur_i, T_{IA}, S_{\max_i}, pr_j, MS_i^{ABS} \right\} \forall i \in n, \forall j \in m, \qquad (2.21)$$

де $aid_i \in \{aid\}$ – ідентифікатор зловмисника (категорія зловмисника); $pur_i \in \{pur_i\}$ – мета зловмисника; T_{IA} – час успішної реалізації загрози; $S_{\max_i}$ – ймовірний збиток системи; $MS_i^{ABS} = \{ms_i\}_{i=1}^{N_{MS^{ABS}}}$ – рекомендації щодо виявлення, реагування ТЗЗІ, $N_{MS^{ABS}}$ – кількість рекомендацій відомих АБС; n – кількість загроз; m – кількість активів БІР.

Множина джерел загроз включає джерела чотирьох видів:

$$DF^{ABS} = \left\{V^{NS}, V^{AS}, TS, PI, NI\right\}, \quad (2.22)$$

де DF^{ABS} – множина джерел загроз безпеці АБС, в якій V^{NS} – клас природних джерел загроз; $V^{AS} = \left\{V^{ASIB}, V^{ASBI}, V^{ASKB}\right\}$ – клас антропогенних загроз, де V^{ASIB} – множина загроз ІБ; V^{ASBI} – множина загроз БІ; V^{ASKB} – множина загроз КБ; *TS* – технічні засоби і системи; *PI* – навмисні зловмисники; *NI* – ненавмисні зловмисники.

Сценарієм реалізації загроз називається один або кілька пов'язаних переходів компонентів АБС в деструктивні стани в результаті впливів джерел загроз. Один або кілька сценаріїв реалізації загроз можуть бути представлені орієнтованим графом *G(V,H)*, в якому: початковою вершиною (v_0) є множина, один з видів або конкретне джерело загроз; проміжними і кінцевими вершинами (v_n) є деструктивні стани компонентів АБС; дугами (h_{ij}) з'єднаються дві вершини, одна з яких є причиною (v_i), а друга – наслідком і результатом переходу (v_j). Сценарій реалізації загроз конфіденційності розглянуто в роботі [74].

Для оцінки показників ступеня небезпеки зловмисників і ступеня реалізації захисних заходів визначимо набори зважених метрик, які набувають значення в інтервалі [0; 1]. Кожна метрика характеризує ступінь відповідності певної ознаки зловмисника або захисний засіб заданому цільовому значенню.

Для оцінки ступеня небезпеки зловмисника будемо вважати, що він має такі характеристики (*Capabilities*) по відношенню до АБС: *C*={мотивація (*motivation, M*), оснащеність/наявне обладнання (*equipment, O*), технічна компетентність (*technical competence, K*), володіння інформацією про АБС і ТЗЗІ (*possession of information on the automated banking system and technical means of information protection, I*), доступні до реалізації загрози права доступу (*access rights, D*), час до моменту реагування ТЗЗІ на атаку (*response time to attack, T*)}. Таким чином, маємо таку множину характеристик зловмисника: *C* = {*M, O, K, I, D, T*}. Для опису множини характеристик використаємо індекс *h*: C_h, де $(\{h\}_1^C)$.

Нехай *j* – послуги безпеки БІР. Основними послугами безпеки БІР є *C* – конфіденційність; *I* – цілісність; *A* – доступність; *Au* – автентичність. Тоді класифікатор за чотирьома послугами безпеки описується виразом вигляду $j = \left\{C, I, A, Au\right\}$.

Позначимо через i поточний номер зловмисника $(\{i\}_1^L)$, через k – поточний номер експерта, який виконував оцінку $(\{k\}_1^K)$. Відповідно, ми будемо мати L зловмисників та K експертів. Позначимо також через w_{kih}^j – експертну оцінку k-го експерта для h-ї характеристики i-го зловмисника для j-ї послуги безпеки.

Тоді середнє значення оцінок усіх експертів за усією сукупністю характеристик усіх зловмисників для j-ї послуги безпеки буде мати вигляд:

$$w^j = \frac{1}{KLC}\sum_{k=1}^{K}\sum_{i=1}^{L}\sum_{h=1}^{C}\alpha_{kih}^j \times w_{kih}^j, \tag{2.23}$$

де α_{kih}^j – ваговий коефіцієнт h-ї метрики i-го зловмисника для j-ї послуги. Вагові коефіцієнти підкоряються умові нормування, тобто $\sum_{k=1}^{K}\sum_{i=1}^{L}\sum_{h=1}^{C}=1$.

Аналогічним чином можна описати ступінь захищеності ТЗЗІ АБС. Для цього використаємо множину характеристик B= {*cryptographic resistance*, стійкість ТЗЗІ (C_r), обсяг ключових даних (*Key data amount*, S_c), складність виконання прямого і оберненого криптографічного перетворення (шифрування/розшифрування БІР) (*encryption/decryption of data*, O_E)}. Таким чином, маємо таку множину характеристик ТЗЗІ: $B = \{C_r, S_c, O_E\}$. Для опису множини характеристик використаємо індекс g: B_g, де $(\{g\}_1^B)$. Позначимо через w_{kg}^j – значення оцінки g-ї характеристики ТЗЗІ k-м експертом для j-ї послуги безпеки у випадку, коли ступінь захищеності системи та деструктивні дії зловмисників незалежні.

Тоді середнє значення оцінок усіх експертів ступені реалізації захисних заходів для j-ї послуги безпеки буде мати вигляд:

$$\psi^j = \frac{1}{KB}\sum_{k=1}^{K}\sum_{g=1}^{B}\left(\beta_{kg}^j \times w_{kg}^j\right), \tag{2.24}$$

де β_{kg}^{j} – ваговий коефіцієнт *g*-ї метрики *j*-ї послуги безпеки для *k*-го експерта. Нормування вагових коефіцієнтів звичайне: $\sum_{k=1}^{K}\sum_{g=1}^{B}\beta_{kg}^{j}=1.$

Для кореляції між ступенем небезпеки зловмисника та характеристиками захисту системи, тобто між множинами *C* та *B*. використаємо матрицю *M* розміром $[C \times B]$, яку іноді називають матрицею парних порівнянь. Якщо *g*-а захисна характеристика B_g повністю блокує *h*-ту властивість зловмисника (або загрозу, яка реалізується цим зловмисником), то $M_{hg}=1.$ в іншому випадку $M_{hg}=0.$ Можливі також проміжні значення, коли загроза/характеристика зловмисника закривається не повністю. Таким чином, M_{hg} – матриця коефіцієнтів, які пов'язують між собою загрози/характеристики зловмисника із захисними заходами системи безпеки.

Тоді нові значення оцінок захисних заходів з використанням матриці *M* можна записати:

$$\left(w_{kg}^{j}\right)_{cor}=M_{hg}\times w_{kg}^{j}.$$

Тоді

$$\psi^{j}=\frac{1}{KB}\sum_{k=1}^{K}\sum_{g=1}^{B}\left(\beta_{kg}^{j}\times\left(w_{kg}^{j}\right)_{cor}\right).$$

Формування експертної групи (кількість експертів) обчислимо за формулою, яка запропонована в роботі [55; 72]:

$$K\geq 0{,}5\left(0{,}33/\beta+5\right), \tag{2.25}$$

де β – помилка результату експертного аналізу або допустима ймовірність помилки.

Узгодженість отриманих оцінок визначається відповідно до [72; 75]. Оцінюється індекс узгодженості оцінок експерта за виразом:

$$C_E=\frac{\lambda_{k_{\max}}-m}{m-1}, \tag{2.26}$$

де $\lambda_{k_{\max}}$ – максимальна власна кількість матриці парних порівнянь *k*-го експерта;

m – розмірність матриці парних порівнянь.

Оцінки експерта вважаються узгодженими, якщо відношення узгодженості $CR = C_E/CIS$, де CIS – середнє значення індексу узгодженості, який визначається в діапазонах (табл. 2.3).

Таблиця 2.3 – Значення CIS і CR від m

m	3	4	5	6	7	8	9	10	11	12
CIS	0,58	0,90	1,12	1,24	1,32	1,41	1,45	1,49	1,51	1,48
CR	$[0;0,05]$	$[0;0,08]$	$[0;0,1]$							

Неприйнятні оцінки повинні бути скоректовані експертом, в іншому випадку їх не слід враховувати при розрахунку результуючого вектора пріоритетів. Узгодженість думок групи експертів визначається за правилом трьох сігм. Неузгоджені оцінки не враховуються при розрахунку результуючого вектора пріоритетів $\overline{B} = \left(\overline{b_1}, \overline{b_2}, ..., \overline{b_m}\right)^T$, $\overline{b_i} = \sqrt[K]{\prod_{k=1}^{K} b_{ik}}$,

де $\overline{b_i}$ – результуючій пріоритет елементу x_i;

K – кількість експертів.

Думки експертів вважаються узгодженими, якщо все пріоритети b_{ik} лежать в інтервалі $\left(\overline{b_i} - 3\sigma_{gi}; \overline{b_i} + 3\sigma_{gi}\right)$, де σ_{gi} – геометричне стандартне відхилення вагового коефіцієнта b_{ik}, яке визначається за виразом:

$$\sigma_{gi} = e^{\left(\sqrt{\frac{1}{K}\sum_{k=1}^{K} \ln \frac{b_{ik}}{b_i}}\right)^2}$$

Довірчий інтервал δ_i визначається за формулою:

$$\delta_i = t_{cm} \times \sigma_{gi} / \sqrt{K}, \qquad (2.27)$$

де t_{cm}=0,95 – критерій Стьюдента.

Крок 2.6. Визначення зв’язку між джерелами загроз і елементами АБС:

$$A^{DF} = \left\| a_{ij}^{DF} \right\|. \quad (2.28)$$

Наступним етапом є визначення узагальненого показника рівня безпеки БІР на основі удосконаленої моделі оцінювання рівня захищеності БІР.

2.3.4. Удосконалення моделі оцінювання рівня захищеності банківських інформаційних ресурсів

Етап 3. Визначення узагальненого показника рівня захищеності БІР на основі удосконаленої моделі.

Визначення захищеності АБС від загроз ІБ, КБ, БІ на БІР пропонується здійснювати на основі удосконаленої моделі рівня захищеності банківських інформаційних ресурсів:

$$G_{OZ}^{ABS} = \begin{Bmatrix} \{I_A\}, \{O^{ABS}\}, \{DF^{ABS}\}, \{RR^{ABS}\}, \\ \{SZ^{ABS}\}, \{ROZ^{ABS}\}, \{UZ_r^{ABS}\} \end{Bmatrix}, \quad (2.29)$$

де $\{I_A\}$ – множина елементів інформаційних активів БІР;

$\{O^{ABS}\}$ – множина елементів ієрархії АБС;

$\{DF^{ABS}\}$ – множина джерел загроз безпеці АБС;

$\{RR^{ABS}\}$ – множина вимог регуляторів до безпеки БІР;

$\{SZ^{ABS}\}$ – множина можливих ТЗЗІ;

$\{ROZ^{ABS}\}$ – дані обліку про результати оцінки захищеності АБС;

$\{UZ_r^{ABS}\}$ – рівень захищеності АБС.

Крок 3.1. Визначення зв’язку між загрозами і ТЗЗІ:

$$A^{DFSZ} = \left\| a_{ij}^{DFSZ} \right\|, \quad (2.30)$$

при цьому $\forall j \in \{I_A\}$, а $\forall i \in \{DF_i\}$.

$$\left\| A^{DF} \right\| = \begin{cases} 1, \text{ якщо для } j\text{-го інформаційного актива існують } i \text{ загрози}, \\ 0, \text{ якщо для } j\text{-го інформаційного актива не існують } i \text{ загрози}. \end{cases} \quad (2.31)$$

Кожен механізм захисту БІР $SZ_i \in \{SZ^{ABS}\}$ характеризується вектором $SZ_i = (T_{SZ}, T_V, C_{SZ})$, де T_{SZ} – тип засобу захисту; T_V – час впровадження; C_{SZ} – вартість.

Для опису зв'язку між загрозами і ТЗЗІ використовується матриця:

$$A^{DFSZ} = \left\| a_{ij}^{DFSZ} \right\|, \tag{2.32}$$

де a_{ij}^{DFSZ} – відображає наявність зв'язку між *i*-ю загрозою порушення безпеки $DF_i \in \{DF^{ABS}\}$ і *j*-м ТЗЗІ $SZ_i \in \{SZ^{ABS}\}$.

У моделі використані такі типи зв'язку: *MZ* – є механізм захисту, що забезпечує протидію її деструктивному впливу $VH_i \in \{VH\}$; *NMZ* – немає механізму захисту для забезпечення протидії *i*-й загрозі.

При цьому $a_{ij}^{DFSZ} \in \{MZ, NMZ\}$, *MZ, NMZ* – наявність зв'язку певного типу між *i*-ю загрозою та *j*-м ТЗЗІ. Для елементів матриці значення визначаються за правилом:

$$\left\| a_{ij}^{DFSZ} \right\| = \begin{cases} MZ, \text{ якщо } i \text{ загроза роскривається } j\text{-м ТЗЗІ}, \\ NMZ, \text{ якщо } i \text{ загроза роскривається } j\text{-м ТЗЗІ}. \end{cases} \tag{2.33}$$

Якщо для всіх $i = m$ $a_{mj}^{DFSZ} = NMZ$, то робиться висновок що ТЗЗІ АБС не здатні захистити БІР від певного деструктивного впливу, а тому для підвищення рівня захищеності АБС необхідно залучати додаткові кошти на механізми захисту.

Крок 3.2. Визначення множини вимог регуляторів $\{RR^{ABS}\}$, яка складається з вимог до забезпечення безпеки БІР – $\{R_{BBI}\}$, зазначених у міжнародних і національних стандартах, множини оцінок ступеня виконання вимог безпеки $\{OV_{BBI}\}$ та множини підсумкового рівня відповідності безпеки БІР вимогам з множини $\{IU_{BBI}\}$:

$$\{RR^{ABS}\} = \{R_{BBI}\} \cup \{OV_{BBI}\} \cup \{IU_{BBI}\}. \tag{2.34}$$

Крок 3.3. Визначення узагальненого показника рівня захищеності АБС, який дозволяє оцінити рівень відповідності ТЗЗІ вимогам регулятора та визначається:

$$OPZ^{ABS} = \sum_{i=1}^{k} OPZ_i, \tag{2.35}$$

де k – кількість окремих показників безпеки;

OPZ_i –окремий показник набуває значення з множини:

OPZ_1 – відсутність неприпустимих ризиків, у разі якщо в ОБС при складанні моделі загроз / моделі зловмисника і оцінки ризиків (якщо виявлені неприпустимі за своїм рівнем ризики, то $OPZ_1 = 0$, в іншому випадку – $OPZ_1 = 1$); OPZ_2 – відсутність небезпечних загроз (якщо виявлені загрози "закриті" механізмами ТЗЗІ, то $OPZ_2 = 1$, у разі, якщо в ОБС при складанні моделі виявлені "незакриті" загрози – $OPZ_2 = 0$); OPZ_3 – рівень відповідності захищеності БІР вимогам регуляторів (якщо визнаний рекомендованим – $OPZ_3 = 1$, в разі, якщо визнано нерекомендованим – $OPZ_3 = 0$).

На підставі отриманих даних системі присвоюється один із трьох рівнів захищеності $UZ^{ABS} = \{\text{низький, середній, високий}\}$ відповідно до правила:

$$UZ^{ABS} = \begin{cases} \text{високий, якщо } OPZ^{ABS} = 3; \\ \text{середній, якщо } 1 \le OPZ^{ABS} \le 3; \\ \text{низький, якщо } OPZ^{ABS} = 0. \end{cases} \tag{2.36}$$

Отримана в результаті аудиту оцінка захищеності БІР дозволяє визначити найбільш цінні інформаційні активи БІР, ефективність використовуваних засобів для їх захисту, а також ступінь відповідності системи ТЗЗІ ОБС вимогам до захисту і рівнем захищеності регулятора, виявити найбільш уразливі місця і виробити рекомендації щодо підвищення, в разі необхідності, захищеності АБС ОБС.

Для оцінки економічної доцільності впровадження того чи іншого механізму ТЗЗІ в АБС ОБС залежно від цінності БІР в АБС введемо такі позначення:

V_{BIn}^{ABS} – цінність БІР для ОБС (сторони, що володіють інформацією, і намагаються її захистити), V_{BIn}^{IA} – цінність БІР для атакуючої сторони (яка намагається отримати інформацію);

SZ^{ABS} – засоби можливих ТЗЗІ;

$SV^{AS} = \left\{ SV^{ASIB}, SV^{ASBI}, SV^{ASKB} \right\}$ – засоби, що виділяються на отримання БІР;

SV^{ASIB} – засоби злому механізмів і ТЗЗІ ІБ в АБС; SV^{ASBI} – засоби злому механізмів і ТЗЗІ БІ в АБС; SV^{ASKB} – засоби злому механізмів і ТЗЗІ КБ:

$$SV^{AS} = \left\{ SV^{ASIB} \right\} \cap \left\{ SV^{ASBI} \right\} \cap \left\{ SV^{ASKB} \right\}. \quad (2.37)$$

Очевидним визнається факт, що безглуздо вкладати кошти в захист або отримання інформації більше, ніж цінність БІР:

$$SZ^{ABS} \le V_{BIn}^{ABS}, \; SV^{AS} \le V_{BIn}^{ABS}. \quad (2.38)$$

Припустимо, ймовірності визначаються за виразами:

$$p_{Z_j} = \frac{q_Z \times SZ^{ABS}}{q_Z \times SZ^{ABS} + q_V \times SV^{AS}}, \quad (2.39)$$

$$p_{V_j} = \frac{q_V \times SV^{AS}}{q_V \times SV^{AS} + q_Z \times SZ^{ABS}}, \quad (2.40)$$

де q_Z, q_V – вагові коефіцієнти, що визначають наскільки кожна зі сторін близька до мети;

P_{Vj} – ймовірність реалізації хоча б однієї *i*-ї загрози *j*-му активу (ймовірність успіху нападаючою стороною);

p_{Zj} – ймовірність захисту від *i*-ї загрози *j*-му активу (ймовірність успіху захищається стороною).

Припустимо, що сума засобів, виділених атакуючою стороною дорівнює цінності БІР, цінність БІР однакова для обох сторін, і протиборчі сторони знаходяться в рівних умовах, тоді економічна вартість витрат на захист БІР не повинна перевищувати:

$$SZ^{ABS} = V_{BIn}^{ABS} \times \frac{\sqrt{5}-1}{2}. \quad (2.41)$$

Ефективність запропонованої моделі оцінювання економічних витрат залежить від точності формулювання ймовірності успіху захисту і визначення цінності БІР.

2.4. Висновки до другого розділу

У другому розділі запропонована концепція, яка ґрунтується на синергетичному підході до вибору найбільш ефективних напрямків досягнення поставлених цілей безпеки БІР в АБС з урахуванням величини ризику на кожному рівні та забезпеченням дієвого контролю за виконанням функцій системи управління інформаційною безпекою організацій банківського сектору. У результаті цього отримані такі наукові та практичні результати:

1. Розроблено концепцію побудови синергетичної моделі загроз безпеки банківських інформаційних ресурсів, базис якої становить трирівнева модель стратегічного управління безпекою банківських інформаційних технологій. Концепція охоплює всі основні напрямки розвитку діяльності банку щодо безпеки банківських інформаційних ресурсів, ґрунтується на синергетичному підході до вибору найбільш ефективних напрямків досягнення цілей безпеки банківських інформаційних ресурсів на кожному з рівнів моделі управління стратегічним управлінням безпеки банківських інформаційних технологій з урахуванням величини ризику на кожному рівні та забезпеченням дієвого контролю за виконанням функцій системи управління інформаційною безпекою організацій банківського сектору.

2. Удосконалено класифікатор загроз безпеці банківських інформаційних ресурсів, який, на відміну від існуючих, ґрунтується на синергетичній моделі загроз, що дозволяє класифікувати загрози за складовими безпеки, видами послуг та рівнями ієрархії інфраструктури автоматизованих банківських систем, оцінювати синергію та гібридність загроз інформаційній безпеці, кібербезпеці, безпеці інформації, ймовірність їх впливу на безпеку банківських інформаційних ресурсів. Розроблено

програмний засіб, що реалізує удосконалений класифікатор. Практична реалізація класифікатора дозволяє в он-лайн режимі формувати експертну оцінку рівня загроз банківських інформаційних ресурсів, аналізувати їх синергію та гібридність, оцінювати ймовірність впливу загроз інформаційній безпеці, кібербезпеці, безпеці інформації на безпеку банківських інформаційних ресурсів без значних витрат інвестицій та людських ресурсів (електронний доступ до ресурсу: http://skl.hneu.edu.ua/).

3. Вперше розроблено метод оцінювання узагальненого показника рівня захищеності банківських інформаційних ресурсів. Розроблено практичну методику для оцінювання рівня захищеності банківських інформаційних ресурсів на основі синергетичної моделі загроз, удосконалених класифікатора загроз та моделі зловмисника, моделі оцінки захищеності банківських інформаційних ресурсів та моделі інфраструктури автоматизованих банківських систем, що дозволяє оптимізувати витрати коштів на побудову системи безпеки банківських інформаційних ресурсів.

Практична значимість полягає у можливості своєчасного оцінювання взаємозв'язків між активами банківських інформаційних ресурсів, елементами інфраструктури, технічними засобами захисту автоматизованих банківських систем і можливими проявами загроз інформаційній безпеці, кібербезпеці та безпеці інформації, що дозволяє своєчасно корегувати керівні документи банку з інформаційної безпеки, планувати інвестування в технічні засоби захисту інформації, формувати превентивні заходи для недопущення реалізації загроз.

Список використаних джерел у другому розділі

1. R. Hryshchuk, and S. Yevseiev, "The synergetic approach for providing bank information security: the problem formulation", *Науково-технычний журнал "Безпека інформації"*, № 22 (1), с. 64 – 74. 2016.

2. Р. В. Грищук, та Ю. Г. Даник; за заг. ред. проф. Ю. Г. Даника, *"Основи кібербезпеки"*, Житомир : ЖНАЕУ, 2016.

3. L. Sun, R. P. Srivastava, and T. J. Mock, "An Information Systems Security

Risk Assessment Model under Dempster-Shafer Theory of Belief Functions", *Journal of Management Information Systems*, Vol. 22, p.3 – 28, 2006.

4. А. В. Потий, та Д. Ю. Пилипенко, "Концепция стратегического управления информационной безопасностью", *Радіоелектронні і комп'ютерні системи*, № 6 (47), с. 53 – 58, 2010.

5. А. В. Потий, та Д. Ю. Пилипенко, "Классификация показателей безопасности информации", *Системи обробки інформації*, Вип. 3(84), с.53 –56. 2010.

6. И. Д. Горбенко, А. В. Потий, и П. И. Терещенко, "Критерии и методология оценки безопасности информационных технологий", [Електронний ресурс]. Доступно: http://www.bezpeka.com/ru/lib/spec/infsys/art108.html. Дата звернення: Груд. 7.2017.

7. Trusted Computer Systems Evaluation criteria, US DoD 5200.28-STD, 1985. [Online]. Available: https://csrc.nist.gov/csrc/media/publications/conference-paper/1998/10/08/proceedings-of-the-21st-nissc-1998/documents/early-cs-papers/dod85.pdf. . Accessed on: Dec. 7.2017.

8. Information Technology Security Evaluation Criteria, v. 1.2. Office for Official publications of the European Communities, 1991. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/ITSicherheitskriterien/itsec-en_pdf.pdf?__blob=publicationFile. Accessed on: Dec. 7.2017.

9. Canadian Trusted Computer Product Evaluation Criteria, v. 3.0. Canadian System Security Centre, Communications Security Establishment, Government of Canada, 1993. [Online]. Available: http://www.btb.termiumplus.gc.ca/tpv2alpha/alpha-eng.html?lang=eng&i=&index=alt&srchtxt=CANADIAN%20TRUSTED%20COMPUTER%20PRODUCT%20EVALUATION%20CRITERIA. Accessed on: Dec. 7.2017.

10. Federal Criteria for Information Technology security. – NIST, NSA, US Government, 1993. [Online]. Available: https://www.commoncriteriaportal.org/files/ccfiles/ccpart1v2.3.pdf. Accessed on: Dec. 7.2017.

11. ISO/IEC 15408-1:1999 – Information technology – Security techniques – Evaluation criteria for IT security – Part1: Introduction and general model. [Online]. Available: https://www.iso.org/ru/standard/27632.html. Accessed on: Dec. 7.2017.

12. ISO/IEC 15408-2:2005– Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional requirements. [Online]. Available: https://www.iso.org/ru/standard/40613.html. Accessed on: Dec. 7.2017.

13. ISO/IEC 15408-3:2008 – Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance requirements. [Online]. Available: https://www.iso.org/ru/standard/46413.html. Accessed on: Dec. 7.2017.

14. ДСТУ ISO/IEC TR 13335-1:2003 Інформаційні технології. Настанови з керування безпекою інформаційних технологій. Частина 1. Концепції та моделі безпеки інформаційних технологій. [Электронный ресурс]. Доступно: http://lindex.net.ua/ua/shop/bibl/500/doc/11423.

15. ДСТУ ISO/IEC TR 13335-2:2003 Інформаційні технології. Частина 2. Настанови з керування безпекою інформаційних технологій. [Электронный ресурс]. Доступно: http://www.premier-hs.com.ua/ru/content/dstu-isoiec-tr-13335-22003-nastanovi-z-kieruvannia-biezpiekoiu-informatsiinikh-tiekhnologhii. Дата звернення: Груд. 7.2017.

16. ДСТУ ISO/IEC TR 13335-3:2003 Інформаційні технології. Настанови з керування безпекою інформаційних технологій. Частина 3. Методи керування захистом інформаційних технологій. [Электронный ресурс]. Доступно: http://lindex.net.ua/ua/shop/bibl/500/doc/11425. Дата звернення: Груд. 7.2017.

17. ДСТУ ISO/IEC TR 13335-4:2005 Інформаційні технології. Настанови з управління безпекою інформаційних технологій. Частина 4. Вибирання засобів захисту. [Электронный ресурс]. Доступно: http://metrology.com.ua/download/iso-iec-ohsas-i-dr/61-iso/290-dstu-iso-iec-tr-13335-4-2005. Дата звернення: Груд. 7.2017.

18. ДСТУ ISO/IEC TR 13335-5:2005 Інформаційні технології. Настанови з управління безпекою інформаційних технологій. Частина 5. Настанова з управління мережною безпекою. [Электронный ресурс]. доступно: http://lindex.net.ua/ua/shop/bibl/500/doc/11427. Дата звернення: Груд. 7.2017.

19. ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements. [Online]. Available: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54534. Accessed on: Dec. 7.2017.

20. ISO/IEC 27002:2013 – Information technology – Security techniques – Code

of practice for information security controls. [[Online]. Available: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54533. Accessed on: Dec. 7.2017.

21. ISO/IEC 27006:2015 – Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems [Online]. Available: http://www.iso.org/iso/home/search.htm?qt=ISO%2FIEC+27006%3A2015+&sort=rel&type=simple&published=on. Accessed on: Dec. 7.2017.

22. Стандарт України СОУ Н НБУ 65.1 СУІБ 1.0:2010. Методи захисту в банківській діяльності. Система управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2005, MOD). [Электронный ресурс]. Доступно: https://kyianyn.files.wordpress.com/2010/12/nbu-27001.pdf. Дата звернення: Груд. 7.2017.

23. Стандарт України СОУ Н НБУ 65.1 СУІБ 1.0:2010. Інформаційні технології. Методи захисту. Звід правил для управління інформаційною безпекою (ISO/IEC 27002:2005, MOD) [Электронный ресурс]. Доступно: http://s-byte.com/useful/27002.pdf. Дата звернення: Груд. 7.2017.

24. CEM-97/017. Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and general model.

25. Д. П. Зегжда, и А. М. Ивашко, *Как построить защищенную информационную систему*, СПб: Мир и семья - 95, 1997.

26. *Методичні рекомендації щодо впровадження системи управління інформаційною безпекою та методики оцінки ризиків відповідно до стандартів Національного банку України*: лист департаменту інформатизації Національного банку України банкам України від 03 березня 2011 р. № 24-112/365. – К.: Національний банк України, 2011.

27. О. В. Потій, та А. В. Лєншин, “Дослідження методів оцінки ризиків безпеці інформації та розробка пропозицій з їх вдосконалення на основі системного підходу”, *Збірник наукових праць ХУПС*, Вип. 2(24), с.85 – 91. 2010.

28. ISO/IEC 27005 – Information technology – Security techniques – Information security risk management [Online]. Available:

http://www.bank.gov.ua/doccatalog/document?id=72235https://exebit.files.wordpress.com/2013/11/iso-27005-2011-ru-v1.pdf. Accessed on: Des. 09, 2017.

29. Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. ГОСТ Р ИСО/МЭК 15408-2-2008, [Електронний ресурс]. Доступно: http://primorsky.ru/authorities/executive-agencies/departments/information-security/Documents/doki-po-ib/. Дата звернення: Груд. 7.2017.

30. М. Кобзарь, и А. Сидак, "Методология оценки безопасности информационных технологий по общим критериям", *Информационный бюлетень Jet Info*, Вып. 6(133), с.2 – 16, 2004.

31. Руководящий документ. Безопасность информационных технологий. Общая методология оценки безопасности информационных технологий. Проект [Електронний ресурс]. Доступно: http://fstec.ru/component/attachments/download/293. Дата звернення: Груд. 7.2017.

32. РС БР ИББС-2.2-2009. Методика оценки рисков нарушения информационной безопасности. [Електронний ресурс]. Доступно: http://www.cbr.ru/credit/gubzi_docs/st22_09.pdf. Дата звернення: Груд. 7.2017.

33. Стандарт України СОУ Н НБУ 65.1 СУІБ 1.0:2010. Методи захисту в банківській діяльності система управління інформаційною безпекою. Вимоги. (ISO/IEC 27001:2005, MOD). К: НБУ., 2010.

34. Постанова Правління Національного банку України від 18 червня 2003 року № 254 " Про затвердження Положення про організацію операційної діяльності в банках України", К: НБУ., 2003.

35. Доктрина інформаційної безпеки України, затверджено Указом Президента України від 25 лютого 2017 року № 47/2017. [Електронний ресурс]. Доступно: http://zakon3.rada.gov.ua/laws/show/47/2017/paran2#n2. Дата звернення: Груд. 7.2017.

36. Указ Президента України від 15 березня 2016 року № 96 "Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України". [Електронний ресурс]. Доступно:

http://zakon3.rada.gov.ua/laws/show/96/2016/paran11#n11. Дата звернення: Груд. 7.2017.

37. Указ Президента України від 12 лютого 2007 року № 105 “Про Стратегію національної безпеки України”. [Електронний ресурс]. Доступно: http://zakon3.rada.gov.ua/laws/show/105/2007. Дата звернення: Груд. 7.2017.

38. Р. В. Грищук, та Ю. Г. Даник, “Синергія інформаційних та кібернетичних дій”, *Труди університету. НУОУ*, № 6 (127), с. 132–143. 2014.

39. В. Л. Бурячок, Р. В. Грищук, та В. О. Хорошко, під заг. ред. проф. В. О. Хорошка, *“Політика інформаційної безпеки”*, ПВП «Задруга»,. 2014.

40. Ю. Г. Даник та ін., “*Основи захисту інформації*” навч. пос., Житомир : ЖВІ ДУТ, 2015.

41. О. К. Юдін “*Інформаційна безпека. Нормативно-правове забезпечення*”, К. : НАУ, 2011.

42. І. С. Іванченко, В. О. Хорошко, Ю. Е.Хохлачова, та Д. В. Чирков під заг. ред. проф. В. О. Хорошка, *“Забезпечення інформаційної безпеки держави”*, К: ПВП “Задруга”, 2013.

43. О. Г. Корченко, О. Є. Архипов, та Ю. О. Дрейс, *“Оцінювання шкоди національній безпеці України у разі витоку державної таємниці”*, монографія, К: наук.-вид.центр НА СБУ України, 2014.

44. А. О. Корченко, Л. М. Скачек, та В. О. Хорошко, під заг. ред. проф. В. О. Хорошка, *“Банківська безпека”* підручник, К: ПВП “Задруга”, 2014.

45. В. И. Ярочкин, *“Безопасность банковских систем”*, М.: Издательство: Ось-89, 416 с., 2012.

46. С. Евсеев, “Методология оценивания безопасности информационных технологий автоматизированных банковских систем Украины”, *Науково-технічний журнал “Захист інформації”*, том. 22, № 2, с. 297 – 309, 2016.

47. С. Евсеев, “Модель нарушителя прав доступа в автоматизированной банковской системе на основе синергетического подхода”, *Науково-технічний журнал “Інформаційна безпека”*, № 2 (26), с. 110 – 120, 2017.

48. С. Евсеев, “Синергетическая модель оценки безопасности банковской информации”, *Науково-технічний журнал “Інформаційна безпека”,* № 4 (24), с. 104 – 118, 2016.

49. Банк данных угроз безопасности информации. [Электроний ресурс]. Доступно : http://bdu.fstec.ru/vul. Дата обращения: Декабрь, 5.2017

50. Р. Грищук, та С. Євсеєв, “Методологія побудови системи забезпечення інформаційної безпеки банківської інформації в автоматизованих банківських системах”, Науково-технічний журнал “Безпека інформації”, том 23, № 3, с. 204 – 214, 2017.

51. О. К. Юдін, С. С. Бучик, А. В. Чунарьова, та О. І. Варченко, “Методологія побудови класифікатора загроз державним інформаційним ресурсам”, *Наукоємні технології*, № 2 (22), с. 200 – 210, 2014.

52. О. К. Юдін, та С. С. Бучик, “Класифікація загроз державним інформаційним ресурсам нормативно-правового спрямування. Методологія побудови класифікатора”, *Захист інформації*, Том 17 (2), с. 108 – 116, 2015.

53. С. С. Бучик, “Теоретичні основи аналізу ризиків дерева ідентифікаторів державних інформаційних ресурсів”, *Наукоємні технології*, № 1 (29), с. 70 – 77. 2016.

54. С. С. Бучик, “Методологія аналізу ризиків дерева ідентифікаторів державних інформаційних ресурсів”, *Захист інформації*, №1 (18 , с. 81 – 89, 2016.

55. С. С. Бучик, “Методика експертного оцінювання функціональних профілів загроз державних інформаційних ресурсів”, *Открытые информационные и компьютерные интегрированные технологии*, № 70, с. 271 – 280, 2015.

56. Р. В Грищук, *Теоретичні основи моделювання процесів нападу на інформацію методами теорій диференціальних ігор та диференціальних* перетворень, Житомир : Рута, 2010.

57. О. Петров, и В. Лахно, “Повышение информационной безопасности автоматизированных ситсем обработки данных на транспорте”, *Information Technology in Selected Areas of Management. – Widawnictwa AGH,* Krakow, pp. 65 – 78, 2016.

58. Р. М. Хмелевський, “Дослідження оцінки загроз інформаційній безпеці об’єктів інформаційної діяльності”, *Сучасний захист інформації*, №4, с. 65 – 70, 2016.

59. В. Г. Жуков, М. Н. Жукова, В. В. Золотарев, и И. В. Ковалев, “Методика построения модели безопасности автоматизированных систем”, *Программные продукты и системы*, № 2, с. 70 – 74, 2012.

60. В. Г. Жуков, М. Н. Жукова, и А. П. Стефаров, “Модель нарушителя прав доступа в автоматизированной системе”, *Программные продукты и системы*, № 2, с. 75 – 78. 2012.

61. М. Н. Жукова, и Н. А. Коромыслов, “Модель оценки защищенности автоматизированной системы с применением аппарата нечеткой логики”, *Известия ЮФУ. Технические науки*, № 12 (149), с. 63 – 69, 2013.

62. С. В. Мельник, “Концептуальні основи організації криптографічного захисту інформації”, *Наукові записки Українського науково-дослідного інституту зв’язку*, № 6, с. 19 – 26, 2015.

63. А. Потий, “Эталонная модель системы процессов защиты информации”, *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні : науково-технічний збірник*, Вип. 1(12), с. 17 – 30, 2006.

64. О. Потій, А. Лєншин, “Методика оцінки відповідності поточної зрілості цільовим орієнтирам”, *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні : науково-технічний збірник*, Вип. 1(12), с. 31 – 43, 2006.

65. А. В. Даурцев, “Разработка математических моделей оценки показателей эффективности программных систем защиты информации в автоматизированных системах электронного документооборота”. [Электронный ресурс]. Доступно: http://cyberleninka.ru/article/n/razrabotka-matematicheskih-modeley-otsenki-pokazateley-effektivnosti-programmnyh-sistem-zaschity-informatsii-v-avtomatizirovannyh. Дата обращения: Декабрь, 5.2017.

66. В. В. Карпов, “Вероятностная модель оценки защищенности средств вычислительной техники с аппаратно-программным комплексом защиты информации от несанкционированного доступа”, *Программные продукты и системы*, № 1, с. 31 – 36, 2003.

67. П. Н. Девянин, *Модели безопасности компьютерных систем: Учеб. пособие*. М. : Изд.центр «Академия», 2005.

68. Н. А. Гайдамакин, *Теоретические основы компьютерной безопасности*. - Екатеринбург: изд-во Урал. Ун-та, 2008.

69. П. В. Ревенков, “Защита информации в банке: основные угрозы и борьба с ними”, [Электронный ресурс]. Доступно: http://www.crmdaily.ru/novosti-rynka-crm/568-zashhita-informacii-v-banke-osnovnye-ugrozy-i-borba-s-nimi.html. Дата обращения: Декабрь, 5.2017.

70. В. С. Аткина, “Модель защищенности организаций банковской системы Российской Федерации”, *Известия ЮФУ. Технические науки*, Вып. 12 (149), с .187 – 193, 2013.

71. ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cybersecurity [Online]. Available: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=44375. Accessed on: Des. 09, 2017.

72. Р. А. Нурдинов, и Т. Н. Батова, “Подходы и методы обоснования целесообразности выбора средств защиты информации”, *Современные проблемы науки и образования.* [Электронный ресурс]. Доступно: http://elibrary.ru/item.asp?id=21285749. Дата обращения: Дек. 7, 2017.

73. РС БС ИББС – 2.2-2009. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки рисков нарушения информационной безопасности, [Электронный ресурс]. –Доступно: www.cbr.ru/credit/gubzi_docs/st22_09.pdf. Дата обращения: Дек. 7, 2017.

74. Ю. Ф. Каторин, Р. А. Нурдинов, и Н. М. Зайцева, “Модель количественной оценки рисков безопасности информационной системы”, [Электронный ресурс]. Доступно: http://www.vestnikmnk/index.php/VMK/article/download/57/56. Дата обращения: Дек. 7, 2017.

75. ISO/IEC 18045:2014 Information technology – Security techniques – Guidelines for cybersecurity [Online]. Available: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=46412. Accessed on: Des. 09, 2017.

76. Д. Домарєв, В. Домарєв та С. Прокопенко, “Методика оцінювання захищеності інформаційних систем за допомогою СУІБ “Матриця”, *Захист інформації*, том 15, №1, с. 80 – 86, 2013.

77. С. В. Павленко, “Метод оцінки захищеності інформаційних систем”, *Системи озброєння і військова техніка*, № 4(20), с. 149 – 154, 2009.

РОЗДІЛ 3
РОЗРОБЛЕННЯ ПІДХОДУ ДО ЗАБЕЗПЕЧЕННЯ ПОСЛУГ БЕЗПЕКИ БАНКІВСЬКИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ НА ГІБРІДНИХ КРИПТО-КОДОВИХ КОНСТРУКЦІЯХ ЗІ ЗБИТКОВИМИ КОДАМИ

3.1. Встановлення властивостей крипто-кодових систем на алгеброгеометричних кодах

Основна перевага симетричних і несиметричних теоретико-кодових схем (ТКС) полягає у високій швидкості перетворення інформації та інтегрованому забезпеченні достовірності та інформаційної прихованості (конфіденційності), що задовольняє основним вимогам безпеки БІР. Загальна класифікація методів криптоперетворення БІР наведена на рис. 3.1.

Рисунок 3.1 – Загальна класифікація методів криптоперетворення БІР

Для забезпечення безпеки БІР перспективним напрямком є використання несиметричних криптосистем на основі ТКС Мак-Еліса і Нідеррайтера, що інтегровано (одним механізмом) забезпечують показники достовірності на рівні 2^9 – 2^{12} і криптостійкості – 2^{30} – 2^{35} групових операцій при її побудові над полем $GF(2^{10})$. На рис. 3.2 наведені результати досліджень швидкодії криптоперетворень сучасними симетричними і несиметричними криптосистемами. У табл. 3.1 наведені результати порівняльних досліджень ефективності криптографічних методів

захисту інформації при фіксованому рівні стійкості:

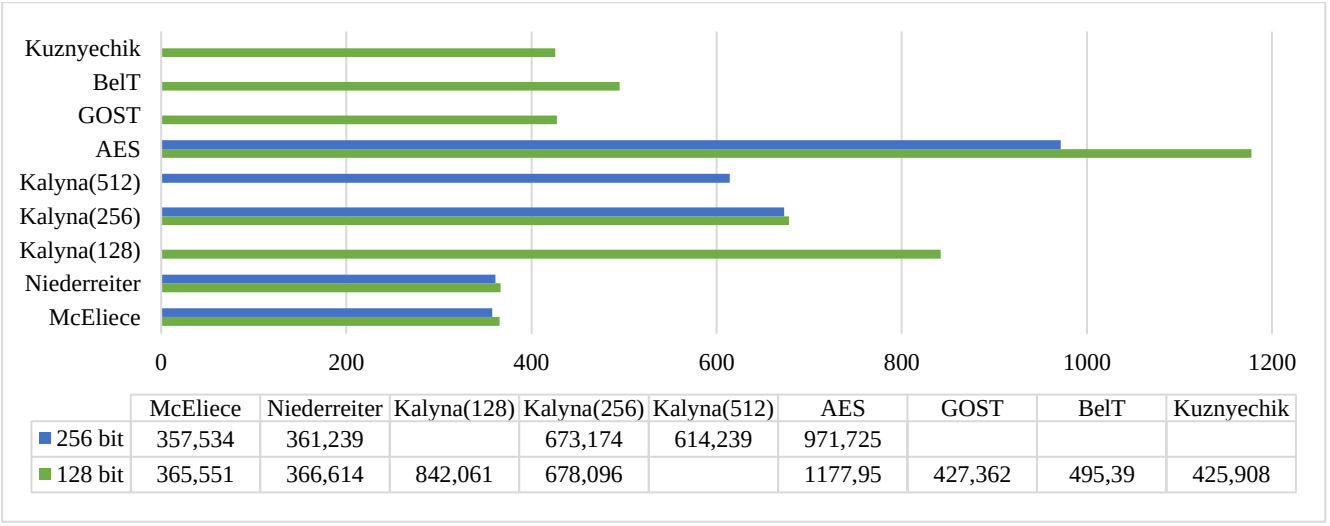
– середньому (складність криптоаналізу найкращим відомим алгоритмом не менше 2^{128} операцій);

– високому (складність криптоаналізу найкращим відомим алгоритмом не менше 2^{256} операцій);

– надвисокому (складність криптоаналізу найкращим відомим алгоритмом не менше 2^{512} операцій).

Таблиця 3.1 – Результати порівняльних досліджень ефективності криптографічних методів захисту інформації при фіксованому рівні стійкості

Методи криптографічного перетворення	Модель безпеки	Довжина ключових даних, біт	Швидкість криптоперет-ворень, біт / с	Додаткові функції
Блокові симетричні шифри	Практична безпека	128, 256, 512	$10^6 – 10^9$	Немає
Потокові симетричні шифри	Практична безпека	128, 256, 512	$10^7 – 10^{10}$	Немає
Несиметричні RSA-подібні криптоалгоритми	Доказова безпека	3248 (128), 15424 (256)	$10^2 – 10^3$	Немає
Несиметричні ККС з використанням кодових конструкцій	Доказова безпека	$0{,}5 \cdot 10^6$ (128), $2 \cdot 10^6$ (256)	$10^6 – 10^8$	Контроль по-милок, під-вищення дос-товірності



	McEliece	Niederreiter	Kalyna(128)	Kalyna(256)	Kalyna(512)	AES	GOST	BelT	Kuznyechik
256 bit	357,534	361,239		673,174	614,239	971,725			
128 bit	365,551	366,614	842,061	678,096		1177,95	427,362	495,39	425,908

Рисунок 3.2 – Результати аналізу швидкодії перетворення інформації

Таким чином, як випливає з наведених результатів порівняльного аналізу (рис. 3.2 та табл. 3.1) несиметричні криптоалгоритми з використанням ТКС

дозволяють реалізувати криптографічний захист інформації за технологією відкритих ключів і забезпечити при цьому швидкість крипто-кодового перетворення інформації зі швидкістю шифрування БСШ. Крім того, практичне використання несиметричних крипто-кодових систем (НККС) захисту інформації дозволяє на основі інтеграції механізмів канального кодування і шифрування комплексно забезпечити безпеку і достовірність даних.

Розглянемо загальну конструкцію ТКС. Зафіксуємо кінцеве поле $GF(q)$. Розглянемо векторний простір $GF^n(q)$ як множину n- послідовності елементів з $GF(q)$ з покомпонентним додаванням і множенням на скаляр. *Лінійний (n, k, d) код C* – це підпростір в $GF^n(q)$, тобто непорожня множина n-послідовності (*кодових слів*) над $GF(q)$, k – *розмірність* лінійного підпростору, d – *мінімальна кодова відстань* (мінімальна вага ненульового кодового слова) [1].

Лінійне підпростір, що ототожнює код C, має ортогональне доповнення, базис якого задається перевірочною матрицею H коду C, тобто матрицею рангу $rank(H) = r$, $r = n - k$. Розмірність перевірочної матриці $r \times n$, причому $G \times H^T = 0$. Якщо розглядати матрицю H як набір базисних векторів деякого лінійного підпростору, отримаємо лінійний код $C^{\perp}$, званий дуальним до C. Довільна n-послідовність c є кодовим словом коду C тоді, якщо вона ортогональна кожному рядку перевірочної матриці H, тобто $c \times H^T = 0$. Вектор S, званий в теорії кодування *синдромом*, може бути обчислений множенням кодового слова з помилками $c^* = c + e$ на транспоновану перевірочну матрицю H коду: $S = c^* \times H^T = c \times H^T + e \times H^T = e \times H^T$, де e – вектор помилок, c^* – спотворене помилками кодове слово.

Очевидно, значення синдрому залежить тільки від вектора помилок і не залежить від кодового слова [1].

Алгеброгеометричні коди мають гарні асимптотичні властивості. При зростанні потужності алфавіту кодових символів асимптотичні властивості таких кодів поліпшуються. Очевидно, що при великій довжині ці коди лежать вище межі Варшамова – Гілберта, що свідчить про високі потенційні характеристиках цих кодів [1; 2]. Таким чином, кодування на алгеброгеометричних кодах забезпечує підвищення достовірності БІР і є одним з перспективних напрямків. Найбільший енергетичний

ефект від завадостійкого кодування досягається при використанні кодів великої довжини [1; 2; 33; 34; 35; 36; 37]. Довжина алгеброгеометричного коду визначається кількістю точок проективної кривої, за якою будується код [1; 4; 15; 23; 29].

Нехай $X(GF(q))$ – множина точок кривої X над кінцевим полем $GF(q)$, $N = |X(GF(q))|$ – їх кількість. Кількість N точок кривої X над $GF(q)$ обмежена зверху виразом Хасе–Вейля [1; 2; 41; 42; 43]:

$$N \le 2\sqrt{q} \cdot g + q + 1, \tag{3.1}$$

де g – рід кривої.

Зафіксуємо кінцеве поле $GF(q)$. Нехай X – гладка проективна алгебраїчна крива в проектному просторі P^n, тобто сукупність рішень $p_1(x_0, x_1, ..., x_n)$, $p_2(x_0, x_1, ..., x_n)$, …, $p_N(x_0, x_1, ..., x_n)$, $\forall\ p\ \in P^n$ системи однорідних незвідних алгебраїчних рівнянь ступеня *degX* з коефіцієнтами з $GF(q)$ [1; 2].

У табл. 3.2 наведена верхня оцінка роду g кривої X.

Таблиця 3.2 – Верхня оцінка роду g кривої X в P^n

deg X	$g(P^2)$	$g(P^3)$	$g(P^4)$	$g(P^5)$	$g(P^6)$
2	0	–	–	–	–
3	1	0	–	–	–
4	3	1	0	–	–
5	6	2	1	0	–
6	10	4	2	1	0
7	15	6	3	2	1
8	21	9	5	3	2
9	28	12	7	4	3
10	36	16	9	6	4

У табл. 3.3 наведена верхня оцінка кількості точок кривої над кінцевим полем.

Таблиця 3.3 – Оцінка верхньої межі кількості точок гладкої проективної кривої

g	$deg\ X$	$N = \lvert X(GF(q)) \rvert$				
		$GF(4)$	$GF(8)$	$GF(16)$	$GF(32)$	$GF(64)$
0	2	5	9	17	33	65
1	3	9	14	25	44	81
2	4	10	18	33	53	97
3	4	17	24	41	66	113
4	5	21	29	49	77	129
5	5		34	57	88	145
6	5		39	65	99	164
7	6		44	73	110	180
8	6		49	81	121	196
9	6		54	89	132	212
10	6		59	97	143	228
11	7		64	105	154	244
12	7		69	113	165	260
13	7			121	176	276
14	7			129	187	292
15	7			137	198	308

Загальна схема алгеброгеометричного кодування вперше запропонована в [44]. Нехай C – клас дивізорів на X ступені α. Тоді C задає відображення $\varphi : X \to P^m$, набір генераторних функцій $y_i = \varphi(x_i)$ задає алгеброгеометричний код довжиною $n \le N$. Кодові характеристики (n,k,d) пов'язані співвідношенням $k + d \ge n - g + 1$. Якщо $2g - 2 < \alpha \le n$, код пов'язаний характеристиками $(n,\alpha - g + 1,d), d \ge n - \alpha$.

Дамо наступне визначення алгеброгеометричного коду.

Властивість 1 [1; 2]. Нехай X – гладка проективна алгебраїчна крива в проектному просторі P^n, тобто сукупність рішень однорідного незвідного алгебраїчного рівняння ступеня $degX$ з коефіцієнтами з $GF(q)$. Розглянемо різноманіття, що відповідають проективним гіперплощинам, заданим в P^n рівняннями $F = 0$, де F – однорідні одночлени ступеня $degF$. Нехай $I(i_1, i_2, ..., i_n)$ –

інформаційна послідовність. Алгеброгеометричний код по кривій X над $GF(q)$ – *лінійний код* довжини $n \le N$, кодові слова $C(c_1, c_2, ..., c_n)$ якого задаються рівністю:

$$\sum_{i=0}^{k-1} i_j F_j(P_i) = c_i \,, \tag{3.2}$$

де $P_i(X_i, Y_i, Z_i)$ – проективні точки кривої X, тобто (X_i, Y_i, Z_i) – рішення однорідного алгебраїчного рівняння, що задають криву X, $i = \overline{1,n}$; $F_j(P_i)$ – значення генераторних функцій в точках кривої.

Це визначення рівносильне матричному поданню алгеброгеометричного коду [1; 2]:

$$G(i_0, i_1, ..., i_{k-1})^T = (c_0, c_1, ..., c_{n-1}),$$

де G – породжувальна матриця розмірності $k \times n$, $k = \alpha - g + 1$, $\alpha = degX \cdot degF$ виду

$$G = \begin{pmatrix} F_0(P_0) & F_0(P_1) & ... & F_0(P_{n-1}) \\ F_1(P_0) & F_1(P_1) & ... & F_1(P_{n-1}) \\ ... & ... & ... & ... \\ F_{k-1}(P_0) & F_{k-1}(P_1) & ... & F_{k-1}(P_{n-1}) \end{pmatrix} = \left\| F_j(P_i) \right\|_{n,k}. \tag{3.3}$$

Властивість 2 [1; 2]. Еліптичною кривою (EC) в афінному просторі A^2 над полем $GF(q)$ називається гладка крива, задана рівнянням

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{3.4}$$

або в P^2 задана однорідним рівнянням

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz + a_6z^3, \tag{3.5}$$

$a_i \in GF(q)$, рід кривої $g = 1$.

Твердження 1 [1; 2]. *Алгеброгеометричний (n, k, d) код* за еліптичною кривою (еліптичний код) над $GF(q)$ побудований через відображення вигляду $\varphi: EC \to P^{k-1}$ пов'язаний характеристиками $k + d \ge n$, причому: $n \le 2\sqrt{q} + q + 1$, $k \ge \alpha$, $d \ge n - \alpha$, $\alpha = 3 \cdot degF$.

Доведення. Нехай EC – гладка проективна еліптична крива в проективному просторі P^2 над $GF(q)$, $g = g(EC) = 1$, $EC(GF(q))$ – множина її точок над $GF(q)$;

$N = EC(GF(q))$ – їх кількість. За теоремою Хасе–Вейля кількість точок гладкої проективної кривої роду g в P^2 над $GF(q)$ обмежена зверху виразом $N \le 2g\sqrt{q} + q + 1$. Для еліптичної кривої цей вираз матиме вигляд $N \le 2\sqrt{q} + q + 1$. За визначенням $n \le N$, відповідно $n \le 2\sqrt{q} + q + 1$.

Нехай C – клас дивізорів на EC степені $\alpha > 0$. Тоді C визначає відображення $\varphi: X \to P^{k-1}$, де $k \ge \alpha$. Набор $y_i = \varphi(x_i)$ задає код. Кількість точок в перетині $\varphi(EC)$ з гіперплощиною дорівнює α, тобто $n - d \le \alpha$. Отже, параметри алгеброгеометричного коду за еліптичною кривою пов'язаний співвідношенням $k + d \ge n$, причому $d \ge n - \alpha$. Ступінь $degEC = 3$, відповідно, $\alpha = 3 \cdot degF$. □

Властивість 3. [1; 2]. Нехай X – гладка проективна алгебраїчна крива в P^n, тобто сукупність рішень однорідного незвідного алгебраїчного рівняння ступеня $degX$ з коефіцієнтами з $GF(q)$, F – однорідні одночлени ступеня $degF$. Алгеброгеометричний код за кривою X над $GF(q)$ – це лінійний код, що складається з усіх слів $(c_1, c_2, ..., c_n)$ довжини $n \le N$, для яких виконується рівність $d + g - 1$ рівнянь:

$$\sum_{i=0}^{n-1} c_i F_j(P_i) = 0, \tag{3.6}$$

де $c_i \in GF(q)$; $d \ge \alpha - 2g + 2$; $\alpha = degX \cdot degF$.

Це визначення рівносильне матричному поданню алгеброгеометричного коду:

$$H(c_0, c_1, ..., c_{n-1})^T = 0,$$

де H – перевірочна матриця коду розмірності $r \times n$, $r = n - k = d + g - 2$.

$$H = \begin{pmatrix} F_0(P_0) & F_0(P_1) & \dots & F_0(P_{n-1}) \\ F_1(P_0) & F_1(P_1) & \dots & F_1(P_{n-1}) \\ \dots & \dots & \dots & \dots \\ F_{r-1}(P_0) & F_{r-1}(P_1) & \dots & F_{r-1}(P_{n-1}) \end{pmatrix} = \left\| F_j(P_i) \right\|_{n,r}. \tag{3.7}$$

Твердження 2. [1; 2]. Еліптичний (n, k, d) код над $GF(q)$, побудований через відображення виду $\varphi: EC \to P^{r-1}$ пов'язаний характеристиками $k + d \ge n$, причому: $n \le 2\sqrt{q} + q + 1$, $k \ge n - \alpha$, $d \ge \alpha$, $\alpha = 3 \cdot degF$.

Конструктивні характеристики еліптичних кодів, побудованих через відображення вигляду $\varphi: EC \to P^{k-1}$ над $GF(q)$, $q = 2^m$, $m = \overline{2,6}$ наведені в табл. 3.4. Вихідні дані побудови алгеброгеометричних кодів (АГК) (модифікованих АГК наведені у додатку Б).

Таблиця 3.4 – Конструктивні кодові характеристики еліптичних кодів, побудованих через відображення $\varphi: EC \to P^{k-1}$ над $GF(q)$, $q = 2^m$, $m = \overline{2,6}$

degF	α	*(n, k, d)*				
		GF(4)	*GF(8)*	*GF(16)*	*GF(32)*	*GF(64)*
1	2	3	4	5	6	7
1	3	9, 3, 6	14, 3, 11	25, 3, 22	44, 3, 41	81, 3, 78
2	6	9, 6, 3	14, 6, 8	25, 6, 19	44, 6, 38	81, 6, 75
3	9	–	14, 9, 5	25, 9, 16	44, 9, 35	81, 9, 72
4	12	–	14, 12, 2	25, 12, 13	44, 12, 32	81, 12, 69
5	15	–	–	25, 15, 10	44, 15, 29	81, 15, 66
6	18	–	–	25, 18, 7	44, 18, 26	81, 18, 63
7	21	–	–	25, 21, 4	44, 21, 23	81, 21, 60
8	24	–	–	–	44, 24, 20	81, 24, 57
9	27	–	–	–	44, 27, 17	81, 27, 54
10	30	–	–	–	44, 30, 14	81, 30, 51
11	33	–	–	–	44, 33, 11	81, 33, 48
12	36	–	–	–	44, 36, 8	81, 36, 45
13	39	–	–	–	44, 39, 5	81, 39, 42
14	42	–	–	–	44, 42, 2	81, 42, 39
15	45	–	–	–	–	81, 45, 36
16	48	–	–	–	–	81, 48, 33
17	51	–	–	–	–	81, 51, 30
18	54	–	–	–	–	81, 54, 27
19	57	–	–	–	–	81, 57, 24
20	60	–	–	–	–	81, 60, 21
21	63	–	–	–	–	81, 63, 18
22	66	–	–	–	–	81, 66, 15
23	69	–	–	–	–	81, 69, 12
24	72	–	–	–	–	81, 72, 9
25	75	–	–	–	–	81, 75, 6
26	78	–	–	–	–	81, 78, 3

Основною метою кодування інформації є контроль (виявлення та виправлення) помилок, що виникли під час передачі повідомлення по каналу з шумами. Для контролю помилок кодуючий пристрій вносить надлишковість (перевірочну частину довжини r, $r=n–k$) в передані дані. На приймальній стороні,

аналізуючи властивості перевірочної частини та її відповідність переданим даним, декодер зменшує вплив помилок, що виникли при передачі.

Завдання розкодування може бути ефективно вирішене (з поліноміальною складністю) для вузького класу кодів, наприклад, завадостійких кодів Боуза–Чоудхури–Хоквингема (БЧХ) і кодів Ріда–Соломона. Одним з найбільш ефективних алгоритмів алгебраїчного декодування кодів БЧХ є алгоритм Берлекемпа–Мессі та його модифікації (поліпшення). Відомо [1; 2; 33; 34; 35; 36; 37], що алгоритм Берлекемпа–Мессі містить кількість реалізації множень, порядку t^2, або, формально, складність алгоритму $O(t^2)$, де t – виправна здатність коду, $t=\lfloor (d-1)/2 \rfloor$. Для великого t використовують прискорений алгоритм Берлекемпа–Мессі, що дозволяє зменшити обчислювальну складність алгоритму. Ще більш ефективним, з точки зору обчислювальної складності, є рекурентний алгоритм Берлекемпа–Мессі. Асимптотична складність декодування кодів Ріда–Соломона в цьому випадку не перевищує величини $O(n\log^2 n)$, причому дуже близька до величини $O(n\log n)$.

Декодування довільного лінійного коду (коду загального положення) є досить складною обчислювальною задачею, складність її вирішення зростає експоненціально. Так, для кореляційного декодування довільного (n, k, d) коду над $GF(q)$ необхідно, в загальному випадку, порівняти прийняту послідовність з усіма q^k кодовими словами і вибрати найближче (в метриці Гемінга). Навіть для невеликих n, k, d і q задача кореляційного декодування дуже трудомістка. Це положення лежить в основі всіх криптосистем на алгебраїчних блокових кодах. Маскуючи код зі швидким алгоритмом декодування (поліноміальної складності) під довільний (випадковий) лінійний код можна уявити задачу декодування для стороннього спостерігача (можливого зловмисника) як обчислювальне складну задачу (експоненційної складності). Для уповноваженого користувача криптосистеми (який має секретний ключ) розкодування – поліномінально здійсненне завдання [2].

3.1.1. Встановлення властивостей несиметричних крипто-кодових систем Мак-Еліса і Нідеррайтера на еліптичних кодах

Розглянемо *теоретико-кодову схему Мак-Еліса*, вперше запропоновану в [31]. Нехай G – породжувальна матриця лінійного (n, k, d) коду над $GF(q)$ з

поліноміальною складністю декодування, X – невироджена $k \times k$-матриця над $GF(q)$, D – діагональна матриця з ненульовими на діагоналі елементами, P – переставна матриця розміру $n \times n$. Перестановочна матриця реалізує перестановку координат вектора у вигляді матричного множення, а саме, елемент p_{ij} матриці P дорівнює 1 тоді і тільки тоді, коли координата з номером i переходить за допомогою перестановки в координату з номером j. В інших випадках $p_{ij} = 0$. Таким чином, матриця P містить в кожному стовпці і в кожному рядку тільки одну одиницю. Добуток матриць $\Lambda = P \times D$ задає перестановки матрицю Λ з ненульовими елементами поля $GF(q)$. Перестановочна матриця Λ (уніпотентна матриця) при перестановці координат вектора зберігає відстань за Хемінгом, тобто $d(a, b) = d(a \times \Lambda, b \times \Lambda)$, де $d(x, y)$ – відстань за Хемінгом між векторами x і y.

Відкритим ключем в несиметричній крипто-кодової системі на основі ТКС Мак-Еліса є породжувальна матриця $G_X = X \times G \times P \times D$, отримана шляхом перемноження породжувальної матриці лінійного (n, k, d) коду над $GF(q)$ на матриці маскування (X, P, D), особистим (закритим) ключем є матриці X, P, D. Закрита інформація (кодограма) являє собою вектор довжиною n і обчислюється за правилом:

$$c_X^* = i \times G_X + e, \tag{3.8}$$

де вектор $c_X = i \times G_X$ належить (n, k, d) коду з породжувальною матрицею G_X; i – k-розрядний інформаційний вектор; вектор e – секретний вектор помилок ваги $\le t$ (сеансовий секретний ключ).

Властивості 1, 2 і результат твердження 1 дозволяють задати НККС Мак-Еліса на основі еліптичних кодів таким чином [2; 11; 23]. Нехай G^{EC} – породжувальна матриця еліптичного (n, k, d) коду над $GF(q)$ виду:

$$G^{EC} = \begin{pmatrix} F_0(P_0) & F_0(P_1) & \dots & F_0(P_{n-1}) \\ F_1(P_0) & F_1(P_1) & \dots & F_1(P_{n-1}) \\ \dots & \dots & \dots & \dots \\ F_{k-1}(P_0) & F_{k-1}(P_1) & \dots & F_{k-1}(P_{n-1}) \end{pmatrix} = \left\| F_j(P_i) \right\|_{n,k}. \tag{3.9}$$

та розмірності $k \times n$, $k = \alpha$, $\alpha = 3 \cdot degF$.

Нехай X – невироджена $k \times k$-матриця над $GF(q)$, D – діагональна матриця з ненульовими на діагоналі елементами, P – перестановочна матриця розмірності $n \times n$. Визначим НККС *Мак-Еліса з еліптичними кодами (EC)*: відкритий ключ – матриця $G_X^{EC} = X \times G^{EC} \times P \times D$, особистий (закритий) ключ – матриці X, P, D.

Закрита інформація (кодограма) являє собою вектор довжини n та визначається за правилом: $c_X^* = i \times G_X^{EC} + e$, де вектор $c_X = i \times G_X^{EC}$, який належить еліптичному (n, k, d) коду з породжувальною матицею G_X^{EC}, i – k-розрядний інформаційний вектор, вектор e – секретний вектор помилок вагою $\le t$.

Розглянемо *теоретико-кодову схему Нідеррайтера*, вперше запропоновану в [32]. Нехай H – перевірочна матриця лінійного (n, k, d) коду над $GF(q)$ з поліноміальною складністю декодування. Нехай X – невироджена $r \times r$-матриця над $GF(q)$, D – діагональна матриця з ненульовими елементами на діагоналі, P – перестановочна матриця розміру $n \times n$. Відкритим (загальнодоступним) ключем в ТКС Нідеррайтера є матриця $H_X = X \times H \times P \times D$, особистим (закритим) ключем є матриці маскування – X, P, D. Закрита інформація (кодограма) S_X є синдром – вектор довжини $r = n - k$, який обчислюється за правилом:

$$S_X = e \times H_X^T, \tag{3.10}$$

де вектор e – вектор довжини n та ваги $\le t$, який несе конфіденційну інформацію.

Уповноважений отримувач конфіденційної інформації (який має особистий ключ) знаходить одне зі q^k рішень виразу $S_X = c_X^* \times H_X^T$. Знайдене рішення – кодове слово з помилками $c_X^* = i \times G_X + e$. Далі, як і в схемі Мак-Еліса, уповноважений користувач будує вектор $\bar{c}^* = c_X^* \times D^{-1} \cdot P^{-1}$ і розкодує отримане слово. Однак, замість відновлення інформаційного слова i', він обчислює кодове слово $c' = i' \cdot G$, а потім і вектор помилок $e' = \bar{c}^* - c'$. На останньому кроці проводиться обчислення вектора $e = e' \times P \times D$, який несе конфіденційну інформацію.

Щоб задати НККС Нідеррайтера на *EC* скористаємося властивістю 3 подання алгеброгеометричного коду, або у матричному подані алгеброгеометричного коду:

$$H\,(c_0, c_1, ..., c_{n-1})^T = 0,$$

де H – перевірочна матриця коду розмірності $r \times n$; $r = n - k = d + g - 2$

$$H = \begin{pmatrix} F_0(P_0) & F_0(P_1) & ... & F_0(P_{n-1}) \\ F_1(P_0) & F_1(P_1) & ... & F_1(P_{n-1}) \\ ... & ... & ... & ... \\ F_{r-1}(P_0) & F_{r-1}(P_1) & ... & F_{r-1}(P_{n-1}) \end{pmatrix} = \left\| F_j\left(P_i\right) \right\|_{n,r}. \qquad (3.11)$$

Властивість 3 і результат твердження 2 (3.4), (3.5) дозволяють визначити НККС Нідеррайтера на основі еліптичних кодів таким чином.

Нехай H^{EC} – перевірочна матриця еліптичного *(n, k, d)* коду над *GF(q)* виду (3.11) і розмірності $r \times n$, $r = \alpha$, $\alpha = 3 \cdot degF$. Нехай X – невироджена $k \times k$-матриця над *GF(q)*, D – діагональна матриця з ненульовими на діагоналі елементами, P – перестановочна матриця розміру $n \times n$. Визначемо несиметричну *схему Нідеррайтера з еліптичних кодом* [7]: відкритий ключ – матриця – $H_X^{EC} = X \times H^{EC} \times P \times D$, секретний (закритий) ключ – матриці маскування X, P, D.

Закрита інформація (кодограма) являє собою вектор довжини n і обчислюється за правилом (3.10). Для формування вектора помилки e (конфіденційної інформації) в роботі [17] розглянуті практичні алгоритми перетворення інформаційного вектора на вектор помилки на основі методу рівновагого кодування.

Доведені твердження 1, 2 і запропоновані НККС з *EC* дозволяють формувати кодограми за несиметричною криптосистемою, тобто використовувати відкритий ключ для обміну закритою інформацією в ОБС.

Загальна класифікація крипто-кодових систем і послуг безпеки, які забезпечують їх використання наведені на рис. 3.3.

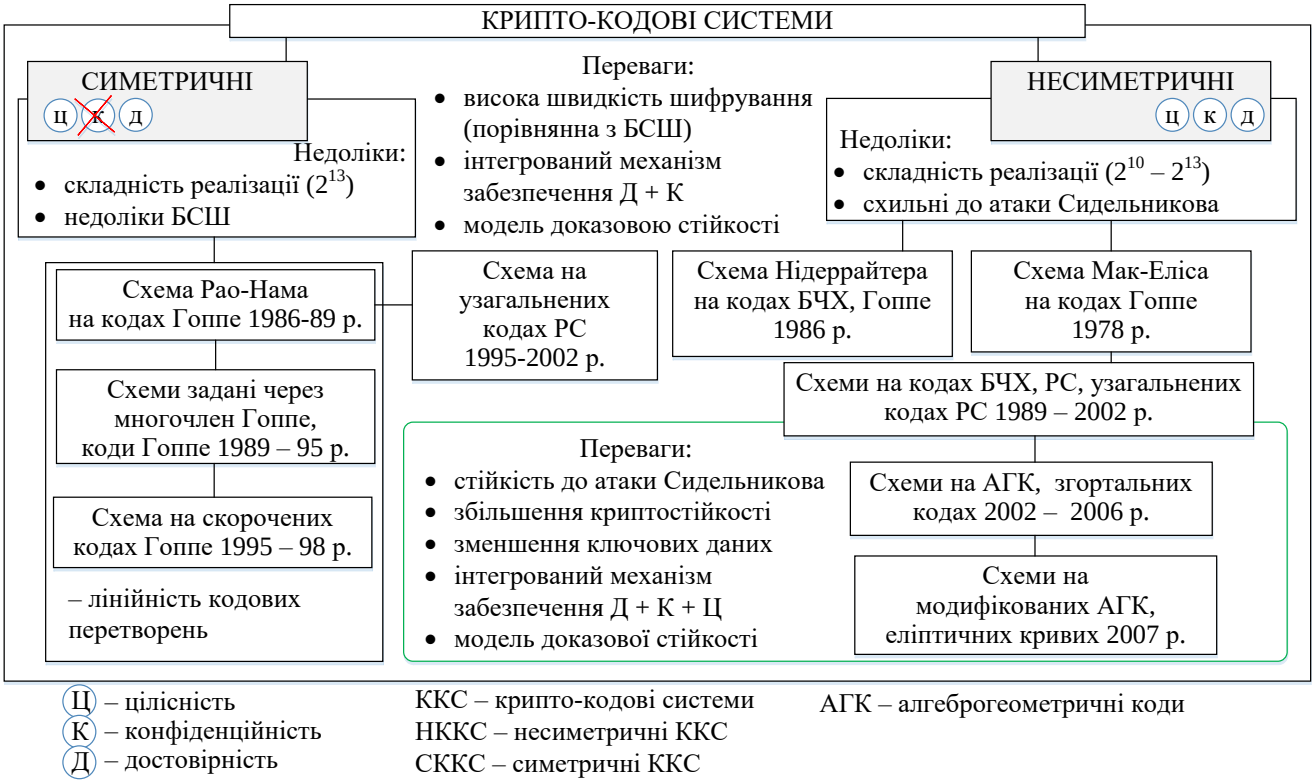


Рисунок 3.3 – Класифікація криптосистем на основі ККС

Разом з тим, проведений в роботах [6; 11; 17] аналіз програмної реалізації НККС Мак-Еліса і Нідеррайтера свідчать про значну складність програмної реалізації, що істотно ускладнює використання НККС в протоколах АБС.

Результати досліджень енергетичних витрат (табл. 3.5) програмної реалізації показали, що для виконання 1000 операцій в середньому застосовується: зчитування символу – 27 тактів, порівняння рядку – 54 тактів, конкатенація рядку – 297 тактів.

Для розрахунку використовувався процесор з тактовою частотою 2 ГГц з урахуванням завантаження операційною системою в 5%.

Для збору наведених значень використовувався інструмент програмування для настроювання використання пам’яті, виявлення витоків пам’яті, а також профілювання – *Valgrind*, а саме його модуль – *Callgrind*.

Таблиця 3.5 – Результати оцінювання енергетичних витрат ККС Мак-Еліса та Нідеррайтера на *EC*

Довжина кодової послідовності		*Niederreiter*			*MacElis*		
Довжина інформ. вектору		10	100	1000	10	100	1000
Кількість викликів функцій, що реалізують елементарні операції	Зчитування символу	1160342	2502422	11018042	30800328	80859933	15923222
	Порівняння рядку	381020	777 560	3663356	10199898	26364634	4 742 960
	Конкате-нація рядку	192770	411 380	1834983	5125564	13415329	2597480
Сума		1734132	3691362	23263662	16516381	46125790	120639896
Довжина виконання функцій в тактах процесора	Зчитування символу	31 329	67 565	297487	831609	2183218	429 927
	Порівняння рядку	20 575	41 988	197821	550794	1423690	256 120
	Конкате-нація рядку	57 253	122 180	544990	1522293	3984353	771 452
Сума		109157	231733	1457498	1040298	2904696	7591261
Час виконання в 10^{-6} с		0,06	0,12	0,77	0,55	1,53	4

Таким чином, для забезпечення послуг безпеки БІР використання класичних теоретико-кодових схем Мак-Еліса і Нідеррайтера можливо тільки при зменшенні енергетичних витрат на їх практичну реалізацію зі збереженням рівня криптостійкості криптосистеми в цілому.

Для зниження енерговитрат криптоперетворень в НККС Мак-Еліса в роботі [6] пропонується використовувати модифіковані НККС (МККС) на модифікованих *EC* (*MEC*).

3.1.2. Аналіз методу маскування еліптичних кодів

Відомі способи модифікації лінійних блокових кодів найдокладніше розглянуті в [1; 2; 33; 34; 35; 36; 37]. На рис. 3.4 наведені найбільш поширені способи модифікації. *Подовження (n, k, d)* лінійного блокового коду полягає в збільшенні довжини $n + x$ шляхом додавання нових інформаційних символів $k + x$. *Розширення (n, k, d)* лінійного блокового коду полягає в збільшенні довжини $n + x$ шляхом додавання нових перевірочних символів $r + x$.

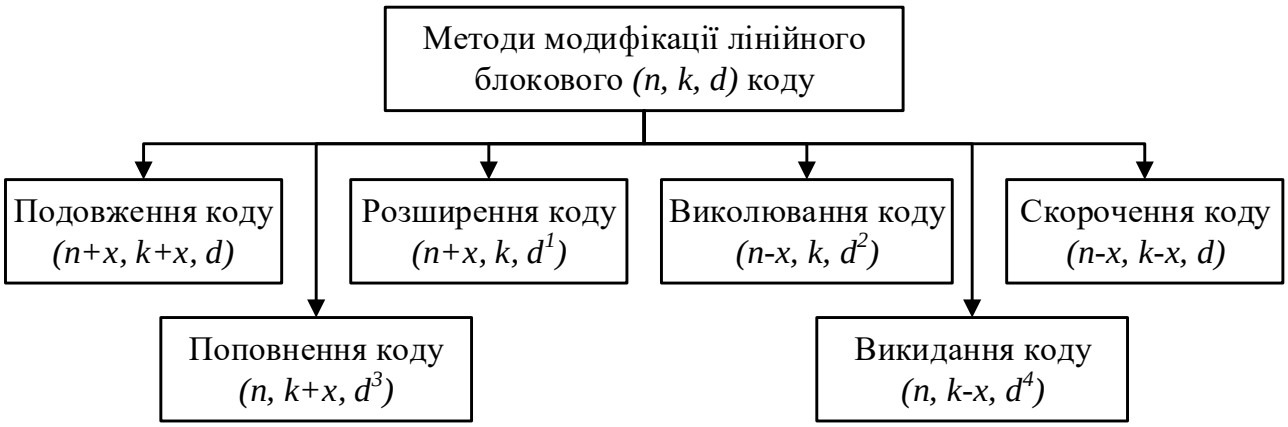


Рис. 3.4. Способи модифікації лінійних блокових кодів

Виколювання (n, k, d) лінійного блокового коду полягає в зменшенні довжини $n - x$ шляхом зменшення перевірочних символів $r - x$. *Скорочення (n, k, d)* лінійного блокового коду полягає в зменшенні довжини $n - x$ шляхом зменшення інформаційних символів $k - x$. *Поповнення (n, k, d)* лінійного блокового коду полягає в збільшенні довжини інформаційних символів $k + x$ без збільшення довжини коду. *Викидання (n, k, d)* лінійного блокового коду полягає в зменшенні інформаційних символів $k - x$ без збільшення довжини коду.

Потенційна стійкість НККС визначається складністю декодування випадкового *(n, k, d)* блокового коду. Отже, для побудови потенційно стійких теоретико-кодових схем необхідно використовувати способи модифікації, що не допускають зниження мінімального кодової відстані. Способи подовження і укорочення лінійних блокових кодів не змінюють мінімальну відстань, і тому дозволяють будувати стійкі до злому НККС [1; 2; 6; 11; 14; 29].

Скористаємося визначенням еліптичних кодів [1; 2; 41]. Справедливі такі властивості:

Властивість 4. Еліптичний *(n, k, d)* код над *GF(q)*, побудований через відображення виду $\varphi: EC \to P^{k-1}$, пов'язаний характеристиками $k + d \geq n$, причому: $n \leq 2\sqrt{q} + q + 1$, $k \geq \alpha$, $d \geq n - \alpha$, $\alpha = 3 \cdot degF$.

Властивість 5. Еліптичний *(n, k, d)* код над *GF(q)*, побудований через відображення виду $\varphi: EC \to P^{r-1}$, пов'язаний характеристиками $k + d \geq n$, причому: $n \leq 2\sqrt{q} + q + 1$, $k \geq n - \alpha$, $d \geq \alpha$, $\alpha = 3 \cdot degF$.

Нехай A – генераторна матриця еліптичного *(n, k, d)* коду над *GF(q)* виду:

$$A = \begin{pmatrix} F_0(P_0) & F_0(P_1) & \dots & F_0(P_{n-1}) \\ F_1(P_0) & F_1(P_1) & \dots & F_1(P_{n-1}) \\ \dots & \dots & \dots & \dots \\ F_{M-1}(P_0) & F_{M-1}(P_1) & \dots & F_{M-1}(P_{n-1}) \end{pmatrix} = \left\| F_j(P_i) \right\|_{n,M}$$

і розмірності $M \times n$, $M = \alpha$, $\alpha = 3 \times degF$.

Для зниження обсягу ключових даних в теоретико-кодовій схемі на еліптичних кодах скористаємося такими особливостями побудови матриці A.

Генераторна матриця A формується в результаті відображення точок еліптичної кривої базисом генераторних функцій. Генераторна матриця еліптичного коду, побудованого по кривій

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz + a_6z^3,$$

$a_i \in GF(q)$, при цьому коефіцієнти багаточлена однозначно задають вигляд кривої і, відповідно, набір проектних точок за якими будується еліптичний код (його генераторна матриця). При цьому справедливе таке твердження.

Твердження 3 [2; 6]. Еліптичний *(n, k, d)* код над *GF(q)* однозначно задається набором $a_1 \dots a_6$, $\forall a_i \in GF(q)$.

Доведення. Розглянемо генераторну матрицю еліптичного *(n, k, d)* коду над *GF(q)*:

$$A = \begin{pmatrix} F_0(P_0) & F_0(P_1) & \dots & F_0(P_{n-1}) \\ F_1(P_0) & F_1(P_1) & \dots & F_1(P_{n-1}) \\ \dots & \dots & \dots & \dots \\ F_{M-1}(P_0) & F_{M-1}(P_1) & \dots & F_{M-1}(P_{n-1}) \end{pmatrix}.$$

Кожен символ генераторної матриці формується шляхом обчислення значення генераторної функції F_j в точці P_i еліптичної кривої. Кількість M генераторних функцій визначається конструктивними характеристиками еліптичного (n, k, d) коду. Вид функцій F_j визначається степенем α відображення точок кривої і, отже, так само задається конструктивними параметрами коду.

Таким чином, якщо задані конструктивні (n, k, d) характеристики еліптичного коду, то унікальність генераторної матриці визначає набір точок $P_1, P_2, \dots, P_n$, в яких обчислюються значення генераторних функцій. Конкретний набір точок з простору P^2 однозначно задається видом багаточлена кривої, тобто набором коефіцієнтів $a_1 \dots a_6$, $\forall a_i \in GF(q)$. □

Висновок 1 [2]. Обсяг секретного ключа (в бітах) у дослідженій крипто-кодової системи на основі ТКС Мак-Еліса, побудованій на еліптичних (n, k, d) кодах над $GF(2^m)$ визначається сумою елементів матриць X, P, D (у бітах) і задається виразом

$$l_{K+} = 5 \times n^2 \times k^2 \times m. \qquad (3.12)$$

Доведення. Дійсно, секретний ключ у схемі Мак-Еліса – генераторна матриця A (породжувальна матриця) і матриці маскування X, P, D. Для визначення секретного ключа (у бітах) еліптичного (n, k, d) коду над $GF(2^m)$, за твердженням 3, достатньо визначити набір коефіцієнтів $a_1 \dots a_6$, $\forall a_i \in GF(2^m)$ і елементи матриць маскування. Всього необхідно зберігати $l_{K+} = 5 \times n^2 \times k^2 \times m$ бітів секретної ключової інформації. □

Вираз (3.12) дозволяє оцінити обсяг секретних ключових даних у НККС Мак-Еліса на *EC*.

Таким чином, запропонований спосіб маскування, заснований на побудові модифікованих НККС на *EC*, в яких секретними даними є параметри еліптичної кривої, дозволяє істотно знизити обсяги ключових даних в порівнянні з класичною схемою Мак-Еліса.

3.1.3. Розроблення методів модифікації еліптичних кодів

Для модифікації еліптичного коду, що не зменшує мінімальну кодову відстань, запропоновано скоротити кількість інформаційних символів.

Нехай $I=(I_1, I_2, \ldots, I_k)$ – інформаційний вектор (n, k, d) блокового коду. Визначимо підмножину h інформаційних символів, $/h/=x$, $x \leq 1/2k$. Помістимо в інформаційний вектор I в підмножину h нулі, тобто $I_i=0, \forall I_i \in h$. На інших позиціях вектора I помістимо інформаційні символи.

При кодуванні інформаційного вектора символи множини h не застосовуються (вони нульові) і їх можна відкинути, а отримане кодове слово буде коротше на x кодових символів. Для модифікації (укорочення) еліптичних кодів будемо використовувати зменшення набору точок кривої.

Справедливі такі твердження [1; 2].

Твердження 4 [1; 2]. Нехай EC – еліптична крива над $GF(q)$, $g=g(EC)$ – рід кривої, $EC(GF(q))$ – множина її точок над кінцевим полем, $N=EC(GF(q))$ – їх кількість. Нехай X і h – непересічні підмножини точок, $X \cup h=EC(GF(q))$, $/h/=x$.

Тоді *укорочений* еліптичний (n, k, d) код над $GF(q)$, побудований через відображення виду $\varphi: X \to P^{k-1}$, пов'язаний характеристиками $k+d \geq n$, причому: $n = 2\sqrt{q} + q + 1 - x$, $k \geq \alpha - x$, $d \geq n-\alpha$, $\alpha=3 \times degF$.

Твердження 5 [1; 2]. *Укорочений* еліптичний (n, k, d) код над $GF(q)$, побудований через відображення виду $\varphi: X \to P^{r-1}$, пов'язаний характеристиками $k+d \geq n$, причому: $n = 2\sqrt{q} + q + 1 - x$, $k \geq n-\alpha$, $d \geq \alpha$, $\alpha=3 \times degF$ (3.13).

Використовуючи результат тверджень 4, 5 задамо МНККС Мак-Еліса на MEC, побудовану через відображення виду $\varphi: X \to P^{k-1}$ та $\varphi: X \to P^{r-1}$. Справедливі такі твердження.

Твердження 6 [1; 2]. Укорочений еліптичний (n, k, d) код над $GF(2^m)$, побудований через відображення виду $\varphi: X \to P^{k-1}$, визначає МНККС на MEC з параметрами:

– розмірність секретного ключа: $l_{K+} = x \cdot \left\lceil \log_2 \left(2\sqrt{q} + q + 1 \right) \right\rceil$; $l_I=(\alpha-x) \cdot m$; (3.14)

– розмірність інформаційного вектора (в бітах): $l_I=(\alpha-x)\times m$; (3.15)

– розмірність кодограми: $l_S=\left(2\sqrt{q}+q+1-x\right)\cdot m$; (3.16)

– відносна швидкість кодування: $R=(\alpha-x)/\left(2\sqrt{q}+q+1-x\right)$. (3.17)

Твердження 7 [1; 2]. Укорочений еліптичний *(n, k, d)* код над $GF(2^m)$, побудований через відображення виду $\varphi: X \to P^{r-1}$, побудованій через відображення виду:

– розмірність секретного ключа визначається виразом (3.14);

– розмірність інформаційного вектора (в бітах): $l_I=\left(2\sqrt{q}+q+1-\alpha\right)\times m$; (3.18)

– розмірність кодограми визначається виразом (3.16);

– відносна швидкість передачі: $R=\left(2\sqrt{q}+q+1-\alpha\right)/\left(2\sqrt{q}+q+1-x\right)$. (3.19)

Розглянемо формальний опис МНККС Мак-Еліса на основі використання методів модифікації і практичні алгоритми формування для забезпечення конфіденційності БІР.

Математична модель НККС з використанням ТКС Мак-Еліса на основі укорочення (скорочення інформаційних символів) формально задається сукупністю наступних елементів [6]:

– множина відкритих текстів – $M=\{M_1, M_2, ..., M_{q^k}\}$, де $M_i=\{I_0, I_{h_1}, .. I_{h_j}, I_{k\text{-}1}\}$, $\forall \mathrm{I}_\mathrm{j} \in GF(q)$; h_j – інформаційні символи дорівнюють нулю, $|h|=\frac{1}{2}k$, тобто $I_i=0,\ \forall I_i \in h$;

– множина закритих текстів *(кодограм)* – $C=\{C_1, C_2, ..., C_{q^k}\}$, де $C_i=(c^*_{X_0}, c^*_{h_1}, ..., c^*_{h_j}, c^*_{X_{n-1}})$, $\forall c^*_{X_j} \in GF(q)$;

– множина прямих відображень (на основі використання відкритого ключа – породжувальної матриці): $\phi=\{\phi_1, \phi_2, ..., \phi_s\}$, де $\phi_i : M \to C_{k-h_j}$, $i=1,2,...,s$;

– множина обернених відображень (на основі використання закритого (особистого) ключа – матриць маскування): $\phi^{-1} = \{\phi_1^{-1}, \phi_2^{-1}, ..., \phi_s^{-1}\}$, де $\phi_i^{-1} : C_{k-h_j} \to M,\ i = 1, 2, ..., s;$

– множина ключів, яка параметризує прямі відображення (відкритий ключ уповноваженого користувача): $K_{a_i} = \{K_{1_{a_i}}, K_{2_{a_i}}, ..., K_{s_{a_i}}\} = \{G_X^{EC_1}{}_{a_i}, G_X^{EC_2}{}_{a_i}, ..., G_X^{ECs}{}_{a_i}\}$, де $G_X^{ECi}{}_{a_i}$ – породжувальна $n \times k$ матриця замаскованого під випадковий код алгеброгеометричного блокового (n, k, d) коду з елементами з $GF(q)$, тобто $\phi_i : M \xrightarrow{K_{ia_i}} C_{k-h_j};\ i = 1, 2, ..., s;$ a_i – набір коефіцієнтів багаточлена кривої $a_1 ... a_6$, $\forall a_i \in GF(q)$, що однозначно визначає конкретний набір точок кривої з простору P^2.

– множина ключів, яка параметризує обернені відображення (особистий (закритий) ключ уповноваженого користувача):

$K^* = \{K_1^*, K_2^*, ..., K_s^*\} = \{\{X, P, D\}_1, \{X, P, D\}_2, ..., \{X, P, D\}_s\}$, $\{X, P, D\}_i = \{X^i, P^i, D^i\}$,

де X^i – маскуюча невироджена випадково рівноймовірно сформована джерелом ключів $k \times k$ матриця з елементами з $GF(q)$; P^i – перестановочна випадково рівноймовірно сформована джерелом ключів $n \times n$ матриця з елементами з $GF(q)$; D^i – діагональна сформована джерелом ключів матриця з елементами з $GF(q)$, тобто $\phi_i^{-1} : C \xrightarrow{K_i^*} M,\ i = 1, 2, ..., s,$ складність виконання оберненого відображення ϕ_i^{-1} без знання ключа $K_i^* \in K^*$ пов'язана з розв'язанням теоретико-складної задачі декодування випадкового коду (коду загального положення).

Вихідними даними для опису розглянутої несиметричної крипто-кодової системи захисту інформації є:

– алгеброгеометричний блоковий *(n, k, d)* код C_{k-h_j} над *GF(q)*, тобто така множина кодових слів $C_i \in C_{k-h_j}$, що виконується рівність $C_i H^T = 0$, де H – перевірочна матриця алгеброгеометричного блокового коду;

– a_i – набір коефіцієнтів багаточлена кривої $a_1 \ldots a_6$, $\forall a_i \in GF(q)$, однозначно визначає конкретний набір точок кривої з простору P^2 для формування породжувальної матриці;

– h_j – інформаційні символи, що дорівнюють нулю, $|h|=1/2k$, тобто $I_i = 0,\ \forall I_i \in h$;

– маскуючі матричні відображення, задані множиною матриць $\{X, P, D\}_i$, де X – невироджена $k \times k$ матриця над $GF(q)$; P – перестановочна $n \times n$ матриця над $GF(q)$ з одним ненульовим елементом в кожному рядку і в кожному стовпці матриці; D – діагональна $n \times n$ матриця над $GF(q)$ з ненульовими елементами на головній діагоналі.

У МНККС Мак-Еліса модифікований (укорочений) алгеброгеометричний (n, k, d) код C_{k-h_j} зі швидким алгоритмом розкодування маскується під випадковий (n, k, d) код C_{k-h_j}* за допомогою множення породжувальної матриці G^{EC} коду C_{k-h_j} на маскуючі матриці, які знаходяться в секреті X^u, P^u і D^u [6], що забезпечує формування відкритого ключа уповноваженого користувача:

$G_X^{ECu} = X^u \cdot G^{EC} \cdot P^u \cdot D^u, \quad u \in \{1,2,...,s\}$, де G^{EC} – породжувальна $n \times k$ матриця алгеброгеометричного блокового (n, k, d) коду з елементами з $GF(q)$, побудована на основі використання вибраних користувачем коефіцієнтів многочлена кривої $a_1 \ldots a_6$, $\forall a_i \in GF(q)$, однозначно, які задають конкретний набір точок кривої з простору P^2.

Формування закритого тексту $C_j \in C_{k-h_j}$ за введеним відкритим текстом $M_i \in M$ і заданим відкритим ключем $G_X^{ECu}{}_{a_i}$, $u \in \{1,2,...,s\}$ здійснюється шляхом формування кодового слова замаскованого коду з додаванням до нього випадково сформованого вектора $e = (e_0, e_1, ..., e_{n-1}) : C_j = \phi_u\left(M_i, G_X^u\right) = M_i \cdot \left(G_X^u\right)^T + e$, причому вага Гемінга (кількість ненульових елементів) вектора e не перевищує виправної здатності використовуваного алгебраїчного блокового коду:

$0 \le w(e) \le t = \left\lfloor \frac{d-1}{2} \right\rfloor$, $\lfloor x \rfloor$ – ціла частина дійсного числа x.

Для кожного закритого тексту, який формується $C_j \in C_{k-h_j}$, відповідний вектор $e=(e_0,e_1,...,e_{n-1})$ являється одноразовим сеансовим ключем, тобто для конкретного E_j вектор e формується випадково, рівноймовірно і незалежно від інших закритих текстів.

У канал зв'язку надходить $C_j^* = C_j - C_{k-h_j}$.

На стороні прийому уповноважений користувач, який знає правило маскування, кількість і місця нульових інформаційних символів може скористатися швидким алгоритмом розкодування алгеброгеометричного коду (поліноміальної складності) для відновлення відкритого тексту [6]: $M_i = \phi_u^{-1}\left(C_j^*,\{\mathrm{X,P,D}\}_\mathrm{u}\right)$.

Для відновлення відкритого тексту уповноважений користувач додає нульові інформаційні символи $C_j^* = C_j + C_{k-h_j}$, з відновленого закритого тексту C_j знімає дію секретних переставної і діагональної матриць P^u і D^u:

$$
\begin{aligned}
C &= C_j^* \cdot \left(D^u\right)^{-1} \cdot \left(P^u\right)^{-1} = \left(M_i \cdot \left(G_X^u\right)^T + e\right) \cdot \left(D^u\right)^{-1} \cdot \left(P^u\right)^{-1} = \\
&= \left(M_i \cdot \left(X^u \cdot G \cdot P^u \cdot D^u\right)^T + e\right) \cdot \left(D^u\right)^{-1} \cdot \left(P^u\right)^{-1} = \\
&= M_i \cdot \left(X^u\right)^T \cdot \left(G\right)^T \cdot \left(P^u\right)^T \cdot \left(D^u\right)^T \cdot \left(D^u\right)^{-1} \cdot \left(P^u\right)^{-1} + e \cdot \left(D^u\right)^{-1} \cdot \left(P^u\right)^{-1} = \\
&= M_i \cdot \left(X^u\right)^T \cdot \left(G\right)^T + e \cdot \left(D^u\right)^{-1} \cdot \left(P^u\right)^{-1}.
\end{aligned}
$$

Після цього отриманий вектор слід розкодувати за алгоритмом Берлекемпа–Мессі [33; 34; 35]:

$$C = M_i \cdot \left(X^u\right)^T \cdot \left(G^{EC}\right)^T + e \cdot \left(D^u\right)^{-1} \cdot \left(P^u\right)^{-1},$$

тобто позбутися другого доданку і співмножника $\left(G\right)^{ECT}$ в першому доданку в правій частині рівності, після чого знімає дію матриці маскування X^u. Для цього отриманий результат розкодування $M_i \cdot \left(X^u\right)^T$ слід помножити на $\left(X^u\right)^{-1}$: $\left(M_i \cdot \left(X^u\right)^T\right) \cdot \left(X^u\right)^{-1} = M_i$. Отримане рішення і є відкритим текстом M_i.

Структурна схема протоколу обміну інформацією в режимі реального часу з використанням МНККС Мак-Еліса з модифікованими (укороченими) еліптичними кодами наведена на рис. 3.5.

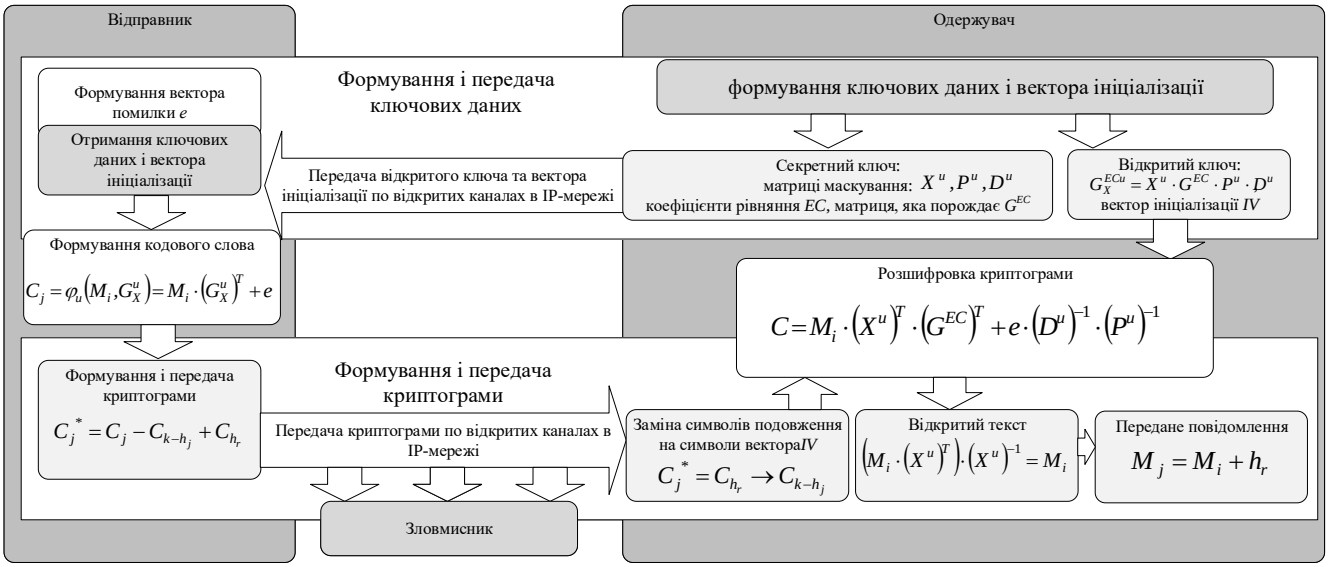
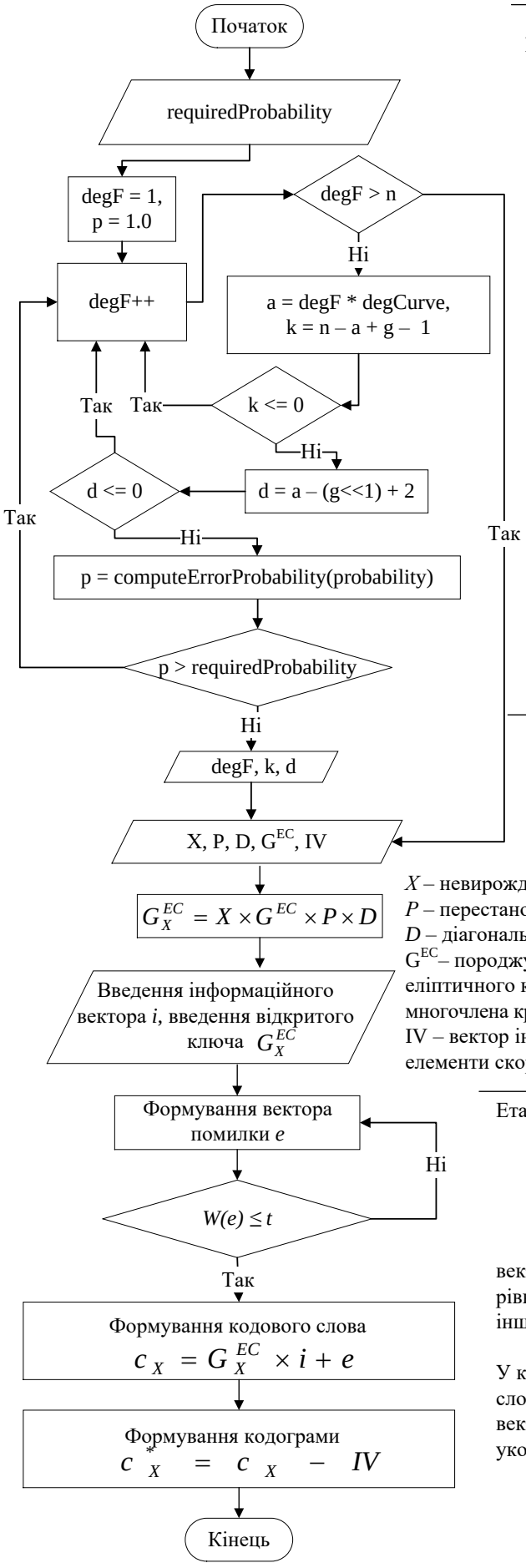


Рисунок 3.5 – Структурна схема протоколу обміну інформацією в режимі реального часу з використанням МНККС Мак-Еліса з укороченими *MEC*

На рис. 3.6 наведений алгоритм формування криптограми / кодограми. Алгоритм розкодування в МНККС Мак-Еліса з укороченим *MEC* наведений на рис. 3.7.

Другий спосіб модифікації лінійного блокового коду, який зберігає мінімальну кодову відстань і збільшує кількість переданих даних, полягає в подовженні його довжини після формування вектора ініціалізації, шляхом скорочення інформаційних символів. Нехай $I = (I_1, I_2, \ldots, I_k)$ – інформаційний вектор (n, k, d) блокового коду. Оберемо підмножину h інформаційних символів, $|h| = x$, $x \le \frac{1}{2} k$ і *сформуємо вектор ініціалізації*. Помістимо в інформаційний вектор I в підмножину h нулів, тобто $I_i = 0, \ \forall I_i \in h$. На інших позиціях вектора I помістимо інформаційні символи. Після цього в позиції вектора ініціалізації додаємо інформаційні символи. Для модифікації (подовження) еліптичних кодів будемо використовувати зменшення набору точок кривої. З цього випливає таке твердження.



Етап 1. Встановлення параметрів коду

requiredProbability – задана ймовірність спотворення блоку,
n – загальна кількість символів в коді (довжина коду),
k – кількість інформаційних символів,
d – мінімальна відстань кодових комбінацій за Хемінгом,
g – рід кривої,
degF – степінь генераторної функції,
degCurve – степінь кривої

Етап 2. Формування особистого і відкритого ключів несиметричної криптосистеми, введення інформаційної посилки

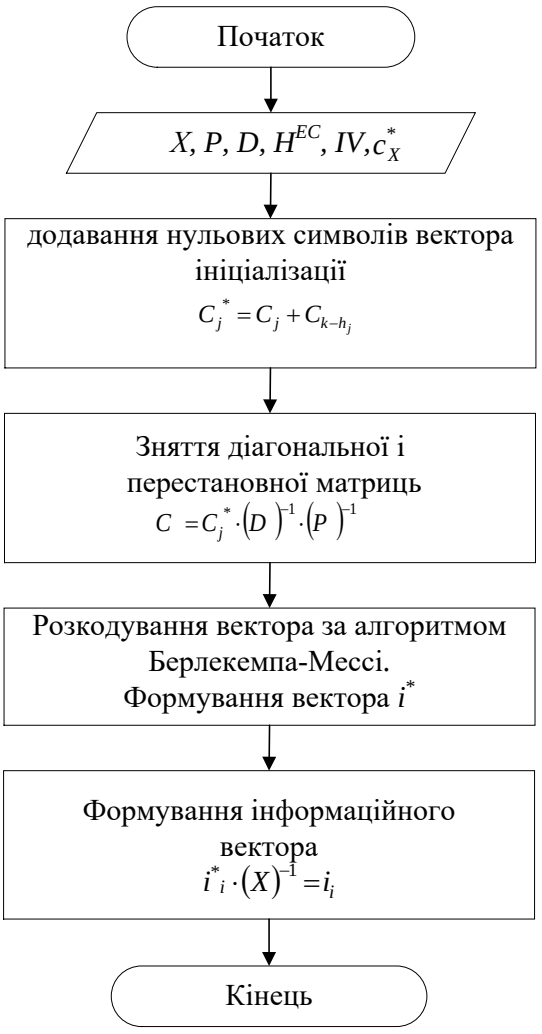
X – невироджена $k \times k$ матриця над $GF(q)$,
P – перестановочна $n \times n$ матриця над $GF(q)$,
D – діагональна $n \times n$ матриця над $GF(q)$,
G^{EC} – породжувальна $k \times n$ матриця еліптичного коду $GF(q)$, a_i – набір коефіцієнтів многочлена кривої $a_1 \ldots a_6$,
IV – вектор ініціалізації, IV= $|h| = ½\ k$ – елементи скорочення

Етап 3. Формування сеансового ключа і кодограми

вектор e формується випадково, рівноймовірно і незалежно від інших закритих текстів

У канал зв'язку надходить кодове слово c_X* без нульових елементів вектора ініціалізації (операція укорочення)

Рисунок 3.6 – Алгоритм формування кодограми в МНККС Мак-Еліса з укороченим *MEC*



Етап 1. Встановлення параметрів коду, введення особистого ключа та кодограми

X – невироджена $k \times k$ матриця над *GF(q)*,
P – перестановочна $n \times n$ матриця над *GF(q)*,
D – діагональна $n \times n$ матриця над *GF(q)*,
H^{EC} – перевірочна $r \times n$ матриця еліптичного коду над *GF(q)*, a_i – набір коефіцієнтів багаточлена кривої $a_1 \ldots a_6$,
IV – вектор ініціалізації, IV= $|h|$ = ½ *k* – елементи скорочення

Етап 2. Розкодування кодограми

Рисунок 3.7 – Алгоритм розкодування в МНККС Мак-Еліса з укороченим *MEC*

Твердження 8. Нехай *EC* – еліптична крива над *GF(q)*, *g = g(EC)* – рід кривої, *EC(GF(q))* – множина її точок над кінцевим полем, *N = EC(GF(q))* – їх кількість. Зафіксуємо підмножину $h_1 \subseteq h$, $/h_1/ = x_1$. Нехай задано еліптичний *(n, k, d)* код над *GF(q)*, побудований через відображення виду $\varphi: X \to P^{k-1}$. Тоді параметри *подовженого* на x_1 символів з *GF(q)* еліптичного коду, побудованого через відображення виду $\varphi:(X \cup h_1) \to P^{k-1}$, $n = 2\sqrt{q} + q + 1 - x + x_1$ будуть пов'язані такими співвідношеннями: $n = 2\sqrt{q} + q + 1 - x + x_1$, $k \geq \alpha - x + x_1$, $d \geq n - \alpha$, $\alpha = 3 \times degF$.

Доведення. Якщо $x_1 < x$, то подовження коду на x_1 еквівалентне укороченню вихідного коду на $x - x_1$. Підставивши ці параметри в вираз (3.12), отримаємо результат висновку 1. □

Висновок 2. Якщо відомий вид еліптичної кривої (набір $a_1 \dots a_6$, $\forall a_i \in GF(q)$), то підмножини h и h_1 повністю визначають модифіковані еліптичні (n, k, d) коди над $GF(q)$, побудовані через відображення виду: $\varphi: X \to P^{k-1}$ и $\varphi: (X \cup h_1) \to P^{k-1}$.

Доведення. Набір коефіцієнтів $a_1 \dots a_6$, $\forall a_i \in GF(q)$ однозначно задає вид еліптичної кривої і, відповідно, набір її точок $EC(GF(q))$. Використовуючи відображення виду $\varphi: EC \to P^M$ і результати тверджень 1–2, побудуємо еліптичний (n, k, d) код над $GF(q)$. Якщо відомі символи подовження, то побудуємо подовжені коди. За твердженням 8 це символи множини h_1, які повністю визначають модифікований еліптичний (n, k, d) код над $GF(q)$. □

Твердження 9 Зафіксуємо підмножину $h_1 \subseteq h$, $|h_1| = x_1$. Нехай задано еліптичний (n, k, d) код над $GF(q)$, побудований через відображення вигляду $\varphi: X \to P^{r-1}$. Тоді параметри *подовженого* на x_1 символів з $GF(q)$ еліптичного коду, побудованого через відображення виду $\varphi: (X \cup h_1) \to P^{r-1}$, будуть пов'язані такими співвідношеннями: $n = 2\sqrt{q} + q + 1 - x + x_1$, $k \geq n - \alpha$, $d \geq \alpha$, $\alpha = 3 \times degF$.

Висновок 3. Якщо відомий вид еліптичної кривої (набір $a_1 \dots a_6$, $\forall a_i \in GF(q)$), то підмножини h и h_1 повністю визначають модифіковані еліптичні (n, k, d) коди над $GF(q)$, побудовані через відображення виду: $\varphi: X \to P^{r-1}$ и $\varphi: (X \cup h_1) \to P^{r-1}$.

Доведення. Набір коефіцієнтів $a_1 \dots a_6$, $\forall a_i \in GF(q)$ однозначно задає вид еліптичної кривої і, відповідно, набір її точок $EC(GF(q))$. Використовуючи відображення виду $\varphi: EC \to P^M$ і результати тверджень 1, 2, побудуємо еліптичний (n, k, d) код над $GF(q)$. Якщо відомі символи подовження, то побудуємо подовжені коди. За твердженням 9 це символи множин h и h_1, які повністю визначають модифікований еліптичний (n, k, d) код над $GF(q)$. □

Результати тверджень 8, 9 та їх висновки дозволяють побудувати модифіковані (подовжені в межах $n \leq 2\sqrt{q} + q + 1$) еліптичні (n, k, d) коди над $GF(q)$.

Задамо алгоритм побудови модифікованих подовжених еліптичних кодів.

Алгоритм побудови подовжених еліптичних кодів.

Крок 1. Зафіксуємо еліптичну криву над *GF(q)*. Знайдемо множину простих точок кривої *EC(GF(q))*: $(P_1, P_2, \ldots, P_N)$. Побудуємо укорочений *(n, k, d)* код над *GF(q)* як результат відображення $\varphi: X \to P^M$.

Крок 2. Зафіксуємо підмножину точок кривої $h_1(GF(q))$: $(P_{x1}, P_{x2}, \ldots, P_{xx1})$, $h_1 \subset h$, $/h_1/ = x_1$.

Крок 3. Побудуємо відображення $\varphi: (X \cup h_1) \to P^M$. Якщо $M = k$, отримаємо *подовжений* еліптичний *(n, k, d)* код над *GF(q)* з параметрами $n = 2\sqrt{q} + q + 1 - x + x_1$, $k \geq \alpha - x + x_1$, $d \geq n - \alpha$, $\alpha = 3 \times degF$. Якщо $M = r$, отримаємо *подовжений* еліптичний *(n, k, d)* код над *GF(q)* з параметрами: $n = 2\sqrt{q} + q + 1 - x + x_1$, $k \geq n - \alpha$, $d \geq \alpha$, $\alpha = 3 \cdot degF$.

Використовуючи результат твердження 8 і його висновок, задамо МНККС Мак-Еліса на подовжених *MEC*, побудованих через відображення виду $\varphi: X \to P^{k-1}$ и $\varphi: (X \cup h_1) \to P^{k-1}$. З цього випливає таке твердження.

Твердження 10. Подовжений еліптичний *(n, k, d)* код над $GF(2^m)$, побудований через відображення виду $\varphi: (X \cup h_1) \to P^{k-1}$, визначає МНККС з параметрами:

– розмірність секретного ключа (в бітах):

$$l_{K+} = (x - x_1) \cdot \left\lceil log_2\left(2\sqrt{q} + q + 1\right)\right\rceil; \tag{3.20}$$

– розмірність інформаційного вектора (в бітах):

$$l_I = (\alpha - x + x_1) \cdot m; \tag{3.21}$$

– розмірність криптограми (в бітах): $l_S = \left(2\sqrt{q} + q + 1 - x + x_1\right) \cdot m$; (3.22)

– відносна швидкість передачі:

$$R = (\alpha - x + x_1) / \left(2\sqrt{q} + q + 1 - x + x_1\right). \tag{3.23}$$

Доведення. Згідно з результатом твердження 10 МНККС Мак-Еліса, побудована з використанням породжувальної матриці *(n, k, d)*-коду над $GF(2^m)$, володіє такими параметрами: розмір секретного ключа $k \times n$ символів з $GF(2^m)$; інформаційний вектор довжини k символів з $GF(2^m)$; довжина кодограми – n

символів з $GF(2^m)$; відносна швидкість передачі – $R = k / n$. Всього точок кривої $N \le 2\sqrt{q} + q + 1$. Отже, для нумерації точок кривої необхідно $\left| log_2\left(2\sqrt{q} + q + 1\right)\right|$ бітів. Якщо потужність підмножини символів укорочення $/h/ = x$, то для позначення всіх символів укорочення потрібно $x \times \left\lceil \log_2\left(2\sqrt{q} + q + 1\right)\right\rceil$ бітів. Ці символи зберігаються в секреті і задають обсяг ключових даних – вираз (3.14). Якщо потужність підмножини символів подовження $/h_1/ = x_1$, то для позначення всіх символів модифікації буде потрібно $(x - x_1) \times \left\lceil \log_2\left(2\sqrt{q} + q + 1\right)\right\rceil$ бітів. Ці символи зберігаються в секреті і задають обсяг ключових даних – вираз (3.20). □

Використовуючи результат твердження 9 і його висновок, задамо МНККС, побудовану через відображення виду $\varphi: X \to P^{r-1}$ и $\varphi: (X \cup h_1) \to P^{r-1}$. З цього випливає таке твердження.

Твердження 11. Подовжений еліптичний *(n, k, d)* код над $GF(2^m)$, побудований через відображення виду $\varphi: (X \cup h_1) \to P^{r-1}$, визначає МНККС з параметрами:

– розмірність секретного ключа визначається виразом (3.20);

– розмірність інформаційного вектора (в бітах):

$$l_I = \left(2\sqrt{q} + q + 1 - \alpha\right) \cdot m; \qquad (3.24)$$

– розмірність кодограми визначається виразом (3.22);

– відносна швидкість передачі:

$$R = \left(2\sqrt{q} + q + 1 - \alpha\right) / \left(2\sqrt{q} + q + 1 - x + x_1\right). \qquad (3.25)$$

Доведення. Згідно з результатом твердження 11, МНККС, побудована з використанням перевірочної матриці алгебраїчного блокового *(n, k, d)* коду над $GF(2^m)$, володіє такими параметрами: інформаційний вектор довжини *k* символів з $GF(2^m)$; довжина кодограми – *n* символів з $GF(2^m)$; відносна швидкість передачі – $R = k / n$. Підставимо параметри модифікованих (укорочених і подовжених) еліптичних *(n, k, d)* кодів над *GF(q)*, побудованих через відображення виду $\varphi: X \to P^{r-1}$ та $\varphi: (X \cup h_1) \to P^{r-1}$ (см. твердження 9) отримаємо, відповідно, вирази (3.24), (3.25) □

Таким чином, результати тверджень 8, 9 та їх висновки дозволяють побудувати модифіковані подовжені еліптичні *(n, k, d)* коди над *GF(q)*. Твердження 10 та 11 дозволяють задати МНККС Мак-Еліса на *MEC*, забезпечуючи таким чином необхідну криптостійкість.

Розглянемо формальний опис МНККС захисту інформації на основі використання методів модифікації.

Математична модель модифікованої несиметричної крипто-кодової системи захисту інформації з використанням алгеброгеометричних блокових кодів на основі МНККС Мак-Еліса на основі подовження (збільшення інформаційних символів) формально задається сукупністю таких елементів:

множина відкритих текстів: $M = \{M_1, M_2, ..., M_{q^k}\}$, де $M_i = \{I_0, I_{h_1}, .. I_{h_{r_j}}, I_{k-1}\}$, $\forall I_j \in GF(q)$, h_j – інформаційні символи що дорівнюють нулю, $/h/ = \frac{1}{2}k$, тобто $I_i = 0$, $\forall I_i \in h$; h_r – інформаційні символи подовження k, $/h/ = \frac{1}{2}k$;

множина закритих текстів *(кодограм)*: $C = \{C_1, C_2, ..., C_{q^k}\}$, де $C_i = (c^*_{X_0}, c^*_{h_{r_1}}, ..., c^*_{h_{r_j}}, c^*_{X_{n-1}})$, $\forall c^*_{X_j} \in GF(q)$;

множина прямих відображень (на основі використання відкритого ключа – породжувальної матриці): $\varphi = \{\varphi_1, \varphi_2, ..., \varphi_s\}$, де $\varphi_i : M \to C_{h_r}$, $i = 1,2,...,s$;

множина обернених відображень (на основі використання закритого (особистого) ключа – матриць маскування): $\varphi^{-1} = \{\varphi_1^{-1}, \varphi_2^{-1}, ..., \varphi_s^{-1}\}$, де $\varphi_i^{-1} : C_{h_r} \to M$, $i = 1,2,...,s$;

множина ключів, яка параметризує прямі відображення (відкритий ключ уповноваженого користувача)): $K_{a_i} = \{K_{1_{a_i}}, K_{2_{a_i}}, ..., K_{s_{a_i}}\} = \{G_X^{EC_1}{}_{a_i}, G_X^{EC_2}{}_{a_i}, ..., G_X^{ECs}{}_{a_i}\}$, де $G_X^{EC_i}{}_{a_i}$ – породжувальна $k \times n$ матриця замаскованого під випадковий код алгеброгеометричного блокового (n,k,d) коду з елементами з $GF(q)$, тобто $\varphi_i : M \xrightarrow{K_{i a_i}} C_{hr}; i = 1,2,...,s$;

a_i – набір коефіцієнтів багаточлена кривої $a_1 \dots a_6$, $\forall a_i \in GF(q)$, що однозначно визначає конкретний набір точок кривої з простору P^2.

множина ключів, яка параметризує обернені відображення (особистий (закритий) ключ уповноваженого користувача)):

$$K^* = \{K_1^*, K_2^*, ..., K_s^*\} = \{\{X,P,D\}_1, \{X,P,D\}_2, ..., \{X,P,D\}_s\}, \{X,P,D\}_i = \{X^i, P^i, D^i\},$$

де X^i – маскуюча невироджена випадково рівноймовірно сформована джерелом ключів $k \times k$ матриця з елементами з $GF(q)$; P^i – перестановочна випадково рівноймовірно сформована джерелом ключів $n \times n$ матриця з елементами з $GF(q)$; D^i – діагональна сформована джерелом ключів $n \times n$ матриця з елементами з $GF(q)$, тобто – $\phi_i^{-1} : C \xrightarrow{K_i^*} M, i = 1,2,...,s$, складність виконання оберненого відображення φ_i^{-1} без знання ключа $K_i^* \in K^*$ пов'язана з розв'язанням теоретико-складної задачі – декодування випадкового коду (коду загального положення).

Вихідними даними при описі розглянутої МНККС є параметри, описані в попередній моделі.

У МНККС Мак-Еліса модифікований (подовжений) алгеброгеометричний *(n, k, d)* код C_{h_r} зі швидким алгоритмом розкодування маскується під випадковий *(n, k, d)* код C_{h_r} * за допомогою множення породжувальної матриці G^{EC} коду C_{k-h_j} на матриці маскування, які зберігаються в секреті X^u, P^u і D^u, що забезпечує формування відкритого ключа уповноваженого користувача:

$$G_X^{ECu} = X^u \cdot G^{EC} \cdot P^u \cdot D^u, \; u \in \{1,2,...,s\},$$

де G^{EC} – породжувальна матриця алгеброгеометричного блокового (n,k,d) коду з елементами з $GF(q)$, побудована на основі використання вибраних користувачем коефіцієнтів многочлена кривої $a_1 \dots a_6$, $\forall a_i \in GF(q)$, що однозначно визначає конкретний набір точок кривої з простору P^2.

Формування закритого тексту $C_j \in C_{h_r}$ за введеним відкритим текстом $M_i \in M$ і заданим відкритим ключем $G_X^{ECu}{}_{a_i}$, $u \in \{1,2,...,s\}$ здійснюється шляхом

формування укороченого кодового слова, а потім подовженням замаскованого коду з додаванням до нього випадково сформованого вектора $e=(e_0,e_1,...,e_{n-1})$:

$$C_j=\phi_u\left(M_i,G_X^u\right)=M_i\cdot\left(G_X^u\right)^T+e$$

Для кожного формованого закритого тексту $C_j\in C_{h_r}$ відповідний вектор $e=(e_0,e_1,...,e_{n-1})$ виступає одноразовим сеансовим ключем, тобто формується випадково, рівноймовірно і незалежно від інших закритих текстів.

У канал зв'язку надходить $C_j^{\ *}=C_j-C_{k-h_j}+C_{h_r}$.

На стороні прийому уповноважений користувач, який знає правило маскування, кількість і місця нульових інформаційних символів може скористатися швидким алгоритмом розкодування алгеброгеометричного коду (поліноміальної складності) для відновлення відкритого тексту:

$$M_i=\varphi_u^{-1}\left(C_j^{\ *},\{X,P,D\}_u\right).$$

Для відновлення відкритого тексту уповноважений користувач заміняє символи подовження на нульові інформаційні символи:

$$C_j^{\ *}=C_{h_r}\rightarrow C_{k-h_j},$$

з відновленого закритого тексту C_j знімає дію секретних перестановочної і діагональної матриць P^u и D^u:

$$\begin{aligned}
C &= C_j^{\ *}\cdot\left(D^u\right)^{-1}\cdot\left(P^u\right)^{-1}=\left(M_i\cdot\left(G_X^u\right)^T+e\right)\cdot\left(D^u\right)^{-1}\cdot\left(P^u\right)^{-1}= \\
&=\left(M_i\cdot\left(X^u\cdot G\cdot P^u\cdot D^u\right)^T+e\right)\cdot\left(D^u\right)^{-1}\cdot\left(P^u\right)^{-1}= \\
&=M_i\cdot\left(X^u\right)^T\cdot(G)^T\cdot\left(P^u\right)^T\cdot\left(D^u\right)^T\cdot\left(D^u\right)^{-1}\cdot\left(P^u\right)^{-1}+e\cdot\left(D^u\right)^{-1}\cdot\left(P^u\right)^{-1}= \\
&=M_i\cdot\left(X^u\right)^T\cdot(G)^T+e\cdot\left(D^u\right)^{-1}\cdot\left(P^u\right)^{-1},
\end{aligned}$$

розкодує отриманий вектор за алгоритмом Берлекемпа–Мессі:

$$C=M_i\cdot\left(X^u\right)^T\cdot\left(G^{EC}\right)^T+e\cdot\left(D^u\right)^{-1}\cdot\left(P^u\right)^{-1},$$

тобто позбавляється від другого доданка і від співмножника $(G)^{EC^T}$ в першому доданку в правій частині рівності, після чого знімає дію матриці маскування X^u.

Для цього отриманий результат розкодування M^*_i слід помножити на $\left(X^u\right)^{-1}$:

$$M^*_i \cdot \left(X^u\right)^{-1} = M_i .$$

Отримане рішення – відкритий текст M_i, до якого додаються символи подовження: $M_j = M_i + h_r$ і є переданим повідомленням.

Структурна схема протоколу обміну інформацією в режимі реального часу з використанням несиметричної криптосистеми на основі МНККС Мак-Еліса з модифікованими (подовженими) еліптичними кодами наведена на рис. 3.8.

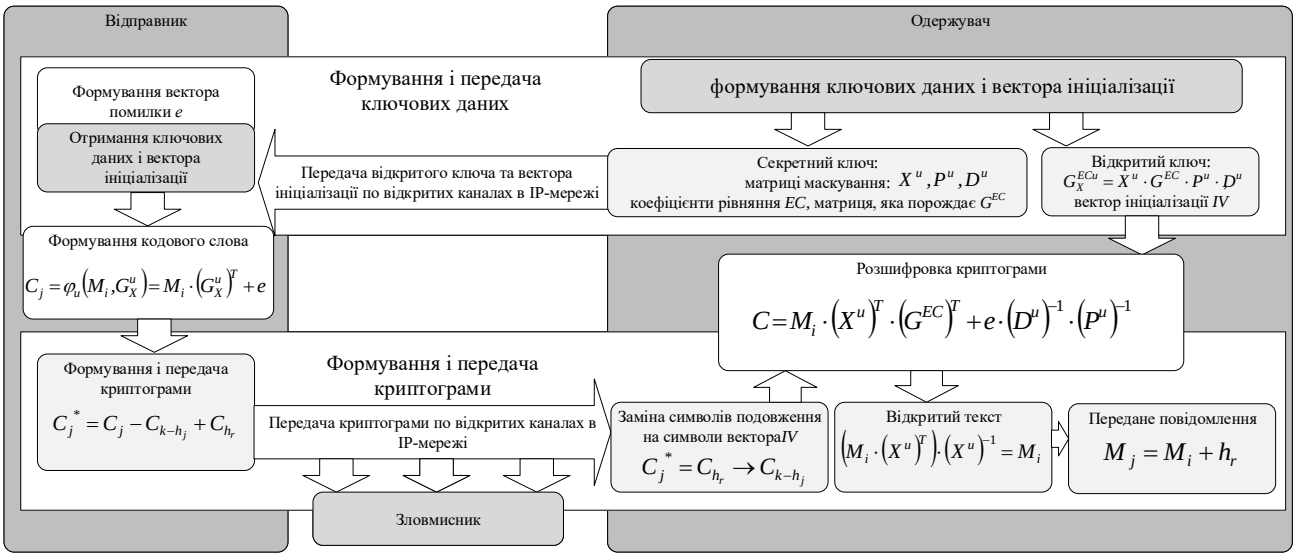
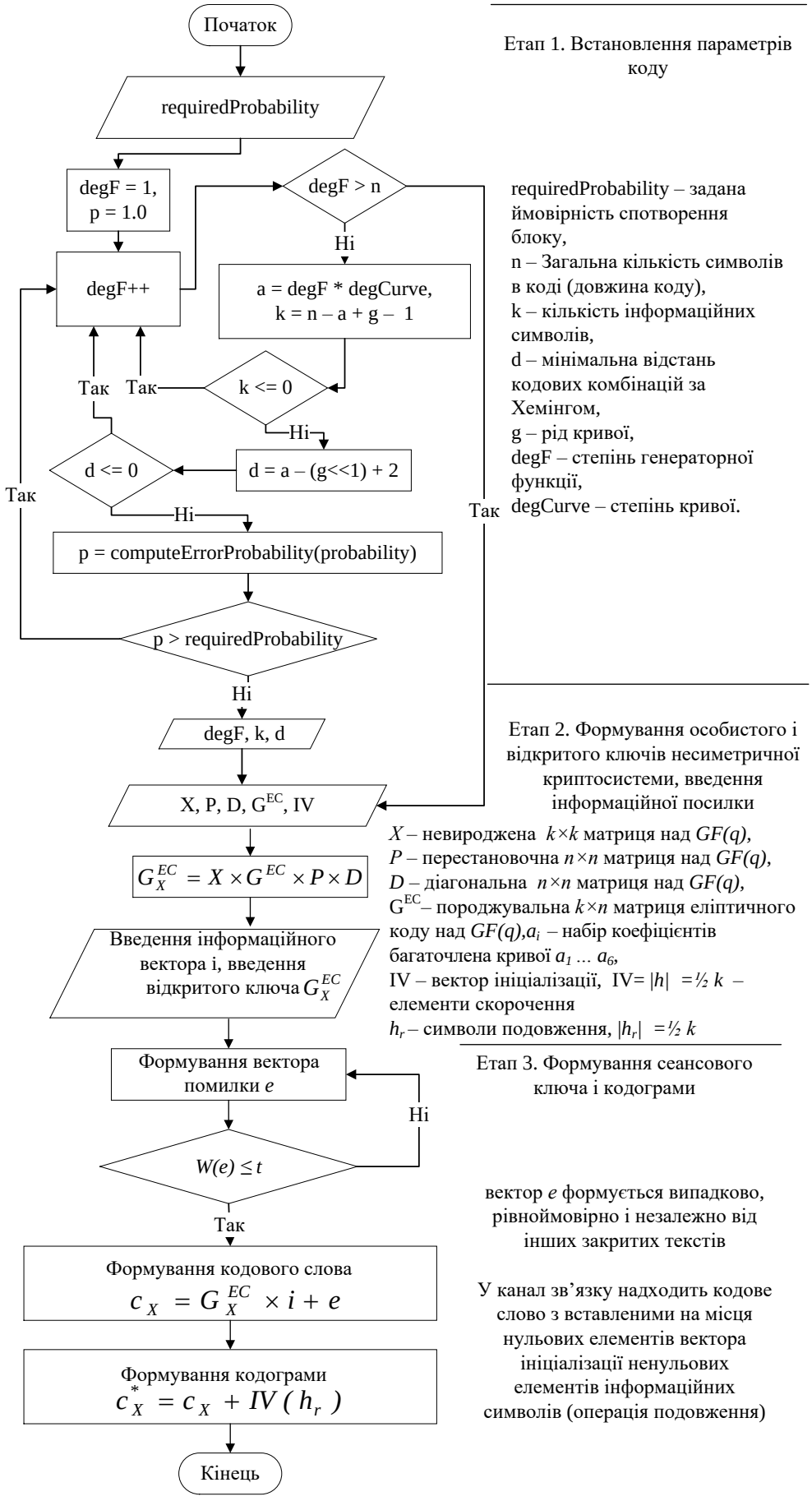


Рисунок 3.8 – Протокол обміну інформацією в режимі реального часу з МНККС з *MEC*

На рис. 3.9 наведений алгоритм кодування в МНККС Мак-Еліса на подовжених *MEC*, алгоритм розкодування наведений на рис. 3.10.



Етап 1. Встановлення параметрів коду

requiredProbability – задана ймовірність спотворення блоку,
n – Загальна кількість символів в коді (довжина коду),
k – кількість інформаційних символів,
d – мінімальна відстань кодових комбінацій за Хемінгом,
g – рід кривої,
degF – степінь генераторної функції,
degCurve – степінь кривої.

Етап 2. Формування особистого і відкритого ключів несиметричної криптосистеми, введення інформаційної посилки

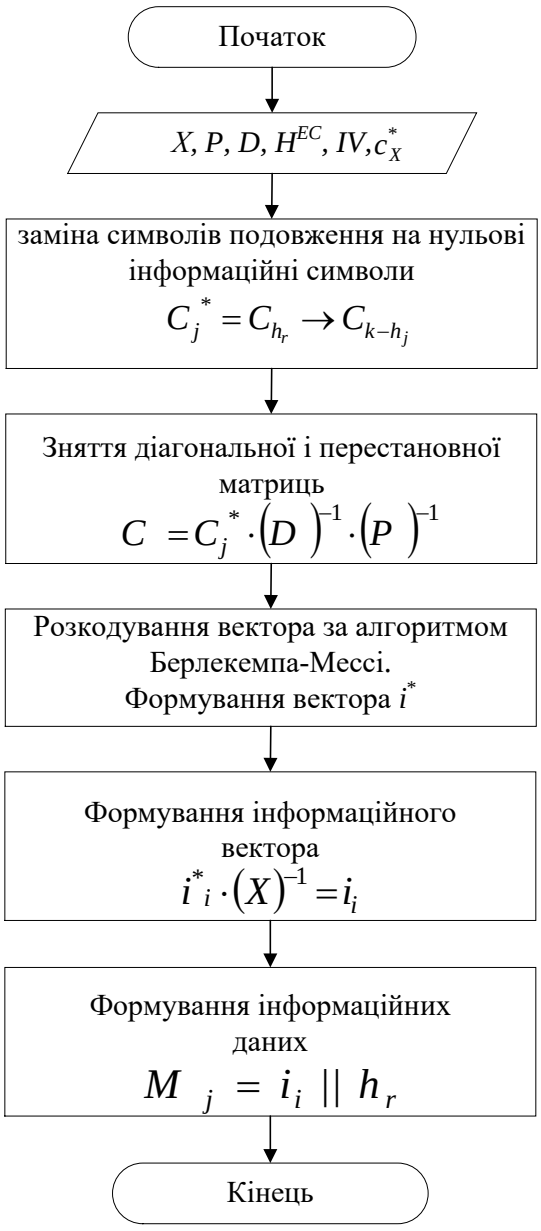
X – невироджена $k \times k$ матриця над *GF(q)*,
P – перестановочна $n \times n$ матриця над *GF(q)*,
D – діагональна $n \times n$ матриця над *GF(q)*,
G^{EC} – породжувальна $k \times n$ матриця еліптичного коду над *GF(q)*, a_i – набір коефіцієнтів багаточлена кривої $a_1 \ldots a_6$,
IV – вектор ініціалізації, IV= $|h| = ½\ k$ – елементи скорочення
h_r – символи подовження, $|h_r| = ½\ k$

Етап 3. Формування сеансового ключа і кодограми

вектор *e* формується випадково, рівноймовірно і незалежно від інших закритих текстів

У канал зв'язку надходить кодове слово з вставленими на місця нульових елементів вектора ініціалізації ненульових елементів інформаційних символів (операція подовження)

Рисунок 3.9 – Алгоритм формування кодограми в МНККС Мак-Еліса на подовжених *MEC*



Етап 1. Встановлення параметрів коду, введення особистого ключа та кодограми

X – невироджена $k \times k$ матриця над $GF(q)$,
P – перестановочна $n \times n$ матриця над $GF(q)$,
D – діагональна $n \times n$ матриця над $GF(q)$,
H^{EC} – перевірочна $r \times n$ матриця елиптичного коду над $GF(q)$, a_i – набір коефіцієнтів багаточлена кривої $a_1 \ldots a_6$,
IV – вектор ініціалізації, IV= $|h| = ½\ k$ – елементи скорочення

Етап 2. Розкодування кодограми

Етап 3. Формування інформаційних даних

Інформаційні дані формуються на основі алгоритму конкатенації інформаційного вектора і символів подовження. У разі виникнення помилки в символах подовження формується кодове слово довжиною n символів з нульовими елементами доповненими до символів подовження і застосовується алгоритм Берлекемпа для їх відновлення

Рисунок 3.10 – Алгоритм розкодування кодограми в МНККС Мак-Еліса на *MEC*

Для оцінки часових і швидкісних показників прийнято використовувати одиницю вимірювання *cpb*, де *cpb* (*cycles per byte*) – кількість тактів процесора, яку необхідно застосувати для обробки 1 байта вхідної інформації. Складність алгоритму обчислюється за виразом: $Per = Utl * CPU\_clock / Rate$, де Utl – утилізація ядра процесора (%); $Rate$ – пропускна здатність алгоритму (байт/с).

У табл. 3.6, 3.7, 3.8, 3.9 наведено результати досліджень залежності довжини кодової послідовності *MEC* (укорочених / подовжених) в МНККС Мак-Еліса від кількості тактів процесора на виконання елементарних операцій в програмній реалізації крипто-кодових систем.

Таблиця 3.6 – Результати досліджень залежності довжини кодової послідовності в МНККС Мак-Еліса на укорочених *MEC* від кількості тактів процесора

Довжина кодової послідовності		*McEliece* на укорочених кодах			*McEliece*		
		10	100	1000	10	100	1000
Кількість викликів функцій, що реалізовують елементарні операції	Читання символу	10294397	28750457	76759874	11018042	30800328	80859933
	Порівняння рядків	3406921	9246748	25478498	3663356	10199898	26364634
	Конкате-нація рядків	1705544	5045748	12379422	1834983	5125564	13415329
Сума		15406862	43042953	114617794	16516381	46125790	20639896
Тривалість виконання функцій * в тактах процесора	Читання символу	295374	810478	2001167	297487	831609	2183218
	Порівняння рядків	178814	531379	1248684	197 821	550794	1423690
	Конкате-нація рядків	544990	1328114	3586486	544 990	1522293	3984353
Сума		1006781	2749548	7247488	1040298	2904696	7591261
Тривалість виконання ** в мсек		0,52	1,37	3,4	0,55	1,53	4

Примітки:

** тривалість 1000 операцій в тактах процесора: читання символу – 27 тактів, порівняння рядків – 54 такти, конкатенація рядків – 297 тактів.*

*** для розрахунку взято процесор з тактовою частотою 2 ГГц з урахуванням завантаження операційної системи 5%.*

Таблиця 3.7 – Результати досліджень оцінки часових і швидкісних показників процедур формування і розкодування інформації в МНККС на укорочених *MEC*

Показники	Довжина кодової послідовності	Пропускна здатність алгоритму, *Rate*, (байтів / с)	Утилізація ядра процесора (%)	Складність алгоритму, *Per* (*cpb*)
Кількість викликів функцій, що реалізують елементарні операції	100	46 125 790	56	61,5
	1000	120 639 896	56	62,0

Таблиця 3.8 – Результати досліджень залежності довжини кодової послідовності в МНККС Мак-Еліса на подовжених *MEC* від кількості тактів процесора

Довжина кодової послідовності		*McEliece* на подовжених кодах			*McEliece*		
		10	100	1000	10	100	1000
Кількість викликів функцій, що реалізують елементарні операції	Читання символу	11432131	33460317	82473442	1101804	3080032	8085993
	Порівняння рядків	3673756	12119867	29469389	3663356	10199898	26364634
	Конкатенація рядків	1947681	6114478	14456729	1834983	5125564	13415329
Сума		17053568	51694662	126399560	16516381	46125790	120639896
Тривалість виконання функцій* в тактах процесора	Читання символу	300479	843705	2745148	297487	831609	2183218
	Порівняння рядків	213478	561754	1739170	197821	550794	1423690
	Конкатенація рядків	578174	1647638	4007883	544990	1522293	3984353
Сума		109157	1092131	3053097	1040298	2904696	7591261
Тривалість виконання ** в мсек		0,56	1,55	4,1	0,55	1,53	4

Таблиця 3.9 – Результати досліджень оцінки тимчасових і швидкісних показників процедур формування і розкодування інформації

Показники	Довжина кодової послідовності	Пропускна здатність алгоритму, *Rate*, (байтів / с)	Утилізація ядра процесора (%)	Складність алгоритму, *Per* (*cpb*)
НККС Мак-Еліса на ЕС	100	46 125 790	56	61,5
	1000	120 639 896	56	62,0
МККС Мак- Еліса на МЕС	100	51 694 662	56	61,7
	1000	126 399 560	56	62,2

Аналіз табл. 3.6, 3.7, 3.8, 3.9 свідчить, що використання модифікованих (укорочених / подовжених) *MEC* дозволяє зменшити енергетичну ємність

програмної реалізації МНККС Мак-Еліса практично в 2 рази, але при цьому забезпечити необхідний рівень криптостійкості при реалізації над меншим полем $GF(2^6 – 2^8)$. Розглянемо основні властивості запропонованих модифікованих криптосистем (швидкість криптоперетворень, складність злому та інш.).

3.1.4. Дослідження властивостей криптосистем на модифікованих еліптичних кодах

Проведемо порівняльне оцінювання параметрів НККС Мак-Еліса на *EC* з МНККС з використанням модифікованих еліптичних кодів. Введемо такі позначення:

l_I – довжина інформаційної послідовності (блока), яка надходить на вхід ККС схеми (в бітах); l_K – довжина відкритого ключа (в бітах); l_{K+} – довжина закритого ключа (в бітах); l_S – довжина кодограми (в бітах); O_K – складність формування кодограми (кількість групових операцій); O_{SK} – складність розкодування кодограми (кількість групових операцій); O_{K+} – складність розв’язання задачі аналізу (кількість групових операцій). Для побудови графіків були використані умовні скорочення (префікси): *uk* – МНККС з укороченими *MEC*; *ud* – МНККС з подовженими *MEC*. При розрахунках параметрів криптосистем були використані поля Галуа: для ТКС Мак-Еліса – $GF\ (2^{10})$; для МНККС з укороченими / подовженими *MEC* – $GF\ (2^6)$.

Для оцінювання *довжини інформаційної послідовності* (в бітах), що надходить на вхід МНККС з *MEC* (n, k, d)-кодом над $GF\ (2^m)$ використаємо вирази:

– для НТКС на *EC*: $l_I = k \times m$;

– для МНККС на укорочених кодах *MEC*: $l_I = 1/2k \times m$;

– для МНККС на подовжених кодах *MEC*: $l_I = k \times m$.

У табл. 3.10 і на рис. 3.11 наведені залежності складності формування кодограми від потужності поля.

З наведених даних видно, що складність формування криптограми для обраної потужності поля Галуа 2^6 на укорочених і подовжених кодах значно нижче

(в 5 разів і більше), ніж в оригінальній реалізації НТКС на *EC*. Відповідно, швидкість формування криптограми істотно збільшується.

Таблиця 3.10 – Залежність складності формування криптограми в різних $GF(2^m)$

$GF(2^m)$	Відносна швидкість кодування, R					
	0.5	0.75	0.5(ud)	0.75(ud)	0.5(uk)	0.75(uk)
3	31	87	242	603	817	968
4	76	340	760	980	2140	6282
5	335	872	2241	6121	8706	11461
6	582	2170	**6348**	**9830**	**10722**	**60760**
7	1023	6172	17092	61751	83000	210170
8	5237	10673	67016	105265	207422	605005
9	10563	50487	98765	510780	710920	1018079
10	**52704**	**103822**	497309	908243	4572881	5561379

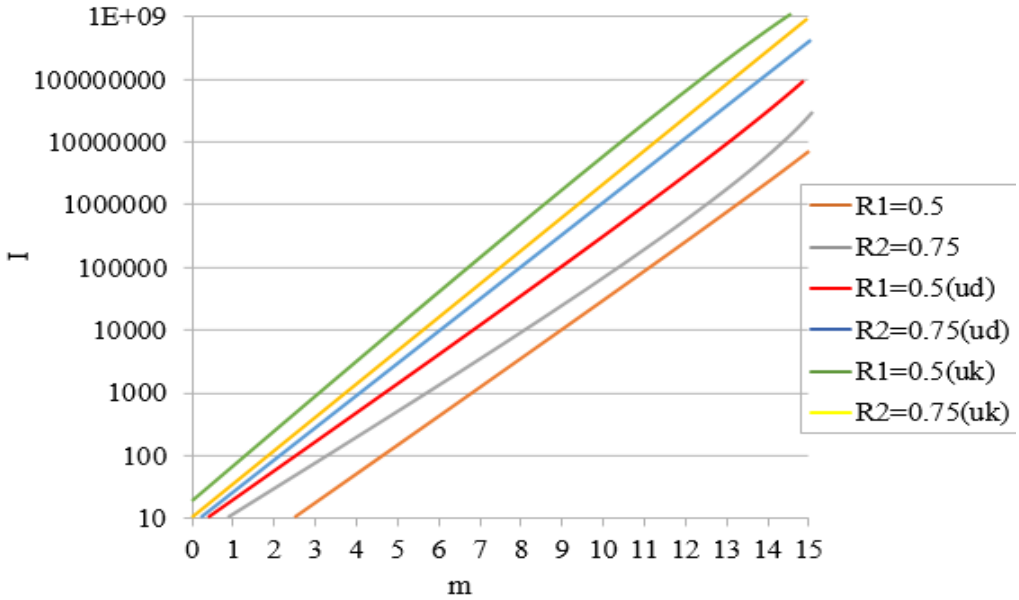


Рисунок 3.11 – Залежність складності формування криптограми в різних $GF(2^m)$

Для оцінювання *довжини кодограми* (в бітах) використаємо такі вирази:

– для НТКС на *EC*: $l_s = n \times m$;

– для МНККС на укорочених *MEC*: $l_S = \left(2\sqrt{q} + q + 1 - 1/2k\right) \times m$;

– для МНККС на подовжених *MEC*: $l_S = \left(2\sqrt{q} + q + 1 - 1/2k + 1/2k\right) \times m$.

У табл. 3.11 та на рис. 3.12 наведені залежності складності розкодування кодограми від потужності поля.

Таблиця 3.11 – Залежності складності розкодування кодограми від потужності поля $GF(2^m)$

$GF(2^m)$	R					
	0.5	0.75	0.5(ud)	0.75(ud)	0.5(uk)	0.75(uk)
1	43	57	78	81	82	96
2	67	98	456	457	457	556
3	120	640	1024	1168	1280	5127
4	680	2378	7672	8232	11028	23674
5	2092	7512	21073	42082	78634	277830
6	12397	61246	**103862**	**281472**	**760553**	**5220573**
7	127523	136495	642648	752018	4566721	19768512
8	1203984	1494284	3564898	3957812	12948312	52694229
9	10637991	12768954	54678128	67458242	92516734	102564872
10	**175645127**	**193648924**	1e+09	1e+09	1e+09	1e+09

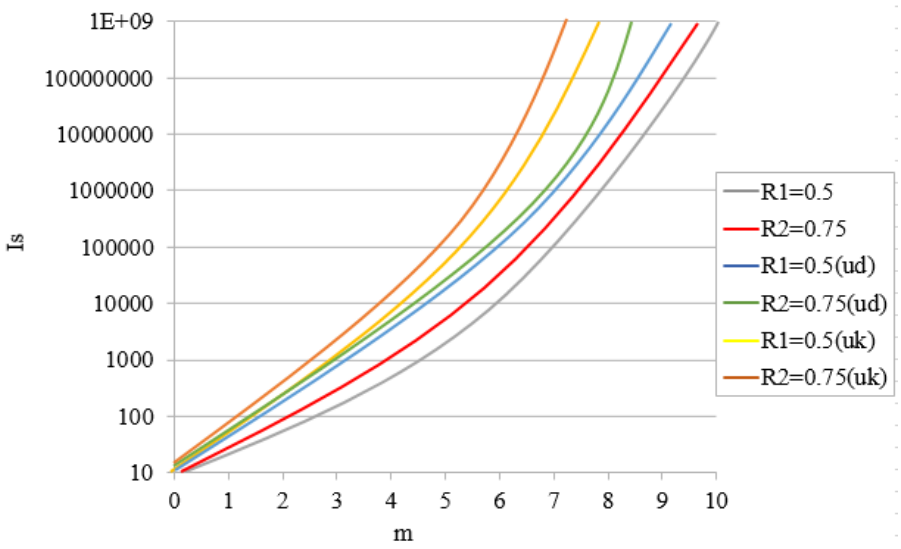


Рисунок 3.12 – Залежність складності розкодування криптограми в різних $GF(2^m)$

Аналіз результатів розрахунків, як і у випадку формування криптограми, свідчить про зростання швидкості розкодування при використанні укорочених і подовжених *МЕС*.

Довжина відкритого ключа (в бітах) визначається сумою елементів матриці G_X^{EC} і задається виразами:

– для НТКС на *ЕС*: $l_K = k \times n \times m$;

– для МНККС на укорочених *МЕС*: $l_K = 1/2k \times \left(2\sqrt{q} + q + 1 - 1/2k\right) \times m$;

– для МНККС на подовжених *МЕС*: $l_K = 1/2k \times \left(2\sqrt{q} + q + 1 - 1/2k + 1/2k\right) \times m$.

Довжина закритого ключа (в бітах) визначається сумою елементів матриць *X, P, D* (в бітах) і задається виразами:

– для НТКС на *ЕС*: $l_{K+} = n^2 \times k^2 \times m$;

– для МНККС на укорочених *МЕС*: $l_{K_+} = 1/2k \left\lceil \log_2\left(2\sqrt{q} + q + 1\right) \right\rceil$,

– для МНККС на подовжених *МЕС*: $l_{K_+} = \left(1/2k - 1/2k\right) \left\lceil \log_2\left(2\sqrt{q} + q + 1\right) \right\rceil$.

У табл. 3.12 і на рис. 3.13 наведені залежності складності злому на основі перестановочного декодування від потужності поля.

Таблиця 3.12 – Залежність складності злому в різних $GF(2^m)$

$GF(2^m)$	*R*					
	0.5	0.75	0.5(ud)	0.75(ud)	0.5(uk)	0.75(uk)
1	1.056	1.38	2.786	2.835	4.122	4.257
2	2.237	3.017	4.978	5.961	6.233	6.781
3	2.868	4.867	7.568	8.120	8.234	9.764
4	4.843	6.613	9.87	12.1	12.647	13.32
5	6.22	8.03	12.017	14.224	14.742	16.892
6	7.891	12.245	**14.983**	**17.483**	**18.767**	**19.76**
7	8.995	13.13	17.14	20.32	21.102	22.93
8	10.37	15.16	19.55	23.23	24.05	26.11
9	11.74	17.18	21.96	26.15	27.002	29.302
10	13.19	19.23	24.37	29.06	29.95	32.484

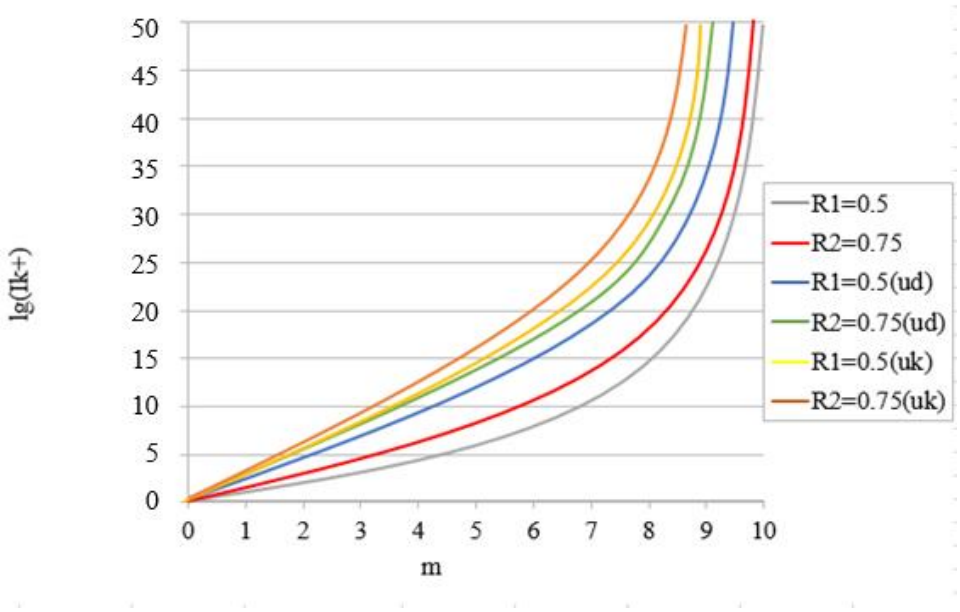


Рисунок 3.13 – Залежність складності злому в різних $GF(2^m)$ (переставне декодування)

Аналіз рис. 3.13 показав, що зменшення потужності поля до 2^6 не привело до істотного зниження складності злому криптограми методом переставного декодування.

Складність формування кодограми оцінюється за такими виразами:

– для НТКС на *ЕС*: при реалізації систематичного кодування: $O_K = (r+1) \times n$;

– для несистематичного кодування: $O_K = (k+1) \times n$;

– для МНККС на укорочених *МЕС*: при реалізації систематичного кодування:

$$O_K = (r+1)\times\left(2\sqrt{q}+q+1-1/2k\right);$$

– для несистематичного кодування:

$$O_K = (k+1)\times\left(2\sqrt{q}+q+1-1/2k\right).$$

– для МНККС на подовжених *МЕС*: при реалізації систематичного кодування: $O_K = (r+1)\times\left(2\sqrt{q}+q+1-1/2k+1/2k\right)$;

– для несистематичного кодування:

$$O_K = (k+1)\times\left(2\sqrt{q}+q+1-1/2k+1/2k\right).$$

Складність розкодування кодограми визначається за такими виразами:

– для НТКС на *EC*: $O_{SK} = 2\times n^2+k^2+4t^2 + (t^2 + t - 2)^2/4$; для МНККС на укорочених *MEC*: $O_{SK} = 2\left(2\sqrt{q}+q+1-1/2k\right)^2 + 1/2k^2 + 4t^2 + \left(t^2+t-2\right)^2/4$;

для МНККС на подовжених *MEC*:

$$O_{SK} = 2\times\left(2\sqrt{q}+q+1-1/2k+1/2k\right)+k^2+4t^2+\left(t^2+t-2\right)^2/4.$$

Складність процесу декодування задається виразом:

– для НТКС на *EC*:

$$O_{K+} = N_{покр}\times n\times r, \qquad (3.26)$$

де $N_{покр} \ge \frac{C_n^{\rho\cdot t}}{C_{n-k}^{\rho\cdot t}} = \frac{n(n-1)...(n-\rho\cdot t-1)}{(n-k)(n-k-1)...(n-k-\rho\cdot t-1)}$, $t = \lfloor (d-1)/2 \rfloor$.

Потенційна стійкість криптосистеми визначається величиною $\rho \times t$, а стійкість системи – $(1-\rho)\times t$.

– для МНККС на укорочених кодах *MEC*: $O_{K+} = N_{покр}\times\left(2\sqrt{q}+q+1-1/2k\right)\times r$;

– для МНККС на подовжених кодах *MEC*:

$$O_{K+} = N_{покр}\times\left(2\sqrt{q}+q+1-1/2k+1/2k\right)\times r.$$

У табл. 3.13 і на рис. 3.14 наведені залежності складності злому і складності кодування для різних швидкостей *EC* (*MEC*).

Таблиця 3.13 – Зведена діаграма складності злому і складності кодування для різних швидкостей *EC*

$lg(l_s)$	0.5	0.75	0.5(ud)	0.75(ud)	0.5(uk)	0.75(uk)
1	4.75	12.1	15.6	18.23	19.12	19.82
2	10.52	21.76	32.47	35.67	38.63	39.18
3	18.22	33.17	43.75	51.61	56.88	58.03
4	21.42	51.75	59.43	72.81	78.92	80.52
5	38.77	61.09	68.26	87.32	94.91	104.56
6	54.13	78.37	**101.72**	**112.46**	**120.83**	**128.79**
7	82.14	83.72	156.75	164.72	182.39	189.74
8	165.84	179.13	223.64	231.57	276.27	287.33
9	358.33	371.09	421.97	428.63	459.81	476.52
10	**672.37**	**684.94**	716.41	722.26	783.46	794.28

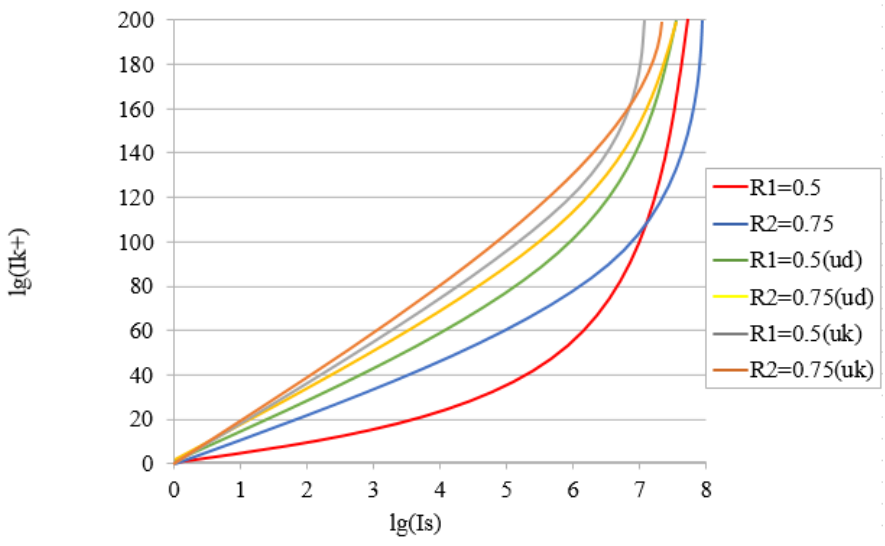


Рисунок 3.14 – Зведена діаграма складності злому і складності кодування для різних швидкостей *EC* (*MEC*)

У табл. 3.14 і на рис. 3.15 наведені залежності обсягу відкритих ключових даних для різних показників стійкості.

Таблиця 3.14 – Залежності обсягу відкритих ключових даних для різних показників стійкості

$lg(l_{k+})$	*R*					
	0.5	0.75	0.5(ud)	0.75(ud)	0.5(uk)	0.75(uk)
5	30	87	240	602	968	799
20	2278137	4351076	926137	987234	1034682	1897092
35	**12329538**	**14097276**	**4253109**	**5237688**	**6126273**	**6832018**
50	22541273	77520337	43076332	60122407	8602376	7027160

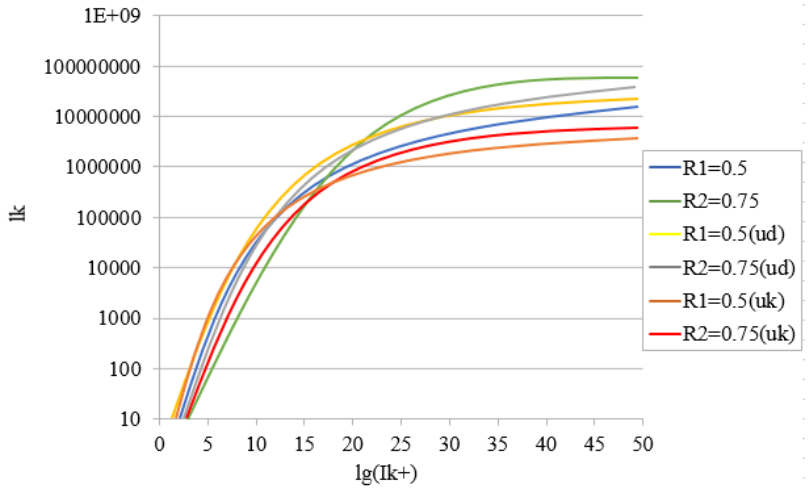


Рисунок 3.15 – Залежності обсягу відкритих ключових даних для різних показників стійкості

Аналіз наведених результатів табл. 3.13, 3.14, та рис. 3.14, 3.15 ясно демонструє за рахунок чого отримано зростання відносної швидкості передачі даних: обсяг ключових даних в системах на укорочених / подовжених кодах вдвічі менший за класичну НККС.

У табл. 3.15 наведені результати досліджень ємнісний характеристики при програмної реалізації від потужності поля.

Таблиця 3.15 – Залежність швидкості програмної реалізації від потужності поля (кількість групових операцій)

Криптосистеми	2^5	2^6	2^7	2^8	2^9	2^{10}
НККС *MacElis* на *EC*	10018042	18048068	32847145	47489784	63215578	**82467897**
МНККС *MacElis* на укорочених *MEC*	10007947	**17787431**	28595014	44079433	61974253	79554764
МНККС *MacElis* на подовжених *MEC*	11156138	**18561228**	33210708	48297112	65171690	84051337

Результуюча табл. 3.15 показує кількість групових операцій програмної реалізації НККС залежно від потужності поля. Видно, якщо для реалізації НККС Мак-Еліса в *GF* (2^{10}) необхідно $82{,}5 \times 10^6$ групових операцій, то реалізація МНККС на укорочених / подовжених *MEC* в *GF* (2^6) вимагає $17{,}7 – 18{,}6 \times 10^6$ групових операцій, тобто в 4,5 рази менше. Розглянемо подальше зменшення енергетичних втрат при практичної реалізації МНККС Мак-Еліса та Нідеррайтера, що запропоновано в наступному підрозділі.

3.2. Розроблення методу забезпечення цілісності та конфіденційності банківських інформаційних ресурсів на гібридних крипто-кодових конструкціях зі збитковими кодами

3.2.1. Дослідження властивостей побудови криптосистем на збиткових кодах

Для забезпечення основних послуг безпеки БІР в умовах зростання загроз ІБ, КБ, БІ пропонується в СКЗІ АБС використовувати гібридні крипто-кодові

конструкції, що засновані на синтезі МНККС Мак-Еліса і Нідеррайтера на *МЕС* та збиткових кодах многоканальної криптографії.

У роботах [39; 40] розглянуто теоретичні та практичні основи побудови збиткових кодів. Під *збитковим текстом розуміється текст, отриманий у результаті подальшої деформації ненадлишкових кодів букв* [39].

Таким чином, необхідною і достатньою умовою збитковості тексту з втратою сенсу є скорочення довжин кодів символів тексту за межами їх надмірності. Як наслідок, збитковий текст має довжину меншу довжини вихідного тексту, і не має сенсу вихідного тексту [39].

Теоретичною основою побудови збиткових текстів є порушення впорядкованості символів вихідного тексту і як наслідок зниження надмірності символів мови в збитковому тексті.

При цьому кількість інформації, що виражає цю впорядкованість, дорівнюватиме зменшенню ентропії тексту в порівнянні з максимально можливою величиною ентропії, тобто рівноймовірній появи будь-якої літери після будь-якої попередньої літери. Методи обчислення інформації, запропоновані в роботі [45], дозволяють виявити співвідношення кількості передбаченої (тобто сформованої за певними правилами) інформації і кількості тієї несподіваної інформації, яку не можна заздалегідь передбачити. Надлишковість тексту визначається за виразом:

$$B(M) = B_A L_0 = \left(log\, N - \frac{H(M)}{L_0} \right) \times L_0 , \qquad (3.27)$$

де M – початковий текст;

B – надлишковість мови ($B = R - r$; R – надлишковість мови ($R = \log N$; N – потужність алфавіту; r – ентропія мови на один символ, $r = H(M) / L$; L – довжина повідомлення M в символах мови));

$H(M)$ – ентропія (невизначеність) повідомлення;

L_0 – довжина повідомлення M символах мови зі змістом;

B_A – надлишковість мови.

Для отримання збиткового тексту (*FTC*) і збитків (*DCH*) використовується метод “ідеального” стиснення після виконання *m* циклів механізму завдання збитку C_m [39; 40].

Кількість циклів, необхідних для зменшення довжини початкового тексту дорівнює:

$$m\rangle \frac{\log n - B_A}{\log \eta}, \tag{3.28}$$

де *n* – потужність представлення символу вихідного тексту;

B_A – надлишковість мови;

η – кількість разів зменшення довжини початкового тексту в *MV*2 на кожному кроці (деякий постійний коефіцієнт).

Кількісною мірою ефективності нанесення збитку є ступінь зміни сенсу, що дорівнює різниці ентропій збиткового тексту і вихідного тексту на різних відрізках довжини збиткового тексту:

$$d = H(FTC) - \sum_{i=1}^{s} H(M_i)\, p_i, \quad \sum_{i=1}^{s} p_i = 1, \quad s = \left[\frac{L_0 - L_{FTC}}{L_{FTC}} \right], \tag{3.29}$$

де M_i – частина вихідного тексту, що відповідає *i*-му відрізку; p_i – її ймовірність; L_0 – довжина M_i, що дорівнює довжині L_{FTC} – збиткового тексту; *s* – кількість відрізків.

Для ергодичності джерела символів вихідного тексту маємо:

$$d_{max} = \log L_{FTC} - H(M_i). \tag{3.30}$$

На рис. 3.16 наведена структурна схема одного кроку універсального механізму заподіяння збитку.

Під *інформаційним ядром* деякого тексту розуміється збитковий текст *CFT*, отриманий у результаті циклічного перетворення універсального механізму заподіяння збитку C_m.

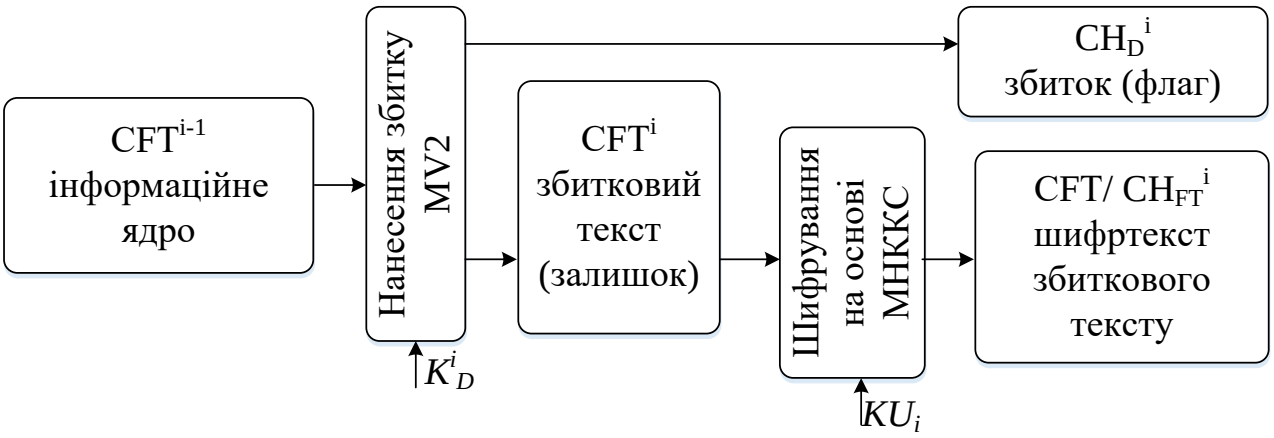


Рисунок 3.16 – Структурна схема одного кроку універсального механізму заподіяння збитку

Універсальний механізм нанесення збитку C_m може бути описаний [39; 40]:

$$CFT / CH_{FT} = E_1\left(M, KU^{EC}\right),$$
$$CHD / CH_D = E_2\left(M, KU^{EC}\right),$$
$$M = E_{1,2}^{-1}(CFT / CH_{FT}, CHD / CH_D, KU^{EC}),$$

$$CFT / CH_{FT} = CFT / CH_{FT}^i, ..., CFT / CH_{FT}^m,$$

де $KU^{EC} = \varphi(K_D^i, ..., K_D^m, KU_1^{EC}, ..., KU_m^{EC},$

$$CHD / CH_D = CHD / CH_D^i, ..., CHD / CH_D^m$$

.

Таким чином, в результаті маємо два шифртексти (збиток (CH_D) і збитковий текст (FTC)), кожен з яких не має сенсу ні в алфавіті початкового тексту, ні в алфавіті шифртекста. Фактично шифртекст вихідного повідомлення (M) подається у вигляді сукупності двох збиткових шифртекстів, кожен з яких окремо не може відновити вихідний текст.

Для відновлення початкової послідовності немає необхідності знати проміжні збиткові послідовності. Необхідно знати тільки останню збиткову послідовність (останній збитковий текст після виконання всіх циклів) і всі збитки з правилами їх нанесення. Основні способи нанесення збитку наведені на рис. 3.17, 3.18 наведені основні протоколи забезпечення послуг безпеки на основі використання збиткових кодів.

Рисунок 3.17 – Основні способи нанесення збитку

Криптографічними збитковими текстами називаються тексти, отримані такими способами [39]:

– збитку початковому тексту з подальшим шифруванням збиткового тексту і / або його збитків;

– нанесення збитку шифртексту;

– нанесення збитку шифртексту збиткового тексту і / або шифртексту збитків.

Основною перевагою запропонованих способів і протоколів забезпечення послуг безпеки на основі використання збиткових кодів є використання не БСШ, а МНККС Мак-Еліса і Нідеррайтера на модифікованих укорочених або подовжених еліптичних кодах для забезпечення криптостійкості збитку і / або збитковому тексту.

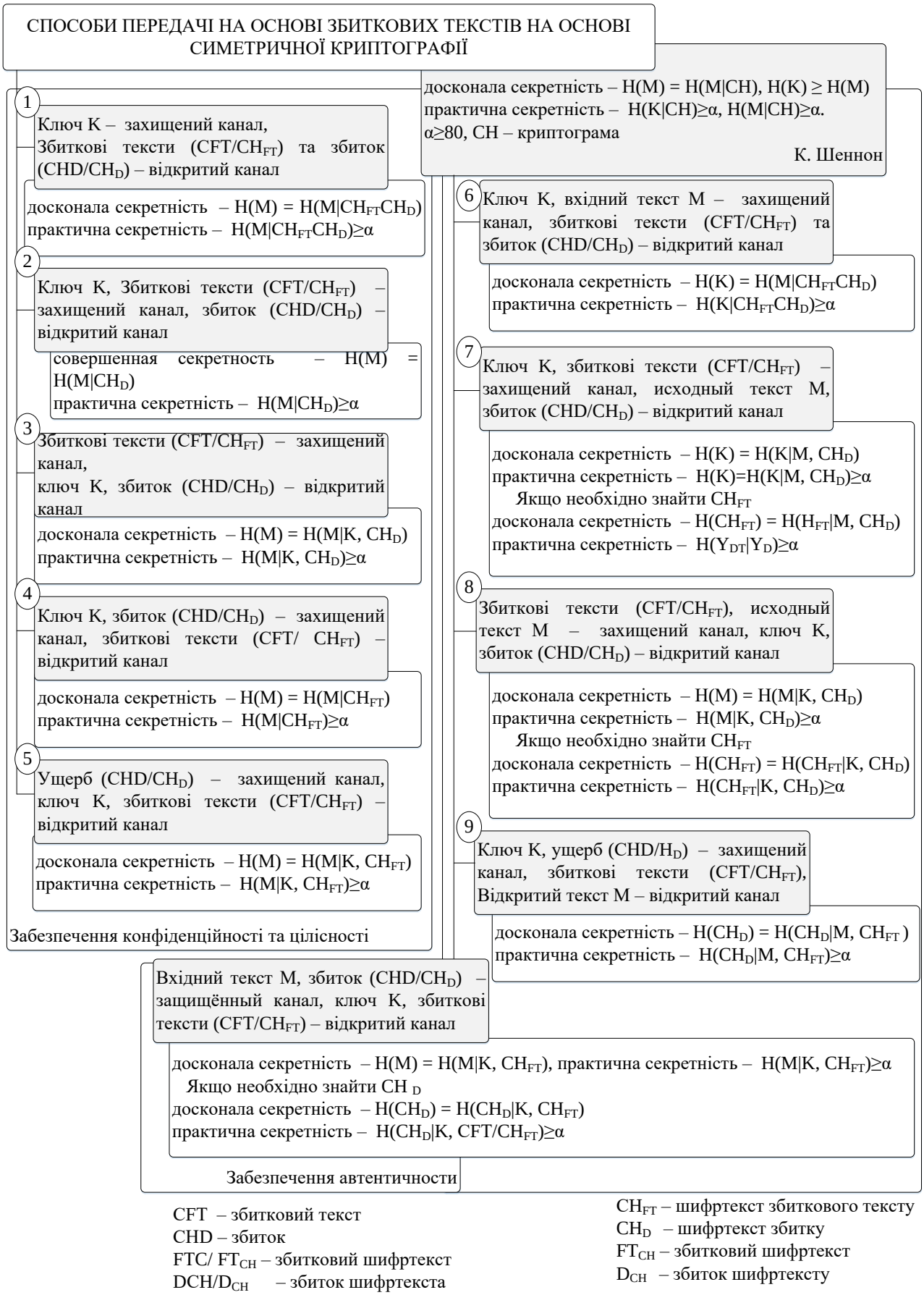


Рисунок 3.18 – Основні протоколи забезпечення послуг безпеки

Відстань єдності для моделі випадкового шифру для якого існує ймовірність отримати осмислений текст при випадковому і рівноймовірному виборі ключа K та спробі дешифрування шифртекста при $N_S = H(K)\frac{2^{HL}}{|I|^L} = 1$ дорівнює:

$$L = U_0 = \frac{H(K)}{\log|I| - H} = \frac{H(K)}{B\log|I|}, \tag{3.31}$$

де B – надлишковість вихідного тексту; H – ентропія на букву осмисленого тексту у вхідному алфавіті I, $|I| > 2$; 2^{HL} – наближене значення кількості осмислених текстів.

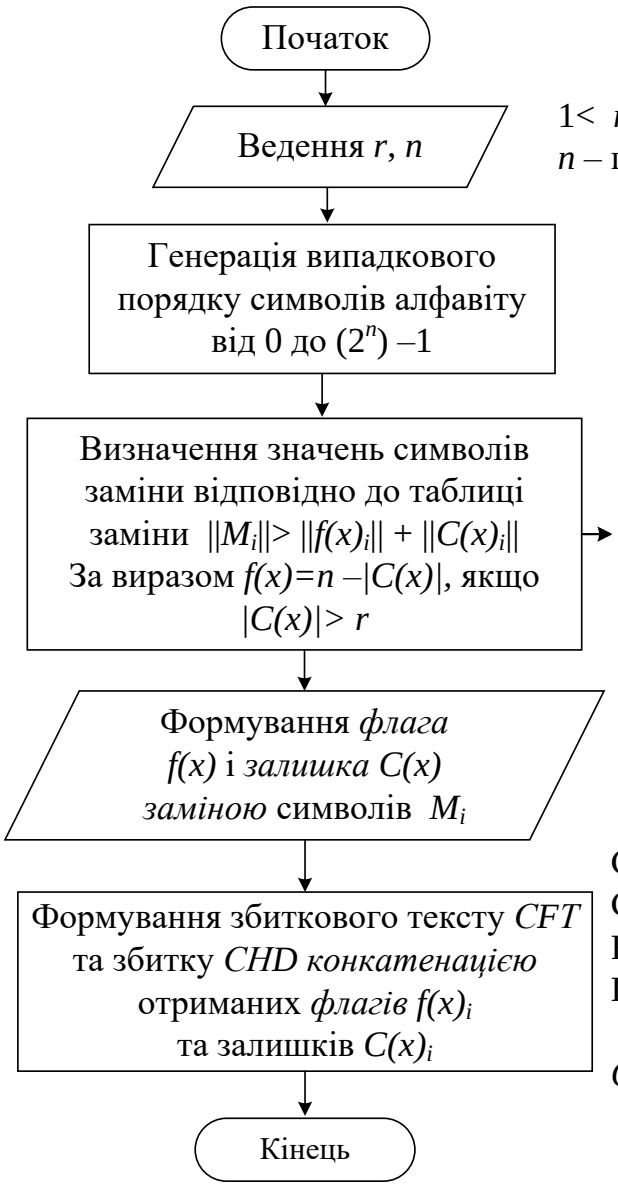
У роботах [39; 40] під *циклічним алгоритмом отримання збиткових текстів* розуміється універсальний механізм нанесення збитку (C_m, де m – кількість циклів), що полягає у випадковій заміні бітового уявлення кожного символу вихідного тексту кортежем меншої або рівної кількості бітів з подальшою їх конкатенацією.

На рис. 3.19 наведений універсальний механізм нанесення збитку (алгоритм *MV*2 (формування збиткового тексту)).

Область визначення перетворення в алгоритмі *MV*2 – множина $\{0, 1\}^n$ – розглядаємо як потужність алфавіту деякого сімейства вихідних текстів, з яким пов'язано деякий розподіл ймовірностей букв цього алфавіту, а символи вихідного тексту – значення дискретного випадкового елемента [39]. Нехай X – випадковий дискретний елемент, який набуває значення $x_i \in \{0,1\}^n$ з імовірністю p_i, і $T = (c, f) \in F_n^r$ – довільне фіксоване перетворення *MV*2.

Тоді для будь-якого $y \in U_{r\,n-1}$ (деякий двійковий рядок з множини рядків змінної довжини) і для будь-якого $1 \le i \le |y|$ виконується така рівність:

$$\#\left\{x \in \{0,1\}^n : c(x) = y\right\} = \#\left\{x \in \{0,1\}^n : c(x) = y^{(i)}\right\}.$$



$1 < r < n$ – додатне ціле число
n – потужність алфавіту

Символ	Довжина залишку	Залишок $C(x)$	Флаг $f(x)$
S_1	r	0^r	$0^{n-r-1}1$
S_2	r	$0^{r-1}1$	$0^{n-r-1}1$
…	…	…	…
$S_2{}^r{}_{+1}$	$r+1$	0^{r+1}	$0^{n-r-2}1$
…	…	…	…
$S_2{}^{n-1}{}_{-2^r}$	$n-2$	1^{n-2}	01
$S_2{}^{n-1}{}_{-2^r+1}$	$n-1$	0^{n-1}	1
…	…	…	…
$S_2{}^n{}_{-2^r}$	$n-1$	1^{n-1}	1
$S_2{}^n{}_{-2^r+1}$	r	0^r	0^{n-r}
…	…	…	…
$S_2{}^n$	r	1^r	0^{n-r}

CFT/ CH_{FT} – шифртекст збиткового текста
CHD/CH_D – шифртекст збитку
FTC/ FT_{CH} – збитковий шифртекст
DCH/D_{CH} – збиток шифртексту
$f(x)$ – флаг (збиток)
$C(x)$ – залишок (збитковий код)

Рисунок 3.19 – Універсальний механізм нанесення збитку – алгоритм *MV*2 (формування збиткового тексту)

Тоді незалежно від розподілу ймовірностей випадкового елемента X для ентропій випадкових елементів FTC/FT_{CH} (збиткового шифртексту) і CHD (збитку) виконуються рівності:

$$H(FTC / FT_{CH}) \le \log(2^n - 2^r),\ H(CHD) \le \log(n - r + 1).$$

Таким чином, при рівномірному розподілі входів (флагів) алгоритму *MV*2 формується рівномірний розподіл виходу (залишку):

$$P(c_k = 0 \left| 0 \le k \le \right| FTC / FT_{CH} \|) = \frac{1}{2}$$

Проведений аналіз способів нанесення збитку показав, що для використання в АБС найбільш підходящими є перший та другий способи нанесення збитку з подальшим криптоперетворенням, що дозволяє знизити потужність алфавіту при формуванні криптограми в МНККС Мак-Еліса. Відстань єдності для першого способу (вираз 3.31) буде трансформовано:

$$U_0 = \frac{\sum_{i=1}^{m} \left(H\left(CHD^{(i)} \right) \right) + H(KU_i^{EC})}{B log \left| I \right|}. \qquad (3.32)$$

Така система базується на непоправності спотворенні збитку і забезпеченні стійкості за рахунок використання в подальшому шифрування на основі МНККС. Це призводить до неможливості дізнатися шифртекст збиткового тексту.

Відстань єдності для другого способу (вираз 3.31) буде трансформовано:

$$U_0 = \frac{H(KU_i^{EC}) + H(FTC/ FT_{CH}) + H(DCH/ D_{CH}) + \sum_{i=1}^{m} \left(H\left(CHD^{(i)} \right) \right) + H(KU_i^{EC})}{B log \left| I \right|}. \qquad (3.33)$$

Другий варіант дозволяє збільшити відстань єдності порівняно з першим способом. У табл. 3.16 наведені результати досліджень залежності довжини вхідної послідовності на алгоритм *MV*2 від кількості тактів процесора на виконання елементарних операцій в програмній реалізації.

Таблиця 3.16 – Результати досліджень залежності довжини вхідної послідовності на алгоритм *MV*2 від кількості тактів процесора

Довжина кодової послідовності		*MV*2		
		10	100	1000
Кількість викликів функцій що реалізовують елементарні операції	сумування	3942	28673	275499
	різниця	1794	3810	23881
	ділення	3274	4804	20104
	множення	19	109	1009
	порівняння	8939	60963	578784
Сума		17968	98359	899277
Тривалість виконання функцій * в мілісекундах	сумування	19.53	93.58	2297.36
	різниця	8.89	12.43	199.14
	ділення	16.22	15.68	167.65
	множення	0.09	0.36	8.41
	порівняння	44.28	198.96	4826.43
Сума		89	321	7499
Тривалість виконання функцій * в мілісекундах		89	321	7499

*Примітки: * Тривалість 1000 операцій в тактах процесора: читання символу – 27 тактів, порівняння рядків – 54 такти, конкатенація рядків – 297 тактів. ** Для розрахунку взято процесор з тактовою частотою 2 ГГц з урахуванням завантаження операційною системою 5%*

У табл. 3.17 подано результати досліджень оцінки часових і швидкісних показників процедур нанесення і зняття збитку.

Таблиця 3.17 – Результати досліджень оцінки часових і швидкісних показників процедур нанесення і зняття збитку

Показники	Довжина кодової послідовності	Час роботи (сек)	Пропускна здатність алгоритму, *Rate* (байт/сек)	Утилізація ядра процесора (*ticks*)	складність алгоритму, *Per* (*cpb*)
Кількість викликів функцій, що реалізують елементарні операції	10	0,089	112,3596	90	0.801
	100	0,321	311,5265	322	1.034
	1000	7,499	133,3511	7500	66.166

Таким чином, проведений аналіз основних принципів побудови МНККС Мак-Еліса і систем багатоканальної криптографії на збиткових кодах дозволяє розробити гібридні криптосистеми на основі модифікованих несиметричних крипто-кодових систем Мак-Еліса і систем багатоканальної криптографії на збиткових кодах. Відмінністю від “класичного” підходу формування гібридної криптосистеми є використання несиметричних крипто-кодових конструкцій (належать до секретних моделей доказової стійкості) зі швидкими криптоперетвореннями (швидкість перетворень порівняна зі швидкістю криптоперетворень в БСШ), що виступають основним механізмом забезпечення стійкості (безпеки) інформації з подальшим використанням алгоритму *MV*2 (системи на збиткових кодах), що забезпечує зниження енергетичних витрат (потужності алфавіту МНККС Мак-Еліса) з подальшою передачею по одному або декількох каналах.

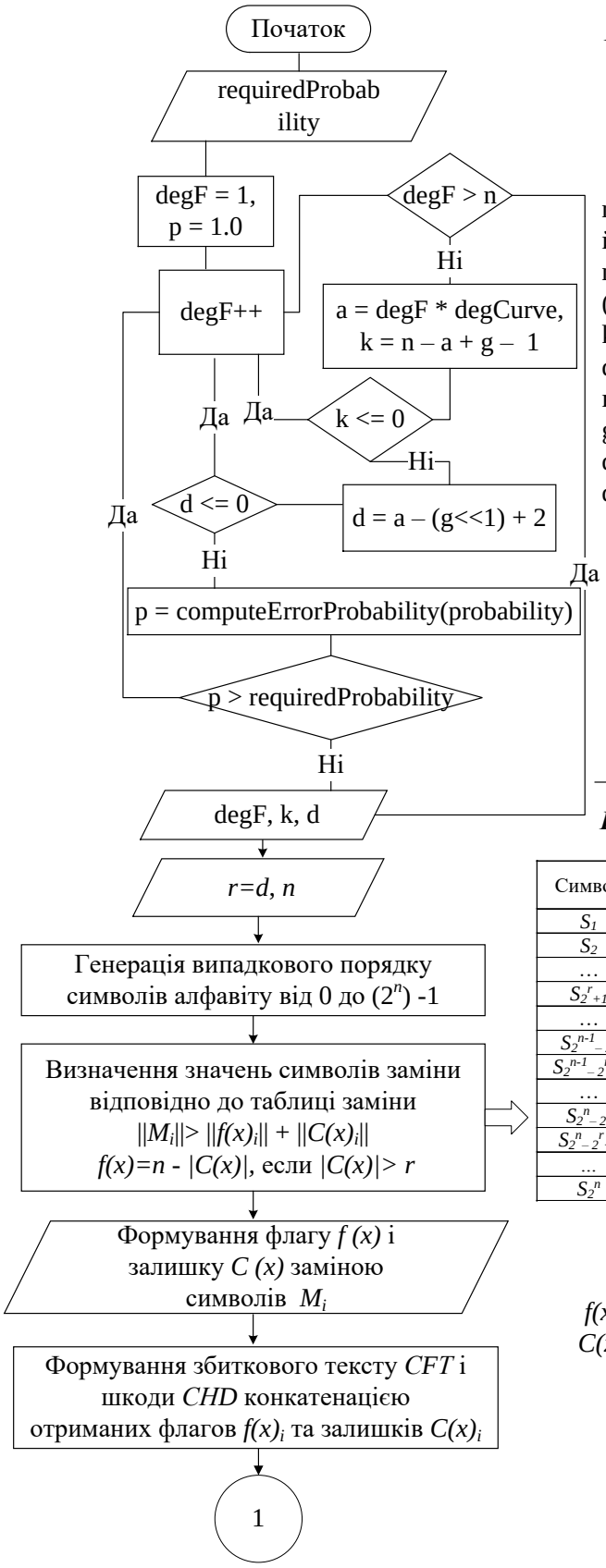
Розглянемо практичні алгоритми формування криптограми і розшифрування в запропонованій гібридній криптосистемі. На рис. 3.20, 3.21, 3.22 наведені алгоритми формування криптограми / кодограми та розкодування кодограми в гібридній криптосистемі (відповідно).

Запропоновані алгоритми гібридної криптосистеми дозволяють у разі приховування збиткового шифртекста CFT / CH_{FT} всі його можливі значення визначити додатковим ключовим полем:

$$U_0 = \frac{H(CFT / CH_{FT}) + \sum_{i=1}^{m}\left(H\left(CHD^{(i)}\right)\right) + H(KU_i^{EC})}{B\log|I|}, \qquad (3.34)$$

У разі додаткового приховування останнього шифртекста збитку CHD / CH_D зважаючи на його малість і сумірність з шифртекстом збиткового тексту CFT / CH_{FT} відстань єдності можна бути додатково збільшити:

$$U_0 = \frac{H(CHD / CH_D) + H(CFT / CH_{FT}) + \sum_{i=1}^{m}\left(H\left(CHD^{(i)}\right)\right) + H(KU_i^{EC})}{B\log|I|}. \qquad (3.35)$$



Етап 1. Встановлення параметрів коду

requiredProbability – задана ймовірність спотворення блоку,
n – загальна кількість символів в коді (довжина коду),
k – кількість інформаційних символів,
d –мінімальна відстань кодових комбінацій за Хемінгом,
g – рід кривої,
degF – степень генераторної функції,
degCurve – степень кривої.

Етап 2. Завдання збитку

Символ	довжина залишку	Залишок $C(x)$	Флаг $f(x)$
S_1	r	0^r	$0^{n-r-1}1$
S_2	r	$0^{r-1}1$	$0^{n-r-1}1$
…	…	…	…
S_{2^r+1}	$r+1$	0^{r+1}	$0^{n-r-2}1$
…	…	…	…
$S_{2^{n-1}-2^r}$	$n-2$	1^{n-2}	01
$S_{2^{n-1}-2^r+1}$	$n-1$	0^{n-1}	1
…	…	…	…
$S_{2^n-2^r}$	$n-1$	1^{n-1}	1
$S_{2^n-2^r+1}$	r	0^r	0^{n-r}
…	…	…	…
S_{2^n}	r	1^r	0^{n-r}

$f(x)$ – флаг,
$C(x)$ – залишок

Рисунок 3.20 – Формування кодограми в гібридній крипто-кодовій конструкції

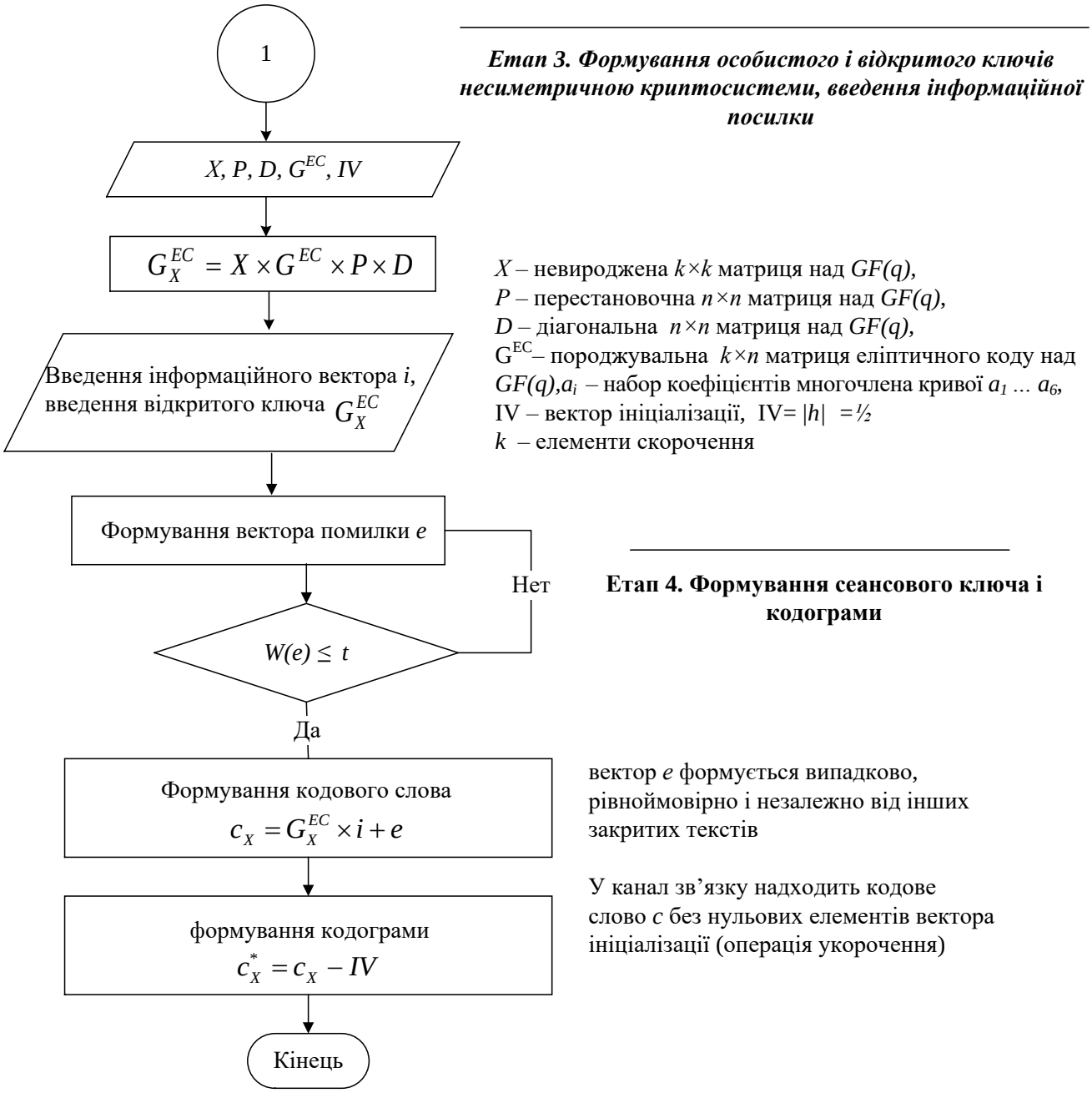


Рисунок 3.21 – Формування кодограми в гібридній крипто-кодовій конструкції

Якщо вихідний текст мав певний сенс, то для такої системи збиткові тексти при повному переборі всього поля ключів шифрування і ключа збитку мають єдиний осмислений текст, рівний вихідному, за умови, що довжина шифртекста більше відстані єдності [8].

Етап 1. Встановлення параметрів коду, введення особистого ключа та кодограми

X – невироджена $k \times k$ матриця над $GF(q)$,
P – перестановочна $n \times n$ матриця над $GF(q)$,
D – діагональна $n \times n$ матриця над $GF(q)$,
G^{EC} – породжувальна $k \times n$ матриця еліптичного коду над $GF(q)$, a_i – набор коефіцієнтів многочлена кривої $a_1 \dots a_6$,
IV – вектор ініціалізації, IV= $|h|$ =½
k – елементи скорочення

Етап 2. Розкодування кодограми

Символ	довжина остатка	залишок $C(x)$	Флаг $f(x)$
M_1	r	0^r	$0^{n-r-1}1$
M_2	r	$0^{r-1}1$	$0^{n-r-1}1$
…	…	…	…
M_2^{r+1}	$r+1$	0^{r+1}	$0^{n-r-2}1$
…	…	…	…
$M_2^{n-1-2^r}$	$n-2$	1^{n-2}	01
$M_2^{n-1-2^r+1}$	$n-1$	0^{n-1}	1
…	…	…	…
$M_2^{n-2^r}$	$n-1$	1^{n-1}	1
$M_2^{n-2^r+1}$	r	0^r	0^{n-r}
…	…	…	…
M_2^n	r	1^r	0^{n-r}

Етап 3. Відновлення повідомлення нанесеному збитку

$f(x)$ – флаг,
$C(x)$ – залишок

Рисунок 3.22 – Розкодування кодограми в гібридній крипто-кодовій конструкції

Таким чином, багатоканальна криптографія на основі збиткових кодів дозволяє здійснювати комплексування криптографічних систем, об'єднуючи під однією концепцією крипто-кодові конструкції (МНККС Мак-Еліса на *MEC*) і системи на збиткових кодах, які доповнюючи один одного, забезпечують необхідні показники безпеки і надійності, і збагачують сумарну систему своїми властивостями.

Розглянемо формальний опис запропонованих ГКККЗК на основі МНККС Мак-Еліса і Нідеррайтера на *MEC*.

3.2.2. Розроблення математичних моделей гібридних крипто-кодових конструкцій на основі несиметричних модифікованих крипто-кодових систем Мак-Еліса та Нідеррайтера на модифікованих алгеброгеометричних кодах

Розглянемо формальний опис модифікованої крипто-кодової системи Мак-Еліса на збиткових кодах.

Для побудови математичної моделі скористаємося основними положеннями роботи [45] для формального математичного визначення секретної системи. В роботі [6] розглянуто формальний опис математичної моделі МНККС Мак-Еліса на модифікованих еліптичних кодах, в роботі [8] розглянутий універсальний механізм заподіяння збитків та способи передачі в системах на збиткових кодах.

Математична модель ГКККЗК Мак-Еліса на основі укорочення (скорочення інформаційних символів) формально задається сукупністю таких елементів [6]:

– множина відкритих текстів – $M = \{M_1, M_2, ..., M_{q^k}\}$, де $M_i = \{I_0, I_{h_1}, .. I_{h_j}, I_{k\text{-}1}\}$,

$\forall \mathrm{I}_\mathrm{j} \in GF(q)$; h_j – інформаційні символи рівні нулю, $/h/ = \frac{1}{2}k$, тобто $I_i=0$, $\forall I_i \in h$;

– множина закритих текстів *(кодограм)* – $C = \{C_1, C_2, ..., C_{q^k}\}$, де $C_i = (c^*_{X_0}, c^*_{h_1}, ..., c^*_{h_j}, c^*_{X_{n-1}})$, $\forall c^*_{X_j} \in GF(q)$;

– множина прямих відображень (на основі використання відкритого ключа – породжувальної матриці): $\phi = \{\phi_1, \phi_2, ..., \phi_s\}$, де $\phi_i : M \to C_{k-h_j}$, $i = 1, 2, ..., s$;

– множина обернених відображень (на основі використання закритого (особистого) ключа – матриць маскування): $\phi^{-1} = \{\phi_1^{-1}, \phi_2^{-1}, ..., \phi_s^{-1}\}$, де $\phi_i^{-1} : C_{k-h_j} \to M$, $i = 1, 2, ..., s$;

– множина ключів, яка параметризує прямі відображення (відкритий ключ уповноваженого користувача):

$$K_{a_i} = \{K_{1_{a_i}}, K_{2_{a_i}}, ..., K_{s_{a_i}}\} = \{G_X^{EC_1}{}_{a_i}, G_X^{EC_2}{}_{a_i}, ..., G_X^{ECs}{}_{a_i}\},$$

де $G_X^{EC_i}{}_{a_i}$ – породжувальна $n \times k$ матриця замаскованого під випадковий код алгеброгеометричного блокового (n, k, d) коду з елементами з $GF(q)$, тобто $\phi_i : M \xrightarrow{K_{ia_i}} C_{k-h_j}$; $i = 1, 2, ..., s$; a_i – набір коефіцієнтів багаточлена кривої $a_1 ... a_6$, $\forall a_i \in GF(q)$, що однозначно визначає конкретний набір точок кривої з простору P^2.

– множина збиткових текстів CFT, $CFT = \{CFT_1, CFT_2, ..., CFT_{q^k}\}$;

– множина збитків CHD, $CHD = \{CHD_1, CHD_2, ..., CHD_{q^k}\}$;

– множина прямого нанесення збитку (на основі використання ключа – K^i_{MV2}, і алгоритму $MV2$) – $E = \{E^1_{K_{MV2}}, E^2_{K_{MV2}}, ..., \phi^S_{K_{MV2}}\}$, $i = 1, 2, ..., s$; $f(x)_i$ – флаг (збиток, CHD), $C(x)_i$ – залишок (збитковий текст, CFT); $f(x)=n-|C(x)|$, якщо $|C(x)| > r$, де r – деякий параметр, $r \in_R Z_{q^m}$, $0 \langle r \langle n$;

– множина відображень $MV2$ F_n^r що задається бієктивним відображенням між множиною перестановок $\{S_1, S_2, ..., S_{2^n}\}$ і множиною $\#F_n^r$, $\#F_n^r = \#\{(c, f)\} = 2^n!$;

– множина осмисленого тексту (на основі використання ключа – K^i_{MV2}, і алгоритму $MV2$) – $E^{-1} = \{E^1_{K_{MV2}}{}^{-1}, E^2_{K_{MV2}}{}^{-1}, ..., E^S_{K_{MV2}}{}^{-1}\}$,

де $E^{-1}_{K_{MV2}} : \|f(x)_i\| + \|C(x)_i\| \to M$, $i = 1, 2, ..., s$; $f(x)_i$ – флаг (збиток, CHD), $C(x)_i$ – залишок (збитковий текст, CFT); $f(x)=n-|C(x)|$, якщо $|C(x)| > r$, де r – деякий параметр, $r \in_R Z_{q^m}$;

– множина ключів, яка параметризує обернені відображення (особистий (закритий) ключ уповноваженого користувача):

$K^* = \{K_1^*, K_2^*, ..., K_s^*\} = \{\{X, P, D\}_1, \{X, P, D\}_2, ..., \{X, P, D\}_s\}$, $\{X, P, D\}_i = \{X^i, P^i, D^i\}$, де X^i – маскуюча невироджена випадково рівноймовірно сформована джерелом ключів $k \times k$ матриця з елементами з $GF(q)$; P^i – перестановочна випадково рівноймовірно сформована джерелом ключів $n \times n$ матриця з елементами з $GF(q)$; D^i – діагональна сформована джерелом ключів матриця з елементами з $GF(q)$, тобто $\phi_i^{-1} : C \xrightarrow{K_i^*} M$, $i = 1, 2, ..., s$, складність виконання оберненого відображення ϕ_i^{-1} без знання ключа $K_i^* \in K^*$ пов'язана з розв'язуванням теоретико-складної задачі декодування випадкового коду (коду загального положення);

– множина ключів перетворення збиткових кодів $K_{MV2}^i \in K_{MV2}$.

Вихідними даними при опису розглянутої несиметричної крипто-кодової системи захисту інформації є:

– алгеброгеометричний блоковий *(n, k, d)* код C_{k-h_j} над *GF(q)*, тобто така множина кодових слів $C_i \in C_{k-h_j}$, що виконується рівність $C_i H^T = 0$, де *H* – перевірочна матриця алгеброгеометричного блокового коду;

– a_i – набір коефіцієнтів багаточлена кривої $a_1 ... a_6$, $\forall a_i \in GF(q)$, що однозначно визначає конкретний набір точок кривої з простору P^2 для формування породжувальної матриці;

– h_j – інформаційні символи, що дорівнюють нулю, $|h| = 1/2k$, тобто $I_i = 0$, $\forall I_i \in h$;

– маскуючі матричні відображення, задані множиною матриць $\{X, P, D\}_i$, де *X* – невироджена $k \times k$ матриця над *GF(q)*; *P* – перестановочна $n \times n$ матриця над *GF(q)* з одним ненульовим елементом в кожному рядку і в кожному стовпці матриці; *D* – діагональна $n \times n$ матриця над *GF(q)* з ненульовими елементами на головній діагоналі;

– *r* – деякий параметр $r \in_R Z_{q^m}$, $Z_{q^m} = \{0, 1, ... 2^n - 1\}$; *n* – деякий параметр $n \in_R Z_{q^n}$, $Z_{q^n} = \{1, ... 2^n\}$;

– множина відображень *MV*2 F_n^r.

У МНККС Мак-Еліса модифікований (укорочений) алгеброгеометричний *(n, k, d)* код C_{k-h_j} з швидким алгоритмом розкодування маскується під випадковий *(n, k, d)* код C_{k-h_j} * за допомогою множення породжувальної матриці G^{EC} кода C_{k-h_j} на маскуючі матриці, які знаходяться в секреті X^u, P^u і D^u [6], що забезпечує формування відкритого ключа уповноваженого користувача:

$G_X^{ECu} = X^u \cdot G^{EC} \cdot P^u \cdot D^u,\ u \in \{1,2,...,s\}$, де G^{EC} – породжувальна $n \times k$ матриця алгеброгеометричного блокового (n, k, d) коду з елементами з $GF(q)$, побудована на основі використання вибраних користувачем коефіцієнтів многочлена кривої $a_1 \ldots a_6$, $\forall a_i \in GF(q)$, що однозначно визначають конкретний набір точок кривої з простору P^2.

Формування закритого тексту $C_j \in C_{k-h_j}$ за введеним відкритим текстом $M_i \in M$ і заданим відкритим ключем $G_X^{ECu}{}_{a_i}$, $u \in \{1,2,...,s\}$ здійснюється шляхом формування кодового слова замаскованого коду з додаванням до нього випадково сформованого вектора $e = (e_0, e_1, ..., e_{n-1}) : C_j = \phi_u\left(M_i, G_X^u\right) = M_i \times \left(G_X^u\right)^T + e$, причому вага Гемінга (кількість ненульових елементів) вектора e не перевищує виправляючої здатності використовуваного алгебраїчного блокового коду:

$0 \le w(e) \le t = \left\lfloor \frac{d-1}{2} \right\rfloor$, $\lfloor x \rfloor$ – ціла частина дійсного числа x.

Для кожного закритого тексту, який формується $C_j \in C_{k-h_j}$, відповідний вектор $e = (e_0, e_1, ..., e_{n-1})$ являється одноразовим сеансовим ключем, тобто для конкретного E_j вектор e формується випадково, рівноймовірно і незалежно від інших закритих текстів.

На алгоритм *MV*2 подається

$C_j^* = C_j - C_{k-h_j}, E_{K_{MV2}} : C_j^* \to \left\| f(x)_i \right\| + \left\| C(x)_i \right\|$.

В канал зв'язку $\left\| f(x)_i \right\|$ та $\left\| C(x)_i \right\|$ при цьому передача може здійснюватися як по одному, так і по двох незалежних каналах.

На стороні прийому уповноважений користувач, який знає правило нанесення збитку F_n^r, маскування, кількість і місця нульових інформаційних символів може скористатися швидким алгоритмом розкодування алгеброгеометричного коду (поліноміальної складності) для відновлення відкритого тексту:

$$E_{K_{MV2}}^{-1}:\left\| f\left(x\right)_i\right\| + \left\|C\left(x\right)_i\right\| \to C_j^{\,*},\ M_i = \phi_u^{-1}\left(C_j^{\,*},\{X,P,D\}_u\right).$$

Для відновлення відкритого тексту уповноважений користувач додає нульові інформаційні символи $C_j^{\,*} = C_j + C_{k-h_j}$, з відновленого закритого тексту C_j знімає дію секретних переставної і діагональної матриць P^u і D^u:

$$\begin{aligned}
C &= C_j^{\,*}\cdot\left(D^u\right)^{-1}\cdot\left(P^u\right)^{-1} = \left(M_i\cdot\left(G_X^u\right)^T + e\right)\cdot\left(D^u\right)^{-1}\cdot\left(P^u\right)^{-1} = \\
&= \left(M_i\cdot\left(X^u\cdot G\cdot P^u\cdot D^u\right)^T + e\right)\cdot\left(D^u\right)^{-1}\cdot\left(P^u\right)^{-1} = \\
&= M_i\cdot\left(X^u\right)^T\cdot\left(G\right)^T\cdot\left(P^u\right)^T\cdot\left(D^u\right)^T\cdot\left(D^u\right)^{-1}\cdot\left(P^u\right)^{-1} + e\cdot\left(D^u\right)^{-1}\cdot\left(P^u\right)^{-1} = \\
&= M_i\cdot\left(X^u\right)^T\cdot\left(G\right)^T + e\cdot\left(D^u\right)^{-1}\cdot\left(P^u\right)^{-1},
\end{aligned}$$

а потім розкодовує отриманий вектор за алгоритмом Берлекемпа–Мессі [33; 34; 35]:

$$C = M_i\cdot\left(X^u\right)^T\cdot\left(G^{EC}\right)^T + e\cdot\left(D^u\right)^{-1}\cdot\left(P^u\right)^{-1},$$

тобто позбувається від другого доданка і від співмножника $\left(G\right)^{ECT}$ в першому доданку в правій частині рівності, після чого знімає дію матриці маскування X^u. Для цього отриманий результат розкодування $M_i\cdot\left(X^u\right)^T$ слід помножити на $\left(X^u\right)^{-1}$: $\left(M_i\cdot\left(X^u\right)^T\right)\cdot\left(X^u\right)^{-1} = M_i$. Отримане рішення являється собою відкритий текст M_i.

Структурна схема протоколу обміну інформацією в режимі реального часу з використанням МНККС Мак-Еліса з модифікованими (укороченими) еліптичними кодами наведена на рис. 3.23, з модифікованими подовженими на рис. 3.24.

Основною відмінністю подовжених кодів є використання положень символів скорочення в МНККС Мак-Еліса, з подальшою їх заміною на інформаційні символи відкритої БІР.

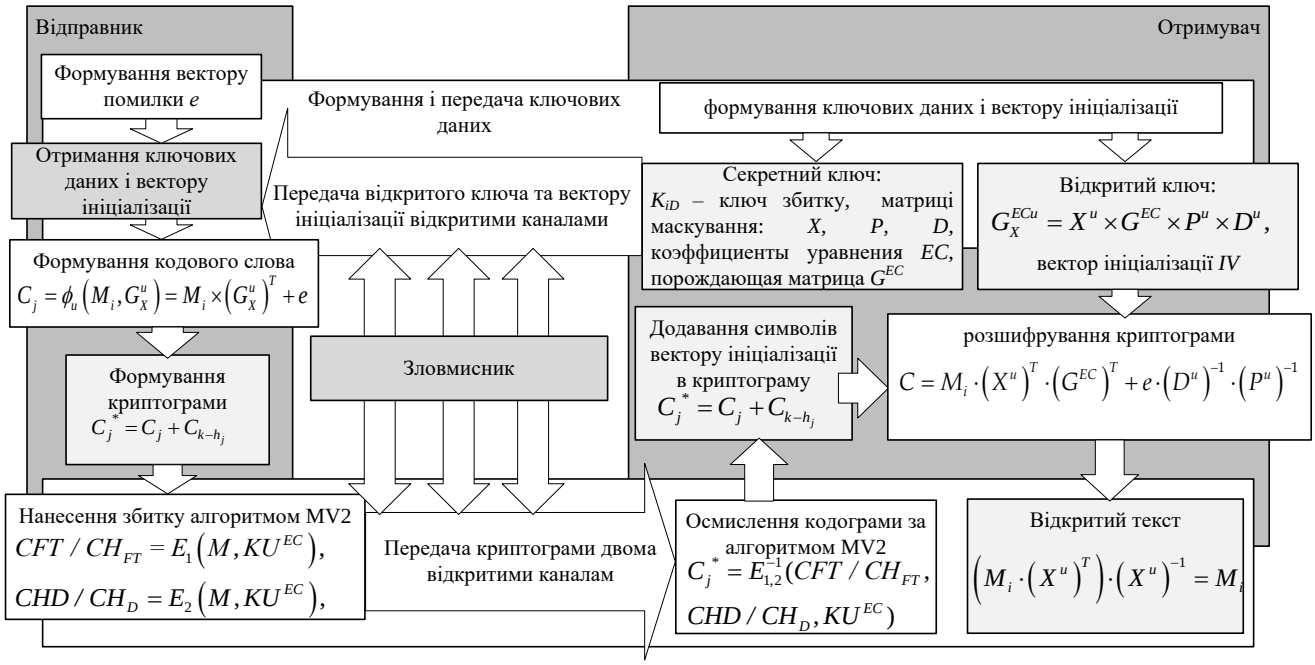


Рисунок 3.23 – Протокол обміну БІР за допомогою ГКККЗК на МНККС Мак-Еліса на укорочених *MEC* за другим способом нанесення збитку

У додатку В наведені приклади протоколів обміну БІР на основі ГКККЗК на *MEC* (укорочених/ подовжених) на основі МНККС Мак-Еліса, лістинг програмного макету запропонованих ГКККЗК на *MEC* наведений у додатку Д.

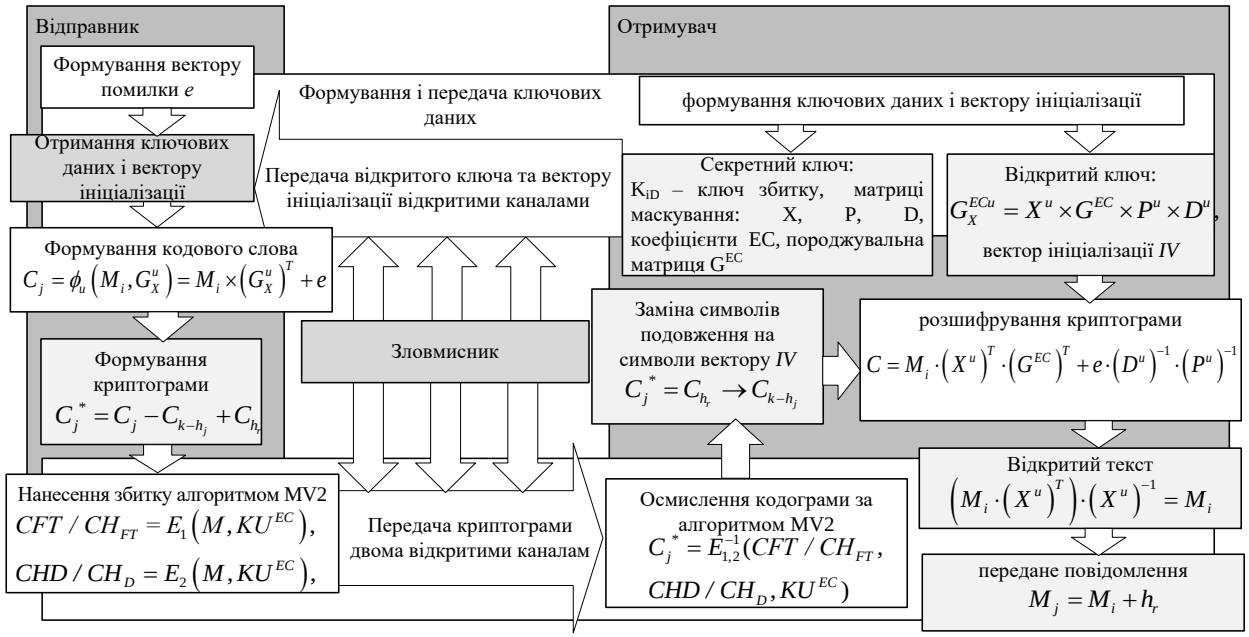


Рисунок 3.24 – Протокол обміну БІР за допомогою ГКККЗК на МНККС Мак-Еліса на подовжених *MEC* за другим способом нанесення збитку

Розглянемо формальний опис математичної моделі гібридної МНККС Нідеррайтера, яка задається сукупністю таких елементів [9]:

– множина відкритих текстів $M = \left\{ M_1, M_{2,} ... M_{q^k} \right\}$, де $M_i = \left\{ e_0, e_{h_1,} ... e_{h_k}, e_{e-1} \right\}$, $\forall e_e \in GF(q)$; h_e – символи вектора помилки, що дорівнюють нулю, $/h/ = \frac{1}{2}e$, тобто $e_i=0$, $\forall e_i \in h$;

– множина закритих текстів $S = \left\{ S_0, S_1, ... S_{q^r} \right\}$, де $S_i = \left\{ S^*_{X_0}, S^*_{h_1}, ... S^*_{h_j}, S^*_{X_r} \right\}$, $\forall S_{X_r} \in GF(q)$;

– множина прямих відображень (на основі використання відкритого ключа - перевірочної матриці еліптичного коду (*EC*): $\varphi = \left\{ \varphi_1, \varphi_2, ..., \varphi_r \right\}$, де $\varphi_i : M \to S_{r-h_e}, i = 1, 2, ..., e$;

– множина обернених відображень (на основі використання закритого (особистого) ключа – матриць маскування) $\varphi^{-1} = \left\{ \varphi_1^{-1}, \varphi_2^{-1}, ..., \varphi_r^{-1} \right\}$, де $\varphi_i^{-1} : S_{r-h_e} \to M, i = 1, 2, ..., e$;

– множина ключів, які параметризують прямі відображення (відкритий ключ уповноваженого користувача):

$$KU_{a_i} = \left\{ KU_{1_{a_i}}, KU_{2_{a_i}}, ..., KU_{r_{a_i}} \right\} = \left\{ H^{EC_1}_{X_{a_i}}, H^{EC2}_{X_{a_i}}, ..., H^{ECr}_{X_{a_i}} \right\},$$

де $H^{EC_i}_{X_{a_i}}$ – перевірочна $r \times n$ матриця замаскованого під випадковий код алгеброгеометричного блокового (n, k, d) коду з елементами $GF(q)$, тобто $\varphi_i : M \xrightarrow{KU_{i_{a_i}}} S^*_{r-h_e}$, $i = 1, 2, ..., e$, a_i – набір коефіцієнтів многочлена кривої $a_1 ... a_6$, $\forall a_i \in GF(q)$, однозначно задає конкретний набір точок кривої з простору P^2;

– множина ключів, які параметризують обернені відображення (особистий (закритий) ключ уповноваженого користувача):

$KR = \{KR_1, KR_2, ..., KR_r\} = \begin{Bmatrix} \{X, P, D\}_1, \\ \{X, P, D\}_2, ..., \{X, P, D\}_r \end{Bmatrix}$, $\{X, P, D\}_i = \{X^i, P^i, D^i\}$, де X^i – маскуюча невироджена випадково рівноймовірно сформована джерелом ключів $k \times k$ матриця з елементами зі $GF(q)$; P^i – перестановочна випадково рівноймовірно сформована джерелом ключів $n \times n$ матриця з елементами з $GF(q)$; D^i – діагональна сформована джерелом ключів матриця з елементами з $GF(q)$, тобто $\varphi_i^{-1} : S^*_{r-h_e} \xrightarrow{KR_i} M$, $i = 1, 2, ..., s.$ Складність виконання оберненого відображення ϕ_i^{-1} без знання ключа $K_i^* \in K^*$ пов'язана з розв'язанням теоретико-складної задачі декодування випадкового коду (коду загального положення).

– множина збиткових текстів *CFT*, $CFT = \{CFT_1, CFT_2, ..., CFT_{q^k}\}$;

– множина збитків *CHD*, $CHD = \{CHD_1, CHD_2, ..., CHD_{q^k}\}$;

– множина прямого нанесення збитку (на основі використання ключа – K^i_{MV2}, і алгоритму *MV*2) – $E = \{E^1_{K_{MV2}}, E^2_{K_{MV2}}, ..., \phi^S_{K_{MV2}}\}$, $i = 1, 2, ..., s$; $f(x)_i$ – флаг (збиток, *CHD*), $C(x)_i$ – залишок (збитковий текст, *CFT*); $f(x)=n-|C(x)|$, якщо $|C(x)| > r$, де r – деякий параметр, $r \in_R Z_{q^m}$, $0 \langle r \langle n$;

– множина відображень *MV*2 F_n^r, що задає бієктивне відображення між множиною перестановок $\{S_1, S_2, ..., S_{2^n}\}$ і множиною $\# F_n^r$, $\# F_n^r = \#\{(c, f)\} = 2^n!$;

– множина осмисленого тексту (на основі використання ключа – K^i_{MV2}, і алгоритму *MV*2) – $E^{-1} = \{E^1_{K_{MV2}}{}^{-1}, E^2_{K_{MV2}}{}^{-1}, ..., E^S_{K_{MV2}}{}^{-1}\}$,

де $E^{-1}_{K_{MV2}} : \| f(x)_i \| + \| C(x)_i \| \to M$, $i = 1, 2, ..., s$; $f(x)_i$ – флаг (збиток, *CHD*), $C(x)_i$ – залишок (збитковий текст, *CFT*); $f(x)=n-|C(x)|$, якщо $|C(x)| > r$, де r – деякий параметр, $r \in_R Z_{q^m}$.

Вихідними даними при описі розглянутої несиметричною крипто-кодової системи захисту інформації є:

– недвійковий рівноважний код над *GF(q)*, тобто множина послідовностей довжини *n* та ваги $w(\varepsilon_i)$;

– алгеброгеометричний блоковий *(n, k, d)* код *C* над *GF(q)*, тобто така множина кодових слів $C_i \in C$, що виконується рівність $C_i H^T = 0$, де H – перевірочна матриця алгеброгеометричного блокового коду;

– *IV* – вектор ініціалізації, *IV*= |*h*| =½ h_e – елементи скорочення (h_e – символи вектора помилки, рівні нулю, /*h*/=*1/2e*, тобто $e_i = 0, \ \forall e_i \in h$);

– маскуючі матричні відображення, задані множиною матриць $\{X, P, D\}_i$, де *X* – невироджена $k \times k$ матриця над *GF(q)*; *P* – перестановочна $n \times n$ матриця над *GF(q)* з одним ненульовим елементом в кожному рядку і в кожному стовпці матриці; *D* – діагональна $n \times n$ матриця над *GF(q)* з ненульовими елементами на головній діагоналі;

– r – деякий параметр, $r \in_R Z_{q^m}, Z_{q^m} = \{0,1,...2^n - 1\}$; n – деякий параметр $n \in_R Z_{q^n}, Z_{q^n} = \{1,...2^n\}$;

– множина відображень *MV*2 – F_n^r.

На основі рівноважного кодування формується закритий текст $C_j \in C$ за введеним відкритим текстом $M_i \in M$ і заданим ключем H_X^{ECu}, $u \in \{1,2,...,s\}$. Це здійснюється шляхом формування синдромної (в термінах завадостійкого кодування) послідовності S_{X_j}, що відповідає рівноважній послідовності $M_i = e = \{e_0, e_1, ..., e_{n-1}\}$: $S_{X_j} = \phi_u\left(M_i, H_X^{ECu}\right) = M_i \times \left(H_X^{ECu}\right)^T$, причому вага Гемінга (кількість ненульових елементів) вектора *e* не перевищує виправної здатності використовуваного алгебраїчного блокового (n,k,d) коду:

$$\forall i : 0 \le w(M_i) \le t = \left\lfloor \frac{d-1}{2} \right\rfloor.$$

Потужність множин *M* та *C* визначається допустимим спектром ваг $w(M_i)$, тобто в загальному випадку (для всіх допустимих значень $w(M_i)$) маємо:

$$m = \sum_{i=0}^{t} (q-1)^i \times C_n^i,$$

де C_n^i – біноміальний коефіцієнт, $C_n^i = \frac{n!}{i! \cdot (n-1)!}$.

Найбільш доцільно величину $w(M_i)$ вибирати відповідно до необхідного значенням безпеки передачі БІР.

Тоді для $w(M_i) = const = w(e)$ маємо: $m = (q-1)^{w(e)} \times C_n^{w(e)}$, а послідовність $M_i = \{e_0, e_1, ..., e_{n-1}\}$ з множини $M = \{M_1, M_2, ..., M_m\}$ формується як результат деякого відображення ψ, реалізованого шляхом надлишкового кодування недвійковими рівноважними кодами ненадлишкових інформаційних послідовностей.

Сформований закритий текст $C_j \in C$ однозначно відповідає вектору $M_i = \{e_0, e_1, ..., e_{n-1}\}$.

Сформуємо вектор ініціалізації $IV=EC–h_j$, де h_j – інформаційні символи, що дорівнюють нулю, $/h/ = \frac{1}{2}k$, тобто $I_i = 0$, $\forall I_i \in h$.

Формування укороченого вектора помилки $e_x=e(A) – IV$.

Відкритий ключ формується шляхом множення перевірочної матриці алгеброгеометричного коду на матриці маскування: $H_X^{ECu} = X^u \cdot H \cdot P^u \cdot D^u$, $u \in \{1, 2, ..., s\}$, де H^{EC} – перевірочна $n \times (n-k)$ матриця алгеброгеометрического блокового (n, k, d) коду з елементами з $GF(q)$.

В алгоритм *MV*2 надходить синдромна послідовність: $S^*_{r-h_e} = (e_n - h_e) \times H_X^{ECT}$.

В *MV*2 синдромна послідовність $S^*_{r-h_e}$ перетворюється на залишок і флаг:

$$E_{K_{MV2}} : S^*_{r-h_e} \to \| f(x)_i \| + \| C(x)_i \|.$$

В канал зв’язку поступає $\| f(x)_i \|$ та $\| C(x)_i \|$, при цьому передача може здійснюватися як за одному, так і по двох незалежних каналах.

На стороні прийому уповноважений користувач, який знає правило нанесення збитку F_n^r, маскування (набір матриць $\{X,P,D\}_u=\{X^u,P^u,D^u\}$) і вектора ініціалізації (кількість і місця нульових символів вектора помилки):

$$E_{K_{MV2}}^{-1}:\left\| f(x)_i \right\| + \left\| C(x)_i \right\| \to S^*_{r-h_e},$$

формує кодову послідовність як одне (будь-яке) з можливих рішень рівняння:

$$S^*_{r-h_e}=c^*_{X_i}\cdot H^T_{X_j},$$

тобто знаходить такий вектор $c^*_{X_i}$, який розкладається на суму: $c^*_{X_i}=c_{X_i}+M_i$, де c_{X_i} – одне (будь-яке) з можливих кодових слів замаскованого коду з перевірочної матрицею $H^T_{X_j}$, тобто $c_{X_i}\times H^T_{X_j}=0$.

Далі уповноважений користувач, використовуючи набір матриць $\{X,P,D\}_u=\{X^u,P^u,D^u\}$, формує вектор: $\bar{c}^*=c^*_X\cdot\left(D^u\right)^{-1}\cdot\left(P^u\right)^{-1}$, тобто демаскує кодову послідовність $c^*_{X_i}$.

Після підстановки отримаємо рівність:

$$\bar{c}^*=c^*_X\cdot\left(D^u\right)^{-1}\cdot\left(P^u\right)^{-1}=\left(c_{X_i}+M_i\right)\cdot\left(D^u\right)^{-1}\cdot\left(P^u\right)^{-1}=$$
$$=c_{X_i}\cdot\left(D^u\right)^{-1}\cdot\left(P^u\right)^{-1}+M_i\cdot\left(D^u\right)^{-1}\cdot\left(P^u\right)^{-1}.$$

Уповноважений користувач, який сформував вектор, має можливість застосувати швидкий (поліноміальної складності) алгоритм завадостійкого декодування і сформувати таким чином вектор $\bar{c}^*=c^*_X\cdot\left(D^u\right)^{-1}\cdot\left(P^u\right)^{-1}$ та вектор $M_i^u=M_i\cdot\left(D^u\right)^{-1}\cdot\left(P^u\right)^{-1}$.

Для відновлення інформаційної рівноважної послідовності M_i достатньо знову помножити вектор M_i^u на матриці маскування D^u та P^u, але в іншому порядку: $M_i = M_i^u \cdot P^u \cdot D^u = M_i \cdot \left(D^u\right)^{-1} \cdot \left(P^u\right)^{-1} \cdot P^u \cdot D^u = M_i$.

Формування шуканого вектора помилки *e*: $M = M_i + IV$

Аналіз практичної реалізації алгоритмів шифрування / розшифрування в ГКККЗК Нідеррайтера показує, що при формуванні криптограми (синдрому) після формування вектора помилки алгоритмом рівноважного кодування на основі вектора ініціалізації (формується ПВП відповідно до [7] в довіреному центрі і передається закритими каналами через АБС банків емітента та еквайра або вектор шифрується алгоритмом *MV*2 і передається двома незалежними відкритими каналами) проводиться скорочення – h_e (символи вектора помилки, що дорівнюють нулю), $/h/=1/2e$, тобто $e_i = 0, \ \forall e_i \in h$.

При розшифруванні криптограми (після отримання вектора помилки, перед використанням алгоритму рівноважного кодування) для отримання інформації вводяться “нульові” символи укорочення. Алгоритми шифрування і розшифрування наведені на рис. 3.25 – 3.26, 3.27 – 3.28 відповідно.

Алгоритм формування криптограми в ГКККЗК Нідеррайтера представимо у вигляді послідовності кроків:

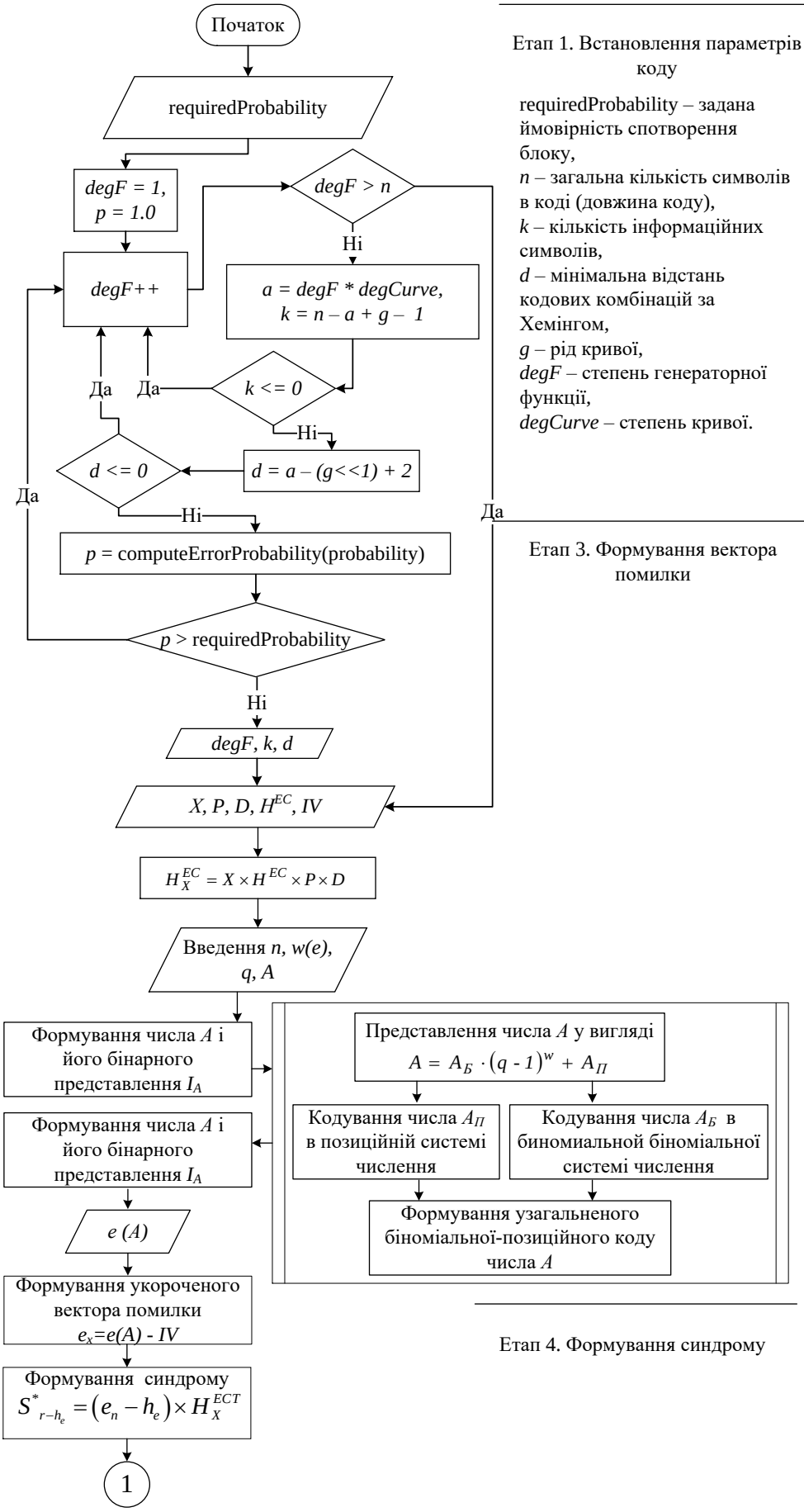
Крок 1. Введення інформації, яка підлягає кодуванню. Введення відкритого ключа H_X^{EC}.

Крок 2. Формування вектора помилки *e*, вага якого не перевищує $\leq t$ – виправляє здатність еліптичного коду на основі алгоритму недвійковий рівноважного кодування [9; 17].

Крок 3. Формування укороченого вектора помилки: $e_x = e(A) - IV$

Крок 4. Формування кодограми: $S^*_{r-h_e} = \left(e_n - h_e\right) \times H_X^{ECT}$.

Крок 5. Формування збиткових тексту (залишок) і флагу (збиток): $E_{K_{MV2}} : S^*_{r-h_e} \rightarrow \left\| f\left(x\right)_i \right\| + \left\| C\left(x\right)_i \right\|$



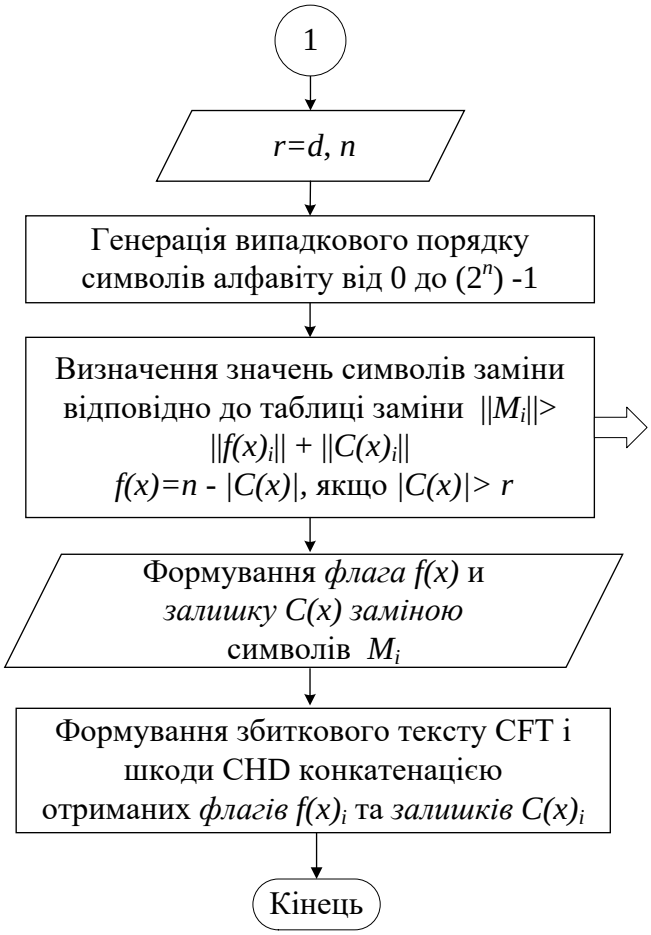
Етап 1. Встановлення параметрів коду

requiredProbability – задана ймовірність спотворення блоку,
n – загальна кількість символів в коді (довжина коду),
k – кількість інформаційних символів,
d – мінімальна відстань кодових комбінацій за Хемінгом,
g – рід кривої,
degF – степень генераторної функції,
degCurve – степень кривої.

Етап 3. Формування вектора помилки

Етап 4. Формування синдрому

Рисунок 3.25 – Формування кодограми в ГКККЗК Нідеррайтера на *MEC*



Етап 5. Нанесення збитків

Символ	довжина остатка	залишок *C(x)*	Флаг *f(x)*
S_1	r	0^r	$0^{n-r-1}1$
S_2	r	$0^{r-1}1$	$0^{n-r-1}1$
…	…	…	…
$S_2{}^r{}_{+1}$	$r+1$	0^{r+1}	$0^{n-r-2}1$
…	…	…	…
$S_2{}^{n-1}{}_{-2^r}$	$n-2$	1^{n-2}	01
$S_2{}^{n-1}{}_{-2^r+1}$	$n-1$	0^{n-1}	1
…	…	…	…
$S_2{}^n{}_{-2^r}$	$n-1$	1^{n-1}	1
$S_2{}^n{}_{-2^r+1}$	r	0^r	0^{n-r}
…	…	…	…
$S_2{}^n$	r	1^r	0^{n-r}

Рисунок 3.26 – Формування кодограми в ГКККЗК Нідеррайтера на *MEC*

Алгоритм розкодування кодограми в ГКККЗК Нідеррайтера представимо у вигляді послідовності кроків:

Крок 1. Отримання осмисленого тексту кодограми на основі алгоритму *MV*2:

$$E^{-1}_{K_{MV2}} : \left\| f\left(x\right)_i \right\| + \left\| C\left(x\right)_i \right\| \to S^*{}_{r-h_e}.$$

Крок 2. Введення кодограми S_X, що розкодовується. Введення закритого ключа – матриць *X*, *P*, *D*.

Крок 3. Знаходження одного з можливих рішень рівняння

$$S^*{}_{r-h_e} = \bar{c}^* \times \left(H^{EC}_X\right)^T.$$

Крок 4. Зняття дії діагональної і переставної матриць:

$$\bar{c}^* = c^*_X \cdot D^{-1} \cdot P^{-1}.$$

Крок 5. Розкодування вектора $\bar{c}^*$. Формування вектора e_x'.

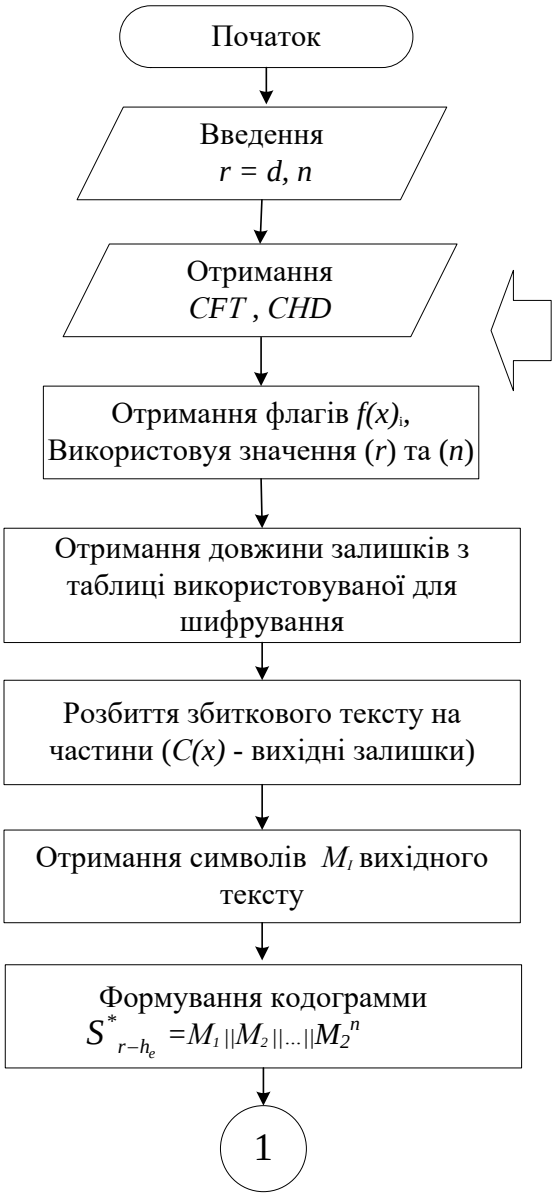
Крок 6. Перетворення вектора e_x'

$$e_x = e_x' \times P \times D.$$

Крок 7. Формування шуканого вектора помилки e:

$$e = e_x + IV$$

Крок 8. Перетворення вектора e на основі використання недвійковий рівноважного коду в інформаційну послідовність.

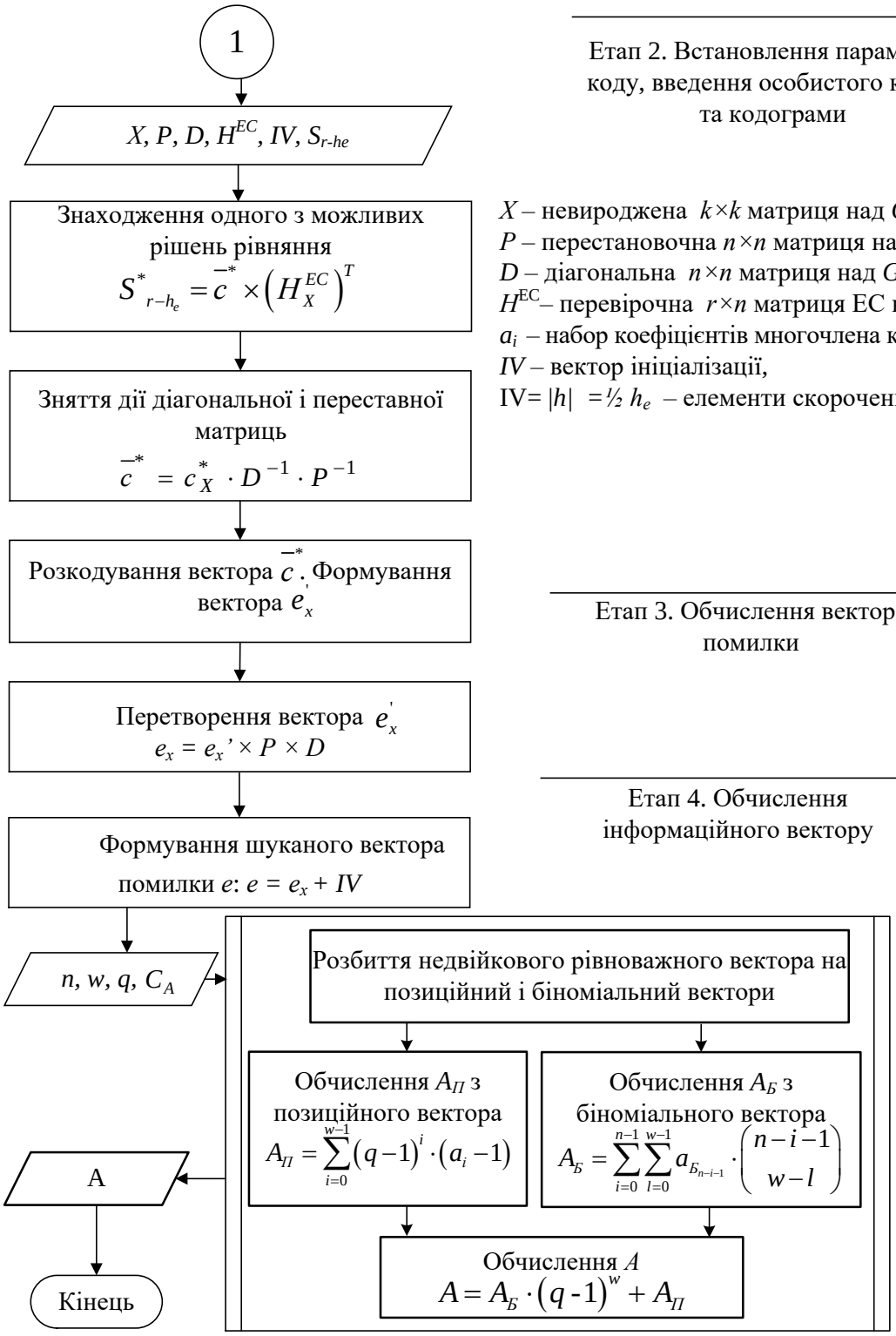


Етап 1. Формування осмисленої кодограми

Символ	довжина остатка	залишок $C(x)$	Флаг $f(x)$
M_1	r	0^r	$0^{n-r-1}1$
M_2	r	$0^{r-1}1$	$0^{n-r-1}1$
…	…	…	…
$M_2^r{}_{+1}$	$r+1$	0^{r+1}	$0^{n-r-2}1$
…	…	…	…
$M_2^{n-1}{}_{-2^r}$	$n-2$	1^{n-2}	01
$M_2^{n-1}{}_{-2^r+1}$	$n-1$	0^{n-1}	1
…	…	…	…
$M_2^n{}_{-2^r}$	$n-1$	1^{n-1}	1
$M_2^n{}_{-2^r+1}$	r	0^r	0^{n-r}
...	…	…	…
M_2^n	r	1^r	0^{n-r}

$f(x)$ – флаг,
$C(x)$ – залишок

Рисунок 3.27 – Розкодування кодограми в ГКККЗК Нідеррайтера на *MEC*



Етап 2. Встановлення параметрів коду, введення особистого ключа та кодограми

X – невироджена $k \times k$ матриця над $GF(q)$,
P – перестановочна $n \times n$ матриця над $GF(q)$,
D – діагональна $n \times n$ матриця над $GF(q)$,
H^{EC} – перевірочна $r \times n$ матриця ЕС над $GF(q)$,
a_i – набор коефіцієнтів многочлена кривої $a_1 \ldots a_6$,
IV – вектор ініціалізації,
IV= $|h|$ =½ h_e – елементи скорочення

Етап 3. Обчислення вектора помилки

Етап 4. Обчислення інформаційного вектору

Рисунок 3.28 – Розкодування кодограми в ГКККЗК Нідеррайтера на *MEC*

Розглянемо властивості запропонованих ГКККЗК Мак-Еліса на *MEC*, проведемо порівняльне оцінювання основних властивостей (швидкості криптоперетворень, складності злому та інш.).

3.2.3. Дослідження властивостей гібридних крипто-кодових конструкцій на збиткових кодах

Проведемо порівняльне оцінювання параметрів МНККС Мак-Еліса на *MEC* з ГКККЗК з використанням модифікованих еліптичних кодів. Введемо такі позначення:

l_I – довжина інформаційної послідовності (блока), яка надходить на вхід ККС схеми (в бітах); l_K – довжина відкритого ключа (в бітах); l_{K+} – довжина закритого ключа (в бітах); l_S – довжина кодограми (в бітах); O_K – складність формування кодограми (кількість групових операцій); O_{SK} – складність розкодування кодограми (кількість групових операцій); O_{K+} – складність розв'язання задачі аналізу (кількість групових операцій); *KC* – коефіцієнт стиснення залишку; K_f – коефіцієнт стиснення прапора; s – кількість відрізків збиткового тексту; $u(n)$, $v(r)$ – додатні числа ключа збитку; $z(m)$ – раунди збитку; L_0 – довжина вихідного тексту; L_{DT} – довжина збиткового тексту.

Для побудови графіків були використані умовні скорочення (префікси): ukh / udh – гібридні ККККЗК з укороченими *MEC* / гібридні ККККЗК з подовженими *MEC*; uk – МНККС з укороченими *MEC*; ud – МНККС з подовженими *MEC*.

При розрахунках параметрів криптосистем були використані поля Галуа: для МНККС з укороченими / подовженими *MEC* – $GF(2^6)$, для гібридних ККККЗК – $GF(2^4)$.

Довжина інформаційної послідовності (в бітах), що надходить на вхід криптосистеми з ЗК визначається за такими виразами:

– для ГККККЗК на укорочених кодах: $l_I = l_z^c + l_z^f$, де $l_z^c = K_c \times L + \frac{1}{K_f} \times s$ – довжина збиткового тексту; $l_z^f = L + u \times s$ – довжина збитку; $s = \left[\frac{L_0 - L_{DT}}{L_{DT}} \right]$ – кількість відрізків збиткового тексту; $K_C = 1 - K_f \approx 0{,}758$ – коефіцієнт стиснення залишку (збиткового тексту) (при $u = 8$, $v = 3$, $z = 5$); $K_f = \frac{2 - 2^{v-u+1}}{u} \approx 0{,}242$ – коефіцієнт стиснення флагу (збитку) (при $u = 8$, $v = 3$, $z = 5$); $z = \frac{log(u \times L) - 7}{log(1/K_C)}$ –

необхідна для рандомізації алгоритму *MV*2, кількість допустимих раундів перетворення;

– для ГККЗК на *подовжених МЕС*: $l_1 = 1/2k \times m + l_z^c + l_z^f$.

У табл. 3.18 і на рис. 3.29 наведені результати досліджень складності формування криптограми в різних $GF(2^m)$.

Таблиця 3.18 – Залежність складності формування криптограми в різних $GF(2^m)$

$GF(2^m)$	R							
	0.5(ud)	0.75(ud)	0.5(uk)	0.75(uk)	0.5(udh)	0.75(udh)	0.5(ukh)	0.75(ukh)
3	242	603	817	968	643	780	923	998
4	760	980	2140	6282	**905**	**1085**	**1563**	**5125**
5	2241	6121	8706	11461	1863	2450	6137	8282
6	**6348**	**9830**	**10722**	**60760**	6273	7016	9183	10341
7	17092	61751	83000	210170	16582	15985	16563	16925
8	67016	105265	207422	605005	65278	65450	66137	68282
9	98765	510780	710920	1018079	95327	96037	97134	97841

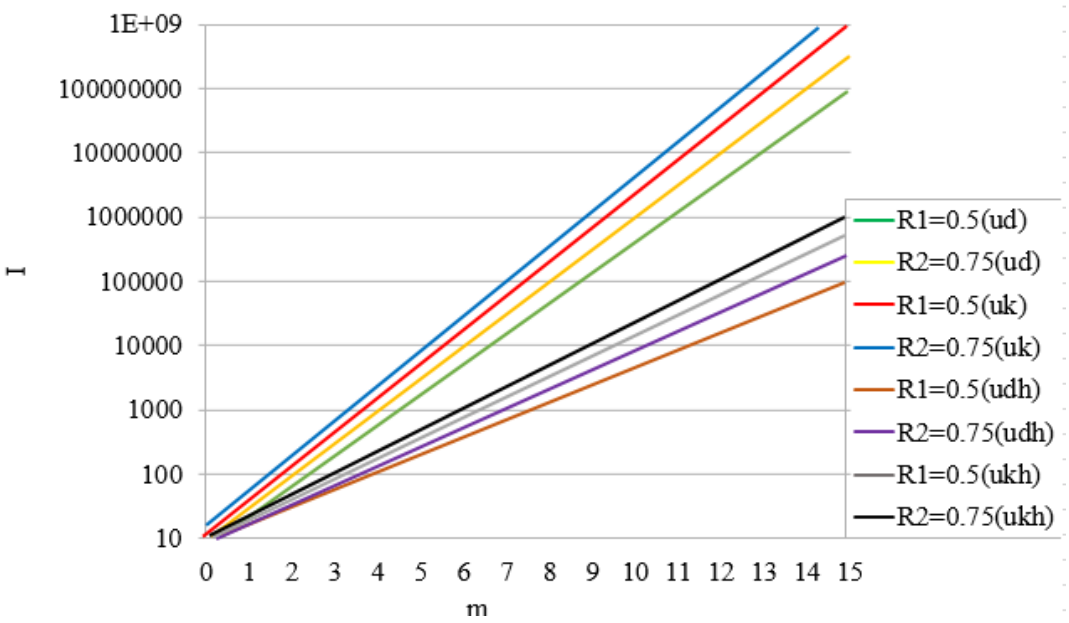


Рисунок 3.29 – Залежність складності формування криптограми в різних $GF(2^m)$

Довжина кодограми (в бітах) визначається за такими виразами:

– для ГККЗК на укорочених *MEC*: $l_S = \left(2\sqrt{q} + q + 1 - 1/2k\right) \times m$;

– для ГККЗК на подовжених *MEC*: $l_S = \left(2\sqrt{q} + q + 1 - 1/2k + 1/2k\right) \times m$.

У табл. 3.19 і на рис. 3.30 наведені результати досліджень складності розкодування криптограми в різних $GF(2^m)$.

Таблиця 3.19 – Результати досліджень складності розкодування криптограми в різних $GF(2^m)$

$GF(2^m)$	R							
	0.5(ud)	0.75(ud)	0.5(uk)	0.75(uk)	0.5(udh)	0.75(udh)	0.5(ukh)	0.75(ukh)
1	78	81	82	96	148	153	1568	1621
2	456	457	457	556	835	897	6112	9624
3	1024	1168	1280	5127	1240	1307	12283	14817
4	7672	8232	11028	23674	**5224**	**11937**	**34673**	**225017**
5	21073	42082	78634	277830	12348	25597	95088	1246572
6	**103862**	**281472**	**760553**	**5220573**	123548	127137	1316373	4383507

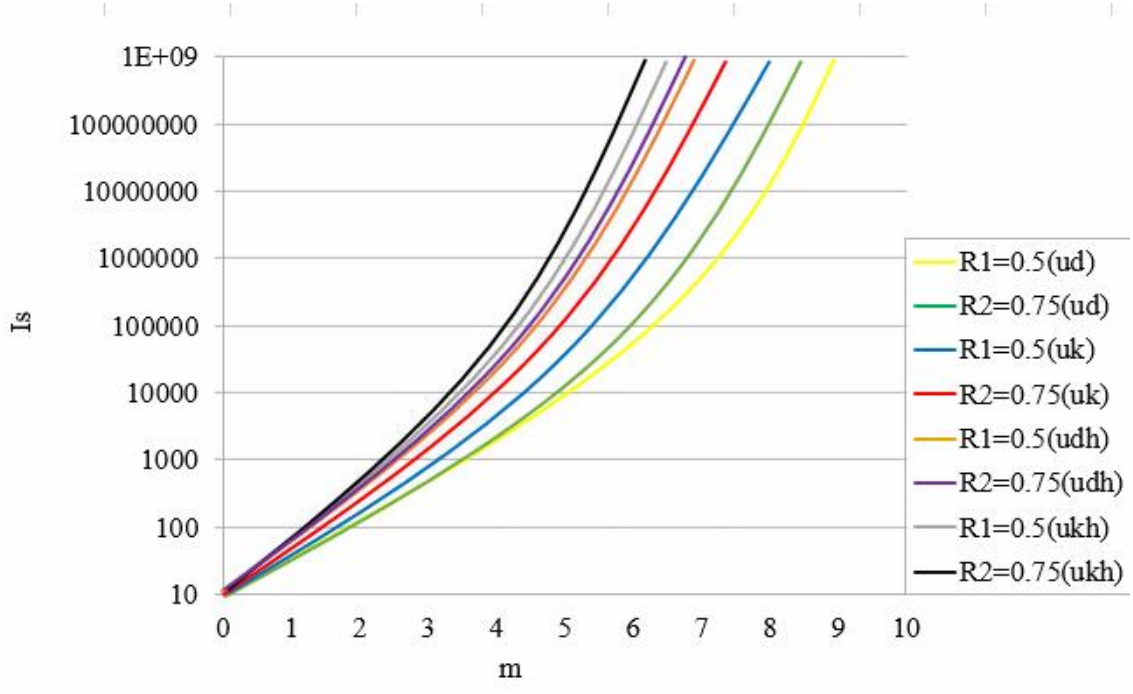


Рисунок 3.30 – Залежність складності розкодування криптограми в різних $GF(2^m)$

Аналіз табл. 3.18, 3.19, рис. 3.29, 3.30 показав, що використання збиткових кодів і подальше зменшення потужності поля Галуа призводить до значного зменшення складності формування (≈ в 12 разів) і розкодування (≈в 20 разів) криптограми.

Довжина відкритого ключа (в бітах) визначається сумою елементів матриці G_X^{EC} і задається виразами:

– для ГККЗК на укорочених *MEC*: $l_K = 1/2k \times \left(2\sqrt{q} + q + 1 - 1/2k\right) \times m$;

– для ГККЗК на подовжених *MEC*: $l_K = 1/2k \times \left(2\sqrt{q} + q + 1 - 1/2k + 1/2k\right) \times m$.

Довжина закритого ключа (в бітах) визначається сумою елементів матриць *X, P, D (в бітах)* і задається виразами:

– для ГККЗК на укорочених кодах:

$$l_{K_+} = 1/2k \left\lceil \log_2 \left(2\sqrt{q} + q + 1\right) \right\rceil + \left|F_u^v\right|,$$

де $\left|F_u^v\right| = 2^u!$ – потужність множини групових перетворень;

– для ГККЗК на подовжених кодах:

$$l_{K_+} = \left(1/2k - 1/2k\right) \left\lceil \log_2 \left(2\sqrt{q} + q + 1\right) \right\rceil + \left|F_u^v\right|.$$

У табл. 3.20 і на рис. 3.31 наведені результати досліджень складності злому алгоритмом переставного декодування в різних $GF(2^m)$.

Таблиця 3.20 – Залежність складності злому ГККЗК над $GF(2^m)$

$GF(2^m)$	*R*							
	0.5(ud)	0.75(ud)	0.5(uk)	0.75(uk)	0.5(udh)	0.75(udh)	0.5(ukh)	0.75(ukh)
1	2.786	2.835	4.122	4.257	1.089	1.864	2.391	3.46
2	4.978	5.961	6.233	6.781	2.569	3.643	4.108	4.962
3	7.568	8.120	8.234	9.764	3.57	4.131	5.382	7.623
4	9.87	12.1	12.647	13.32	**4.92**	**5.817**	**6.836**	**8.972**
5	12.017	14.224	14.742	16.892	7.591	8.617	10.13	12.005
6	**14.983**	**17.483**	**18.767**	**19.76**	10.85	12.53	14.673	14.962

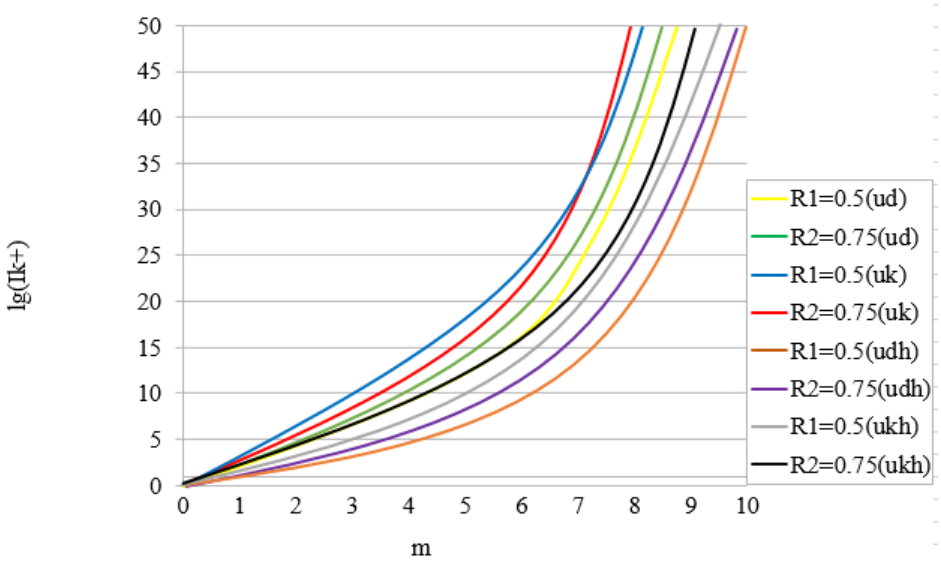


Рисунок 3.31 – Залежність складності злому ГККККЗК над *GF* (2^m) (переставне декодування)

Очевидним результатом зниження потужності поля є, як це демонструють табл. 3.20 і графік на рис. 3.31, подальше зменшення складності злому, яка, як це показано подальшими статистичними тестами, цілком компенсується універсальним алгоритмом стиснення *MV*2.

Складність формування кодограми визначається виразами:

– для ГККККЗК на укорочених *MEC*: при реалізації систематичного кодування визначається виразом: $O_K = (r+1)\times\left(2\sqrt{q}+q+1-1/2k\right)+O\left(\frac{1-K_C^u}{K_f}\times L\right)$;

для несистематичного кодування:

$$O_K = O_K = (k+1)\times(k+1)\times\left(2\sqrt{q}+q+1-1/2k\right)+O\left(\frac{1-K_C^u}{K_f}\times L\right);$$

– для ГККККЗК на подовжених *MEC*: при реалізації систематичного кодування визначається виразом: $O_K = (r+1)\times\left(2\sqrt{q}+q+1-1/2k+1/2k\right)+O\left(\frac{1-K_C^u}{K_f}\times L\right)$;

для несистематичного кодування:

$$O_K = (k+1)\times\left(2\sqrt{q}+q+1-1/2k+1/2k\right)+O\left(\frac{1-K_C^u}{K_f}\times L\right).$$

Складність розкодування кодограми визначається такими виразами:

– для ГККЗК на укорочених *МЕС*:

$$O_{SK} = 2\times\left(2\sqrt{q}+q+1-1/2k\right)^2+1/2k^2+4t^2+\left(t^2+t-2\right)^2/4+O\left(\frac{\alpha-z\times\log k}{\left|K_z^c\times L\right|}\right);$$

– для ГККЗК на подовжених *МЕС*:

$$O_{SK} = 2\times\left(2\sqrt{q}+q+1-1/2k+1/2k\right)^2+k^2+4t^2+\left(t^2+t-2\right)^2/4+O\left(\frac{\alpha-z\times\log k}{\left|K_z^c\times L\right|}\right).$$

Складність процесу декодування визначимо виразами*:*

– для ГККЗК на укорочених *МЕС*:

$$O_{K+} = N_{покр}\times\left(2\sqrt{q}+q+1-1/2k\right)\times r+N_{F\ або}\left(N_K\right),\qquad \text{де}\qquad N_F\approx\frac{K_C{}^z}{2^{1-K_C{}^{z+1}}}\times\left|F\right|;$$

K_C=97/128; $|F|$ – сумарна довжина вихідних флагів (збитків) (біт) – при відомому зловмисникові залишку (збитковому тексті) і заданих флагах (збитках), при невідомому ключі – $N_K\approx 2^{1190\times z}$; z = 16;

– для ГККЗК на подовжених *МЕС*:

$$O_{K+} = N_{покр}\times\left(2\sqrt{q}+q+1-1/2k+1/2k\right)\times r+N_{F\ \text{або}}\left(N_K\right).$$

У табл. 3.21 і на рис. 3.32 наведені результати досліджень складності злому і складності кодування для різних швидкостей R в різних *GF* (2^m). У табл. 3.22 і на рис. 3.33 наведені результати досліджень залежності обсягу відкритих ключових даних ГККЗК на *МЕС* для різних показників стійкості.

Таблиця 3.21 – Складність злому і складності кодування для різних швидкостей R

$\lg(l_s)$	R							
	0.5(ud)	0.75(ud)	0.5(uk)	0.75(uk)	0.5(udh)	0.75(udh)	0.5(ukh)	0.75(ukh)
1	15.6	18.23	19.12	19.82	7.21	9.17	12.54	14.56
2	32.47	35.67	38.63	39.18	21.46	23.72	27.48	29.82
3	43.75	51.61	56.88	58.03	31.68	33.83	37.38	38.43
4	59.43	72.81	78.92	80.52	**41.72**	**42.27**	**47.48**	**58.23**
5	68.26	87.32	94.91	104.56	56.63	58.91	62.86	66.53
6	**101.72**	**112.46**	**120.83**	**128.79**	72.32	74.79	89.5	97.71

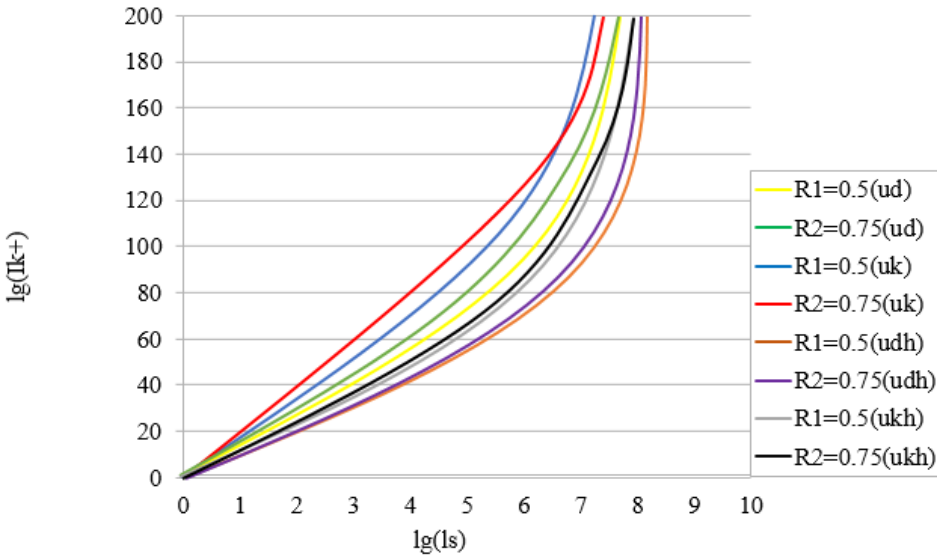


Рисунок 3.32 – Зведена діаграма складності злому і складності кодування ГККК3К

Таблиця 3.22 – Залежності обсягу відкритих ключових даних ГККК3К для різних показників стійкості

$lg(l_{k+})$	0.5(ud)	0.75(ud)	0.5(uk)	0.75(uk)	0.5(udh)	0.75(udh)	0.5(ukh)	0.75(ukh)
5	240	602	968	799	812	827	853	898
20	926137	987234	1034682	1897092	87531	95019	312560	402843
35	**4253109**	**5237688**	**6126273**	**6832018**	**421108**	**650389**	**957648**	**1121732**
50	43076332	60122407	8602376	7027160	1032562	2340561	3867228	4218394

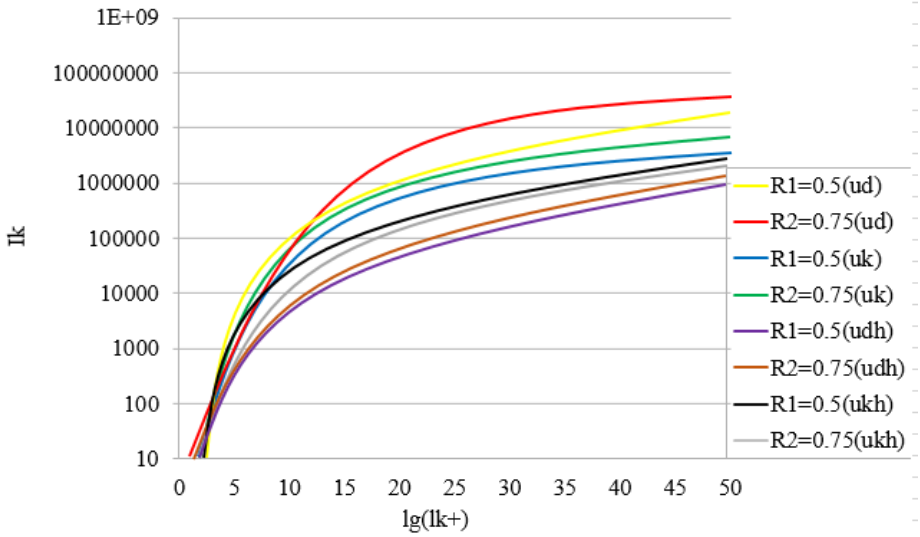


Рисунок 3.33 – Залежності обсягу відкритих ключових даних ГККК3К для різних показників стійкості

У табл. 3.23 наведено результати досліджень ємнісних характеристик при програмній реалізації від потужності поля. Як і при дослідженні МНККС отримали суттєве зменшення відкритих ключових даних для ГККККЗК, що і зумовлює сумарне збільшення відносної швидкості передачі. Природним продовженням досліджень, очевидно, має бути тестування статистичних характеристик запропонованих криптокодових конструкцій з метою отримання об'єктивних традиційних даних про їх криптостійкість та порівняння з відомими криптоалгоритмами.

Таблиця 3.23 – Залежність швидкості програмної реалізації від потужності поля (кількість групових операцій)

Криптоалгоритми	2^4	2^5	2^6	2^7	2^8	2^9	2^{10}
MacElis на укорочених *MEC*	8293075	10007947	**17787431**	28595014	44079433	61974253	79554764
MacElis на подовжених *MEC*	8506422	11156138	**18561228**	33210708	48297112	65171690	84051337
ГККККЗК на МНККС *MacElis* на подовжених *MEC*	**5612316**	7900315	14892945	25565274	42279183	58963778	76564173
ГККККЗК на МНККС *MacElis* на укорочених *MEC*	**5942627**	7905257	14682411	25595014	42116327	58468143	75474764

Для проведення статистичних досліджень стійкості досліджуваних криптосистем скористаємося пакетом *NIST STS* 822 [46]. Результати досліджень наведені в табл. 3.24.

Таблиця 3.24 – Результати досліджень статистичної безпеки

Криптосистеми	Кількість тестів, в яких тестування пройшли більше 99% послідовностей	Кількість тестів, в яких тестування пройшли більше 96% послідовностей	Кількість тестів, в яких тестування пройшли менше 96% послідовностей
НККС *MacElis*	149 (78,83%)	189 (100%)	0 (0%)
МНККС *MacElis* на укорочених *MEC*	151 (79,89%)	189 (100%)	0 (0%)
МНККС *MacElis* на подовжених *MEC*	152 (80,42%)	189 (100%)	0 (0%)
ГККККЗК на подовжених *MEC*	**153** (80,95%)	189 (100%)	0 (0%)
ГККККЗК на укорочених *MEC*	**155** (82 %)	189 (100%)	0 (0%)

Табл. 3.24 продемонструвала, що не зважаючи на зменшення потужності поля Галуа до $GF(2^6)$ для МНККС і $GF(2^4)$ для ГККККЗК, статистичні

характеристики таких крипто-кодових конструкцій виявилися, як мінімум, не гірше традиційних НККС Мак-Еліса на $GF(2^{10})$. Всі криптосистеми пройшли 100% тестів, причому найкращий результат показала ГККККЗК на укорочених *MEC*: 155 з 189 тестів пройдено на рівні 0,99, що становить 82% від усієї кількості тестів. При цьому традиційна НККС Мак-Еліса на $GF(2^{10})$ показала 149 тестів на рівні 0,99.

Таким, чином запропоновані методи забезпечення основних послуг безпеки БІР: конфіденційності і цілісності дозволяють інтегровано забезпечити необхідний рівень стійкості та достовірність БІР. Розглянемо запропонований метод забезпечення автентичності даних на основі ГККККЗК Мак-Еліса і Нідеррайтера.

3.3. Розроблення методу забезпечення автентичності банківських інформаційних ресурсів на основі двофакторної автентифікації на гібридних крипто-кодових конструкціях зі збитковими кодами

3.3.1. Дослідження протоколів двофакторної автентифікації

Відповідно до міжнародних стандартів *ISO 7498, ISO / IEC 10181* для забезпечення необхідних показників безпеки визначено п’ять базових загальноприйнятих послуг, основними з яких являються лише дві: автентичність та цілісність, для їх забезпечення використовуються механізми безпеки, більшість з яких реалізується на основі криптографічних методів перетворення інформації.

Основні механізми забезпечення цілісності та автентичності БІР на різних рівнях інфраструктури АБС засновані на використанні стандартів блоково-симетричних шифрів (3*DES*, ГОСТ 28147-2009). Прикладом програмної реалізації розглянутих механізмів є програмні засоби криптографічного захисту інформації “Грифон-Б” та “Грифон-Л” призначених для криптографічного захисту конфіденційної інформації в автоматизованих банківських системах [47; 48].

Програмний засіб “Грифон-Б” призначений для криптографічного захисту конфіденційної інформації в автоматизованих банківських системах та застосовується для обміну інформацією всередині корпоративної мережі банку, з клієнтами, що працюють з системою “Клієнт-Банк”, в системах обслуговування пластикових карт [47]. Програмний засіб криптографічного захисту інформації

“Грифон-Л” [48] призначений для використання у сфері банківської діяльності, зокрема, для обміну конфіденційною (в т.ч. фінансовою) інформацією всередині корпоративної мережі банку, з клієнтами, які працюють за системою “Клієнт-Банк”, в системах обслуговування пластикових карт та ін. Основні технічні характеристики даних програмних засобів захисту наведені в табл. 3.25.

Таблиця 3.25 – Основні характеристики програмних засобів захисту

Характеристики	“Грифон-Б”	“Грифон-Л”
Основні функції програми	Тест гешування, у т.ч. шифрування простою заміною; Одержання чисел *p, q* (512 біт і 1024 біт); Тест створення і перевірки ЕЦП; Тести швидкодії (шифрування, гешування, генерації чисел, ЦП); Просте і адресне шифрування рядка або файлу; Гешування рядка або файлу; Генерація загальносистемних параметрів; Генерація ключа користувача; Зміна пароля на секретному ключі; Підпис рядка або файлу; Загальний секретний ключ за алгоритмом Діффі-Геллмана	
Стандарти	ГОСТ 28147-2009. Алгоритм криптографічного перетворення; ГОСТ 34.311-95. Функція гешування; ГОСТ 34.310-95. Процедура вироблення і перевірки електронного підпису на базі асиметричного криптографічного алгоритму. Схема розподілу ключів Діффі-Геллмана. Стандарт X9.17 для генерації сеансових ключів.	
Швидкодія на ПК з процесором 633 МГц забезпечує	шифрування області пам’яті в режимі простої заміни – не менш 5 Мб/с; гешування області пам’яті – не менш 1.5 Мб/с; обчислення ЦП – не більше 0.015 с; перевірка ЦП – не більше 0.020 с; генерація загального ключа по методу Діффі-Хеллмана – не більше 0.015 с.	шифрування області пам’яті в режимі простої заміни – не менш 2.5 Мб/с; гешування області пам’яті – не менш 1 Мб/с; обчислення ЦП при довжині ключа 512 біт – не більше 0.02 с; перевірка ЦП – не більше 0.03 с; генерація загального секретного – не більше 0.02 с.

Таким чином, для забезпечення автентичності БІР використовуються симетричні і несиметричні криптоалгоритми, цифровій підпис та функції гешування на основі *MAC* і *MDC*-кодів [4; 10; 12; 13; 14; 22; 24; 25].

Для забезпечення автентичності у сфері фінансів при створенні сервісів інтернет-банкінгу, мобільного банкінгу, як правило, використовується електронний цифровий підпис, на основі багатофакторної або розширеної автентифікації. Вона заснована на складеному автентифікаторі, розділеному фізично, що значно підвищує безпеку використання інформації, щонайменше, з боку користувачів, які підключаються до інформаційних систем по захищених і незахищених каналах комунікацій.

Двофакторна автентифікація або *2FA* – це метод ідентифікації користувача в будь-якому сервісі, де використовуються два різних типи автентифікаційних даних. Введення додаткового рівня безпеки забезпечує більш ефективний захист аккаунта від несанкціонованого доступу. Застосовуючи такий тип *2FA*, користувач вводить на першому рівні автентифікації персональний пароль. На наступному етапі він повинен ввести маркер *OTP* (*OTP – One–time Password Algorithm*), зазвичай відправлений за допомогою *SMS* на його мобільний пристрій. *OTP* буде доступний тільки тому, хто, як передбачається в теорії, ввів недоступний сторонньому пароль [49; 50]. Методи строгої (двофакторної) автентифікації найчастіше використовуються в фінансовій сфері, але в принципі можуть застосовуватися практично в будь-якій іншій області. Загальна класифікація методів багатофакторної автентифікації наведена на рис. 3.34.

Виділяють декілька основних способів побудови систем двофакторної автентифікації [52]:

1. *ПЗ для ідентифікації конкретного ПК*. В комп’ютер встановлюється спеціальна програма, що використовує в ньому криптографічний маркер. Тоді в процесі автентифікації будуть задіяні два фактори: пароль і маркер, вбудований в ПК. Оскільки маркер постійно знаходиться на даному комп’ютері, користувачеві для входу в систему потрібно лише ввести ім’я користувача та пароль.

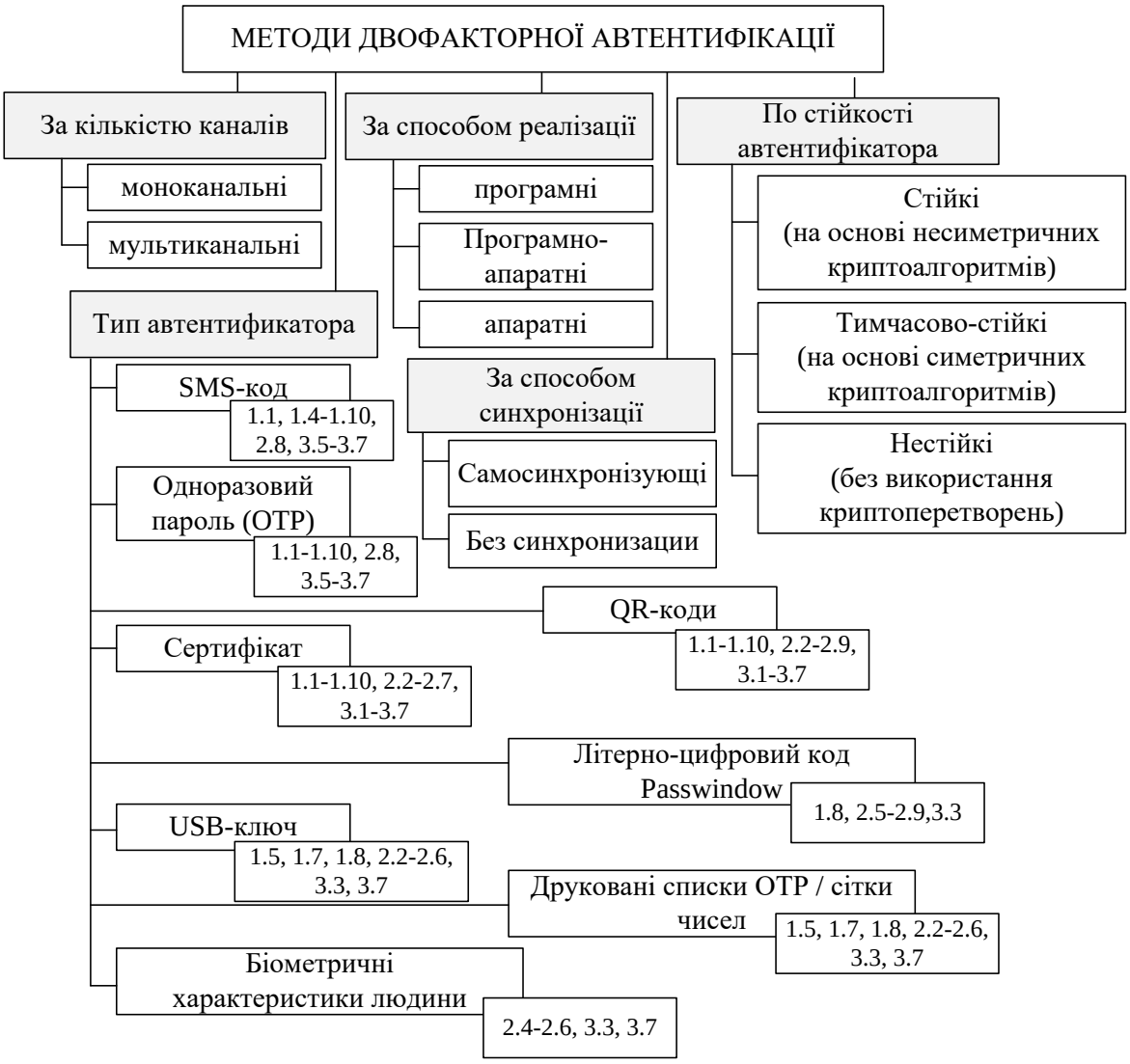


Рисунок 3.34 – Класифікація методів багатофакторної автентифікації

2. *Біометрія*. Використання біометрії як вторинного фактора ідентифікації здійснюється шляхом ідентифікації фізичних характеристик людини (відбиток пальця, оболонка очей тощо).

3. *Одноразовий e-mail* або *sms-пароль*. Використання як вторинного фактору ідентифікації *OTP*-пароля можливо шляхом відправлення другого одноразового пароля на зареєстрований адресу електронної пошти або на мобільний телефон.

4. *Токен з одноразовим паролем*. Користувачеві видається пристрій, який генерує постійно змінювані паролі. Саме ці паролі і вводяться користувачем додатково до звичайних паролів при автентифікації.

5. *Контроль зовні*. Цей метод передбачає дзвінок з банку на попередньо зареєстрований телефонний номер. Користувач повинен ввести пароль по

телефону, і тільки після цього він отримає доступ до системи.

6. *Ідентифікація з використанням гаджетів*. Такого роду ідентифікація здійснюється шляхом приміщення криптографічної мітки на який-небудь пристрій користувача (наприклад, встановлені на *USB*-накопичувач, *iPad*, карту пам'яті тощо.). При реєстрації користувач повинен під'єднати цей пристрій до ПК.

7. *Картка з шаром, що зішкрібається*. Користувачеві видається картка з *PIN*-кодом, який використовується лише один раз.

Розглянутий в роботах [5; 7; 9; 51] аналіз методів багатофакторної автентифікації виявив основні переваги та недоліки систем *2FA*:

*Методи на основі SMS-сповіщенн*я. Їх перевагою є генерація *OTP*-кодів при кожному вході і передача по додатковому каналу. Перехоплення логіна і пароля користувача за основним каналом не приведуть зловмисника до банківської інформації клієнта. Недоліками прив'язки *OTP*-пароля до телефонного номеру клієнта є те, що використання відкритого каналу стільникового зв'язку не дозволяє забезпечити конфіденційність *OTP*-кодів, використання тільки стільникових каналів призводить до "втрати" двофакторної автентифікації. Існує теоретична ймовірність підміни номера через послугу оператора або працівників салонів зв'язку.

Використання методів з додатками-автентифікатора (*QR*-коди) дозволяє підтримувати кілька акаунтів в одному автентифікаторі і формувати первинний ключ, немає необхідності використовувати стільникові лінії зв'язку, генерація *OTP*-паролів на основі криптоалгоритмів. Основними недоліками є використання автентифікатора на тому ж пристрої, з якого здійснюється вхід призводить до "втрати" двофакторності, доступ зловмисника до первинного ключа користувача призводить до злому системи автентифікації.

Перевірка входу за допомогою мобільних додатків дозволяє автоматизувати процес автентифікації без участі користувача на основі перевірки особистого ключа автентифікації на мобільному додатку. *Основними недоліками* є: втрата / розкриття особистого ключа призводить до злому системи автентифікації, можливість отримання *SMS*-повідомлень за рахунок синхронізації між *iPhone* і *Mac*, використання автентифікатора на тому ж пристрої, з якого здійснюється вхід,

призводить до “втрати” багатофакторності.

Фізичні (або апаратні) токени є найбільш надійним способом двофакторної автентифікації. Найчастіше вони представлені у вигляді *USB*-брелків з власним процесором, що генерує криптографічні ключі, які автоматично вводяться при підключенні до комп’ютера. Перевагами є відсутність використання додаткових мобільних додатків, ПЗ, токени є повністю незалежними девайсами. До *недоліків* належить те, що використання декількох акаунтів призводить до ’зв’язки токенів, що не підтримується всіма застосунками.

Резервні ключі, є запасним варіантом на випадок втрати / крадіжки смартфона, на який приходять одноразові паролі або коди підтвердження. Втрата / крадіжка резервних ключів призводить до руйнування конфіденційності системи автентифікації.

Штрих-коди системи Passwindow забезпечують унікальні статичні зображення послідовності символів, що генеруються динамічно сервером автентифікації без використання криптоалгоритмів. Будь-яке втручання або підробка шаблону штрих-коду буде пасивно представлене користувачеві у вигляді появи комбінацій в шаблоні, який не відповідає сподіванням. Істотним *недоліком* є можливість підбору унікального штрих-коду картки, запропонованого у роботі [5].

Використання біометрії як вторинного фактора ідентифікації здійснюється шляхом ідентифікації фізичних характеристик людини (відбиток пальця, райдужна оболонка ока і т.п.). *Перевагами методів* є використання унікальних фізіологічних характеристик людини, відсутність додаткових мобільних додатків і ПЗ. Істотним *недоліком* є специфічні вимоги до програмно-апаратних пристроїв зчитування біометричних даних користувача. Таким чином, в автоматизованих банківських системах, як правило, застосовуються системи багатофакторної автентифікації, засновані на одноразових *e-mail* або *sms-паролях* і різних типах токенів. Для забезпечення конфіденційності в стандарті дистанційного банкінгу для передачі банком *OTP*-кодів необхідно використовувати шифрований і незалежний від операторів канал їх доставки. Такий підхід не піддається впливу більшості відомих загроз, крім соціальної інженерії, що експлуатує людський фактор.

3.3.2. Аналіз загроз, актуальних для сучасних протоколів двофакторної автентифікації

Проведений аналіз загроз [59; 60; 61; 62; 63; 64] вказує на істотну їх трансформацію і гібридність. Від суто загроз ІБ, КБ, БІ на інфраструктуру АБС, ознаки гібридності загроз почали виникати внаслідок одночасного впливу на об’єкт захисту – БІР за рахунок виникнення явища синергізму [59].

На рис. 3.35 наведений синергетичний підхід до класифікації загроз багатофакторної автентифікації, який поєднується з наведеною на рис. 3.34 класифікацією методів *2FA*.

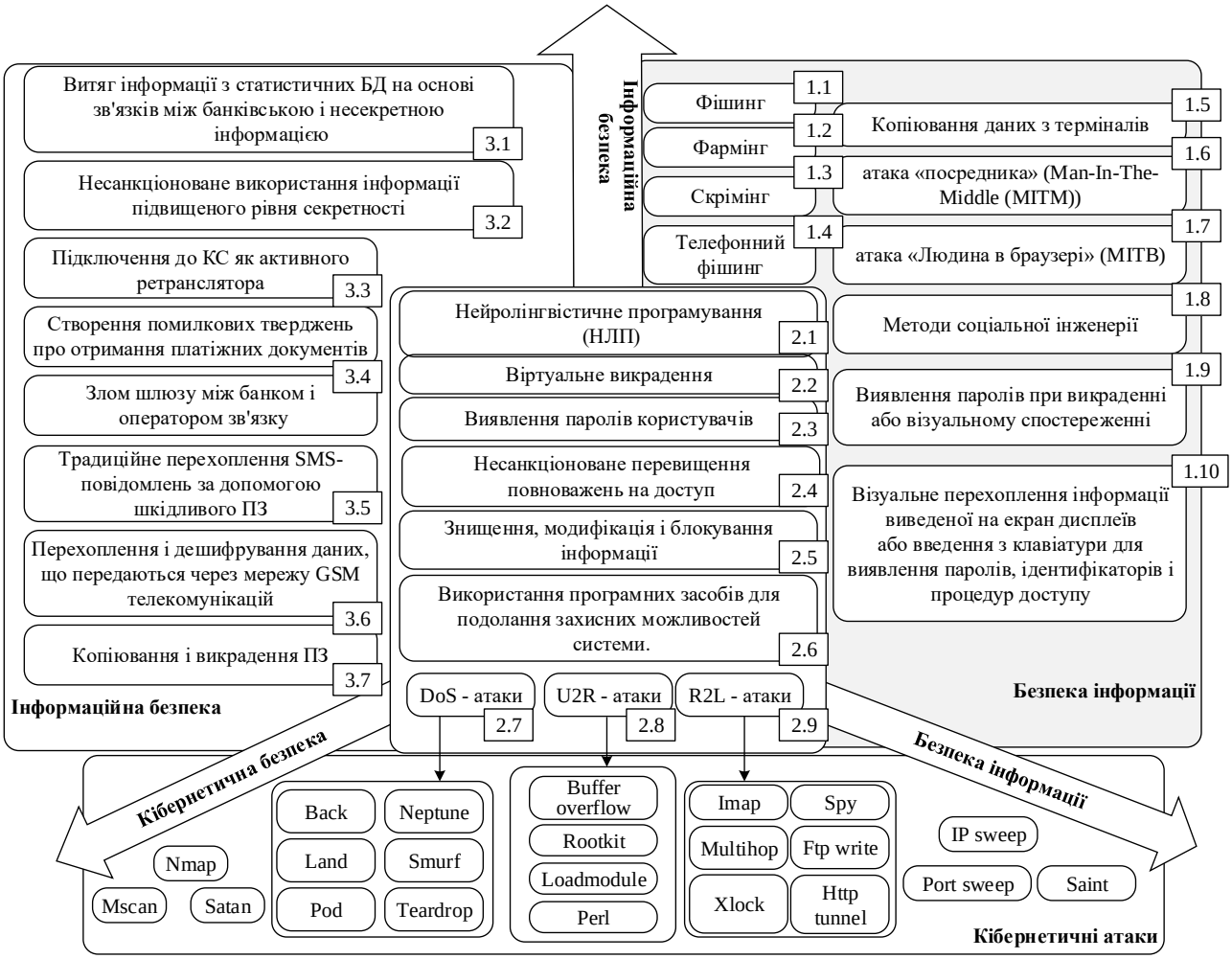


Рисунок 3.35 – Синергетична модель загроз безпеки БІР для протоколів *2FA*

Аналіз сучасних систем автентифікації показав, що їх безпека визначається шляхом ділення різниці між вартістю атак і вигоди для атакуючого на вартість захисту від них. Таким чином, дорогі, хоча і більш безпечні методи, наприклад,

криптографічні *PKI*-пристрої з власними захищеними каналами зв'язку, екранів і клавіатур оцінюються низько за шкалою безпеки. Водночас банківські системи все ще переважно спираються на найдешевший і, здавалося б , найменш захищений спосіб використання *PIN*-кодів і паролів. Загальна вартість і складність розгортання таких пристроїв часто переважає користь від їх надвисокої безпеки.

Загрози безпеці в мережі АБС можна розділити на мережеві атаки (інформація, що надходить з віддаленого агента) і локальні атаки, які походять від шкідливих програм вже, встановлених на системі клієнта, наприклад, троянів, руткітів, тощо. Часто оцінки безпеки автентифікації зосереджені головним чином на мережевих атаках, припускаючи, що термінал (тобто настільний комп'ютер, ноутбук або мобільний пристрій) є захищеною платформою [5; 50; 51; 52]. Проте, часто зловмисник отримує повний доступ до ПК жертви через приховані процеси зв'язку, які залишилися від шкідливих програм, що використовують невиправлені діри в безпеці ліцензійного програмного забезпечення.

Типовими методами атак на БІР є:

Злом он-лайнових баз даних – викрадення інформації, що зберігається в торгових базах, даних.

Людина посередник / фішинг – третя сторона втручається і уособлює клієнта і сервера, змушуючи записувати і / або змінювати повідомлення один одного.

Атаки в області соцінженерії – клієнтів обманюють з метою вивідати їх особисті дані для подальшої передачі хакеру.

"Людина в браузері"– шкідлива програма, що встановлюється на комп'ютері жертви, для повідомлення хакеру даних про мережеву активність, натискання клавіш, а також даних захоплених з екрану, дозволяючи йому перехоплювати дані переказу коштів, в яких кошти можуть бути мимоволі спотворені шляхом зміни інформації, що відображається в браузері користувача.

Атака з повним перебором паролів користувачів – сервер опитується з усіма можливими комбінаціями паролів.

Проста крадіжка – подробиці про автентифікацію, що записані або зберігаються на картці можуть бути фізично викрадені і скопійовані.

Спостереження зі спини – зловмисник може непомітно спостерігати, як користувач вводить деталі своєї угоди.

З поширенням *GSM*, смартфонів і планшетів підключених до мережі, навіть ця перевага безпеки може бути втрачена, якщо автентифікація транзакції користувача здійснюється на самому мобільному пристрої. Крім того, зростання небажаного програмного забезпечення для мобільних пристроїв тепер дозволяє зловмисникові отримати доступ до кодів автентифікації, відправлених через *SMS* не тільки за допомогою традиційного перехоплення за допомогою шкідливого ПЗ [53], але і шляхом перехоплення і дешифрування даних, що передаються через мережу *GSM*-телекомунікацій [55].

Атаки автентифікації мобільних пристроїв успішно проводяться і без таких технологій. Замість цього зловмисник просто видає себе за користувача пристрою і просить, щоб усі *SMS*-повідомлення направлялися на інший номер телефону протягом всієї атаки [55]. Інший метод перевірки автентичності використовує камеру мобільного пристрою для читання зображення штрих-коду на робочій станції користувача, який закодований з *OTP*-інформацією про транзакції. Цей метод містить помилку, припускаючи, що операційна система на мобільному пристрої користувача не піддається впливу до шкідливого ПЗ, як і всі інші форми програмного забезпечення, що працює з мережею [57].

У разі використання *біометричної автентифікації* дані про користувача пропонуються для онлайн-автентифікації. Однак біометричні пристрої автентифікації не можуть взаємодіяти з локальними пристроями або мережі, не наражаючись на небезпеку атакам шкідливих програм і / або атакам “посередника” [54]. Цей метод так само неможливо повторно змінити після того, як зловмисник видав себе за користувача, використовуючи біометричну автентифікацію.

Біометрична автентифікація надає користувачеві зручний спосіб генерації онлайн імені користувача, однак при прослуховуванні мережі і зараженого мобільного пристрою загальна продуктивність безпеки таких методів не краще, ніж при використанні звичайного імені та пароля користувача.

Електронні апаратні маркери бувають декількох видів і містять різні функції безпеки автентифікації. Найбільш часто апаратні маркери генерують одноразові паролі, використовуючи криптографічні алгоритми з внутрішнім ключем або, частіше, секретний ключ генерується на основі загального, синхронізованого значення системного часу. Користувач читає відображені пристроєм цифри і вручну вводить їх в свої термінали для перехресного посилання з сервером перевірки автентичності.

Цей простий метод електронної генерації *OTP* залишається вразливим до атак "посередника", оскільки користувачі повинні розголошувати *OTP* без засобів перевірки контексту автентифікації.

У відповідь на це багато виробників маркерів додали невелику цифрову клавіатуру, помітно збільшивши розмір маркера, але дозволяючи користувачеві вводити інформацію про конкретні транзакції, зашифровані за допомогою секретного ключа, перш ніж користувач вводить результат у своєму терміналі. Це є одним з типів перевірки або підписання транзакції, і дійсно забезпечує деякий захист від атаки "посередника".

Проте, цей метод як і раніше уразливий для атак, при використанні трудомісткого процесу ручного підписання транзакції. Час і увага, необхідні для виконання ручної операції, успішно використовуються для відволікання користувача від контексту інформації про угоди, які користувач приймає, і, отже, атаки можуть бути успішно здійснені в масовому масштабі [58].

Друковані списки OTP / сітки чисел. Більш старий метод надання одноразових паролів – це друковані списки випадково згенерованих кодів зв'язку або кодів авторизації транзакцій на аркуші паперу або скетч-картці. Кожен код доступу, запитується в послідовності і використовується для перевірки автентичності однієї транзакції.

Альтернативою може бути друкована таблиця символів, і сервер автентифікації видасть штрих-код, запитуючи символи, розташовані в певних координатах.

Обидва методи використовують ключі і сигнали, які можуть бути повідомлені вербально. Це дозволяє зловмисникові запитати користувача про наступний дійсний

код через шкідливі програми, використовуючи соціальну інженерію або фішинг-атаки. Крім того, відносно низька ентропія списків або сіток вимагає частої зміни ключів, щоб запобігти повтору запиту коду зловмисником.

Ці методи залишаються уразливими для повного спектра атак “посередника” з тих же причин, що і всі методи автентифікації з невідомим контекстом.

Підроблені (ослаблені) штрих-коди. Зловмисник може спробувати послабити захист *PassWindow*, змінюючи частоту кадрів з цього (перехопленого) штрих-коду, перш ніж доставити ослаблений (спрощений) штрих-код користувача. Цей метод зменшує ентропію штрих-коду, щоб змінити деталі, які могли б спростити аналіз перехоплення запитів / відповідей. Однак явно пошкоджений штрих-код, пасивно попереджає користувача про спробу нападу, викликаючи його підозри про використання обчислювальної техніки і комунікаційних каналів.

Ця атака вимагає значної кількості перехоплень хакером: від 20 – 30 в разі малих шаблонів, сотень – для великих шаблонів, декількох тисяч – у разі використання методу в анімаційному режимі підвищеної безпеки.

Розглянемо дієвий метод злому двофакторної автентифікації на основі *PassWindow*.

3.3.3. Використання двофакторної автентифікації на основі *PassWindow* та аналіз її безпеки

PassWindow є способом забезпечення двофакторної автентифікації в он-лайн середовищі. Вона включає в себе дві частини матриці – фізичний ключ з друкованим рисунком на переносній пластиковій пластині і цифровий шаблон штрих-коду представлений у вигляді зображення на звичайному електронному екрані, наприклад, на дисплеї ноутбука або мобільного пристрою. Вони генерують користувачеві унікальний одноразовий пароль і набір цифр для окремої транзакції, коли накладаються один на одного. Цей пароль потім використовується для он-лайн-автентифікації і перевірки автентичності транзакцій. Інформація про конкретну транзакції поміщена в ці цифри, наприклад, номер передбачуваного рахунку або суми транзакції. Це дозволяє користувачеві візуально підтвердити

справжність прийнятого запиту на автентифікацію. Ці особливості роблять *PassWindow* одним з дуже небагатьох доступних на сьогодні механізмів автентифікації, які забезпечують надійний захист від новітніх мережевих загроз безпеці “атак посередника” (*Man-In-The-Middle* (*MITM*)) [65].

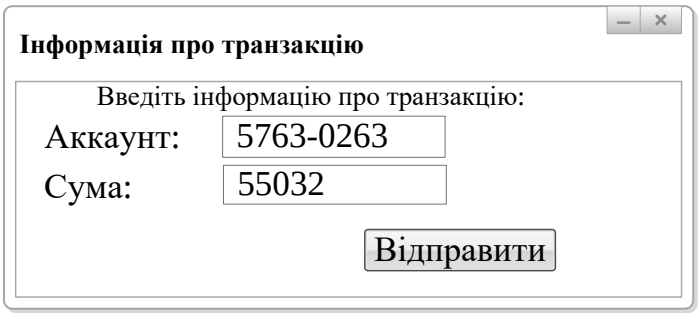
Технологія *PassWindow* базується на унікальній здатності частини матриць передавати інформацію таким чином, що вона розшифровується тільки при накладенні фізичного шаблону знаків передбачуваного одержувача (цю інформацію користувач має) після чого відображається шаблон штрих-коду (*challenge pattern*) на електронних мережевих пристроях користувача, таких, як комп’ютер, смартфон і т. п.

Поєднання ключа і шаблону штрих-коду показує закодовану інформацію тільки єдиному користувачеві, причому повний перегляд шаблону можливий тільки з прямого ракурсу. Будь-перехоплення штрих-коду через електронні пристрої означає, що інформація при витоку ні є достатньої для того, щоб зловмисник дізнався секретний ключ шаблону користувача протягом всього терміну діяльності карти.

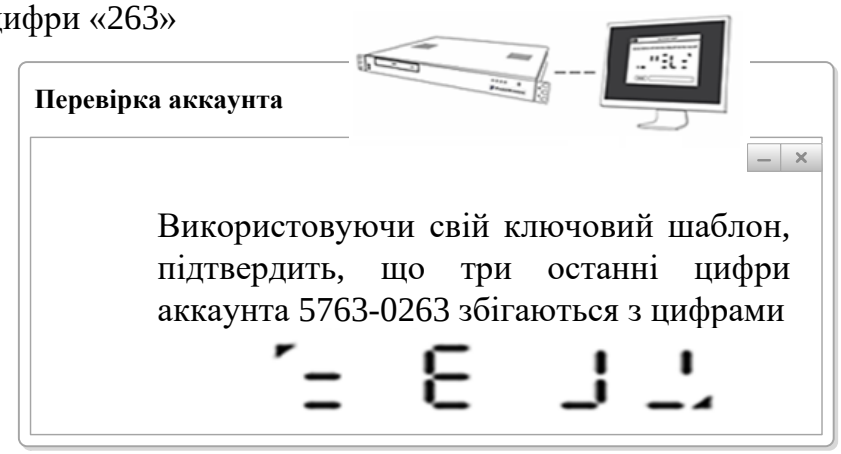
Шаблони штрих-коду *PassWindow* можуть існувати у вигляді унікальних статичних зображень послідовності символів або у вигляді більш розширеної анімаційної версії, яка є основною темою цього документа. Ці анімовані штрих-коди складаються з послідовності статичних шаблонів, кожен з яких містить закодовані символи або ж нічого не означають і просто динамічно додають ентропію в весь шаблон [65]. Послідовності шаблонів штрих-коду генеруються динамічно сервером автентифікації таким чином, що кожен є унікальним (і, отже, мають сенс) тільки при використанні разом з ключем, до якого вони підходять. Основні етапи системи *PassWindow* наведені на рис. 3.36.

Проведений аналіз загроз системи *PassWindow* в роботі [5] показав, що найбільш ефективною загрозою є аналітична атака на секретний ключ (штрих-код карти). Для успішної роботи алгоритму слід зробити від трьох до п’яти сесій моніторингу (передачі клієнтом *OTP* банку). Алгоритм моніторингу пластикових карт *PASSWINDOW* наведений на рис. 3.37.

1. Користувач вводить інформацію про транзакції для автентифікації



2. Після цього сервер автентифікації *PassWindow* створює штрих-код з одноразовим ключем і також специфічну інформацію: останні три цифри «263»



3. Користувач накладає карту з ключем і візуально перевіряє збіги інформації про транзакції, після цього він вводить одноразовий пароль, щоб провести автентифікацію транзакції

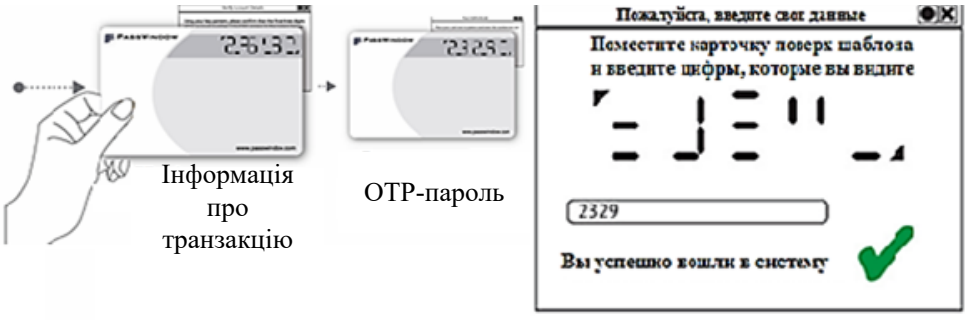


Рисунок 3.36 – Основні етапи роботи *PassWindow*

В інтересах тестування вразливості *PassWindow* до такого нападу був побудований алгоритм злому, який намагається використовувати ці принципи для виконання зазначеного аналізу, який підтверджує практичну складову запропонованого алгоритму, незалежно від кількості переданих цифр.

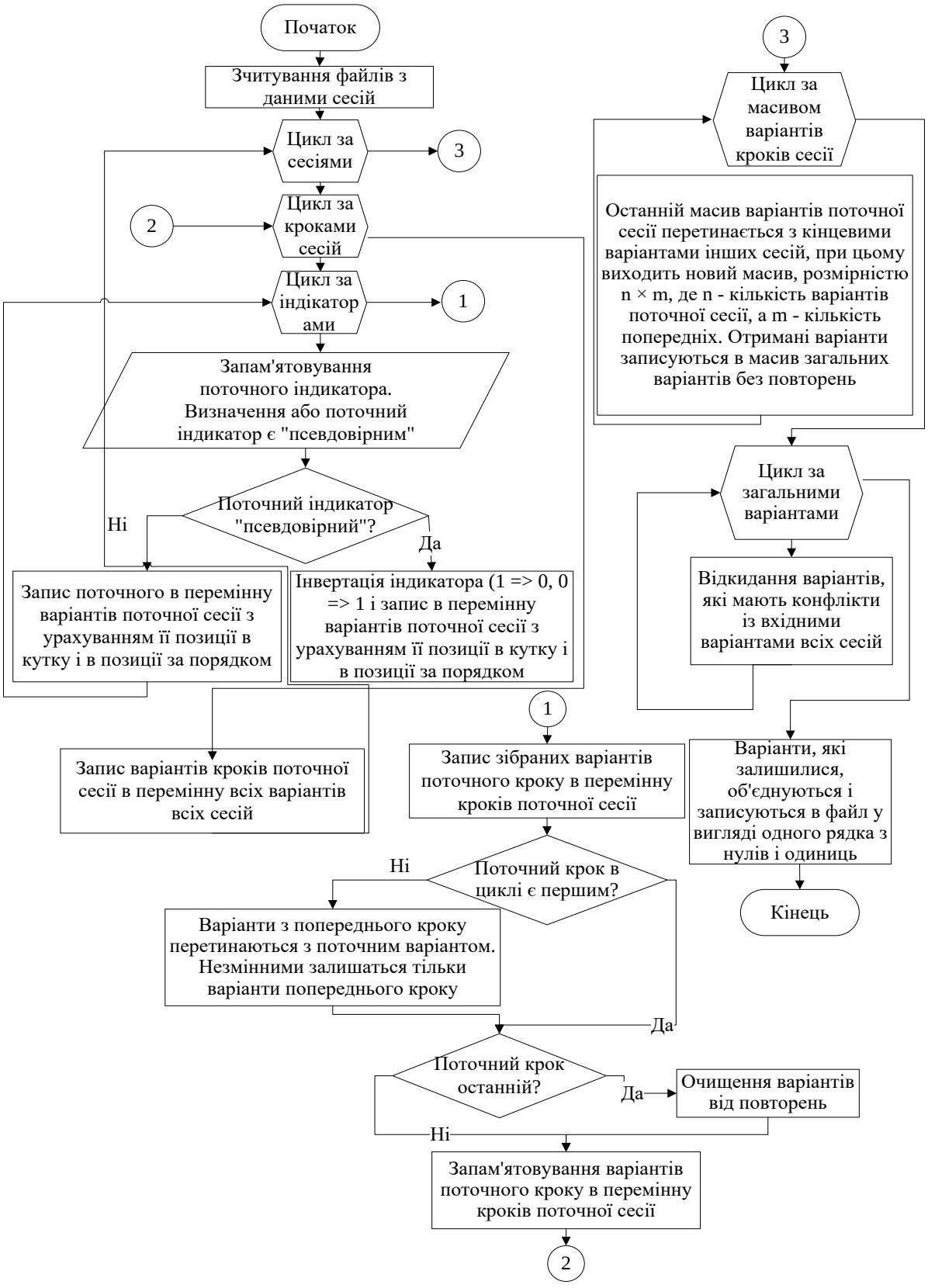


Рисунок 3.37 – Алгоритм моніторингу системи *PASSWINDOW*

Алгоритм моніторингу пластикових карт на основі системи *PassWindow* дозволяє за 3 – 5 сесій сформувати унікальний штрих-код персональної картки і складається з таких кроків (рис. 3.37):

1. Моніторинг каналу зв'язку і отримання даних за сесіями.

2. Переведення даних у клас індикатора (у вигляді бінарного коду), з яким є можливість оперувати як з об'єктом (клас індикатора являє собою масив з 7-ми одиниць / нулів).

3. Перевірка можливості формування "цифр" в кожній позиції картки (цикл за всіма сесіями). Всередині циклу починається цикл за кожною послідовністю – по черзі кожен індикатор представляється "вірним" (вважаємо, що в ньому була цифра).

Всередині циклу проводиться перевірка – якщо поточна позиція "вірна", тоді створюється варіант, в який записується інвертований індикатор генератора, якщо ця позиція "невірна" – записується індикатор. Після кожного циклу всередині однієї послідовності відбувається перетин з варіантами минулого послідовності, тобто $N_i \cap N_j$) –кінцеві кортежі (варіанти) проглядаються і викидаються копії;

4. Перегляд усіх послідовностей у всіх сесіях. Перетин усіх кортежів між сесіями по черзі (перша сесія з другою, результат їх перетину з третьою сесією і т. д.). Після кожного перетину кортежі суміжній сесії – кортежі "звільняються" від копій.

5. Перетин кортежів всіх сесій між собою. Цикл за всіма кортежами – кожен варіант (він же кортеж) перевіряється на вхідних даних – на даних генератора, якщо він має конфлікт з яким індикаторів, то такий кортеж (варіант) відкидається. В результаті залишиться тільки один варіант, який не має конфліктів ні з однією з послідовностей всіх сесій;

6. Висновок кінцевого варіанта записується у файл *output.txt* в форматі бінарного рядка.

Таким чином, запропонований алгоритм моніторингу системи *PassWindow* дозволяє за 3–5 сесій передачі *OTP*-паролів сформувати унікальний штрих-код карти користувача і отримати повний доступ до його банківських рахунків.

3.3.4. Дослідження методів побудови *OTP*-паролів

Тенденції консюмеризації в АБС призводять до того, що користувачам доводиться використовувати різні типи пристроїв для доступу до ресурсів фінансових послуг АБС. Це може бути стаціонарний або мобільний комп'ютер, планшет або смартфон [14; 66]. Технологія одноразових паролів, може допомогти реалізувати строгу двофакторну автентифікацію, і не вимагає істотних витрат на впровадження і підтримку [14; 66]. *OTP* практично невразливий для атаки мережевого аналізу пакетів і додатково вимагає від користувача введення *PIN*-коду, що є додатковим фактором автентифікації [14; 66]. Таким чином формується двофакторна автентифікація користувача в системі на основі володіння чимось (*Authentication by Ownership*) або на основі знання чого-небудь (*Authentication by Knowledge*) [66]. Зворотною стороною використання *OTP*-паролів є можливість "перехоплення" зловмисником тексту (*SMS*-повідомлення) з однією частиною токена. Зловмисники можуть скомпрометувати *2FA* на основі тексту декількома способами: на основі методів соціальної інженерії (переадресація повідомлень через провайдера), перехопленням повідомлення за допомогою *IMSI*-уловлювача (*International Mobile Subscriber Identity* – міжнародний ідентифікатор мобільного абонента), використання недоліків в протоколах, які дозволяють операторам зв'язку обмінюватися даними між мережами [67; 68]. З цієї причини Національний інститут стандартів і технологій США (*NIST*) в [69] пропонує заборонити використання двофакторну автентифікацію на основі *OTP*-паролів для служб, які підключаються до державних ІТ-систем. Таким чином, виникає суперечність між використанням *OTP*-паролів у протоколах двофакторної автентифікації і забезпеченням безпеки їх використання.

У роботі [69] пропонуються такі рівні достовірності автентифікації (*Authenticator Assurance Levels* (*Aals*), які наведені на рис. 3.38.

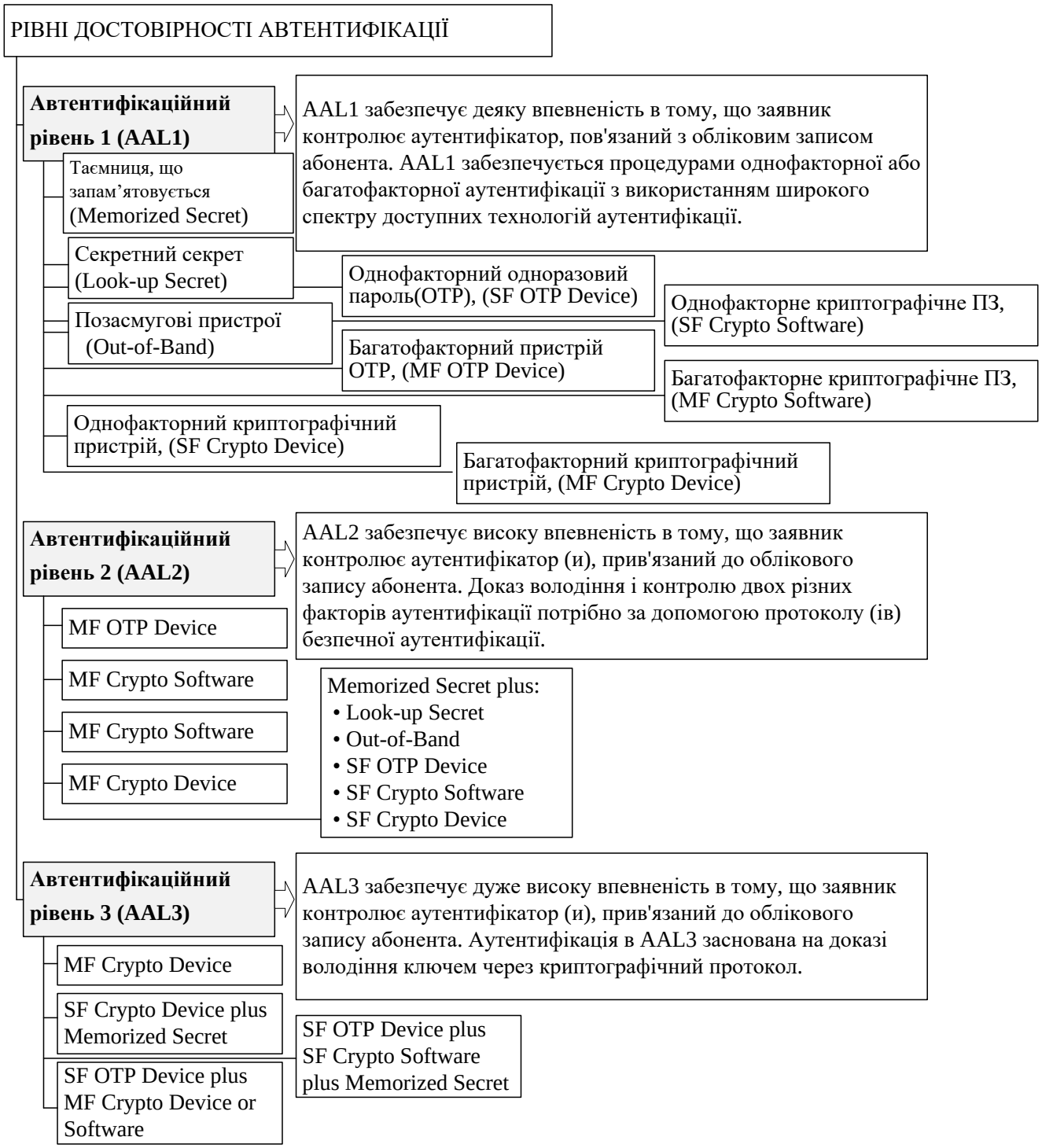


Рисунок 3.38 – Рівні достовірності автентифікації та механізми формування *OTP*-паролів

Проведений аналіз вимог в [69; 70; 71; 72] до методів формування *OTP*-паролів дає можливість зробити такі висновки:

–*секретний автентифікатор*, що *запам'ятовується* – зазвичай називається *паролем* або, якщо числовий, *PIN*. Він є секретним значенням, що призначене для

вибору й запам’ятовування користувачем, повинен складатися з 8-ми символів, бути досить складним для запам’ятовування й зберігається в секреті. Для формування секретного автентифікатора пропонується використовувати алгоритми формування *MAC*-кодів: *HMAC* [*FIPS* 198-1], *SHA*-3 [*FIPS* 202], *CMAC* [*SP* 800-38*B*] або *Kecacak Message Authentication Code* (*KMAC*), що настроюється *SHAKE* (*cSHAKE*) або *Parallelhash* [*SP* 800-185];

– *секретні автентифікатори Look-Up* – являють собою фізичний або електронний запис, у якому зберігається набір секретів, що спільно використовуються між заявником і *CSP* (*Center for Security Policy* – центр політики безпеки). Для створення списку секретів використовуються стандартизовані генератори випадкових бітів [*SP* 800-*90Ar1*] [72];

– *позасмуговий автентифікатор* – фізичний пристрій, який однозначно адресується й може безпечно зв’язуватися з верифікатором через окремий канал зв’язку, що називається вторинним каналом. Пристрій контролюється заявником і підтримує частковий зв’язок за вторинним каналом, окремо від первинного каналу для електронної автентифікації. Для формування вторинного каналу можуть використовуватися мережі загального користування, що комутуються (*4G LTE*). Автентифікатор передається у зашифрованому вигляді [73];

– *однофакторний OTP-пристрій* генерує *OTP*. Ця категорія включає апаратні пристрої й програмні генератори *OTP*, установлені на мобільних гаджетах. Ці пристрої мають вбудований секрет, який використовується як ключ для генерації *OTP* і не вимагає активації через другий фактор. Для формування ключа використовуються симетричні й несиметричні криптоалгоритми. *OTP* відображається на пристрої й уводиться вручну для передачі у верифікатор, доводячи таким чином право володіння й керування пристроєм;

– *багатофакторний пристрій OTP* генерує *OTP* для використання при автентифікації після активації за допомогою додаткового автентифікатора. Пристрій використовує апаратні пристрої й програмні генератори *OTP* на основі симетричних криптоалгоритмів, або функцій гешування, які встановлені на мобільних гаджетах. Інший фактор автентифікації реалізовується за допомогою

якогось вбудованого вхідного майданчика, інтегрального біометричного зчитувача (наприклад, відбитка пальця) або прямого комп'ютерного інтерфейсу (наприклад, *USB*-порт). *OTP* відображається на пристрої й уводиться вручну для передачі у верифікатор;

– *однофакторний криптографічний автентифікатор програмного забезпечення* – це криптографічний ключ, що зберігається на диску або якому-небудь іншому "м'якому" носії. Однофакторні криптографічні автентифікатори програмного забезпечення інкапсулюють секретний ключ, унікальний для автентифікатора. Автентифікація здійснюється шляхом перевірки володіння й контролю ключа;

– *однофакторний криптографічний пристрій* являє собою апаратний пристрій, який виконує криптографічні операції з використанням захищеного криптографічного ключа й надає вихід автентифікатора через пряме з'єднання з кінцевою точкою користувача. Пристрій використовує вбудовані симетричні або асиметричні криптографічні ключі й не вимагає активації через інший фактор автентифікації. Автентифікація здійснюється шляхом перевірки володіння пристроєм за протоколу автентифікації;

– *багатофакторний криптографічний автентифікатор програмного забезпечення* – криптографічний ключ, що зберігається на диску або якому-небудь іншому "м'якому" носії, який вимагає активації через інший фактор автентифікації. Автентифікація здійснюється шляхом перевірки володіння й контролю ключа;

– *багатофакторний криптографічний пристрій* – апаратний пристрій, який виконує криптографічні операції з використанням одного або декількох захищених криптографічних ключів і вимагає активації через інший контент автентифікації. Автентифікація здійснюється шляхом перевірки володіння пристроєм і контролю ключа. Вихід автентифікатора забезпечується прямим підключенням до кінцевої точки користувача й значною мірою залежить від конкретного криптографічного пристрою й протоколу. Багатофакторні автентифікатори криптографічних пристроїв використовують захищене від несанкціонованого доступу обладнання, щоб інкапсулювати секретний ключ. На рис. 3.39 наведені основні загрози

автентифікаторам, які можна класифікувати на основі атак на типи факторів автентифікації [50].

Рисунок 3.39 – Класифікація загроз за типом автентифікатора

Проведений аналіз загроз на основі синергетичного підходу до оцінки загроз

[74] показав, що зловмисники на сьогоднішній день використовують комплексний підхід до одержання персональних даних і автентифікаторів користувачів утворювачів послуг АБС. Як правило, методи злому засновані на поєднанні методів соціальної інженерії з традиційними методами “маскараду” й проникнення.

Крім цього використовуються й нові види кібератак, що дозволяють ефективно вбудовувати шкідливе ПЗ на мобільні засоби зв’язку, що у свою чергу приводить до зниження рентабельності методів багатофакторної автентифікації на основі *SMS*-повідомлень і *OTP*-паролів в АБС.

Таким чином, виникає необхідність використання додаткових засобів забезпечення конфіденційності передачі автентифікаторів у відкритих системах мобільного зв’язку/ *4G LTE*, що комутуються. У наступному розділі пропонується метод двофакторної автентифікації на основі ГКККЗК на *MEC*, який дозволяє усунути це протиріччя.

3.3.5. Розроблення протоколу двофакторної автентифікації на гібридних крипто-кодових конструкціях зі збитковими кодами

Проведений аналіз атак на автентифікатори схем багатофакторної автентифікації з використанням *OTP*-паролів дозволяє сформулювати основні вимоги до таких протоколів:

– збільшення факторів багатофакторної автентифікації;

– збільшення довжини секретів, використання стійких стандартизованих криптоалгоритмів;

– використання процедур шифрування при передачі відкритими каналами глобальної мережі Інтернет (ГМІ), мобільними відкритими мережами;

– підвищення вимог до рівня забезпечення безпеки в системних і мережевих пристроях ГМІ та мобільних мереж;

– підвищення рівня інформаційної й кіберграмотності користувачів.

Для забезпечення вимог авторами пропонується використовувати крипто-кодові системи, наведені в роботах [6; 7; 8]. У роботах [8; 9], де розглянуті практичні алгоритми побудови гібридних крипто-кодових конструкцій на збиткових кодах, що

дозволяють удосконалити схему багатофакторної автентифікації з метою підвищення рівня криптостійкості й достовірності автентифікатора, який формується.

Для цього банківська картка (БК) повинна містити такі елементи даних [7; 9]:
1) індекс відкритого ключа центру сертифікації: оскільки термінал може працювати з декількома центрами сертифікації, то ця величина специфікує, який із ключів необхідно використовувати терміналу при роботі з даною картою;

2) сертифікат відкритого ключа емітента, що підписується відповідним центром сертифікації;

3) сертифікат відкритого ключа БК, що підписується емітентом і формується на основі МНККС Мак-Еліса;

4) модуль і експоненту відкритого ключа емітента;

5) модуль і експоненту відкритого ключа БК;

6) Секретний ключ БК.

Термінал, який підтримує схему багатофакторної автентифікації, повинен зберігати відкриті ключі всіх центрів сертифікації й асоційовану інформацію, що стосується кожного із ключів.

Термінал повинен також уміти вибирати відповідні ключі на основі індексу (1) і деякої спеціальної ідентифікаційної інформації.

Для підтримки багатофакторної автентифікації банківська картка (БК) користувача повинна мати свою власну ключову пару (відкритий і секретний ключі автентифікатора). Відкритий ключ БК зберігається на БК у сертифікаті відкритого ключа. Кожний відкритий ключ БК сертифікується банком-емітентом, а довірений центр сертифікації сертифікує відкритий ключ банка-емітента. Це означає, що для перевірки автентифікатора карти терміналу спочатку необхідно перевірити два сертифікати для того, щоб відновити й автентифікувати відкритий ключ БК, який потім застосовується при перевірці автентифікатора БК.

Процес запропонованого методу автентифікації складається з п’яти етапів.

1. Відновлення терміналом відкритого ключа центру сертифікації. Термінал зчитує індекс, ідентифікує й отримує модуль відкритого ключа центру сертифікації,

що зберігаються в ньому – матриці маскування (*X, P, D*), рівняння кривої для алгеброгеометричного коду (АГК), і асоційовану інформацію, вибирає відповідні алгоритми.

2. Одержання вектора ініціалізації (секретних “місць” у векторі помилки – бітів укорочення) від банку-емітента. Формування *OTP*-пароля (вектора помилки на основі модифікованої крипто-кодової системи Нідеррайтера).

3. Формування автентифікатора на основі використання МНККС Мак-Еліса. Одержання кодового слова (автентифікатора) шляхом складання отриманого кодового слова із сеансовим ключем.

4. Формування збиткового тексту автентифікатора й збитку [39; 40].

5. Перевірка дійсності автентифікатора. Знаходження кратності вектора помилки й порівняння з отриманим. Структура запропонованого методу двофакторної автентифікації на основі ГКККЗК наведена на рис. 3.40.

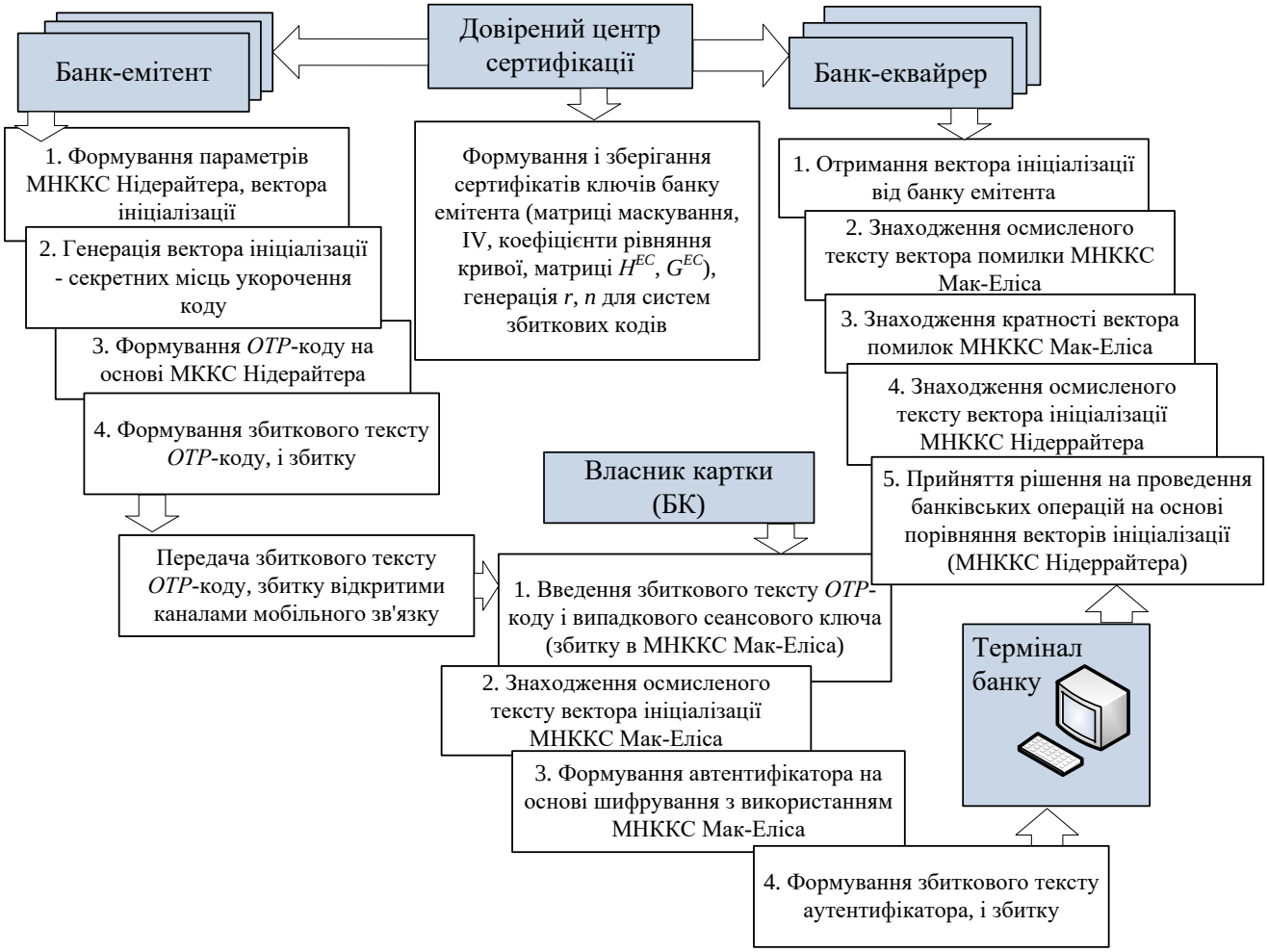


Рисунок 3.40 – Структурна схема вдосконаленого методу *2FA* на основі ГКККЗК

Таким чином, використання гібридних крипто-кодових конструкцій на збиткових кодах дозволяє збільшити кількість токенів автентифікатора, використовувати дві несиметричні крипто-кодові системи, два/чотири канали передачі збиткового тексту автентифікатора й збитку.

Масштабованість програмного модуля шляхом зміни параметрів МНККС Нідеррайтера й/або Мак-Еліса залежно від висунутих вимог до комунікаційних каналів АБС, забезпечує його програмну реалізацію в мобільних гаджетах і сумісність із протоколами інтернет-банкінгу ОБС.

3.3.6. Дослідження властивостей запропонованого методу двофакторної автентифікації

Запропонований вдосконалений метод строгої двофакторної автентифікації з *OTP*-паролями на основі крипто-кодових конструкцій МНККС Мак-Еліса й Нідеррайтера дозволяє усунути основний недолік цього протоколу *2FA* – передачу окремих токенів автентифікатора відкритими каналами мобільного зв'язку. Структурна схема практичної реалізації, запропонованої *2FA* на ГККККЗК наведена на рис. 3.41.

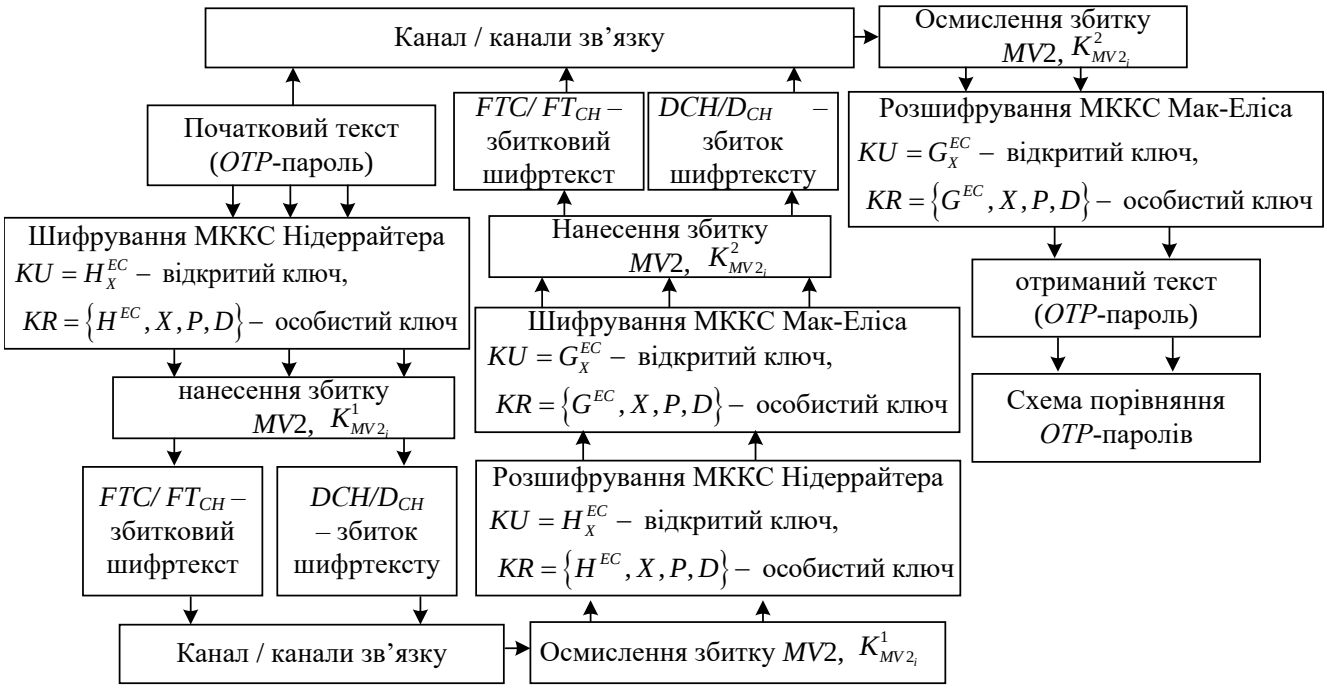


Рисунок 3.41 – Структурна схема практичної реалізації протоколу *2FA* на ГККККЗК

Оцінка криптостійкості запропонованої ГККК на збиткових кодах

Для оцінки криптостійкості скористаємося запропонованим у роботі [8] ентропійним методом оцінки криптостійкості.

Запропонована гібридна криптосистема за другим способом завдання збитків – завдання збитків шифртексту розглянутого в роботах [39; 40], порівнянна за стійкістю. У цьому випадку маємо сукупність збиткових шифртекстів і збитків, причому всі окремо не відповідають вихідному осмисленому тексту.

При повній сукупності збиткових шифртекстів і всіх збитків відбувається збільшення відстані єдності за рахунок додаткових ключів завдання збитків шифртексту. Таким чином, додаткове шифрування дозволяє одержати збільшену відстань єдності:

$$U_0 = \frac{\begin{array}{l} H\left(H^{EC}\right)+H\left(X_N^{EC}\right)+H\left(P_N\right)+H\left(D_N\right)+ \\ +H\left(G^{EC}\right)+H\left(X_{Mc}^{EC}\right)+H\left(P_{Mc}\right)+H\left(D_{Mc}\right)+ \\ +\sum_{i=1}^{m}H\left(\left(K_{MV2_N}^{i}\right)+H\left(K_i\right)\right)+\sum_{i=1}^{m}H\left(\left(K_{MV2_{Mc}}^{i}\right)+H\left(K_i\right)\right) \end{array}}{B\log\left|I\right|}, \qquad (3.36)$$

де U_0 – відстань єдності; H^{EC}, X_N^{EC}, P_N, D_N – особистий ключ у МНККС Нідеррайтера; G^{EC}, X_{Mc}^{EC}, P_{Mc}, D_{Mc} – особистий ключ у МНККС Мак-Еліса; $K_{MV2_N}^{i}$ – ключ у ГКККЗК Нідеррайтера; $K_{MV2_{Mc}}^{i}$ – ключ у ГККК Мак-Еліса; $\left|I\right|$ – кількість осмислених текстів; B – надлишковість вихідного тексту; m – кількість збитків.

Вираз (3.36) дозволяє оцінити стійкість запропонованих гібридних крипто-кодових конструкцій Мак-Еліса й Нідеррайтера на збиткових кодах.

Таким чином, запропонований метод забезпечує подальше використання протоколу строгої автентифікації з *OTP*-паролями, без істотної зміни каналів зв’язку, підвищення швидкодії використаних криптоалгоритмів, які забезпечують протидію гібридним атакам на БІР.

3.4. Висновки до третього розділу

Таким чином, у третьому розділі дисертаційної роботи наведено результати наукових досліджень, пов'язаних із забезпеченням послуг конфіденційності, цілісності та автентичності БІР, зокрема розроблено і досліджено експериментально методи гібридних крипто-кодових конструкцій на збиткових кодах. На основі оцінок ефективності ТЗЗІ в АБС для забезпечення конфіденційності, цілісності БІР запропоновано нові механізми на основі ГККЗК, які дозволяють будувати несиметричні криптосистеми, що забезпечують відповідний рівень безпеки та достовірності. У результаті досліджень було отримано такі результати:

1. Розроблено метод забезпечення конфіденційності та цілісності банківських інформаційних ресурсів на гібридних крипто-кодових конструкціях зі збитковими кодами. Метод базується на модифікованій крипто-кодовій системі Мак-Еліса на модифікованих алгеброгеометричних кодах, що інтегровано (одним механізмом) забезпечує безпеку банківських інформаційних ресурсів (безпечний час – $T_Б$> 200 р., стійкість до криптоаналізу P_K <10^{25}–10^{35} групових операцій), достовірність передачі банківських інформаційних ресурсів в автоматизованих банківських системах ($P_{пом}$ <10^{-9}) та зменшення енергетичних витрат на їх практичну реалізацію в 10 – 12 разів (шифрування, розшифрування) за рахунок зменшення порядку *GF (q)*. Впровадження запропонованого методу дозволяє підвищити рівень захищеності банківських інформаційних ресурсів та забезпечити своєчасне реагування на вимоги міжнародних і національних регуляторів безпеки банківських інформаційних ресурсів за рахунок зміни окремих параметрів та модифікації застосування модифікованих крипто-кодових систем Мак-Еліса і Нідеррайтера з системами багатоканальної криптографії на збиткових кодах.

2. Розроблено метод двофакторної автентифікації на гібридних крипто-кодових конструкціях зі збитковими кодами на основі модифікованих крипто-кодових систем Мак-Еліса і Нідеррайтера з *MEC*, що дозволяє забезпечити рівень стійкості *OTP*-паролів при передачі відкритими каналами зв'язку та зберегти можливість подальшого використання протоколу двофакторної автентифікації на

основі *SMS*-повідомлень. Не зважаючи на зменшення потужності поля Галуа до $GF(2^6)$ для модифікованих крипто-кодових систем і $GF(2^4)$ для гібридних крипто-кодових конструкцій на збиткових кодах, статистичні характеристики таких крипто-кодових конструкцій виявилися, як мінімум, не гірше традиційних схем Мак-Еліса над $GF(2^{10})$. Всі криптосистеми пройшли 100% тестів, причому найкращий результат показала гібридна крипто-кодова конструкція на укорочених *MEC*: 155 з 189 тестів пройдено на рівні 0,99, що становить 82% від усієї кількості тестів. При цьому традиційна схема Мак-Еліса на $GF(2^{10})$ показала 149 тестів на рівні 0,99.

Список використаних джерел у третьому розділі

1. О. О. Кузнецов, С. П. Євсеєв, С. В. Кавун, та О. Г. Король *Сигнали і коди. Алгебраїчні методи синтезу*. Монографія. Харків, Україна: Вид. ХНЕУ, 2009.

2. О. О. Кузнецов, С. П. Євсеєв, та С. В. Кавун *Захист інформації та економічна безпека підприємства*. Монографія. Харків, Україна: Вид. ХНЕУ, 2009.

3. С. П. Евсеев, и О. Г. Король, “Исследование коллизионных свойств кодов аутентификации сообщений UMAC”. *Информационные технологии и системы в управлении, образовании, науке*. Коллективная монография [под. редакцией В. С. Пономаренко]. Харків, Україна: Цифрова друкарня, с. 25 – 38, 2013.

4. С. П. Євсеєв, О. Ю. Йохов, та О. Г. Король *Гешування даних в інформаційних системах*. Монографія. Харків, Україна: Вид. ХНЕУ, 2013.

5. С. П. Евсеев, и Т. А. Свердло, “Исследование угроз методов двухфакторной аутентификации”. *Информационные технологии и защита информации в информационно-коммуникационных системах*: Коллективная монография [под. редакцией В. С. Пономаренко]. Харків, Україна: Вид-во ТОВ “Щедра садиба плюс”, с. 141 – 154, 2015.

5. С Евсеев, и В Абдулаев, “Алгоритм мониторинга метода двухфакторной аутентификации на основе системы Passwindow”, *Восточно-европейский журнал передовых технологий*, вып. 2/2(74), с. 9 – 15, 2015. *(Scopus)*

6. С Евсеев, О Король, Х Рзаев, и З Иманова, “Разработка модифицированной несимметричной крипто-кодовой системы Мак-Элиса на укороченных эллиптических кодах”, *Восточно-европейский журнал передовых технологий*. том 4, 9(82), с. 18 – 26, 2016. *(Scopus)*

7. S Yevseiev, H Kots, and Y Liekariev, “Developing of multi-factor authentication method based on Niederreiter-McEliece modified crypto-code system”, *Восточно-европейский журнал передовых технологий*, 6/4(84), с. 11 – 23, 2016 *(Scopus)*

8. S Yevseiev, O Korol, and H Kots, “Construction of hybrid security systems based on the crypto-code structures and flawed codes”, *Восточно-европейский журнал передовых технологий*, 4/9(88), с. 4 – 20, 2017. *(Scopus)*

9. S Yevseiev, H Kots, S Minukhin, O Korol, and A Kholodkova, “The development of the method of multifactor authentication based on hybrid crypto-code constructions on defective codes”, *Восточно-европейский журнал передовых технологий*, 5/9(89), с. 19 – 35, 2017. *(Scopus)*

10. С Євсеєв, “Анализ методов построения универсальных классов хеш-функций”, *Вісник Державного університету інформаційно-комунікаційних технологій*, том 7 (№ 4), с. 337 – 345, 2009.

11. С Евсеев, и Б Томашевский, “Исследование теоретико-кодовых схем для комплексного обеспечения безопасности и достоверности данных в информационных системах”, *Науковий вісник Чернівецького університету. Серія: Комп’ютерні системи та компоненти*, том 2, вип.1, с. 6 – 14, 2011.

12. А Кузнецов, О Король и С. Евсеев, “Исследование коллизионных свойств кодов аутентификации сообщений UMAC”, *Прикладная радиоэлектроника*, том 11, № 2, с. 171 – 183, 2012.

13. С. Евсеев, О. Король, и Л. Пархуць, “Разработка модели и метода каскадного формирования МАС с использованием модулярных преобразований” *Захист інформації: науково-технічний журнал*, том 15, № 3, с. 186 – 196, 2013.

14. С. Евсеев, и О. Король, “Исследование методов двухфакторной аутентификации”, *Системи обробки інформації*, № 2(118), с. 81 – 87, 2014.

15. S. Yevseiev, T. Sverdlo, and O. Korol, “Mécanismes intégrés de sécurité et de fiabilité des données dans les systèmes d’information basés sur la théorie des codes correcteurs d’erreurs”, *French Journal of Science and Education*, № 2(12), p. 358 – 368, 2014.

16. S. Evseev, and B. Tomashevsky, “Two-factor authentication methods threats analysis”, *Радіоелектроніка, інформатика, управління*, вип. 1(32), с. 52 – 59, 2015.

17. С. Евсеев, Х. Рзаев, и А. Цыганенко, “Анализ программной реализации прямого и обратного преобразования по методу недвоичного равновесного кодирования”, *Науково-технічний журнал “Безпека інформації”*, том 22, № 2, с. 196 – 203, 2016.

18. С. Евсеев, “Использование ущербных кодов в крипто-кодовых системах”, *Системи обробки інформації*, №, 5 (151) с. 109 – 121, 2017.

19. С. Євсеєв, С. Остапов, та Р. Королев, “Використання міні-версій для оцінки стійкості блоково-симетричних шифрів”, *Науково-технічний журнал “Безпека інформації”,* том 23, № 2, с. 100 – 108, 2017.

20. С. Євсеєв, О. Андрощук, та В. Федорченко, “Побудова систем безпеки інформаційно-телекомунікаційних систем на основі комплексного крипто-графічного підходу”, *Збірник наукових праць Нац. академії Держ. прикор. служби України ім. Богдана Хмельницького. Серія : військові та технічні науки* [гол. ред. Олексієнко Б. М.], № 2 (72), с. 258 – 268., 2017.

21. С. Євсеєв, та О. Король, “Дослідження загроз методів двофакторній автентифікації”, *Вісник національного університету “Львівська політехніка”*, № 806, с. 62 – 71, 2014.

22. С. Евсеев, и О. Король, “Метод каскадного формирования МАС-кодов на основе модулярных преобразований”, *Известия Высших технических учебных заведений Азербайджана*, № 1 (89), с. 71 – 78, 2014.

23. С. Евсеев, и О. Мисюра, “Крипто-кодовые системы с открытым ключом на алгебраических кодах”, на “*Securitatea informaţională 2008*”, (ed. a 5-a jubiliară), Grigore Bilostecinic, 2008, p. 64 – 66.

24. С. Евсеев, О. Король, и В. Ковтун, “Аутентификация данных с использованием ключевых хеширующих функций”, *II Міжнародної науково-*

практичної конференції "Проблеми й перспективи розвитку IT-індустрії", Харків, 2010, с. 215 – 216.

25. С. Евсеев, и О. Король, "Метод универсального хеширования на основе модулярных преобразований", *III Міжнародна науково-практична конференція "Проблеми й перспективи розвитку IT-індустрії"*, Харків, 2011, с. 131 – 132.

26. С. Евсеев, С. Головашич, и И. Воронцов, "Исследование механизмов двусторонней аутентификации сообщений с использованием пластиковых карточек PASSWINDOW", *IV Міжнародна науково-практична конференція "Проблеми й перспективи розвитку IT-індустрії"*, Харків, 2012, с. 221.

27. С. Евсеев, "Исследование методов двухфакторной аутентификации / С. Евсеев", *VII міжнародна науково-практична конференція "Сучасні проблеми і досягнення в галузі радіотехніки, телекомунікацій та інформаційних технологій"*, Запоріжжя, 2014, с. 331 – 332.

28. С. Евсеев, и Т. Свердло, "Исследование угроз методов двухфакторной аутентификации", *VII Міжнародна науково-практична конференція "Проблеми і перспективи розвитку IT-індустрії"*, Харків, 2015, с. 26.

29. С. Евсеев, и И. Белодед, "Крипто-кодовая система на модифицированных кодах", *V Міжнародна науково-технічна конференція "Методи та засоби кодування, захисту й ущільнення інформації"*, Вінниця, 2016, с. 47 – 50.

30. С. Євсеєв, та І. Білодід, "Використання збиткових кодів в гібридних крипто-кодових конструкціях", П'ята міжнародна науково-технічна конференція "Проблеми інформатизації", Черкаси – Баку – Бельсько-Бяла – Полтава, 2017 с. 11.

31. R. J. McEliece, "A Public-Key Criptosystem Based on Algebraic Theory", *DGN Progres Report 42-44, Jet Propulsi on Lab. Pasadena*, CA. January – February, p. 114 – 116, 1978.

32. H. Niederreiter, "Knapsack-Type Cryptosystems and Algebraic Coding Theory", *Probl. Control and Inform. Theory*, V.15, p. 19 – 34, 1986.

33. Р. Блейхут, *Теория и практика кодов, контролирующих ошибки*: пер. с англ., М.: Мир, 1986.

34. Дж.-мл. Кларк, *Кодирование с исправлением ошибок в системах цифровой связи*: пер. с англ. / под ред. Б. С. Цыбакова, М.: Радио и связь, 1987.

35. Ф. Дж. Мак-Вильямс, и Н. Дж. А. Слоэн, *Теория кодов, исправляющих ошибки*, М. : Связь, 1979.

36. В. М. Мутер, *Основы помехоустойчивой телепередачи информации*, Л.: Энергоатомиздат. Ленингр. отд-ние, 1990.

37. Т. Касами, Н. Токура, Е. Ивадари, и Я. Инагаки, *Теория кодирования*: пер. с япон. под ред. Б. С. Цыбакова и С. И. Гельфанда, М.: Мир, 1978.

38. В. М. Сидельников, “Криптография и теория кодирования”, *Материалы конференции “Московский университет и развитие криптографии в России”*, МГУ, 2002, с. 1 – 22.

39. В. А. Мищенко, Ю. В. Виланский, *Ущербные тексты и многоканальная криптография*, Минск, Энциклопедикс, 2007.

40. В. А. Мищенко, Ю. В. Виланский, В. В. Лепин, *Криптографический алгоритм MV 2*, Минск, 2006.

41. А. А. Болотов и др., *Алгоритмические основы эллиптической криптографии*, М.: МЭИ, 2000.

42. Г. Л. Кацман, М. А. Цфасман, “Спектры алгеброгеометрических кодов” // *Проблемы передачи информации*, т. 23, № 4, с. 19 – 34, 1987.

43. И. Р. Шафаревич, *Основы алгебраической геометрии*, М.: Наука,1972.

44. В. Д. Гоппа, “Коды на алгебраических кривых”, Докл. АН СССР, т. 259, № 6, с. 1289 – 1290. 1981.

45. К. Шеннон, *Работы по теории информации и кибернетике*, М. ИЛ., 1963.

46. A. Rukhin, J. Soto. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. NIST Special Publication 800-22, 2000.

47. Программное средство криптографической защиты информации “Грифон-Б”. [Електронний ресурс], доступно : http://www.banksoft.com.ua/index.php?id=28. [Електронний ресурс], доступно :

48. Программное средство “Библиотека функций криптографической защиты информации “Грифон-Л”. [Електронний ресурс] , доступно: http://www.banksoft.com.ua/index.php?id=27. Дата звернення груд.1, 2017.

49. Решение по многофакторной аутентификации 2FA One [Електронний ресурс], доступно : https://habrahabr.ru/company/1cloud/blog/277901/. Дата звернення груд.1, 2017.

50. Digital Authentication Guideline. [Online]. Available: http://www.3dnews.ru/936742?from=related-grid&from-source=940476/. Accessed on December 1, 2017

51. Дистанционное банковское обслуживание клиентов: способы защиты транзакций. [Електронний ресурс] , доступно: http://www.prostobiz.ua/rko/stati/distantsionnoe_bankovskoe_obsluzhivanie_klientov_sposoby_zaschity_tranzaktsiy. Дата звернення груд.1, 2017.

52. Настройка двухфакторной аутентификации. [Електронний ресурс] , доступно: http://support.citrix.com/proddocs/topic/web-interface-impington/nl/ru/wi-configure-two-factor-authentication-gransden.html?locale=ru. Дата звернення груд.1, 2017.

53. Man In The Mobile Attacks Highlight Weaknesses In Out-Of-Band Authentication [Online] / Information week, 2010. – Available: http://www.darkreading.com/risk/man-in-the-mobile-attacks-highlight-weaknesses-in-out-of-band-authentication/d/d-id/1134495. Accessed on December 1, 2017.

54. Zeitz, C. Security issues of Internet-based biometric authentication systems: risks of Man-in-the-Middle and BioPhishing on the example of BioWebAuth [Online] / C. Zeitz, T. Scheidat, J. Dittmann, C. Vielhauer, E. G. Agulla, E. O. Muras, C. G. Mateo, J. L. Alba Castro // Security, Forensics, Steganography, and Watermarking of Multimedia Contents X, 2008. – 12 p. – Available at: http://spie.org/Publications/Proceedings/Paper/10.1117/12.767632, doi: 10.1117/12.767632

55. E. Barkan, E. Biham, N. Keller, Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication, *Journal of Cryptology*, vol. 21, Issue 3, pp. 392–429. 2008, doi: 10.1007/s00145-007-9001-y

56. Winterford, B. $45k stolen in phone porting scam [Online] / B. Winterford // ITnews, 2011. Available: http://www.itnews.com.au/News/282310,45k-stolen-in-phone-porting-scam.aspx/0. Accessed on December 1, 2017.

57. Schwartz, M. J. Zeus Banking Trojan Hits Android Phones [Online] / M. J. Schwartz // Information week, 2011. Available: http://www.informationweek.com/mobile/zeus-banking-trojan-hits-android-phones/d/d-id/1098909. Accessed on December 1, 2017.

58. Trojan Writers Target UK Banks With Botnets [Online] / TechWorld, 2010. Available: http://news.techworld.com/security/3228941/trojan-writers-target-uk-banks-with-botnets. Accessed on December 1, 2017.

59. Р. В. Грищук, Ю. Г. Даник *Основи кібернетичної безпеки: Монографія*; за заг. ред. Ю. Г. Данника, Житомир: ЖНАЕУ, 2016.

60. Кибербезопасность 2016–2017: От итогов к прогнозам. [Электронный ресурс], доступно: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Cybersecurity-2016-2017-rus.pdf. Дата звернення груд.1, 2017.

61. Rise of IoT Botnets Showcases Cybercriminals' Ability to Find New Avenues of Attack // [Online]. Available : http://storage.pardot.com/44731/127332/Cybercrime_Trends_Report___2016_Year_in_Review__1_.pdf. Accessed on December 1, 2017.

62. Исследование HP: Средний годовой ущерб от кибератак вырос до 15 млн долл. на организацию // [Электронный ресурс]., доступно : http://www.connect-wit.ru/issledovanie-hp-crednij-godovoj-ushherb-ot-kiberatak-vyros-do-15-mln-doll-na-organizatsiyu.html. Дата звернення груд.1, 2017.

63. CISCO: Кибератаки на индустриальные системы усиливаются, а доверие к имеющимся системам защиты падает // [Электронный ресурс], доступно : https://www.cisco.com/c/ru_ru/about/press/press-releases/2016/01-21a.html. Дата звернення груд.1, 2017.

64. Банк данных угроз безопасности информации [Электроний ресурс], доступно : http://bdu.fstec.ru/vul. Дата звернення груд.1, 2017.

65. Slyman, M. An evaluation of hypothetical attacks against the PassWindow authentication method [Online] / M. Slyman, S. O'Neil, G. H. Nicolae, B. van der Merwe The PassWindow method, 2009. Available: http://www.passwindow.com/evaluation_of_hypothetical_attacks_againag_passwindo.pdf. Accessed on December 1, 2017.

66. SHA-3 Derived Functions: cSHAKE, KMAC, TupleHash and ParallelHash // [Online]. Available: https://csrc.nist.gov/publications/.../800-185/sp800_185_draft.pdf. Accessed on December 1, 2017.

67. Guide for Cybersecurity Event Recovery, [Online]. Available: https://nvlpubs.nist.gov/nistpubs/.../NIST.SP.800-184.pdf. Accessed on December 1, 2017.

68. Security requirements for cryptographic modules, [Online]. Available: https://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf. Accessed on December 1, 2017.

69. Guide to LTE Security, [Online]. Available: https://csrc.nist.gov/publications/drafts/800-187/sp800_187_draft.pdf. Accessed on December 1, 2017.

70. Annex A: Approved Security Functions for FIPS PUB 140-2, [Online]. Available: https://csrc.nist.gov/publications/fips/fips140-2/fips1402annexa.pdf. Accessed on December 1, 2017.

71. Annex B: Approved Protection Profiles for FIPS PUB 140-2, [Online]. Available: https://csrc.nist.gov/publications/fips/fips140-2/fips1402annexb.pdf. Accessed on December 1, 2017.

72. Annex C: Approved Random Number Generators for FIPS PUB 140-2, [Online]. Available: https://csrc.nist.gov/publications/fips/fips140-2/fips1402annexc.pdf. Accessed on December 1, 2017.

73. Л. Шапиро. Аутентификация и одноразовые пароли. Часть 2. Внедрение OTP для аутентификации в AD. [Электронный ресурс], доступно: https://elibrary.ru/item.asp?id=20464277. Дата звернення груд.1, 2017.

74. С. Евсеев, "Синергетическая модель оценки безопасности банковской информации", *Науково-технічний журнал "Інформаційна безпека"*, № 4 (24), с. 104 – 118, 2016.

РОЗДІЛ 4
РОЗРОБЛЕННЯ ПІДХОДУ ОЦІНЮВАННЯ БАНКІВСЬКИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ З УРАХУВАННЯМ КОМПЛЕКСНОГО ПОКАЗНИКА ЕФЕКТИВНОСТІ ІНВЕСТИЦІЙ В ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ БАНКІВСЬКИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ

4.1. Розроблення методу оцінювання банківських інформаційних ресурсів з урахуванням комплексного показника ефективності інвестицій в забезпечення безпеки банківських інформаційних ресурсів в умовах дії гібридних загроз

4.1.1. Розроблення комплексного показника ефективності інвестицій в забезпечення безпеки банківських інформаційних ресурсів

Розвиток ОБС тісно пов’язаний з інтенсивним розвитком як інформаційних технологій комп’ютерної системи Інтернет, так і її інформаційних ресурсів.

ОБС належить до критично важливих інфраструктур, які мають ключове значення для громадського порядку, економічної стабільності і національної безпеки держав, її захист стосується питань національної безпеки і тому входить в компетенцію держави [1; 18]. Інформаційні технології АБС є невід’ємною частиною бізнес-процесів ОБС, в яких для забезпечення безперервної і безпечної обробки і циркуляції БІР використовується система захисту інформації на основі ТЗЗІ.

Приймаючи рішення про фінансування на створення і підтримання на всіх етапах життєвого циклу системи ЗІ ОБС прагнуть суттєво зменшити матеріальні збитки в процесі своєї діяльності. Витрати на забезпечення режиму безпеки БІР становить до 30% всіх витрат на інформаційну систему [2; 3; 4; 5; 6; 7; 20]. Однак лише 10% підприємств здійснюють ефективне інвестування в ІБ, 40% – піддаються безлічі ризиків порушення безпеки БІР.

Таким чином, проблема ефективного інвестування ІБ БІР в умовах стрімкого зростання кількості гібридних атак на елементи інфраструктури АБС залишається

не вирішеною. Це підтверджується аналізом опублікованих робіт та існуючих підходів [9; 12; 15; 16; 20].

Одним з основних питань ОБС є оцінка ефективності прийняття заходів для забезпечення всіх складових безпеки (ІБ, КБ, БІ) інформаційних активів БІР для отримання максимального прибутку. Оцінювання ефективності інвестицій в безпеку БІР на сьогодні є актуальною проблемою, тому що для оцінки інвестицій в безпеку підприємства (ОБС) необхідно співвідносити витрати на ІС і одержувані переваги від використання ТЗЗІ з точки зору фінансової та організаційної перспектив [3].

Аналіз останніх досліджень [4; 5; 6; 7; 9; 12; 16; 17; 20] показав, що в ринкових умовах будь-яке підприємство ОБС зосереджено на підтримці конкурентоспроможності.

Безперервний обіг інформаційного активу БІР, зв’язок між інформаційними ресурсами АБС, ефективне функціонування АБС, в яких вони обробляються, впливають на кінцеві фінансові показники комерційних банків України.

Прийнято вважати, що витрати на забезпечення безпеки БІР ОБС ефективні, якщо вони забезпечують виконання вимог державних нормативних документів і стандартів, НБУ, а також концепції ІБ комерційного або державного банку.

Таке розуміння пов’язане з тим, що для об’єктивної оцінки економічного ефекту ІБ немає універсальних методів. Відсутність обґрунтованих і загальноприйнятих методів оцінки інвестицій в безпеку БІР часто створює ситуацію суперечності між передбачуваними результатами, отриманими при впровадженні ТЗЗІ в АБС ОБС, і завданнями оптимізації витрат, що обмежують інвестиційні можливості ОБС.

Під *економічним ефектом* зазвичай розуміють перевищення вартісних оцінок кінцевих результатів відповідних заходів над сукупними витратами ресурсів на їх проведення за розрахунковий період [2; 7; 8; 20].

Складність оцінки ефективності заходів безпеки БІР ОБС обумовлена цілою низкою обставин. Відповідно до теорії оцінки ефективності систем, якість будь-якого об’єкта, в тому числі і СЗІ, проявляється лише в процесі його використання

за призначенням (цільове функціонування), тому об'єктивною є оцінка ефективності застосування [9; 12; 15]. Проведений аналіз методів оцінки ефективності інвестицій показав [2; 3; 4; 5; 6; 7; 8; 9; 12; 15; 20], що умовно вони поділяються на три групи: фінансові (традиційні, кількісні), якісні (евристичні) і ймовірного характеру (витратні). Загальна класифікація методів оцінки інвестицій наведена на рис. 4.1.

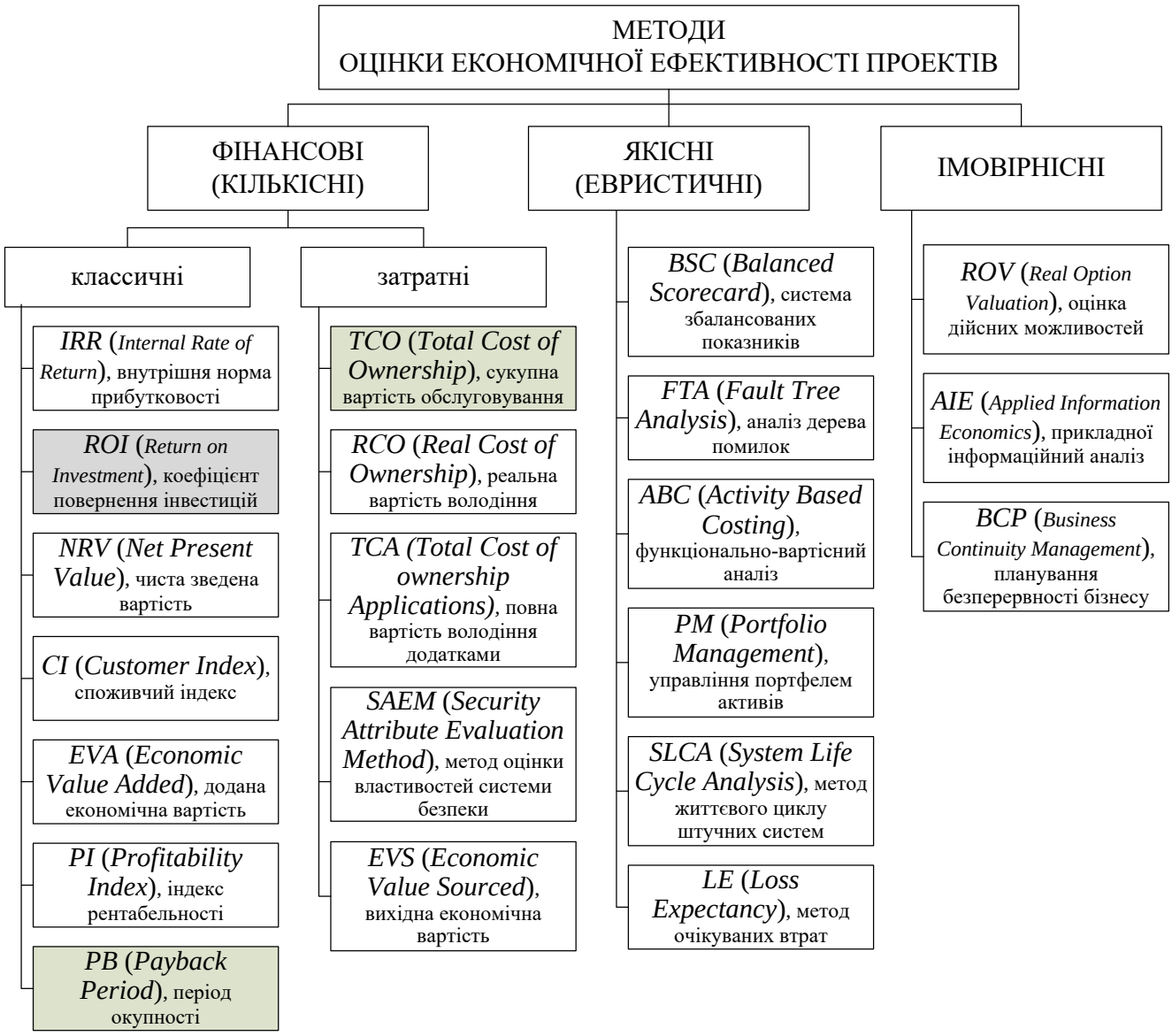


Рисунок 4.1 – Класифікація методів оцінки економічної ефективності проектів

Для оцінки економічної складової ефективності IT-проектів у світовій практиці найчастіше використовують основні показники *фінансової групи*: коефіцієнт рентабельності інвестицій (*ROI*), чиста зведена вартість (*NPV*), внутрішня норма рентабельності (*IRR*), період окупності (*Payback Period*),

економічна привабливість (*EVA*), збалансована система показників (*BSC*), сукупна вартість обслуговування (*TCO*) і т.п.

Однак при спробі оцінити чистий прибуток від реалізації проекту з безпеки БІР виникають суттєві труднощі, тому що методи спочатку призначені для аналізу фінансових інвестиційних інструментів, враховують переважно прямі витрати і їх прямі ефекти і просто не враховують у своїх математичних моделях важливі нефінансові параметри і ефекти при реалізації проекту безпеки. Ця група методів не дозволяє адекватно оцінити реальний економічний ефект реалізації проекту комплексу засобів захисту інформації (КСЗІ) [3; 6;12; 15; 19; 20].

Затратні методи оцінки (див. рис. 4.1) можна застосувати тільки в динаміці. При цьому відсутність статистичних даних в силу конфіденційності БІР, не дозволяє інвесторові провести обґрунтований розрахунок ризиків АБС.

Ця група методів передбачає порівняння оцінюваного проекту з уже реалізованими, при цьому методи фактично не можуть знайти широкого застосування в умовах жорсткої конкурентної середовища і з урахуванням діючих в компаніях ОБС режимів конфіденційності. Більше того, такий аналіз шляхом порівняння проекту КСЗІ – відповідно розкриття його складу – з проектами інших ОБС (конкурентів) і третіх осіб парадоксальний і суперечить основній меті самого проекту [5; 16; 18; 20].

Група евристичних методів пропонує комплексний підхід до оцінки, однак має свої недоліки при оцінці проектів КСЗІ ОБС. Так, метод збалансованої системи показників *BSC* (рис. 4.1) спрямований на розробку стратегії управління на основі стратегічних карт, і базується на групуванні (об’єднані) цілей та показників за категоріями: фінанси, клієнти, процеси, розвиток тощо. Однак застосування методу не передбачає створення стратегічного плану розвитку ОБС і не вимагає відмови від традиційних інструментів планування і контролю [7]. Метод *FTA* базується на двох пов’язаних припущеннях про те, що компоненти системи руйнуються випадковим чином відповідно з відомими ймовірностями руйнувань, і на найнижчому рівні дерева складові відмови незалежні один від одного. Основними недоліками методу є: невизначеність оцінок ймовірностей базисних подій, що

впливає на оцінку ймовірності виникнення кінцевої події; в деяких ситуаціях початкові події не пов'язані між собою, і часом важко встановити, чи враховані всі важливі шляхи до кінцевої події [4]. Методи *LE, PM, SLCA* засновані на порівнянні втрат від порушень політики безпеки, з якими може зіткнутися ОБС, і інвестиціями в безпеку ОБС. Методи спираються на результати аналізу експертних груп ОБС, на підставі яких будуються моделі "Як є" і "Як буде". Результати роботи експертної групи значною мірою суб'єктивні і не дають об'єктивної оцінки сформульованих ризиків. Ці недоліки характерні для всієї групи емпіричних методів оцінки.

Група імовірнісних методів оцінки (див. рис. 4.1) пропонує завчасне впровадження специфічних систем управління / менеджменту якістю (СМЯ) в компанії ОБС, вимагає значних витрат фінансових, трудових і часових ресурсів, спрямована не стільки на оцінку окремих проектів, скільки на загальне керівництво діяльністю підприємства ОБС і підходять тільки для дорогих тривалих проектів [5].

Крім того, розглянуті методи не враховують головне – БІР циркулює в умовах одночасної дії на систему загроз інформаційній безпеці, кібербезпеці та безпеці інформації. Тільки підхід який враховує гібридні загрози (їх синергію) на складові безпеки (ІБ, КБ, БІ) БІР дозволяє одержати повноцінну та адекватну оцінку рівня інвестування в безпеку БІР, що суттєво впливає на величину інвестицій в безпеку банківського сектору та відкриває шляхи до прийняття обґрунтованих управлінських рішень з питань забезпечення безпеки.

Таким чином, проведений аналіз методів оцінок ефективності інвестицій в безпеку ОБС показав, що формування об'єктивної оцінки ефективності інвестицій в безпеку БІР дуже трудомісткий процес, і, як правило, оцінка заходів безпеки в ОБС зводиться до знаходження категорій:

ROI, 'Return on Investment" – коефіцієнт повернення інвестицій;

TCO, "Total Cost of Ownership" – сукупна вартість обслуговування;

PB, "*Payback Period*" – період окупності.

Для оцінки безпеки банківських інформаційних ресурсів, з урахуванням комплексного показника ефективності інвестицій, які виділяються на забезпечення безпеки БІР скористаємося підходом, запропонованим в роботах [3; 12; 13].

Специфіка підходу ґрунтується на запропонованих математичній моделі синергетичної оцінки загроз і удосконаленій моделі зловмисника на основі синергетичного підходу, удосконаленого класифікатора загроз БІР [10; 11], і зводиться до розрахунку ризиків порушення безпеки БІР в умовах одночасної дії на систему загроз інформаційній безпеці, кібербезпеці та безпеці інформації. Такий підхід дозволяє оцінити безперервність функціонування бізнес-процесів (інформаційних процесів) в АБС і коефіцієнта внутрішньої норми рентабельності інвестицій.

Розгляд безпеки БІР як інформаційного процесу, а не продукту, дає можливість інтерпретувати безпеку інформаційних активів як багатофункціональний процес управління ризиками порушення режиму безпеки ОБС. У результаті управління ризиками можна досягти балансу інформаційних ризиків для діяльності ОБС, знижуючи потенційні гібридні загрози на складові безпеки (ІБ, КБ, БІ), спрямовані на обчислювальні засоби, що обробляють інформаційні ресурси. Результатами балансу ризиків інформаційних активів БІР є вибір ефективного методу управління, який дозволяє максимально точно визначити параметри безпеки БІР, і отримати максимальний прибуток від вкладених коштів на побудову КСЗІ в АБС [13].

Формальний опис моделі оцінювання безпеки банківських інформаційних ресурсів, яка враховує комплексний показник ефективності інвестицій, що виділяються на забезпечення безпеки БІР в умовах дії гібридних загроз можна записати так [3; 10; 11; 12; 13; 14; 19]:

$$W_{ABS}^{effinv} = \begin{Bmatrix} I_{O^{ABS}}, \Delta^{ABS}, \left\{DF^{ABS}\right\}, rang^{ABS}, \left\{SZ^{ABS}\right\}, d^{ABS}, D^{ABS} \\ ROI^{ABS}, NPV^{ABS}, ROSI^{ABS}, r^{ABS}, CV^{ABS}, OU^{ABS} \end{Bmatrix}, \quad (4.1)$$

де $I_{O^{ABS}}$ – значення інформаційного активу;

Δ^{ABS} – ознака ефективності витрат;

$\left\{DF^{ABS}\right\}$ – множина джерел загроз на складові безпеці: ІБ, КБ, БІ БІР [10];

$rang^{ABS}$ – ранг процесу розробки ТЗЗІ (СЗІ) – витрати на розробку ТЗЗІ;

$\left\{SZ^{ABS}\right\}$ – множина ТЗЗІ (СЗІ) [10];

d^{ABS} – зведена вартість грошового потоку;

ROI^{ABS} – коефіцієнт повернення інвестицій;

NPV^{ABS} – чиста зведена вартість;

$ROSI^{ABS}$ – рентабельність інвестицій в ТЗЗІ (СЗІ);

r^{ABS} – коефіцієнт рентабельності в безпеку БІР;

CV^{ABS} – ступінь ризику в одиницю середнього доходу;

D^{ABS} – дохід від використання ТЗЗІ (СЗІ);

OU^{ABS} – оцінка доходу від використання ТЗЗІ (СЗІ).

Значимість інформаційного активу БІР оцінимо за виразом:

$$I_{O^{ABS}} = \frac{E_{BIn}^{ABS}}{Y_{BIn}^{ABS}}, \tag{4.2}$$

де E_{BIn}^{ABS} – вартість інформаційного ресурсу АБС;

Y_{BIn}^{ABS} – капітал, вкладений в експлуатацію цього БІР.

Ознаку ефективності витрат Δ^{ABS} оцінимо за таким виразом:

$$\Delta^{ABS} = \frac{e}{b}, \tag{4.3}$$

де e – очікуваний економічний ефект;

b – витрати на розробку ТЗЗІ (СЗІ).

Якщо комерційний банк ОБС розглядає доцільність реалізації того чи іншого проекту, то, в простішому випадку він може розрахувати чисту зведену вартість NPV^{ABS} прибутку і витрат, які принесе проект і порівняти їх. Іншими словами, прибуток від інвестицій повинен перевищувати витрати, а рівень прибутковості ОБС встановлює самостійно [3].

$$ROI^{ABS} = NPV_{inv}^{ABS} - NPV_{zt}^{ABS}, \tag{4.4}$$

де NPV_{inv}^{ABS} – прибуток від інвестицій в ТЗЗІ (СЗІ) АБС;

NPV_{zt}^{ABS} – витрати в ТЗЗІ (СЗІ) АБС;

ROI^{ABS} – прибутковість інвестицій в ТЗЗІ (СЗІ) АБС.

Такий же підхід застосуємо для оцінки доцільності інвестування в безпеку БІР. Основна відмінність – інвестиції в безпеку БІР не приносять прибуток, а лише гіпотетично запобігають витратам. Таким чином, ТЗЗІ АБС ОБС повинні запобігти витратам на більшу суму, ніж кошти, витрачені на їх розробку і впровадження в ТЗЗІ (СЗІ) АБС, що і буде свідчити про рентабельність інвестицій в ТЗЗІ ($ROSI^{ABS}$) [3; 15]:

$$ROSI^{ABS} = NPV^{ABS}_{zbtszi} - NPV^{ABS}_{zvtszi}, \tag{4.5}$$

де NPV^{ABS}_{zbtszi} – витрати на усунення компрометації безпеки без впроваджених ТЗЗІ (СЗІ);

NPV^{ABS}_{zvtszi} – витрати на усунення компрометації безпеки з впровадженими ТЗЗІ (СЗІ).

При цьому чиста зведена вартість NPV^{ABS} розраховується за виразом:

$$NPV^{ABS}_{zbtszi} = \sum_{i=1}^{N} \frac{ALE_i}{(1+r)^i},\ NPV^{ABS}_{zvtszi} = C_{sz} + \sum_{i=1}^{N} \frac{ALE_i}{(1+r)^i}, \tag{4.6}$$

де N – кількість інтервалів інвестування;

ALE_i – очікувані втрати в i-му періоді;

r – ставка дисконтування;

C_{sz} – вартість засобів захисту.

Для отримання синергетичного ефекту підвищення рівня захищеності БІР в АБС в умовах протидії гібридним загрозам на складові безпеки (ІБ, КБ, БІ) необхідно враховувати комплексування загроз:

$$DF^{ABS} = \{V^{NS}\} \cup \{V^{AS}\}, \tag{4.7}$$

де $\{V^{AS}\} = \{V^{ASBI}\} \cap \{V^{ASIB}\} \cap \{V^{ASKBr}\}$, в яких V^{NS} – клас природних джерел загроз; $V^{AS} = \{V^{ASIB}, V^{ASBI}, V^{ASKBr}\}$ – клас антропогенних загроз, де V^{ASIB} – множина загроз інформаційній безпеці; V^{ASBI} – множина загроз безпеці інформації; V^{ASKB} – множина загроз кібербезпеці. Кожен елемент з множини загроз $DF_i \in \{DF^{ABS}\}$, може бути представлений таким вектором значень. DF_i *(p,u,risk)*, де p – ймовірність реалізації

загрози; *u* – потенційний збиток; *risk* – ризик, виражений в якісній формі, що набуває один з двох станів T_{risk}={допустимий, недопустимий }={α_{r1},α_{r2}}.

При оцінці ризику БІР застосуємо методику розрахунку *Annual loss expectancy – ALE*, тобто очікуваних втрат в кожен період оцінки:

$$ALE^{ABS} = \sum_{i=1}^{n} I\left(O_{DF}^{ABS}\right)F_i, \tag{4.8}$$

де $\left\{O_{DF}^{ABS}\right\}$ – множина загроз;

$I\left(O_{DF}^{ABS}\right)$ – вартісні наслідки реалізації загрози;

ALE^{ABS} – очікуваний збиток від реалізації;

F_i – частота (можливість) реалізації загрози.

Витрати на розробку ТЗЗІ (СЗІ) АБС ОБС визначаються *рангом*. Оцінка рангу розробки ТЗЗІ (СЗІ) АБС ОБС $rang^{ABS}$ здійснюється за виразом:

$$rang^{ABS} = \frac{SUM \times p}{s_{OPZ}^{ABS}}, \tag{4.9}$$

де *SUM* – очікуваний прибуток від впровадження ТЗЗІ (СЗІ) в АБС ОБС;

p – ймовірність успіху використання ТЗЗІ (СЗІ);

s_{OPZ}^{ABS} – витрати на розробку, впровадження та підтримки рівня захищеності ТЗЗІ (СЗІ).

Наведена вартість грошового потоку d^{ABS} оцінюється за виразом:

$$d^{ABS} = D_r + ROI^{ABS}, \tag{4.10}$$

де D_r – коефіцієнт дисконтування;

ROI^{ABS} – прибутковість інвестицій в ТЗЗІ (СЗІ) АБС.

Коефіцієнт рентабельності інвестицій в безпеку БІР r^{ABS} обчислюється за виразом:

$$r^{ABS} = \sum_{t=1}^{T} \frac{CF_t}{\left(1 + ROSI^{ABS}\right)^t}, \tag{4.11}$$

де *t* – початок часового періоду;

CF_t – грошовий потік в період часу *t*;

$ROSI^{ABS}$ – дохід від реалізації проекту;

T – кінець часового періоду.

Оцінку ступеня ризику на одиницю середнього прибутку CV^{ABS} отримаємо, використовуючи вираз:

$$CV^{ABS} = \frac{\sigma(E)}{\mu(E)}, \tag{4.12}$$

де $\sigma(E)$ – середньоквадратичне відхилення витрат на реалізацію ТЗЗІ (СЗІ) ОБС;

$\mu(E)$ – математичне сподівання на реалізацію ТЗЗІ (СЗІ) ОБС.

Прибуток D^{ABS} від використання ТЗЗІ (СЗІ) оцінимо за виразом:

$$D^{ABS} = Cost_1 P_D - Cost_2 (1 - P_D), \tag{4.13}$$

де P_D – ймовірність отримання доходу;

$(1 - P_D)$ – ймовірність отримання збитків;

$Cost_1, Cost_2$ – одиниці вартості інформаційного активу.

Запропонована модель базується на оцінці безпеки БІР, яка враховує комплексний показник ефективності інвестицій, що виділяються на забезпечення безпеки банківських інформаційних ресурсів і дисконтуванні майбутніх грошових надходжень і витрат. Таким чином, ця модель враховує зміну інвестицій в безпеку БІР ОБС з плином часу.

Характеристикою зміни інвестиційного потоку є його *інтенсивність l(t)* – середня кількість змін, що відбуваються в потоці за одиницю часу [13]. Інтенсивність дозволяє оцінити інтервали часу $\Delta t_{[i-q]}$ між змінами, що відбулися в потоці, використовуючи вираз [13; 15; 19]:

$$\Delta t_{[i-q]}(t) = \frac{K}{l(t)}, \tag{4.14}$$

де *K* – сумарна кількість змін інвестицій;

l(t) – інтенсивність інвестиційного потоку;

$i, q \in [1; n]$ – порядкові номери змін; $i \geq q$.

Зміни процесів інвестування в безпеку БІР ОБС описуються у вигляді кінцевого автомата H^{ABS}, стани якого описує вираз [13; 15; 19]:

$$H^{ABS} = \left\langle S_j^I, value, \Pi, S_0^I \right\rangle, \tag{4.15}$$

де S_j^I – кінцевий стан інвестицій;

$value$ – значення змін інвестицій;

Π – функція переходів інвестицій зі стану *k* в стан *j*;

S_0^I – початковий стан інвестицій.

Функція переходів інвестицій Π зі стану *k* в стан *j* оцінюється за виразом:

$$\Pi = S_k^I \times value \to S_{k+1}^I \times value \to \ldots \to S_j^I . \tag{4.16}$$

Оцінку потенційних збитків U^{ABS} інформаційного активу отримаємо з виразу:

$$U^{ABS} = p_{rj} u_j , \tag{4.17}$$

де p_{rj} – ймовірність реалізації хоча б однієї загрози *j*-му активу;

u_j – цінність *j*-го активу.

Розрахунок ймовірності реалізації хоча б однієї загрози для кожного активу виконується за виразом:

$$p_{rj} = 1 - \prod_{i=1}^{m} \left(1 - pr_{ij}\right), \tag{4.18}$$

Таким чином, оцінка загального очікуваного збитку OU^{ABS} складається з потенційних збитків і визначається за виразом:

$$OU^{ABS} = \sum_{j=1}^{n} U^{ABS} . \tag{4.19}$$

Отримана оцінка дозволяє врахувати синергізм і гібридність сучасних загроз на складові безпеки І(Б, КБ, БІ) БІР, забезпечити якісні і кількісні показники інвестування в безпеку БІР: ROI^{ABS} (коефіцієнт повернення інвестицій), NPV^{ABS} (чисту зведену вартість), $ROSI^{ABS}$ (рентабельність інвестицій в ТЗЗІ (СЗІ). Такий підхід дозволяє динамічно і своєчасно оцінювати безпеку БІР з урахуванням

рентабельності інвестування, що забезпечує підвищення рівня безпеки БІР в цілому.

Для забезпечення процесу оптимізації інвестування на основі експертної оцінки визначаються параметри інтегрального критерію оцінки ефективності інвестицій в безпеку БІР ОБС.

Кожному параметру присвоюються вагові категорії за правилом Фішберна [14], заснованому на тому, що зміна вагових коефіцієнтів критеріїв підпорядковується спадній арифметичній прогресії. При цьому перший критерій (i = 1), розташований першим в строго впорядкованому за важливістю ранжируваному ряду критеріїв i = 1, 2, ..., n, є найбільш важливим і має найбільший ваговий коефіцієнт. Це правило задається виразом:

$$w_i = \frac{2(N - n + 1)}{N(N + 1)}, \tag{4.20}$$

де w_i – ваговий коефіцієнт Фішберна для критерію оцінки ефективності інвестицій в безпеку БІР ОБС;

N – загальна кількість параметрів інтегрального критерію оцінки ефективності інвестицій в безпеку БІР ОБС;

n – порядковий номер параметра, i кількість параметрів в інтегральному критерії оцінки.

Згідно з формулою Фішберна маємо:

$$w_1 = \frac{2 \times N}{N(N + 1)},\ w_N = \frac{2}{N(N + 1)},\ \gamma = \frac{w_1}{w_N} = N, \tag{4.21}$$

де γ – кратність відмінності вагових коефіцієнтів один від одного.

Таким чином, формуємо систему вагових коефіцієнтів Фішберна W_{Φ}^{ABS}, з умовами:

$$w_i \in [0;1],\ W_{\Phi}^{ABS} = \sum_{i=1}^{N} w_i, \tag{4.22}$$

де $i \in [1; N]$.

Як оптимізаційні заходи в роботах [12; 13; 15; 19] пропонується використовувати оцінку сукупної вартості витрат на ліквідацію наслідків реалізації загрози та інших причин виведення з ладу ТЗЗІ і сумарні виплати джерел фінансування.

Оцінка сукупної вартості витрат M^{ABS} ліквідації наслідків реалізації загрози та інших причин виведення з ладу ТЗЗІ здійснюється за виразом:

$$M^{ABS} = \sum_{i=1}^{m} C_i , \tag{4.23}$$

де C_i – вартість *i*-ї міри;

m – загальна кількість вжитих заходів.

Оцінка сумарних виплат c_i джерел фінансування формується за формулою:

$$c_i = \sum_{i=1}^{n} A_{i,j} , \tag{4.24}$$

де c_i – сумарні виплати *j*-му джерелу фінансування;

$A_{i,j}$ – виплати *j*-му джерелу фінансування;

$i, j = 1 \ldots n$; n – кількість джерел фінансування.

Запропонована модель оцінювання безпеки БІР, яка враховує комплексний показник ефективності інвестицій, які виділяються на забезпечення безпеки БІР дозволяє забезпечити підвищення ефективності інвестицій шляхом мінімізації витрат на безпеку БІР ОБС в умовах протидії гібридних загроз.

Мінімізація витрат на безпеку БІР ОБС проводиться оптимізаційним процесом, який можна записати у вигляді такого виразу:

$$\min\left(E_1^{ABS} b_1 + E_2^{ABS} b_2 + \ldots + E_j^{ABS} b_n\right), \tag{4.25}$$

де E_j^{ABS} – *j*-й критерій оптимізації, $j = 1 \ldots n$, n – кількість критеріїв;

b_n – ознака використання *j*-го джерела фінансування,

$$b_n = \begin{cases} 1, \text{якщо джерело фінансування} \\ \text{використано}, \\ 0, \text{якщо джерело фінансування} \\ \text{не використано} \end{cases}. \quad (4.26)$$

У рамках запропонованої моделі оцінки БІР з урахуванням комплексного показника ефективності інвестицій в безпеку БІР ОБС оцінюються такі параметри – сукупна вартість витрат ліквідації наслідків реалізації загрози чи інші причини виведення з ладу систем захисту інформації і сумарні виплати джерел фінансування для того, щоб визначити допустимі рівні ризиків порушення безпеки БІР ОБС. При цьому забезпечується мінімізація збитку, а витрати на безпеку БІР ОБС є ефективними, тому що прибуток, отриманий від впровадження СЗІ, більше ніж вкладений капітал [13; 15; 19].

Узагальнивши параметри, які використовуються в рамках запропонованої моделі, визначимо інтегральний критерій ефективності інвестицій в безпеку БІР ОБС, використовуючи вираз:

$$W_{ABS}^{effinv} = \sum_{i=1}^{N} w_i M^{ABS}. \quad \ldots(4.27)$$

Таким чином, модель ефективності інвестицій в безпеку БІР ОБС може знаходиться в різних станах S^{ABS}, які можна описати у вигляді такої множини:

$$S^{ABS} = \left\{ S_1^{ABS}, S_2^{ABS}, ..., S_m^{ABS} \right\}, \quad (4.28)$$

де S^{ABS} – множина можливих станів моделі;

S_1^{ABS} – початковий стан моделі;

S_m^{ABS} – кінцевий стан моделі.

Таким чином, запропонований метод на відміну від відомих дозволяє оптимізувати витрати коштів на побудову системи безпеки БІР в умовах впливу гібридних загроз при одночасному забезпеченні заданого рівня їх безпеки.

Для оцінювання якості обслуговування об’єктів АБС щодо забезпечення безпеки БІР запропонована методика оцінки функціональної ефективності обміну даними в мережі АБС, що ґрунтується на простому багатофакторному аналізі, у ній враховуються як технічні показники мережі (швидкість передачі даних, імовірність і час доставки пакета і ін.), показники безпеки технічних засобів захисту інформації, так і економічні параметри (вартість масштабування, обслуговування мережі, ефективність інвестицій в безпеку і т.п.).

4.1.2. Розроблення методики оцінювання стійкості криптосистем експрес-методом на основі ентропійного методу оцінки випадковості вихідної послідовності

Для порівняльної оцінки ефективності (криптостійкості) симетричних криптоалгоритмів, як правило, використовують методи лінійного і диференціального криптоаналізу, основні етапи та їх ефективність розглянуті в роботі [23]. Проведений аналіз свідчить, що і диференціальний, і лінійний аналіз повних шифрів вимагає залучення експертів, значних економічних, обчислювальних та людських затрат. Запропонована і розроблена в роботах [24; 25; 26; 27; 28; 29; 30; 31; 32; 33] нова методологія оцінки стійкості блоково-симетричних шифрів до атак диференціального та лінійного криптоаналізу побудована на встановленому факті, що всі сучасні блочні шифри після декількох початкових циклів шифрування набувають властивості випадкових підстановок відповідного ступеня [28; 30].

Основою розроблюваного підходу є положення, згідно з яким більші шифри повторюють властивості своїх зменшених моделей. У роботах [25; 26; 27; 28; 29; 30; 31; 32; 33] було показано, що більші версії шифрів при їх використанні в режимі шифрування скорочених (16-бітов та 32-бітов) блоків даних повторюють закони розподілу ймовірностей переходів *XOR*-таблиць і таблиць зсувів лінійних апроксимацій, властивих відповідним законам розподілення ймовірностей своїх зменшених версій. Останні, в свою чергу, після декількох початкових циклів шифрування приходять до законів розподілу ймовірностей переходів *XOR* таблиць і зсувів таблиць апроксимацій випадкових підстановок [28; 30].

Порівняння механізмів безпеки на алгоритмах традиційної криптографії, криптографії з відкритим ключем, гібридних криптосистем можливе на підставі комплексного показника, що враховує критерії криптостійкості, швидкодії криптоперетворень, прозорості процедур шифрування для користувача, розподіл ключових послідовностей, інвестицій в ІБ, що не дозволяє без значних часових і економічних витрат визначити їх ефективність. На рис. 4.2 наведена запропонована ідеологія.

Рисунок 4.2 – Запропонована ідеологія кафедри БІТ ХНУРЕ

Подібні дослідження міні-версій проводилися і зарубіжними авторами. Так, в роботах F.-X. Standaert з колегами [34; 35] досліджувалася різниця між теоретичною та практичною стійкістю шифрів, введеної Л. Кнудсеном [36], причому була підтверджена її істотна залежність від розміру блоку. Перевірка гіпотези еквівалентності ключів на міні-версіях *AES* показала, що її необхідно проводити на повнорозмірних ключах, для яких даний шифр і був спроектований.

Отримані результати в роботі [23] спрощених версій БСШ для оцінки доказової безпеки повномасштабних моделей шифрів до атак диференціального і лінійного криптоаналізу на основі збільшення розміру входу в шифр підтверджують можливість їх використання. Адекватність результатів оцінки властивостей спрощеної моделі БСШ залежить від вибору коефіцієнта масштабування, який визначає властивості своїх прототипів повних шифрів.

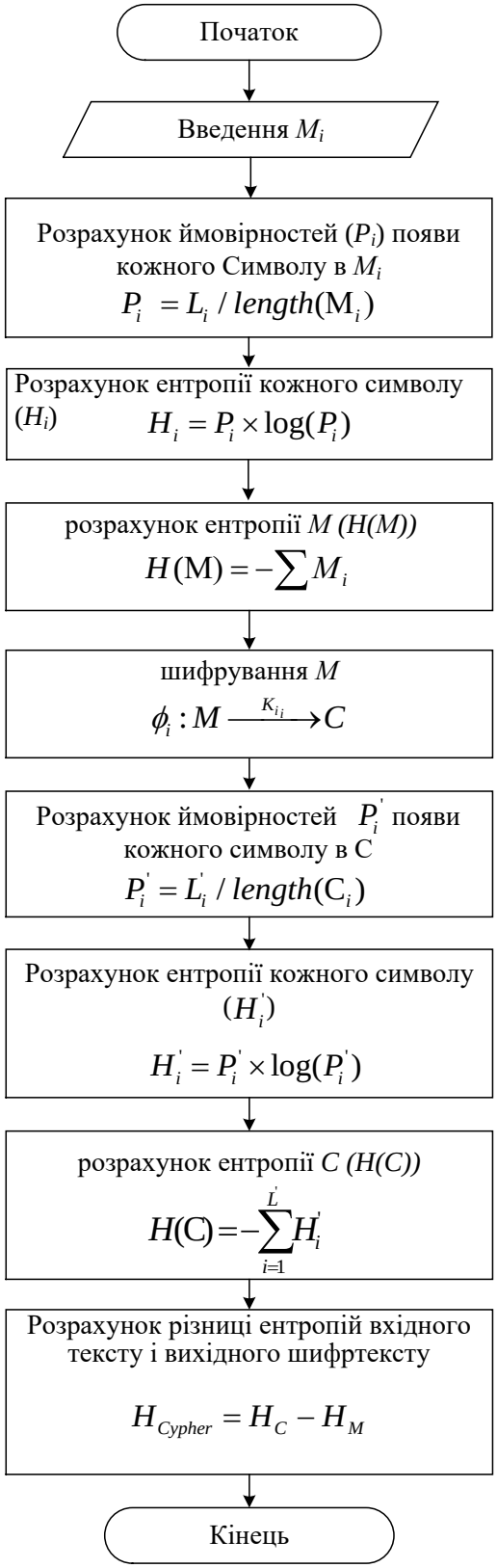
Вибір значення коефіцієнта повинен бути пропорційний максимальному ресурсу розрахункових засобів, використовуваних для проведення досліджень. Для кожного блочного симетричного шифру (з числа відомих ітеративних БСШ) існує цілком визначена кількість циклів, після якого шифр набуває властивостей випадкової послідовності. Подальше нарощування кількості циклів не впливає на підсумкові диференціальні та лінійні властивості шифру, що дає можливість “скоротити” кількість ітерацій і збільшити швидкість криптоперетворень.

Разом з тим, для збереження всіх властивостей прототипів в спрощених моделях необхідною умовою їх адекватності є використання *mini-S-box*-ів з основними показниками ефективності нелінійних вузлів замін (збалансованість, нелінійність, автокореляція) на рівні даних показників повномасштабних шифрів.

Таким чином, для вибору того чи іншого алгоритму БСШ достатньо оцінити його вихідну послідовність на випадковість.

Для оцінки стійкості криптоалгоритмів різних моделей криптосистем пропонується використовувати експрес-аналіз на основі ентропійного методу, використовуваного в пакеті статистичних досліджень випадкової величини *NIST STS* 822 [37]. Запропонований експрес-аналіз дозволяє без значних обчислювальних, економічних та людських витрат на інтуїтивному рівні порівняти не тільки стійкість різних криптоалгоритмів (криптосистем), але і їх програмну реалізацію.

Алгоритм ентропійного методу оцінки криптостійкості наведено на рис. 4.3. У табл. 4.1 наведені результати досліджень стійкості і програмної ефективності реалізації блокових і потокових шифрів різної складності.



Розрахунок ентропії вихідного повідомлення визначеної довжини

M_i – вихідне повідомлення,
P_i – ймовірність появи i-го символу в M_i,
L_i – кількість i-х символів в M_i,
H_i – ентропія i-го символу,
$H(M)$ – ентропія M

Розрахунок ентропії шифрованого повідомлення визначеної довжини

C – криптограма,

P_i' – Ймовірність появи i-го символу в C,

$H(C)$ – ентропія C,

L_i' – кількість i-х символів в C,

H_i' – ентропія i-го символу в криптограмі.

Рисунок 4.3 – Алгоритм тестування криптосистеми на стійкість на основі ентропійного методу оцінки випадковості

Для проведення досліджень використовувалися БСШ: *DES*, 3*DES*, ГОСТ-28147-2009, Калина-256, *AES*-256. Для реалізації потокового шифру використовувалися генератори псевдовипадкової послідовності двох різних типів: на правилі “60” клітинних автоматів в його класичному вигляді без модифікацій і криптографично стійкий генератор *SecureRandom* з криптобібліотеки *Java*, який позиціонується як придатний для криптографічних застосувань; для оцінки несиметричного криптоалгоритму використовувався алгоритм *RSA*.

Таблиця 4.1 – Результати досліджень стійкості криптоалгоритмом експрес-методом

№	Шифр	Ентропія вхідного тексту	Ентропія криптограми	різниця між ентропіями	% ентропії, який додається шифром
1	Клітинні автомати, правило “60”	0,5023775 (5,023775)	0,6820179 (6,820179)	0,1796404 (1,796404)	35,7580505
2	Криптостійкий генератор *SecureRandom* з *Java*	0,5023767 (5,023767)	0,7999982 (7,999982)	0,2976215 (2,976215)	59,2426958
3	*DES*	0,469276	0,812043	0,342767	73,0416642
4	*3DES*	0,469276	0,812043	0,342767	73,0416642
5	ГОСТ 28147-2009	0,469276	0,811348	0,342072	72,8935637
6	Калина-256	0,469276	0,954519	0,485243	103,4024753
7	*AES*-256	0,469276	0,95454	0,485264	103,4069503
8	*RSA*	0,469276	1	0,530724	113,094213214

У табл. 4.1 підраховувалася ентропія вхідного і зашифрованого тексту, різниця, а також відсоток ентропії, що додається до ентропії відкритого тексту самим шифром. Аналіз табл. 4.1 дає можливість оцінити внесок самого шифру в підсумкову ентропію зашифрованого повідомлення. Оскільки всі вони тестувалися в однакових умовах, можна судити про їх відносні показники.

У цьому сенсі варто відзначити *AES*-подібні шифри (*SPN*-системи, підстановочно-переставні схеми). Обидва таких шифру, і Калина-256, і *AES*-256

внесли найбільший вклад, понад 103% в ентропію відкритого тексту. Таким чином, обидва шифри володіють найкращим розсіюванням. Приблизно однакові показники продемонстрував блоково-симетричний шифр ГОСТ-28147-2009 – 72,89% проти 73,04% у *DES* / 3*DES*. Ймовірно, це тільки підтверджує висновки про максимально можливу міру розсіювання, як характеристику архітектури БСШ.

Для порівняння було проведено експерименти з використанням потокових шифрів на основі двох різних генераторів псевдовипадкової ключової послідовності. Шифрування проводилося за правилом додавання за “модулем два”.

У першому випадку – це генератор на основі клітинних автоматів (правило “60”). Це не криптостійкий генератор, послідовність якого не проходить тестування NIST STS 822, а другий позиціонується як криптостійкий генератор *SecureRandom* з криптобібліотеки *Java*. В обох випадках отримані значення ентропії, набагато менші, ніж у класичних БСШ, що не дозволяє говорити про якісне шифруванні з їх допомогою.

Алгоритм несиметричної криптографії забезпечує найвищий досліджений показник понад 113% в ентропію відкритого тексту, що підтверджує його доказову криптостійкість.

Таким чином, наведені результати дозволяють стверджувати, що простий експрес-метод на основі ентропійного методу оцінювання випадковості криптограми дає можливість експрес-оцінки якості використовуваних шифрів без залучення експертних оцінок, великих економічних, обчислювальних та людських затрат. Така експрес-методика доступна будь-якому користувачеві, що має мінімальні знання з теорії інформації. Більше того, таким чином можна оцінювати різні реалізації шифрів, що дозволить вибрати найкращу (оптимальну) програмну реалізацію, яка підходить для умов і вимог користувача. Наприклад, комп’ютерних експериментах використані дві реалізації алгоритму *DES*. Одна з них, показана в табл. 4.1 під номером 3, демонструвала приріст ентропії після шифрування в 73,04% від вхідного тексту, інша – 64,4%.

Природно, для практичних цілей має сенс вибрати першу реалізацію, оскільки, очевидно, що її характеристики розсіювання кращі. Таким чином,

експрес-аналіз дозволяє оцінити якість реалізації класичних (та інших) криптоалгоритмів з метою вибору оптимальної криптобібліотеки з множини існуючих на ринку.

Розглянемо отримані результати з точки зору максимального криптографічного захисту інформації. Показником такого захисту буде ентропія зашифрованого виконуваного файлу, що наведено в табл. 4.2.

Таблиця 4.2 – Оцінка максимального криптографічного захисту інформації

№	Шифр	Ентропія вхідного тексту	Ентропія криптограми	Ймовірність крипто-захисту, P_c
1	Клітинні автомати, правило “60”	0,469276	0,637079949	0,637079949
2	Криптостійкий генератор *SecureRandom* з *Java*	0,469276	0,747287753	0,747287753
3	*DES*	0,469276	0,812043	0,812043
4	*3DES*	0,469276	0,812043	0,812043
5	ГОСТ 28147-2009	0,469276	0,811348	0,811348
6	Калина	0,469276	0,954519	0,954519
7	*AES*-256	0,469276	0,95454	0,95454
8	*RSA*	0,469276	1,000	1,000
9	Ідеальний шифр		1,000	1,000

Відомо, що максимально можливий криптографічний захист дає так званий “Ідеальний шифр” за Шеноном, який в результаті шифрування дає випадкове число [38]. Такий файл матиме максимальну ентропію, яка в бінарному випадку дорівнює одиниці. Будемо вважати, що шифрування таким шифром дасть максимальний криптографічний захист, і приймемо її за 1. Ймовірність захисту таким шифром дорівнює одиниці. Природно, неідеальні шифри не дають такої ймовірності криптографічного захисту.

На рис. 4.4 наведені результати досліджень усередненої ентропії криптограм різних БСШ осмисленого відкритого тексту довжиною $M = 10^8$ біт, з інтервалом $N = 5 \times 10^6$ біт.

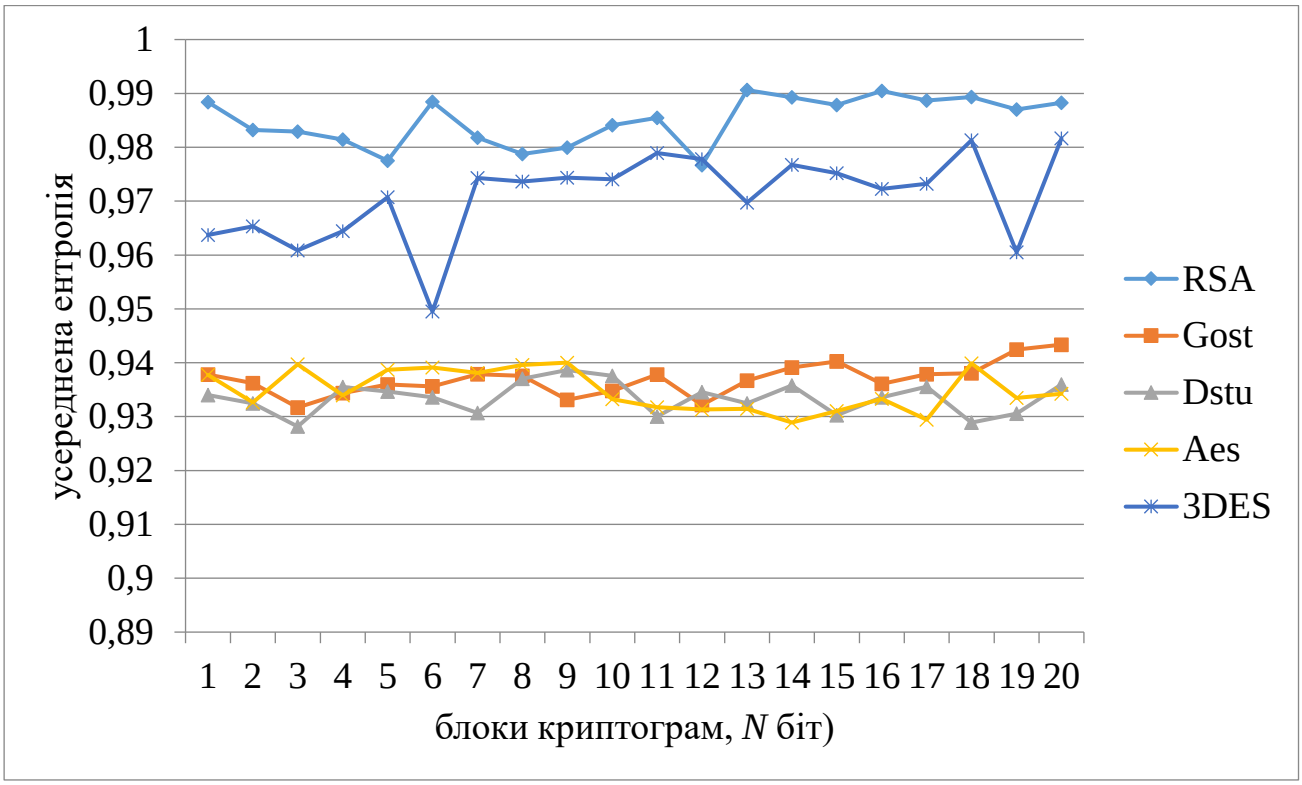


Рисунок 4.4 – Результати досліджень усередненої ентропії блоків криптограм

Аналіз рис. 4.4 практично підтверджує можливість використання експрес-методу щодо вибору програмного забезпечення механізмів безпеки на основі криптоалгоритмів.

Таким чином, запропонована методика оцінювання стійкості криптоалгоритмів дає можливість ранжувати всі досліджені шифри через ймовірність криптографічного захисту. Цей показник можна використовувати для різних методик оцінки захищеності комплексних систем захисту різних комп'ютерних мереж (АБС ОБС), що свідчить про його універсальність.

4.2. Розроблення комплексного показника оцінювання функціональної ефективності передачі банківської інформаційних ресурсів

Технології віддаленого доступу і відкриті ресурси мережі Інтернет, які використовуються в АБС ОБС, дозволяють істотно розширити спектр фінансових

послуг через Інтернет-банкінг та *Web*-ресурси АБС. Для забезпечення складових безпеки (ІБ, КБ, БІ) БІР, як правило, використовуються сертифіковані НБУ стандартизовані криптографічні механізми на основі процедур симетричної і несиметричної криптографії. Проведений аналіз стандартів в роботі [39] показав, що ключовим моментом принципів управління ІБ є оцінювання ризиків. Фактично ризик являє собою інтегральну оцінку того, наскільки ефективно наявні засоби захисту здатні протистояти інформаційним атакам. Практика показує, що сьогодні можна чітко виділити дві основні групи методів оцінювання ризиків безпеки [39; 40; 41].

Перша група методів дозволяє встановити рівень ризику шляхом оцінювання ступеня відповідності визначеному набору вимог щодо забезпечення інформаційної безпеки. Друга група методів оцінювання ризиків ІБ базується на визначенні ймовірності реалізації атак, а також рівнів їх збитку. У такому разі значення ризику обчислюється окремо для кожної загрози і в загальному випадку є добутком імовірності реалізації загрози на величину потенційних збитків від цієї загрози. Значення збитку визначається власником інформації, а ймовірність реалізації загрози обчислюється групою експертів, які проводять процедуру аудиту. У табл. 4.3, 4.4 наведені результати досліджень основних методик оцінки ризиків, які використовуються в ОБС.

Таблиця 4.3 – Методики оцінки ризиків

Методика оцінки	Переваги	Недоліки	Підходи
NIST	- Детальний опис можливих ризиків інформаційних активів - Для підприємств різного розміру	- Довготривалий процес аналізу - Деякі функції не автоматизовано	Евристичний
FAIR	- Комплексний аналіз - Симуляційна модель - Висока ефективність	- Для крупних банків та підприємств	Ймовірнісний

Продовження таблиці 4.3

Методика оцінки	Переваги	Недоліки	Підходи
IT-Grundshutz	- Гнучкість методу надає змогу проводити аналіз для будь-якої організації - Налаштовується на нові або існуючі активи	- Потребує теоретичної обізнаності процесу аналізу ризиків - Висока вартість ліцензії	Евристичний
OCTAVE	- Швидке впровадження - Обслуговує малі та середні за розміром підприємства	- Відсутність автоматизації - Не враховує специфіку банківської сфери	Евристичний
IRAM	- Відносна простота впровадження - Легкість в експлуатації менеджерами банківських установ	- Висока вартість ліцензії - Робота тільки з існуючими інформ. активами	Інформаційний
EBIOS	- Велика кількість користувачів - Генерація звітів	- Лише для комерційних та державних установ	Інформаційний
RISK WATCH	- Простота впровадження та експлуатації - Гнучкість - Висока ефективність	- Аналіз ризиків лише на програмно-технічному рівні - Висока вартість ліцензії	Інформаційний
MEHARI	- Заснований на аналізі формул та параметрів - Формує оптимальну множину контрзаходів - У вільному доступі	- Застосовуваний до систем, що побудовані тільки за стандартом ISO	Евристичний
MAGERIT	- Систематичний метод аналізу - Кількісна оцінка - Гнучкість	- Результуючі дані залежать від людського фактору	Евристичний
CRAMM	- Детальне визначення існуючих ризиків - Ефективність використання	- Важкість у розумінні - Висока вартість ліцензії. - Робота тільки з існуючими інформ. активами	Ймовірнісний

Кінець таблиці 4.3

Методика оцінки	Переваги	Недоліки	Підходи
Методика НБУ	- Детальний аналіз ресурсів банківської системи - Використання ризик-орієнтованого підходу	- Заснований на множині стандартів - Враховує специфіку лише українських банківських систем	Інформаційний
Методика Корченко	- Застосування ознакового принципу для опису різних класів КБа - Дозволяє розширювати ознаковий простір для опису нових класів	-Не дає можливості зробити оцінку матеріальної втрати від реалізованої загрози	Інформаційний

Таблиця 4.4 – Результати досліджень методик оцінки ризиків

Методика	Атрибути							
	Якісна оцінка	Кількісна оцінка	Комплексна оцінка	Країна походження	Застосування у ОБС	Програмна реалізація	Ефективність контрзаходів	Простота розуміння
NIST	+			США	+	+	-	-
FAIR			+	США			+	+
EBIOS	+			Франція	+	+	+	-
MEHARI			+	Франція				
OCTAVE	+			США	+			
IT-GRUNDSHULTZ	+			Німеччина			+	
IRAM	+			Європа				+/-
RISK WATCH		+		США	+	+	+	+
FRAP	+			США				
CRAMM			+	Великобританія	+	+	+/-	+/-
MAGERIT	+	+		Іспанія	+	+		
Методика НБУ	+			Україна	+		-	+
Методика Корченко	+			Україна			+/-	+

Взаємозв’язок між методами виявлення атак і методиками оцінки ризиків наведено на рис. 4.5.

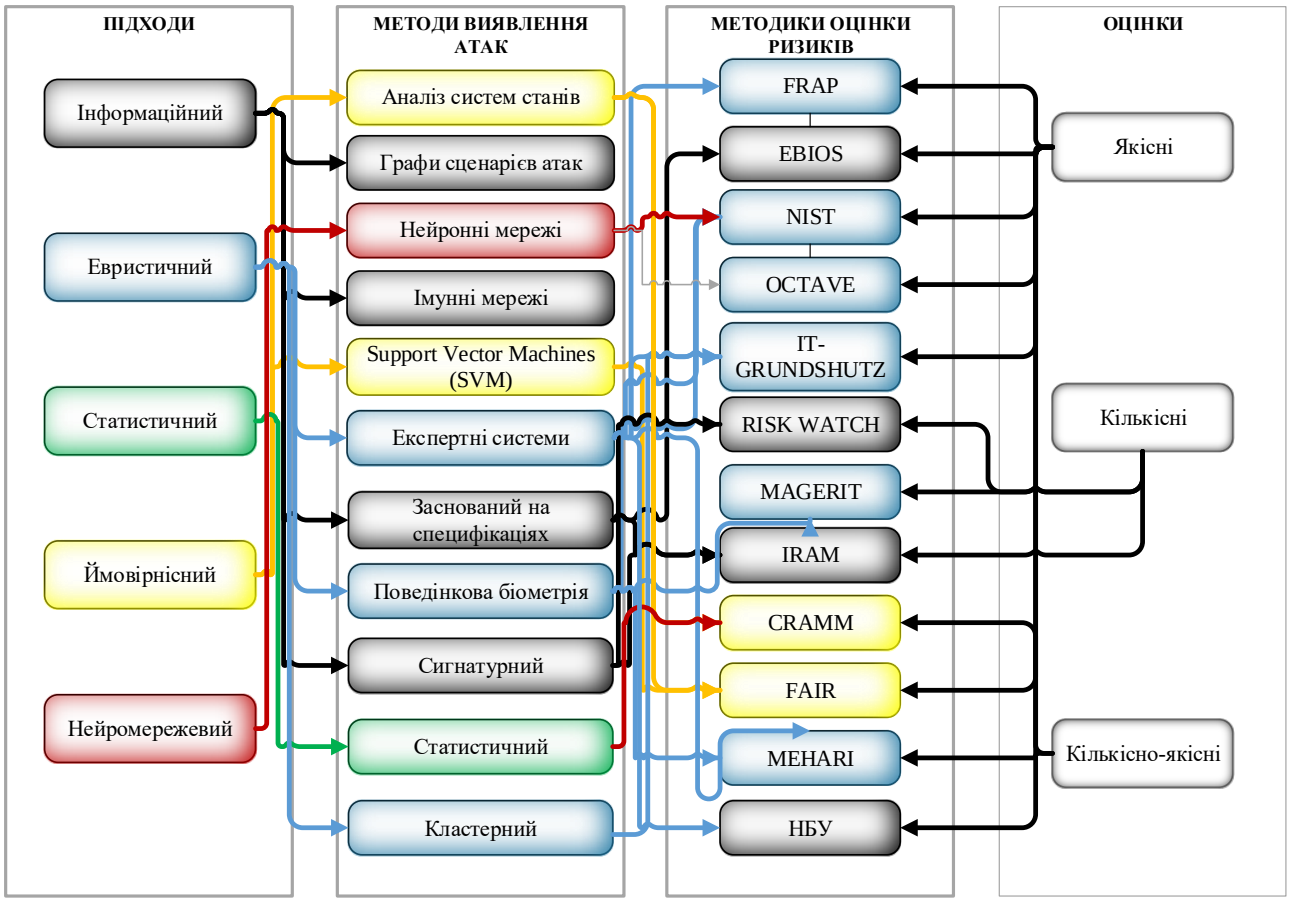


Рисунок 4.5 – Взаємозв'язок між методами виявлення атак та методиками оцінки ризиків

Проведений аналіз табл. 4.3, 4.4 і рис. 4.5 показав, що розглянуті методи та методики не дозволяють провести оцінювання функціональної ефективності, заснованої на показниках як технічних, так і економічних [42].

Аналіз публікацій та стандартів якості обслуговування (*Quality of Service*, *QoS*) в *IP*-мережах [43; 44; 45; 46; 47; 48; 49; 50] дозволив визначити основні технічні показники *QoS* – надійність та безпеку. На рис. 4.6 наведено результати синтезу гібридності загроз складових безпеки (ІБ, КБ, БІ) БІР на основі кібернетичного та інформаційного впливу на складові показників якості обслуговування *QoS*.

Таким чином, для оцінювання емерджентних властивостей функціональної ефективності АБС необхідно використовувати комплексний показник якості який базується на основних показниках безпеки та надійності, що в свою чергу забезпечує протидію гібридним загрозам на БІР та елементи інфраструктури АБС.

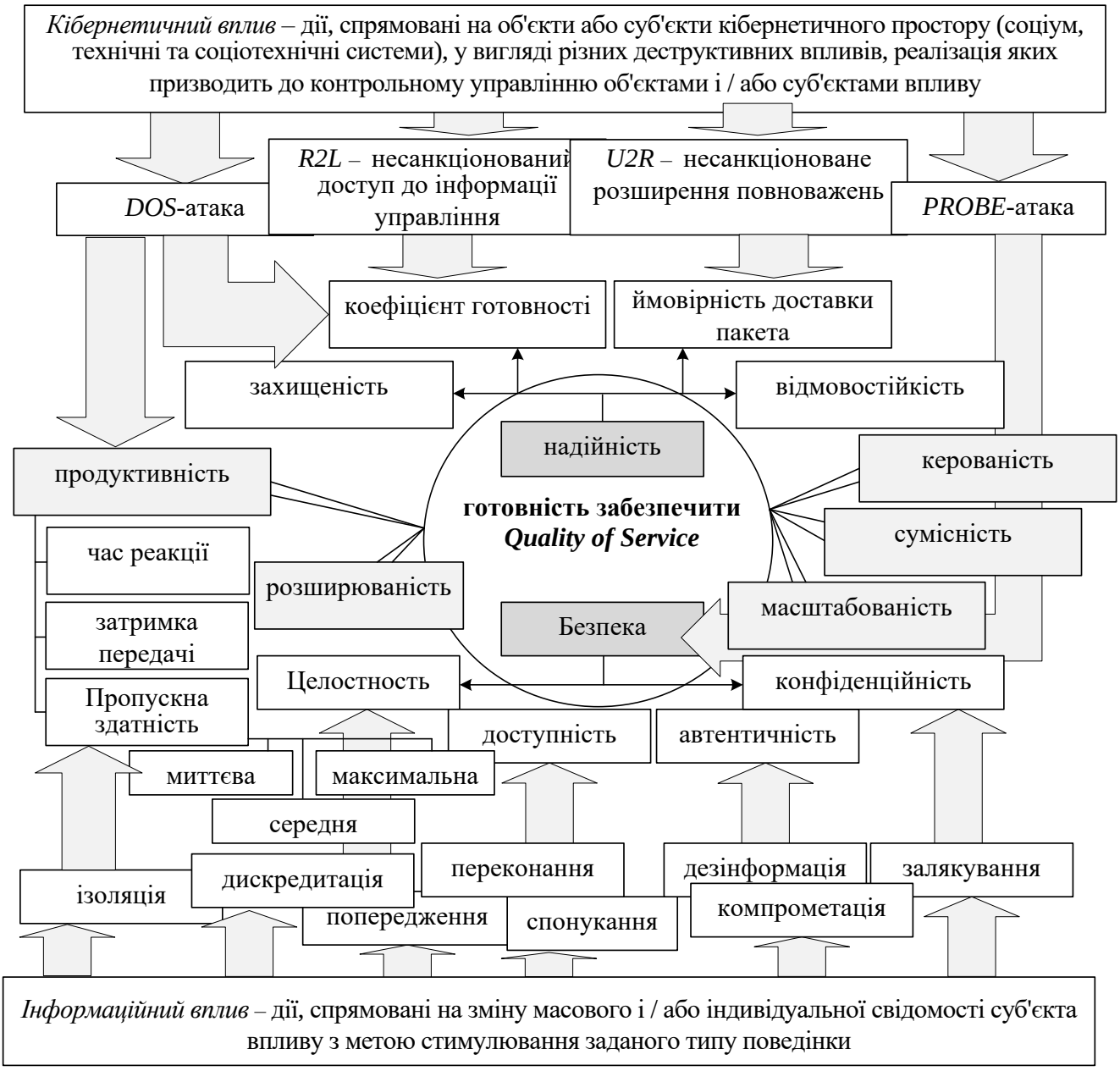


Рисунок 4.6 – Аналіз синтезу гібридності загроз складових безпеки (ІБ, КБ, БІ) БІР на основі кібернетичного та інформаційного впливу на складові показників якості обслуговування *QoS*

Якість послуги характеризується сукупністю таких основних споживчих властивостей [51; 52; 53; 54; 55]: забезпеченістю, зручністю використання, дієвістю, безпекою та іншими властивостями, специфічними для кожної послуги. Крім таких технічних характеристик мереж, як продуктивність, латентність, масштабованість, ступінь прозорості для кінцевих користувачів, вкрай важливими характеристиками є комплексні показники надійності: коефіцієнт готовності і

середній час недоступності в рік. Від показників надійності безпосередньо залежить доступність інформаційних сервісів для користувачів.

Крім того, від надійності мережі побічно також залежать продуктивність і латентність мережі, оскільки пожежі і відмови в мережі ведуть до необхідності повторної передачі блоків даних, а це з рештою зумовлює збільшення затримок при передачі та зменшення обсягів переданих даних за одиницю часу [53]. Для оцінки технічної складової функціональної ефективності [42] скористаємося загальним показником ефективності обміну даними, що включає швидкість достовірної та конфіденційної передачі даних в комп'ютерній мережі АБС і дозволяє порівняти ефективність існуючих протоколів при обміні даними між двома вузлами, що розглянуто в роботах [51; 54; 55].

При розгляді функціонування *IP*-мережі, яка використовується в АБС ОБС, загальний показник ефективності обміну даними повинен включати в себе показники безпеки і часткові показники системи зв'язку – достовірність і оперативність. Основними критеріями оцінки ефективності *секретних систем* прийнято вважати такі [56; 57; 58; 59; 60; 61; 62; 63]:

1. *Криптографічна стійкість* (кількість секретності), яку оцінюють, як складність розв'язання задачі криптоаналізу найкращим відомим методом.

2. *Обсяг ключових даних*. Симетрична криптосистема оперує загальними для всіх користувачів секретним ключем. У цьому випадку його поширення вимагає захищених каналів зв'язку, а отже, ключ не повинен бути занадто великим, щоб не виникли проблеми з його розподілом, і не дуже маленьким, щоб його складно було зламати повним перебиранням. У разі асиметричної криптосистеми один з ключів може бути загальнодоступним, його поширюють по відкритих каналах зв'язку.

3. *Складність виконання прямого і зворотного криптографічного перетворення* (шифрування/розшифрування повідомлень). Ці операції повинні бути простішими, щоб їх легко можна було реалізувати на практиці.

4. *Розмноження кількісті помилок*. У деяких типах шифрів помилка в одній літері, допущена при шифруванні або передаванні, призводить до великої кількості

помилок в розшифрованому тексті. Природно, бажано мінімізувати це поширення помилок.

5. *Збільшення обсягу повідомлення*. У деяких типах секретних систем обсяг повідомлення збільшується в результаті операції шифрування. Цей небажаний ефект потрібно мінімізувати.

Для оцінювання складових ефективності криптоалгоритмів пропонується використовувати швидкий та інтуїтивно зрозумілий експрес-метод, який дозволяє забезпечити ранжирування стійкості та програмну ефективність реалізації криптоалгоритмів.

Стійкість системи безпеки в АБС до можливих дій зловмисника визначається на основі теореми множення ймовірностей незалежних подій за виразом:

$$B = P_c \times W_{synerg}^{IB,KB,BI}, \tag{4.29}$$

де B – стійкість системи безпеки в АБС;

P_c.– ймовірність криптозахисту ТЗЗІ в АБС;

$W_{synerg}^{IB,KB,BI}$ – ймовірність реалізації синергетичної атаки на БІР на складові безпеки (ІБ, КБ, БІ).

Під *достовірністю* розуміють властивість системи, що характеризує її спроможність забезпечувати точне відтворення переданих повідомлень в пунктах прийому [65]. Достовірність залежить від параметрів самої *IP*-мережі, ступеня її технічної досконалості і умов роботи (тип та стан каналів зв'язку, метеорологічні показники, вид та інтенсивність завад, організаційних заходи дотримання правил радіообміну і експлуатації апаратури) [54; 55; 65]. Кількісно достовірність передачі може визначатися:

– ймовірністю помилкового прийому одиничного елемента (втрат достовірності):

$$P_0 = \lim_{n_{заг} \to \infty} \frac{n_{пом}}{n_{заг}},$$

де P_0 – ймовірність помилкового прийому одиничного елемента;

ймовірність помилки біта в каналі передачі даних;

$n_{пом}$ – кількість помилково прийнятих одиничних елементів;

$n_{заг}$ – загальна кількість переданих одиничних елементів;

– ймовірністю помилкового прийому пакету даних:

$$P_{помп} = \lim_{N_{озаг} \to \infty} \frac{N_{пом}}{N_{заг}},$$

де $P_{пом\,п}$ – ймовірність помилкового прийому пакету; $N_{пом}$ – кількість помилково прийнятих кодових послідовностей (пакетів); $N_{заг}$ – загальна кількість переданих кодових послідовностей (пакетів).

– ймовірністю правильного прийому одиничного елемента $P_{0\,пр}$ та ймовірністю правильного прийому пакету: $P_{пр.п}$, причому:

$$P_{0\,пр} + P_0 = 1; \quad P_{пр.п} + P_{пом\,п} = 1,$$

де $P_{0пр}$ – ймовірність правильного прийому одиничного елемента;

$P_{пр.п}$ – ймовірність правильного прийому пакету;

Ймовірності помилкового і правильного прийому одиничного елемента (P_0 й $P_{0пр}$) фактично є характеристиками дискретного каналу зв'язку, ймовірності $P_{пом\,п}$ та $P_{пр.п}$ є характеристиками комп'ютерної мережі в цілому, так як вони визначаються не тільки характером та інтенсивністю завад в каналі зв'язку, видом і швидкістю модуляції, а й способом захисту від помилок в системі [54; 55; 65].

Час доставки інформації [54; 55; 65] – інтервал часу від початку надходження повідомлення даних на вхід передавальної частини комп'ютерної мережі до початку його видачі одержувачу даних на стороні прийому. При передачі конфіденційної інформації, крім того, в час доставки входить час шифрування відправником пакетів даних і час розшифрування пакетів одержувачем, відповідним криптоалгоритмом.

Аналіз часу шифрування і розшифрування переможців конкурсів криптоалгоритмів *AES* і *NESSIE* [58; 59;60; 61; 62; 63; 64] показує, що для несиметричних алгоритмів складність реалізації криптографічних перетворень на

3 – 5 порядків вище, ніж у аналогічних систем блоково-симетричних шифрів, гібридні крипто-кодові конструкції на збиткових кодах, забезпечують швидкість криптоперетворень на рівні БСШ.

Таким чином, в *IP*-мережі з автоперезапитом (вирішальним зворотним зв'язком) час доставки пакету дорівнює [51; 54]: $t_д = t_д' + \Delta t_д + t_ш + t_{рш}$ – для симетричних криптоалгоритмів, $t_д = t_д' + \Delta t_д + (t_ш + t_{рш})^s$ – для несиметричних (гібридних на КККЗК) криптоалгоритмів,

де $t_д$ – час доставки пакету;

$t_д'$ – час доставки пакету з першої посилки;

$\Delta t_д$ – час багатократного повторення передачі інформації при погіршенні якості каналу;

$t_ш$ – час шифрування пакету даних криптоалгоритмом;

$t_{рш}$ – час розшифрування одержувачем пакету даних.

Час $t_д$ доставки повідомлення в задану адресу залежить від багатьох чинників: структури каналів, надійності та завантаженості мережі, методу комутації, наявності та характеру завад, що призводять до помилок і повторних передач. Він є випадковою величиною, яка характеризується щільністю розподілу $f(t_д)$.

У каналах зв'язку з високою інтенсивністю помилок P_0 підвищення достовірності призводить до збільшення часу доставки $t_д$ через зменшення кількості повторних посилок пакету, і навпаки, зниження часу доставки $t_д$ за рахунок зменшення кількості повторних посилок пакету веде до зниження достовірності [51; 54]. Однак більшість реальних каналів передачі даних є нестаціонарними, ймовірність одиночної помилки в них змінюється в часі в широких межах від 10^{-9} до 10^{-12} (див. табл. 4.8) [51; 54; 67].

Загальною вимогою до достовірності інформації є мінімізація ймовірності помилкового прийому символів повідомлення $P_{пом}$ або, що еквівалентно, максимізація ймовірності правильного прийому $P_{пр.п}$. У той же час на сьогоднішній день вимоги до достовірності інформації істотно зросли і, відповідно до [44; 45], припустима

ймовірність помилкового прийому символів повідомлення становить $P_Д < 10^{-7} – 10^{-9}$, залежно від категорії цінності інформації, її пріоритетності та обладнання.

Для того щоб розрахувати комплексний показник ефективності комп'ютерних мереж передачі даних на основі різних технологій, необхідно використовувати багатофакторний аналіз, оскільки в цих випадках враховуються абсолютно різні чинники: вартість розгортання мережі, швидкість передачі даних, імовірність та час доставки пакету і т. д. Кожен з наведених показників може бути розрахований окремо тим чи іншим методом, однак для розрахунку інтегрального показника єдиної кількісної методики не існує. Зазвичай в таких випадках використовують моделі багатофакторного аналізу, найпростіша з яких була задіяна і в нашому випадку.

Для оцінки комплексного показника ефективності були розроблені опорні таблиці, що дозволяють виділити діапазони зміни необхідних параметрів і визначити їх в умовних балах. Цей простий метод дозволяє отримати досить адекватні результати оцінки, і крім того, об'єднати їх з результатами точних розрахунків за окремими конкретними параметрами.

В опорних табл. 4.5 – 4.10 наведені параметри систем передачі даних, які враховуються в інтегральному показнику функціональної ефективності *IP*-мережі.

Таблиця 4.5 – Вартість розгортання мережі

Бали	Опис параметру
1	Дуже висока вартість
2	Висока вартість
3	Середня вартість
4	Низька вартість
5	Дуже низька вартість

Таблиця 4.6 – Швидкість передачі даних

Бали	Опис параметру
1	Мала (10Мб/с)
2	Середня (100 Мб/с)
3	Висока (1Гб/с)
4	Дуже висока (10Гб/с)
5	Надзвичайно висока (40 Гб/с)

Таблиця 4.7 – Ймовірність доставки пакету

Бали	Опис параметру
1	Мала (> 0)
2	Середня (0.95)
3	Висока (0.97546)
4	Дуже висока (0.999999)

Таблиця 4.8 – Час доставки пакету

Бали	Опис параметру
1	Дуже великий (1875 с)
2	Великий
3	Середній
4	Малий (0.006 с)
5	Дуже малий (0.0003 с)

Таблиця 4.9 – Затримка пакету

Бали	Опис параметру
1	Велика
2	Середня
3	Мала

Таблиця 4.10 – Продуктивність мережі

Бали	Опис параметру
1	Мала
2	Середня
3	Висока

Таким чином, на основі моделі багатофакторного аналізу можливо описати абсолютно різні параметри, які в інший спосіб аналітично об'єднати практично неможливо. Для порівняння існуючих технологій передачі даних було відібрано наступні: пакетна комутація за стандартами глобальних обчислювальних мереж (ГОМ): *X.25; Frame Relay; Ethernet, Fast Ethernet; Gigabit, 10 Gb, 40 Gb Ethernet*. Порівняльні характеристики зазначених технологій показані в табл. 4.11 – 4.13.

Таблиця 4.11 – Порівняльна характеристика протоколу *Ethernet*

Технологія ГОМ	Вартість	Швидкість передачі даних, Мбіт/с	Довжина пакету, біт	Ймовірність правильної доставки пакету, $P_{пр.п}$	Час доставки пакету, $t_д$, с
Ethernet	середня	10	1518	0.95	0.006
Fast Ethernet	середня	100	1518	0.95	0.006
Gigabit Ethernet	висока	1000	1518	0.99999	0.006
10 GbE	висока	10 000	1518	0.99999	0.006
40GbE	висока	40 000	1518	0.99999	0.006

Таблиця 4.12 – Ймовірносно-часові характеристики технологій ГОМ

Технологія ГОМ	Вартість	Швидкість передачі даних, Мбіт/с	Довжина пакету, біт	Ймовірність $P_{пр.п}$	Час доставки пакету, $t_д$, с
X.25 (V.34)	середня	10	1056	0.97546	1875
Frame Relay	середня	100	12048	> 0	0.0003
Fast Ethernet	середня	100	1518	0.95	0.006

Таблиця 4.13 – Порівняння *Ethernet*, пакетної комутації та *Frame Relay*

Показники	*Fast Ethernet*	Пакетна комутація (*X.25*)	*Frame Relay*
Мультиплексування з часовим розділенням	немає	немає	немає
Статистичне мультиплексування	Так	Так	Так
Поділ портів	Так	Так	Так
Висока продуктивність	Так	немає	Так
Затримка	низька	висока	низька

Використовуючи дані з табл. 4.5 – 4.13, отримуємо таблицю узагальненої ефективності мереж передачі даних, де відібрані показники вже подано в умовних балах в діапазоні від 1 до 5.

Таблиця 4.14 – Узагальнена ефективність мереж передачі даних

Технологія	Умовні бали							
	група						Узагальнений індекс ефективності	Відносна ефективність,%
	1	2	3	4	5	6		
X.25	3	1	3	1	1	1	9	0,25
Frame Relay	3	2	1	5	3	3	270	7,37
Ethernet	3	1	2	4	3	3	216	5,89
Fast Ethernet	3	2	2	4	3	3	432	11,79
Gigabit Ethernet	2	3	4	4	3	3	864	23,59
10 Gb Ethernet	2	4	4	4	3	3	1152	31,45
40 Gb Ethernet	1	5	4	4	3	3	720	19,66
Всього:							3663	100

Група: 1 – вартість розгортання мережі;

2 – швидкість передачі даних;

3 – ймовірність доставки пакету;

4 – час доставки пакету;

5 – затримка пакету;

6 – продуктивність мережі.

Результати, показані в табл. 4.13 наведені на рис. 4.7, 4.8.

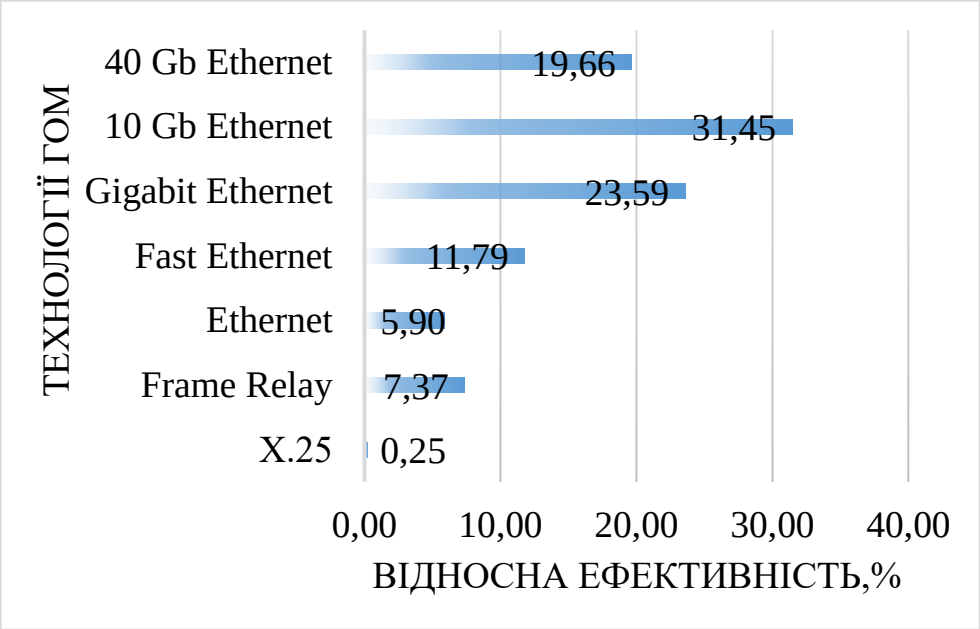


Рисунок 4.7 – Комплексний показник ефективності різних технологій комп'ютерних мереж

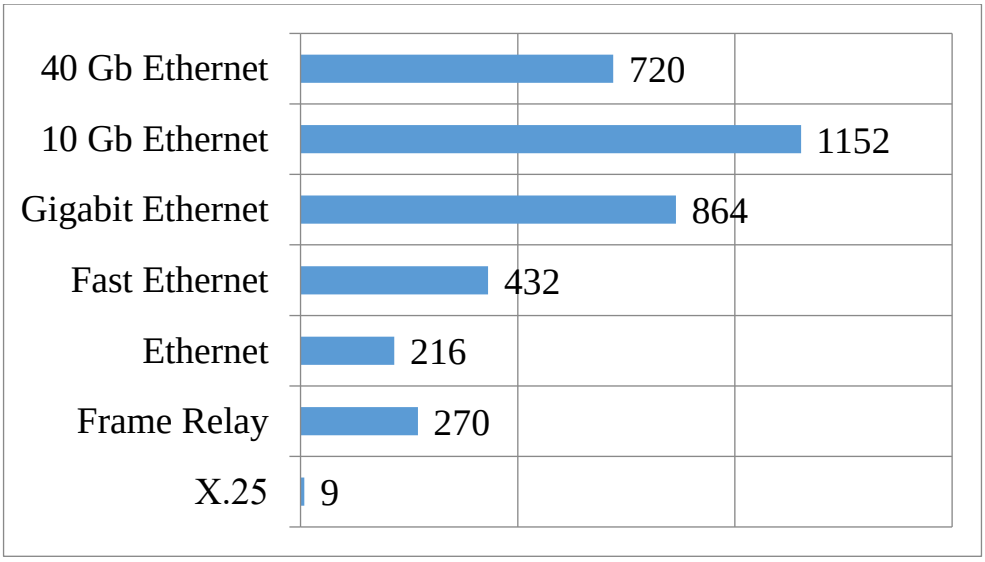


Рисунок 4.8 – Нормований показник ефективності різних технологій КМ, W_{norm}

Як видно з табл. 4.14 і рис. 4.7, 4.8, запропонований простий підхід дозволяє отримати досить адекватний результат. Видно, що на сьогодні найбільш ефективним за сукупністю наведених показників є *10 Gb Ethernet*. Популярний для комерційних комунікацій *Fast Ethernet* вже не в повній мірі забезпечує зростаючий трафік, а *40 Gb Ethernet* залишається досить дорогим для кінцевого споживача, що не дозволяє класифікувати його як оптимальну мережеву інфраструктуру.

Разом з тим, *10Mb Ethernet, Frame Relay,* а також пакетна комутація *X.25*, розглядаються навіть з точки зору найпростішого аналізу, як застарілі технології, що не відповідають сучасним реаліям.

Ґрунтуючись на проведених дослідженнях, пропонується комплексний показник функціональної ефективності АБС. Структура побудови показника така, що в ньому об'єднані дві основні характеристики системи:

– забезпечення безпеки БІР в умовах дії гібридних загроз на складові безпеки (ІБ, КБ, БІ) БІР;

– необхідна ймовірність досягнення мети з необхідним показником забезпечення конфіденційності у визначених умовах зовнішнього середовища і при певному рівні впливу внутрішніх випадкових факторів;

витрати на досягнення мети з необхідною ймовірністю і економічні витрати на реалізацію побудови та інвестування в ТЗЗІ КСЗІ в АБС з урахуванням необхідного показника якості обслуговування передачі даних.

Таким чином, показник функціональної ефективності мережі АБС на основі моделі багатофакторного аналізу задається виразом:

$$W\left(u_i\right)=\frac{n^{(u_i)}-t^{(u_i)}}{n^{(u_i)}}\times B^{(u_i)}\times P_{np.n}^{(u_i)}\times W_{effinv}\times W_{norm}, \qquad (4.30)$$

де $W(u_i)$ – показник ефективності мережі АБС, для обраної стратегії (метод підвищення достовірності) u_i;

$n^{(u_i)}$ – кількість інформаційних розрядів пакета для обраної стратегії u_i;

$t^{(u_i)}$ – час доставки пакета t для обраної стратегії u_i;

$B^{(u_i)}$ – стійкість системи безпеки для обраної стратегії u_i, який базується на результатах оцінювання стійкості запропонованим експрес-методом та результатах оцінювання протидії гібридним загрозам на складові безпеки (ІБ, КБ, БІ) БІР (4.29);

$P_{\text{пр п}}^{(u_i)}$ – ймовірність правильної доставки пакета для обраної стратегії;

U – множина допустимих стратегій (методів підвищення достовірності, використовуваних в мережі АБС на основі *IP*-мережі);

W_{effinv} – комплексний показник ефективності інвестицій в забезпечення безпеки банківських інформаційних ресурсів (див. під. 4.1);

W_{norm} – нормований багатофакторний показників ефективності.

Такий підхід дозволяє без значних економічних, обчислювальних та людських ресурсів враховувати не тільки технічні, але й економічні параметри ТЗЗІ АБС, що дозволяє точніше оцінювати її функціональну ефективність, враховувати результати досліджень при масштабуванні мережі АБС, виборі ТЗЗІ щодо побудови та підтримання КСЗІ, аналіз протидії загрозам на складові безпеки (ІБ, КБ, БІ) БІР, їх гібридність і синергізм, мінімізацію затрат та дієвий контроль за програмними засобами КСЗІ АБС.

Запропонована методика оцінювання функціональної ефективності передачі БІР на основі комплексного показника дозволяє отримати ***емерджентні властивості*** на основі синтезу комплексного показника ефективності інвестицій в забезпечення безпеки банківських інформаційних ресурсів, результатів оцінювання сучасних загроз на БІР та елементи інфраструктури АБС, їх гібридність та синергізм, результатів оцінювання експрес-методом стійкості і ефективності програмної (програмно-апаратної) реалізації криптографічних алгоритмів.

4.3. Висновки до четвертого розділу

Таким чином, у четвертому розділі отримано результати наукових досліджень, пов’язаних із розробкою методу оцінювання безпеки банківських інформаційних ресурсів, який ґрунтується на комплексному показнику ефективності інвестицій з урахуванням гібридності та синергізму атак на складові безпеки (ІБ, КБ, БІ). Для оцінювання якості обслуговування об’єктів АБС щодо безпеки БІР запропонована методика оцінки функціональної ефективності обміну даними в мережі АБС, яка ґрунтується на простому багатофакторному аналізі, в якій враховуються як технічні показники мережі (швидкість передачі даних, імовірність і час доставки пакета і ін.), показники безпеки технічних засобів

захисту інформації, так і економічні параметри (вартість масштабування, обслуговування мережі, ефективність інвестицій в безпеку і т.п.). У результаті досліджень було отримано такі результати.

1. Набув подальшого розвитку метод оцінювання безпеки банківських інформаційних ресурсів, що на, відміну від відомих, враховує комплексний показник ефективності інвестицій, які виділяються на забезпечення безпеки банківських інформаційних ресурсів, що дозволяє оптимізувати витрати коштів на її побудову в умовах впливу гібридних загроз при одночасному забезпеченні заданого рівня їх безпеки. Практична реалізація методу дозволяє комплексно оцінювати основні показники інвестування в забезпечення безпеки банківських інформаційних ресурсів з урахуванням синергетичного оцінювання загроз інформаційній безпеці, кібербезпеці та безпеці інформації.

2. Розроблено методику оцінювання функціональної ефективності обміну даними в мережі АБС, що ґрунтується на простому багатофакторному аналізі, в якій враховуються як технічні показники мережі (швидкість передачі даних, імовірність і час доставки пакета і ін.), показники безпеки технічних засобів захисту інформації, так і економічні параметри (вартість масштабування, обслуговування мережі, ефективність інвестицій в безпеку і т.п.). Запропонована методика оцінки функціональної ефективності АБС дозволяє без істотних часових та експертних витрат проводити оцінку стану якості обслуговування користувачів АБС, використовувати результати оцінки функціональної ефективності АБС для її масштабування, підвищення технічних показників мережі, безпеки інформаційних ресурсів АБС.

Список використаних джерел у четвертому розділі

1. Г. П. Леоненко, и А. Ю. Юдин, “Проблемы обеспечения информационной безопасности систем критически важной информационной инфраструктуры Украины”, *Information Technology and Security,* № 1(3), с. 44 – 48, 2013.

2. А. А. Синяк, и Н. Е. Губенко, “Анализ методов оценки эффективности затрат в информационную безопасность”, *ИУС и КМ. Секция 4. Web-технологии и ИБ*, с. 444 – 446. 2012.

3. В. П. Первадчук, и В. А. Белецкий, “Оценка эффективности инвестирования в информационную безопасность предприятия на основе нечетких множеств”, *Вестник ИжГТУ*, № 1(49), с. 51 – 53, 2011.

4. Е. В. Зубарева, и А. А. Бабенко, “Методы оценки инвестиций в информационную безопасность предприятия”, [Электронный ресурс], доступно: www.volsu.ru/download.php?id=000028639-1.pdf. Дата звернення: Груд., 4, 2017.

5. К. Г. Хомяков, и Л. В. Каницкая, “Оценка эффективности инвестиций в комплексные системы защиты информации компаний нефтегазового комплекса для принятия взвешенного инвестиционного решения”, *Экономика. Фундаментальные исследования*, Вып. № 2, с. 5173 – 5177, 2015.

6. И. М. Ажмухамедов, и Т. Б. Ханжина, “Оценка экономической эффективности мер по обеспечению информационной безопасности”, *Вестник АГТУ. Сер.: Экономика*, Вып. № 1, с. 185 – 190, 2011.

7. С. А. Петренко, “Оценка затрат на кибербезопасность”, *Труды ИСА РАН*, т.27, с. 235 – 265, 2006.

8. Н. Кожокару, “Эффективность инвестиций в области информационной безопасности”, [Электронный ресурс], доступно: http://www.securitylab.ru/bitrix/exturl.php?goto=http://1.bp.blogspot.com/-7Lhsq9eFw7U/VhZrMFnOLJI/AAAAAAAAHqk/AHT9E2u8R9E/s1600/risk-taxanomy.bmp. Дата звернення: Груд., 4, 2017.

9. Е. Н. Ефимов, и Г. М. Лапицкая, “Оценка эффективности мероприятий информационной безопасности в условиях неопределенности”, *Бизнес-Информатика. Математические методы и алгоритмы решения задач бизнес-информатики*, Вып. №1(31), с. 51 – 57, 2015.

10. С. Евсеев, “Синергетическая модель оценки безопасности банковской информации”, *Науково-технічний журнал “Інформаційна безпека”*, № 4 (24), с. 104 – 118, 2016.

11. С. Евсеев, “Модель нарушителя прав доступа в автоматизированной банковской системе на основе синергетического подхода”, *Науково-технічний журнал “Інформаційна безпека”*, № 2 (26), с. 110 – 119, 2017.

12. С. С. Жаринова, и А. А. Бабенко, “Оптимизация инвестиций в информационную безопасность предприятия”, *ГУ-УНПК: Информационные системы и технологии*, Вып. 3 (83), с. 114 – 123, 2014.

13. С. С. Жаринова, и А. А. Бабенко, “Модель эффективности инвестиций в информационную безопасность предприятия”, [Электронный ресурс], доступно: www.volsu.ru/download.php?id=000026221-1.pdf. Дата звернення: Груд., 4, 2017.

14. В. М. Постников, и С. Б. Спиридонов, “Методы выбора весовых коэффициентов локальных критериев”, *Издатель ФГБОУ ВПО “МГТУ им. Н.Э. Баумана”*, Эл № ФС 77 – 48211, Вып. № 3, с.267 – 287, 2016.

15. С. Евсеев, “Оценка эффективности инвестиций в безопасность организаций банковского сектора на основе синергетической модели угроз”, *Системи обробки інформації*, № 2(148), с. 88 – 94, 2017.

16. О. Г. Корченко, О. Є. Архипов, та Ю. О. Дрейс, *Оцінювання збитку національній безпеці України у розвитку витоку державної таємниці.* Київ, наук.-вид. центр НА СБ України, 2014.

17. Р. В. Грищук, та Ю. Г. Даник; за заг. ред. проф. Ю. Г. Даника, *Основи кібербезпеки*, Житомир, ЖНАЕУ, 2016.

18. А. О. Корченко, Л. М. Скачек, та В. О. Хорошко, *Банківська безпека*, Київ, ПВП “Задруга”, 2014.

19. С. Євсеєв, та О. Король, “Комплексний показник ефективності інвестицій в безпеку банківської інформації на основі синергетичної моделі загроз” на *VI Міжнародної наукової конференції “Інформація, комунікація, суспільство 2017”*, Славське, 2017. с. 18 – 19.

20. А. Архипов, “Применение экономико-стоимостных моделей информационных рисков для оценивания предельных объемов инвестиций в безопасность информации”, *Науково-технічний журнал “Захист інформації”,* том 17, №3, с. 211 – 218, 2015.

21. С. Голощапов, “100GB Ethernet: основные принципы”. [Электронный ресурс], доступно: www.lastmile.su/journal/article/2820. Дата звернення: Груд., 4, 2017.

22. С. П. Евсеев, Д. В. Сумцов, О. Г. Король, и Б. П. Томашевский, “Анализ эффективности передачи данных в компьютерных системах с использованием интегрированных механизмов обеспечения надежности и безопасности”, *Восточно-европейский журнал передовых технологий*, № 2/2(44), с. 45 – 49, 2010.

23. С. П. Євсеєв, С. Е. Остапов, та Р. В. Корольов, “Використання міні-версій для оцінки стійкості блоково-симетричних шифрів”, *Науково-технічний журнал “Безпека інформації”*, том.23, № 2, с. 100 – 108, 2017.

24. И. Д. Горбенко, В. И. Долгов, И.В. Лисицкая, и Р.В. Олейников, “Новая идеология оценки стойкости блочных симметричных шифров к атакам дифференциального и линейного криптоанализа”, *Прикладная радиоэлектроника*, том 9, № 3, с. 312 – 320, 2010.

25. В. И. Долгов, и И. В. Лисицкая, *Методология оценки стойкости блочных симметричных шифров к атакам дифференциального и линейного криптоанализа: монография*. Харьков: Издательство «Форт», 2013.

26. И. В. Лисицкая, “О новой методике оценки стойкости блочных симметричных шифров к атакам дифференциального и линейного криптоанализа”, *Системи обробки інформації*, вип. 4 (94), с. 167 – 173, 2011.

27. И. В. Лисицкая, “Методология оценки стойкости блочных симметричных шифров”, [Электронный ресурс], доступно: https://cyberleninka-.ru/article/n/metodologiya-otsenki-stoykosti-blochnyh-simmetrichnyh-shifrov. Дата звернення: Груд., 4, 2017.

28. И. В. Лисицкая, “Большие шифры – случайные подстановки. Сравнение дифференциальных и линейных свойств шифров, представленных на украинский конкурс, и их уменьшенных моделей”, [Электронный ресурс], доступно: https://cy-berleninka.ru/article/n/bolshie-shifry-sluchaynyepod-stanovki-sravnenie-differentsialnyh-i-lineynyh-svoystv-shifrov-predstavlennyh-na-ukrainskiy-konkurs-i-ih. Дата звернення: Груд., 4, 2017.

29. И. В. Лисицкая, К. Е. Лисицкий, М. Ю. Родинко, И. А. Головко, И. И. Жариков, М. А. Корниенко, и М. В. Кулеба, “Эксперементальные данные по определению динамических показателей прихода блочных симметричных шифров к состоянию случайности”, *Радіоелектроніка, інформатика, управління*, № 1, с. 129 – 141, 2017.

30. И. В. Лисицкая, и А. А. Настенко, “Большие шифры – случайные подстановки”, *Межведомственный научн. технический сборник «Радиотехника»*, Вып. 166, с. 50 – 55, 2011.

31. Л. Сорока, А. Кузнецов, И. Московченко, и С. Исаев, “Исследование дифференциальных свойств блочно-симметричных шифров, *Системи обробки інформації*, випуск 6 (87), с. 286 – 295, 2010.

32. И. Лисицкая, А. Кузнецов, и С. Исаев, “Линейные свойства блочных симметричных шифров, представленных на украинский конкурс”, *Прикладная радиоэлектроника: научно-техн. журнал*, Том 10, № 2, с. 135 – 140, 2011.

33. И. В. Лисицкая, Т. А. Гриненко, и С. Ю. Бессонов, “Анализ дифференциальных и линейных свойств шифров rijndael, serpent, threefish при 16-битных входах и выходах”, *Восточно-Европейский журнал передовых технологий*, с. 50-54. 2015.

34. G. Piret, and F.-X. Standaert, “Provable security of block ciphers against linear cryptanalysis: a mission impossible?”, *Designs, Codes and Cryptography*, V. 50, № 3, p. 325 – 338, 2009.

35. Collard B., and F.-X. Standaert, “Experimenting linear cryptanalysis”, *Advanced Linear Cryptanalysis*, V.116, p. 90 – 117, 2011.

36. L. R. Knudsen “Practically Secure Feistel Ciphers”. *Proc. Fast Software Encryption, Cambridge*, 1993, Springer, V.809, p. 211 – 221, 1994.

37. A. Rukhin, and J. Soto. *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*. NIST Special Publication 800-22, 09.2000, 164 p.

38. K. Shennon, *Raboty po teorii informacii i kibernetike*. M. IL. 1963.

39. С. П. Евсеев, “Методология оценивания безопасности информационных технологий автоматизированных банковских систем Украины”, *Ukrainian Scientific Journal of Information Security*, vol. 22, issue 3, p. 297 – 309, 2016.

40. С. Евсеев, О. Король, и А. Сочнева, “Анализ оценки рисков кибербезопасности банковской информации”, *Сборник научных трудов НАУ “Защита информации”*, вып. 23, с. 109 – 128, 2016.

41. С. Евсеев, А. Сочнева, О. Король, и В. Абдулаев, “Анализ методик оценки рисков нарушения безопасности банковской информации”, *Известия Высших технических учебных заведений Азербайджана*. том.19, № 2 (106), с. 77 – 86, 2017.

42. А. П. Смирнов, *Функциональная эффективность* // [Электронный ресурс], доступно: https://www.ngpedia.ru/id625108p1.html. Дата звернення: Груд., 4, 2017.

43. МСЭ-Т Е.800 Определение терминов, относящихся к качеству обслуживания, [Електронний ресурс], доступно : https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-E.800-200809. Дата звернення: Груд., 4, 2017.

44. ISO 9000:2015(ru) Quality management systems – Fundamentals and vocabulary [Online], available: https://www.iso.org/obp/ui/#iso:std:iso:9000:ed-4:v1:en. Accessed on: December, 4, 2017

45. Стандарт ГОСТ РВ 51987 “Информационная технология, комплекс стандартов на АС” [Электронный ресурс], доступно : http://gearletitbit.weebly.com/blog/gost-rv-51987-2002. Дата звернення: Груд., 4, 2017.

46. Яновский Г. Г., Качество обслуживания в сетях IP [Электронный ресурс], доступно : niits.ru/public/2008/2008-006.pdf. Дата звернення: Груд., 4, 2017.

47. Шриниваса Вегешны, “Качество обслуживания в сетях IP” [Электронный ресурс] доступно : http://it-ebooks.ru/publ/cisco/cisco_ip_quality_of_service/11-1-0-293. Дата звернення: Груд., 4, 2017.

48. Quality of Service (QoS) in a network with software (SDN): an overview [Online], available: https://doi.org/10.1016/j.jnca.2016.12.019. Accessed on: December 4, 2017.

49. A single quality of service (QoS) survey in OPS / OBS networks [Online], available: https://doi.org/10.1016/j.yofte.2017.05.016.

50. Modeling of network access protocols for network quality analysis [Online], available: 10.1109/ISORC.2015.47. Accessed on: December 4, 2017.

51. С. П. Євсеєв, С. Е. Остапов, Х. Н. Рзаєв, та В. І. Ніколаєнко, "Оцінка обміну даними в глобальних обчислювальних мережах на основі комплексного показника якості обслуговування мережі", *Науковий журнал Радіоелектроніка, інформатика, управління*, № 1(40), с. 115 – 128, 2017.

52. Quality of Service: Implementation of a new structure and new measurement methodology [Электронный ресурс]. – Режим доступа к ресурсу: 10.1109/INFOMAN.2017.7950439.

53. А. И. Каяшев, П. А. Рахман, и М. И. Шарипов, Анализ показателей надежности локальных компьютерных сетей, *Вестник УГАТУ*, Уфа., т. 17, № 5 (58), с. 140–149, 2013.

54. С. П. Евсеев, Д. В. Сумцов, О. Г. Король, и Б. П. Томашевский, Анализ эффективности передачи данных в компьютерных системах с использованием интегрированных механизмов обеспечения надежности и безопасности, *Восточно-европейский журнал передовых технологий*, № 2/2(44), с. 45 – 49, 2010.

55. С. Євсеєв, "Інтегрований показник якості обслуговування користувачів глобальних обчислювальних мереж", *VIII Міжнародна науково-технічна конференція "Інформаційно-комп'ютерні технології – 2016"*, Житомир, 2016, с. 17 – 18.

56. С. В. Ленков, Д. А. Перегудов, и В. А. Хорошко, *Методы и средства защиты информации*: *Несанкционированное получение информации* [в 2 т.]; (под ред. В. А. Хорошко), К.: Арий, т. 1, 2008.

57. С. В. Ленков, Д. А. Перегудов, и В. А. Хорошко, *Методы и средства защиты информации*: *Информационная безопасность* [в 2 т.]; (под ред. В. А. Хорошко), К.: Арий, т. 2, 2008.

58. Ю. И. Горбенко, и И. Д. Горбенко, *Инфраструктура открытых ключей. Электронная цифровая подпись. Теория и практика*. Харьков. Форт, 2010.

59. И. Д. Горбенко, и Ю. И. Горбенко, *Прикладная Криптология*, Харьков. Форт, 2012.

60. О. О. Кузнецов, Р. В. Олійников, Ю. І. Горбенко, А. І. Пушкарьов, О. В. Дирда, та І. Д. Горбенко, “Обґрунтування вимог, побудування та аналіз перспективних симетричних криптоперетворень на основі блочних шифрів”, *Вісник Національного університету "Львівська політехніка". Комп’ютерні системи та мережі*, № 806, с. 124 – 141, 2014.

61. Б. Шнайер *Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си* [Пер. с англ.], М.: Издательство ТРИУМФ, 2002.

62. Н. А. Молдовян, А. А. Молдовян, и М. А Еремеев *Криптография: от примитивов к синтезу алгоритмов*, СПб.: БХВ, Петербург, 2004.

63. С. Э. Остапов, С. П. Евсеев, и О. Г. Король *Технологии защиты информации*, Черновцы: Издательский дом “РОДОВИД”, 2014.

64. В. Столлингс *Криптография и защита сетей: принципы и практика*[Пер. с англ.]; 2-е изд.М. : ИД “Вильямс”, 2001.

65. Б. Скляр *Цифровая связь. Теоретические основы и практическое применение*. Изд. 2-е, испр./ Пер. с англ. М.: Издательский дом “Вильямс”, 2003.

66. S. Yevseiev, V. Ponomarenko, and O. Rayevnyeva, “Assessment of functional effectiveness of the corporate scientific-educational network based on comprehensive indicators of service quality”, *Восточно-европейский журнал передовых технологий*, 6/2 (90), с. 4 – 15, 2017.

67. О. Г. Король, “Оцінка якості обслуговування глобальної мережі на основі технологій Ethernet за допомогою комплексного показника”, *Системи обробки інформації*, – № 2(148), с. 88 – 94. 2017.

РОЗДІЛ 5
ВЕРИФІКАЦІЯ ТА ДОСЛІДЖЕННЯ РОЗРОБЛЕНИХ МОДЕЛЕЙ ТА МЕТОДІВ. ПОБУДОВА МЕТОДОЛОГІЇ ПОБУДОВИ СИСТЕМИ БЕЗПЕКИ БАНКІВСЬКИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ

5.1. Порівняльний аналіз ефективності передачі банківських інформаційних ресурсів на основі розробленого комплексного показника оцінювання функціональної ефективності передачі банківських інформаційних ресурсів

Для підвищення значення показника функціональної ефективності комп'ютерної мережі в роботі [1] розглянуті різні способи управління обміном даними: без зворотного зв'язку з виявленням *r*-кратних помилок; без зворотного зв'язку з виправленням *t*-кратних помилок. І найчастіше використовувані протоколи управління: з розв'язувальним зворотним зв'язком і безперервною передачею кадрів ($РЗЗ_{БПК}$) "Повернення-на-*N*"; з розв'язувальним зворотним зв'язком і позитивною квитанцією ($РЗЗ_{ПК}$).

Проведені дослідження в роботах [1; 2; 3] показали, що для забезпечення максимального рівня функціональної ефективності *IP*-мереж необхідно використовувати протоколи з розв'язувальним зворотним зв'язком і безперервною передачею кадрів ($РЗЗ_{БПК}$) "Повернення-на-*N*"; з розв'язувальним зворотним зв'язком і позитивною квитанцією ($РЗЗ_{ПК}$).

Крім того, детальне дослідження статистичних властивостей послідовностей помилок в реальних каналах зв'язку [4; 5; 6; 7; 8; 9] показало, що помилки є залежними і володіють тенденцією до гуртування (пакетування), тобто між ними існує певна залежність – кореляція. Велику частину часу інформація проходить каналами зв'язку без спотворень, а в окремі моменти часу виникають згущення помилок, так звані пакети (пачки, групи) помилок. Всередині пакетів помилок ймовірність помилки виявляється значно вище середньої ймовірності помилок, обчисленої для значного часу передачі.

У таких умовах способи захисту, оптимальні для гіпотези незалежних помилок, виявляються неефективними при використанні їх в реальних каналах зв'язку. Для урахування статистичних властивостей послідовностей помилок в реальних каналах зв'язку розглянемо модель дискретного каналу з пам'яттю.

У такій моделі у вихідних даних замість ймовірності помилки біта P_0 необхідно задати такі чотири канальних параметра:

– ймовірність виникнення пакета помилок – P_n;

– ймовірність помилки усередині пакета – P_ε;

– математичне сподівання m_{ln} довжини пакета помилок;

– середньоквадратичне відхилення σ_{ln} довжини пакета помилок.

При розрахунках приймалося: $P_n=10^{-5}\div10^{-2}$; $P_\varepsilon=0{,}8$; $m_{ln}=10$; $\sigma_{ln}=2$.

Для мережі АБС з розв'язувальним зворотним зв'язком і безперервною передачею кадрів "Повернення-на-*N*" значення показника ефективності визначається виразом:

$$W\left(u_3\right)=\frac{n^{(u_3)}-t^{(u_3)}}{n^{(u_3)}}\times B^{(u_3)}\times P_{np.n}^{(u_3)}\times W_{effinv}\times W_{norm}, \qquad (5.1)$$

$W(u_i)$ – показник ефективності мережі АБС для обраної стратегії (метод підвищення достовірності) u_i;

$n^{(u_i)}$ – кількість інформаційних розрядів пакета для обраної стратегії u_i;

$t^{(u_i)}$ – час доставки пакета t для обраної стратегії u_i;

$B^{(u_i)}$ – стійкість системи безпеки для обраної стратегії u_i;

$P_{\text{пр п}}^{(u_i)}$ – ймовірність правильної доставки пакета для обраної стратегії;

U – множина допустимих стратегій (методів підвищення достовірності, використовуваних в мережі АБС на основі *IP*-мережі);

W_{effinv} – комплексний показник ефективності інвестицій в забезпечення безпеки банківських інформаційних ресурсів;

W_{norm} – нормований багатофакторний показників ефективності;

$$m_t^{(u_3)} = \frac{n}{C} + \frac{L}{V_p} + t_{ш} + t_{рш} +$$

$$+ \frac{\sum_{i=0}^{\infty}\left\{\left[1-(1-P_n)^{n+i}\right]\cdot\left[\Phi\left(\frac{i+1-m_{l_n}}{\sigma_{l_n}}\right)-\Phi\left(\frac{i-m_{l_n}}{\sigma_{l_n}}\right)\right]\right\}\cdot\left\{1-\frac{1}{2^r}\cdot\left[\frac{1}{2}-\Phi\left(\frac{r+1-m_{l_n}}{\sigma_{l_n}}\right)\right]\right\}}{1-\sum_{i=0}^{\infty}\left\{\left[1-(1-P_n)^{n+i}\right]\cdot\left[\Phi\left(\frac{i+1-m_{l_n}}{\sigma_{l_n}}\right)-\Phi\left(\frac{i-m_{l_n}}{\sigma_{l_n}}\right)\right]\right\}}\times \quad (5.2)$$

$$\times\left(\frac{n+s}{C}+2\frac{L}{V_p}\right),$$

$$P_{пр.п}^{(u_3)} = \frac{1-\sum_{i=0}^{\infty}\left\{\left[1-(1-P_{\text{п}})^{n+i}\right]\cdot\left[\Phi\left(\frac{i+1-m_{l_n}}{\sigma_{l_n}}\right)-\Phi\left(\frac{i-m_{l_n}}{\sigma_{l_n}}\right)\right]\right\}}{1-\sum_{i=0}^{\infty}\left\{\left[1-(1-P_n)^{n+i}\right]\cdot\left[\Phi\left(\frac{i+1-m_{l_n}}{\sigma_{l_n}}\right)-\Phi\left(\frac{i-m_{l_n}}{\sigma_{l_n}}\right)\right]\right\}\cdot\left\{1-\frac{1}{2^r}\cdot\left[\frac{1}{2}-\Phi\left(\frac{r+1-m_{l_n}}{\sigma_{l_n}}\right)\right]\right\}}. \quad (5.3)$$

Для мережі АБС з розв'язувальним зворотним зв'язком і позитивною квитанцією кадрів значення показника ефективності визначається як:

$$W\left(u_4\right) = \frac{n^{(u_4)} - t^{(u_4)}}{n^{(u_4)}} \times B^{(u_4)} \times P_{пр\,п}^{(u_4)} \times W_{effinv} \times W_{norm}, \quad (5.4)$$

де

$$t^{(u_4)} = \frac{n+s}{C} + 2\frac{L}{V_p} + t_{ш} + t_{рш} + \frac{n}{C}\times$$

$$\times\frac{\sum_{i=0}^{\infty}\left\{\left[1-(1-P_n)^{n+i}\right]\cdot\left[\Phi\left(\frac{i+1-m_{l_n}}{\sigma_{l_n}}\right)-\Phi\left(\frac{i-m_{l_n}}{\sigma_{l_n}}\right)\right]\right\}\cdot\left\{1-\frac{1}{2^r}\cdot\left[\frac{1}{2}-\Phi\left(\frac{r+1-m_{l_n}}{\sigma_{l_n}}\right)\right]\right\}}{1-\sum_{i=0}^{\infty}\left\{\left[1-(1-P_n)^{n+i}\right]\cdot\left[\Phi\left(\frac{i+1-m_{l_n}}{\sigma_{l_n}}\right)-\Phi\left(\frac{i-m_{l_n}}{\sigma_{l_n}}\right)\right]\right\}}, \quad (5.5)$$

$$P_{пр.п}^{(u_4)} = 1-\sum_{i=0}^{\infty}\left\{\left[1-(1-P_n)^{n+i}\right]\cdot\left[\Phi\left(\frac{i+1-m_{l_n}}{\sigma_{l_n}}\right)-\Phi\left(\frac{i-m_{l_n}}{\sigma_{l_n}}\right)\right]\right\}\times$$

$$\times\frac{1-\sum_{i=0}^{\infty}\left\{\left[1-(1-P_n)^{n+i}\right]\cdot\left[\Phi\left(\frac{i+1-m_{l_n}}{\sigma_{l_n}}\right)-\Phi\left(\frac{i-m_{l_n}}{\sigma_{l_n}}\right)\right]\cdot\left\{1-\frac{1}{2^r}\cdot\left[\frac{1}{2}-\Phi\left(\frac{r+1-m_{l_n}}{\sigma_{l_n}}\right)\right]\right\}\right\}^N}{1-\sum_{i=0}^{\infty}\left\{\left[1-(1-P_n)^{n+i}\right]\cdot\left[\Phi\left(\frac{i+1-m_{l_n}}{\sigma_{l_n}}\right)-\Phi\left(\frac{i-m_{l_n}}{\sigma_{l_n}}\right)\right]\cdot\left\{1-\frac{1}{2^r}\cdot\left[\frac{1}{2}-\Phi\left(\frac{r+1-m_{l_n}}{\sigma_{l_n}}\right)\right]\right\}\right\}}, \quad (5.6)$$

На рис. 5.1, 5.2 наведені результати досліджень оцінки функціональної ефективності комп’ютерної мережі АБС нормованим багатофакторним показником ефективності на основі використання БСШ.

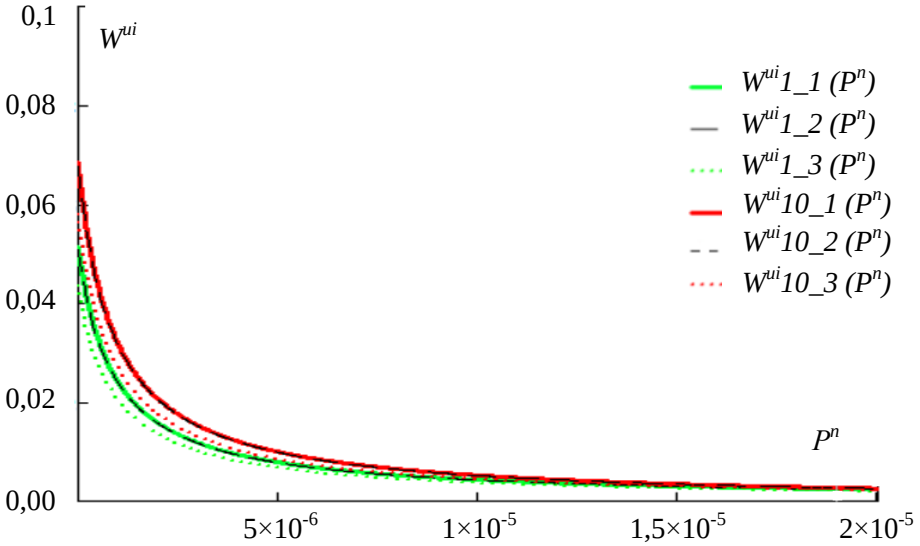


Рисунок 5.1 – Результати досліджень функціональної ефективності мережі АБС з розв’язувальним зворотним зв’язком і безперервною передачею кадрів “Повернення-на-*N*” з використанням методики *FAIR*

При проведенні досліджень криптостійкості використовувався експрес-метод оцінки на основі ентропійного методу і результати методики оцінки економічних витрат на основі методики *FAIR* (результати досліджень наведені в роботі [2], рис. 5.1). Вихідними даними до проведення досліджень є: технології 1 *Gbit Ethernet*, 10 *Gbit Ethernet* з розв’язувальним зворотним зв’язком і безперервною передачею кадрів “Повернення-на-*N*”; $W_{synerg}^{IB,KB,BI} = 0.0022839$; $t_{ш,\ рш} = 0{,}01$ с; $P_C^{AES} = 0.95454$; $P_C^{Kalyna256} = 0.9454519$; $P_C^{3DES} = 0.812043$; $n = 1518$; $C = 36000$; $P_{пр.\ п} = 0{,}99$.

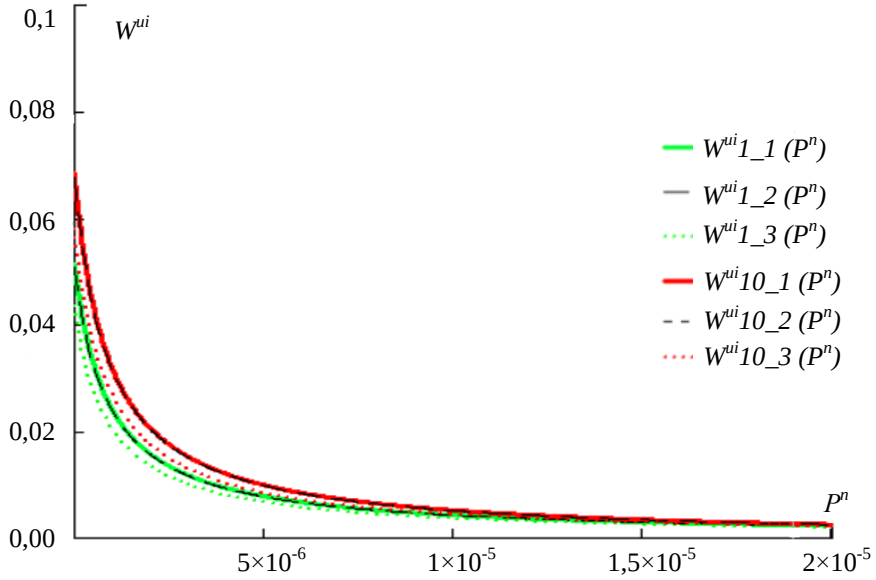


Рисунок 5.2 – Результати досліджень функціональної ефективності мережі АБС з розв'язувальним зворотним зв'язком і безперервною передачею кадрів "Повернення-на-*N*" з використанням методики оцінювання інвестицій

При проведенні досліджень (рис. 5.2) оцінювання криптостійкості БСШ виконано на основі запропонованого експрес-методу, оцінка економічних витрат в ТЗЗІ ґрунтується на запропонованій методиці (див. підп. 4.1.1). Вихідними даними для проведення досліджень є: технології 1 *Gbit Ethernet*, 10 *Gbit Ethernet* з розв'язувальним зворотним зв'язком і безперервною передачею кадрів "Повернення-на-*N*"; $W_{synerg}^{IB,KB,BI} = 0.0022839$; $t_{ш,\ рш} = 0{,}01$ с; $P_C^{AES} = 0.95454$; $P_C^{Kalyna256} = 0.9454519$; $P_C^{3DES} = 0.812043$; $n = 1518$; $C = 36000$; $P_{пр.\,n} = 0{,}99$.

Порівняльний аналіз результатів на рис. 5.1, 5.2 показав її адекватність і гнучкість. Запропонована методика дозволяє уніфікувати оцінку ефективності обміну даними в глобальних протоколах *IP*-мереж з урахуванням економічних витрат на програмно-апаратні засоби і технології, що забезпечують необхідні показники безпеки і надійності функціональної ефективності АБС ОБС, а також необхідне значення показника якості обслуговування *IP*-мережі, яка є базисом НСМЕП ОБС. Практичне використання введеного показника дозволить більш точно оцінювати ефективність протоколів обміну даними, які використовуються в глобальних протоколах *IP*-мереж АБС. Крім того, такий

підхід дозволить більш детально вирішувати завдання з масштабуванням і розширюваністю мережі АБС, оскільки включає не тільки технічні, але й економічні показники функціональної ефективності, що дуже важливо для забезпечення необхідної якості обслуговування користувачів АБС. Отримані вирази ефективності передачі даних в мережі АБС при різних способах управління обміном даних дозволяють отримати порівняльні кількісні оцінки стійкості програмної (програмно-апаратної) реалізації ТЗЗІ, можливу реалізацію гібридних загроз на БІР, ефективності інвестицій в ТЗЗІ, комплексного показника ефективності при використанні різних протоколів управління обміну даними в мережах на основі *Ethernet*-технологій.

5.2. Узагальнення одержаних результатів: методологія синтезу та аналізу запропонованих моделей та методів забезпечення безпеки банківських інформаційних ресурсів

У сучасних умовах, як показала практика, важлива роль у забезпеченні національної безпеки України та особливо її економічної складової належить процесам забезпечення інформаційної безпеки держави у банківському секторі. Ключову роль при побудові системи безпеки БІР, як складової національних інформаційних ресурсів держави, відіграє теорія та практика в якій науково-методологічна база є основою для прийняття обґрунтованих та ефективних управлінських рішень суб’єктами забезпечення інформаційної безпеки держави на усіх рівнях.

Зміни останнього десятиліття, що відбулися в ОБС призвели до об’єднання інформаційних та комп’ютерних мереж в єдиний інформаційний та кібернетичний простір. Інтеграційні процеси розвитку АБС обумовили істотно розширили спектр електронних послуг державних і комерційних банків світу та України. У результаті, суттєво трансформувалися і загрози у такому національному інформаційному ресурсі держави, як БІР.

Загрози набули ознак гібридності. Від суто загроз інформаційній, кібернетичній безпеці та безпеці інформації БІР прояви ознак гібридності

почали виникати унаслідок одночасного впливу на об’єкт захисту – БІР, за рахунок виникнення явища синергізму.

Відомо, що методологічний базис в будь-якій галузі безпеки являє собою ключові компоненти самої теорії безпеки та ґрунтується на методах і моделях, необхідних і достатніх для дослідження проблеми безпеки та вирішення практичних задач відповідного призначення. Так, нині в галузі інформаційної безпеки існує достатньо велика кількість методологій. Зокрема проведено аналіз методологій, які пов’язані з розробленням наукового базису для синтезу таких систем безпеки [10; 11; 12; 13; 14; 15; 16; 17; 18; 19; 20]: синтезу та аналізу диференціально-ігрових моделей та методів моделювання процесів кібернападу на державні інформаційні ресурси [10], оцінки рівня захищеності державних ресурсів від соціотехнічних атак [11]; оцінювання шкоди національній безпеці у сфері охорони державної таємниці [12], побудови та застосування безпечних бездротових сенсорних мереж з випадковими параметрами мережі [13], захисту державних інформаційних ресурсів [14], аналізу стану комплексу технічного захисту інформації [15], аналізу ризиків дерева ідентифікаторів державних інформаційних ресурсів [16], побудови систем виявлення аномалій породжених кібератаками [17], систем аналізу та оцінки ризиків втрат інформаційних ресурсів [18], комплексного захисту людини та соціальних груп від негативного інформаційно-психологічного впливу [19], адаптивних систем оцінювання ризиків безпеки ресурсів інформаційних систем [20] та ін. Однак проаналізовані методології не враховують синергізм та ознаки гібридності загроз на складові безпеки БІР, а саме [21; 22; 23]: інформаційної безпеки, кібербезпеки, безпеки інформації. Тому усі вони потребують кардинального перегляду з погляду створення методологічного базису для побудови системи безпеки БІР як України зокрема, так і світу в цілому.

Виходячи з аналізу [24; 25; 26; 27; 28] можна стверджувати, що одним з пріоритетних напрямків підвищення рівня безпеки БІР зокрема та подальшої стабілізації ІБ держави в цілому є принципово нове вирішення проблеми безпеки організацій банківського сектору держави шляхом створення

сучасних методів і засобів захисту БІР від гібридного нападу на основі комплексування ознак загроз ІБ, КБ, БІ на БІР, технічні об’єкти її інфраструктури. Так, вагомі наукові результати при вирішенні проблеми ІБ держави та розкриття окремих її складових в ОБС одержано в наукових працях [25, 26, 28; 29; 30; 31; 32] та ін., але незважаючи на це проблема залишається актуальною не тільки для України, а й для світової спільноти.

Виходячи з єдиних системних позицій [28; 30; 31; 32] та потреби реалізації комплексного підходу до побудови прогресивних систем безпеки БІР в умовах гібридизації та комплексування загроз ІБ, КБ, БІ нині існує об’єктивне протиріччя між високими вимогами практики до систем безпеки БІР та недосконалістю, а подекуди й відсутністю дієвих науково обґрунтованих методологічних засад її забезпечення.

Проведений аналіз керівних документів з організації побудови системи безпеки БІР в [21; 22; 23; 33; 34; 35; 36; 37] показав, що до сьогодні розглянуті лише окремі складові методології оцінювання рівня безпеки інформаційних технологій, застосовуваних в ОБС. Усі вони ґрунтуються на моделях безпеки – забезпечення конфіденційності, цілісності та доступності (моделі КЦД). Застосування моделі КЦД не враховує невід’ємну складову банківських транзакцій – послугу автентичності – стан БІР, при якому інформація забезпечує підтвердження автентичності джерела (авторизованого користувача і / або процесу) інформації. Крім цього, відсутність синергетичного підходу до аналізу ризиків, єдиної методології оцінювання безпеки інформаційних технологій в стандартах банківського сектору не дозволяє своєчасно виробляти відповідні політики, нові підходи і заходи для безпеки БІР. Відомо, що своєчасне виявлення і аналіз ризиків є невід’ємною частиною проблеми безпеки БІР. Фактично ризик являє собою інтегральну оцінку того, наскільки ефективно існуючі засоби захисту інформації здатні протистояти атакам на БІР. На практиці існує дві основні групи методів оцінювання ризиків безпеки [38; 39; 40]. Перша група дозволяє встановити рівень ризику шляхом оцінювання ступеня відповідності визначеному набору

вимог до забезпечення ІБ. Друга базується на визначенні ймовірності реалізації атак, а також рівнів їх збитку. Але обидві групи методів також не враховують гібридності сучасних атак на ОБС, тому не дозволяють своєчасно реагувати на їх прояви.

Перспективним підходом забезпечення безпеки БІР є одночасне та раціональне поєднання організаційних заходів та технічних засобів, спрямованих на забезпечення ІБ, КБ та БІ, що зрештою позначається на інвестиціях банку, вкладених у безпеку. При цьому комплексування сил і засобів безпеки у кожному окремому випадку не є ефективним та таким, що не гарантує досягнення очікуваного безпекового синергетичного ефекту [41; 63].

Таким чином, як зрозуміло з вищевикладеного, на основі існуючого методологічного апарату досить проблематично, а в деяких випадках і неможливо досягнути поставленої мети дослідження.

Спираючись на відомий підхід до побудови методологій [10; 11; 12; 13; 14; 15; 16; 17; 18; 19; 20] на основі досліджень [41; 42; 43; 44; 45; 46; 47; 48; 49; 50; 51; 52; 53; 54; 55; 56; 57; 58; 59; 60; 62; 63] пропонується принципово нова методологія побудови системи забезпечення БІР.

Вона містить п’ять етапів (рис. 5.3, 5.4): 1) визначення ймовірності впливу загроз ІБ, КБ, БІ на безпеку БІР; 2) визначення узагальненого показника рівня захищеності БІР; 3) оцінювання ефективності інвестицій в забезпечення безпеки БІР; 4) побудова інтегрованих механізмів забезпечення конфіденційності, цілісності, автентичності та достовірності БІР; 5) визначення стану та формування стратегій безпеки БІР. Реалізація методології, з урахуванням розроблених у дисертації методів і засобів, дасть можливість забезпечити підвищення рівня захищеності БІР в умовах дії гібридних загроз, раціональну організацію системи забезпечення безпеки БІР в умовах одночасної дії на систему загроз ІБ, КБ та БІ.

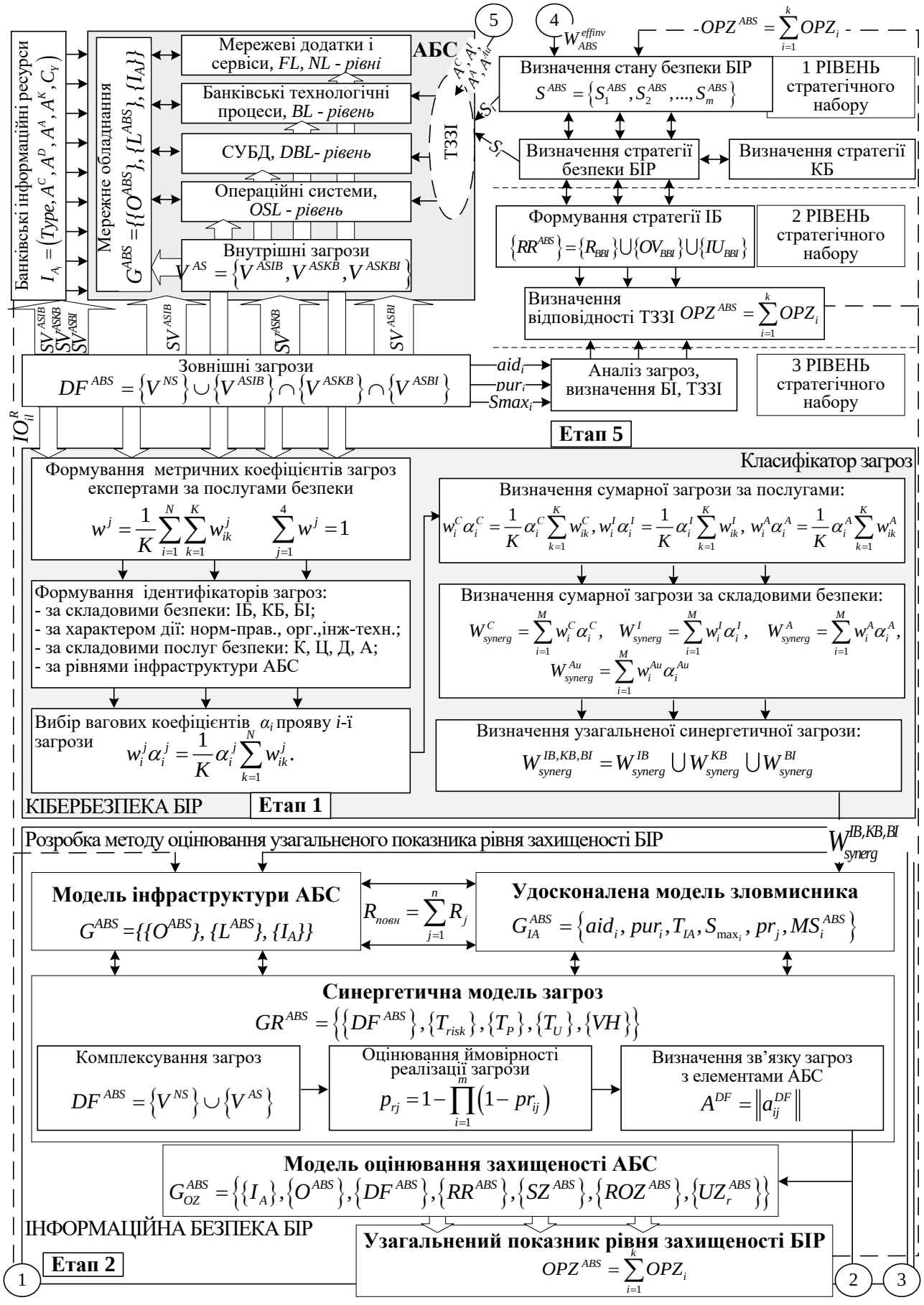


Рисунок 5.3 – Схема методології побудови системи безпеки банківських інформаційних ресурсів

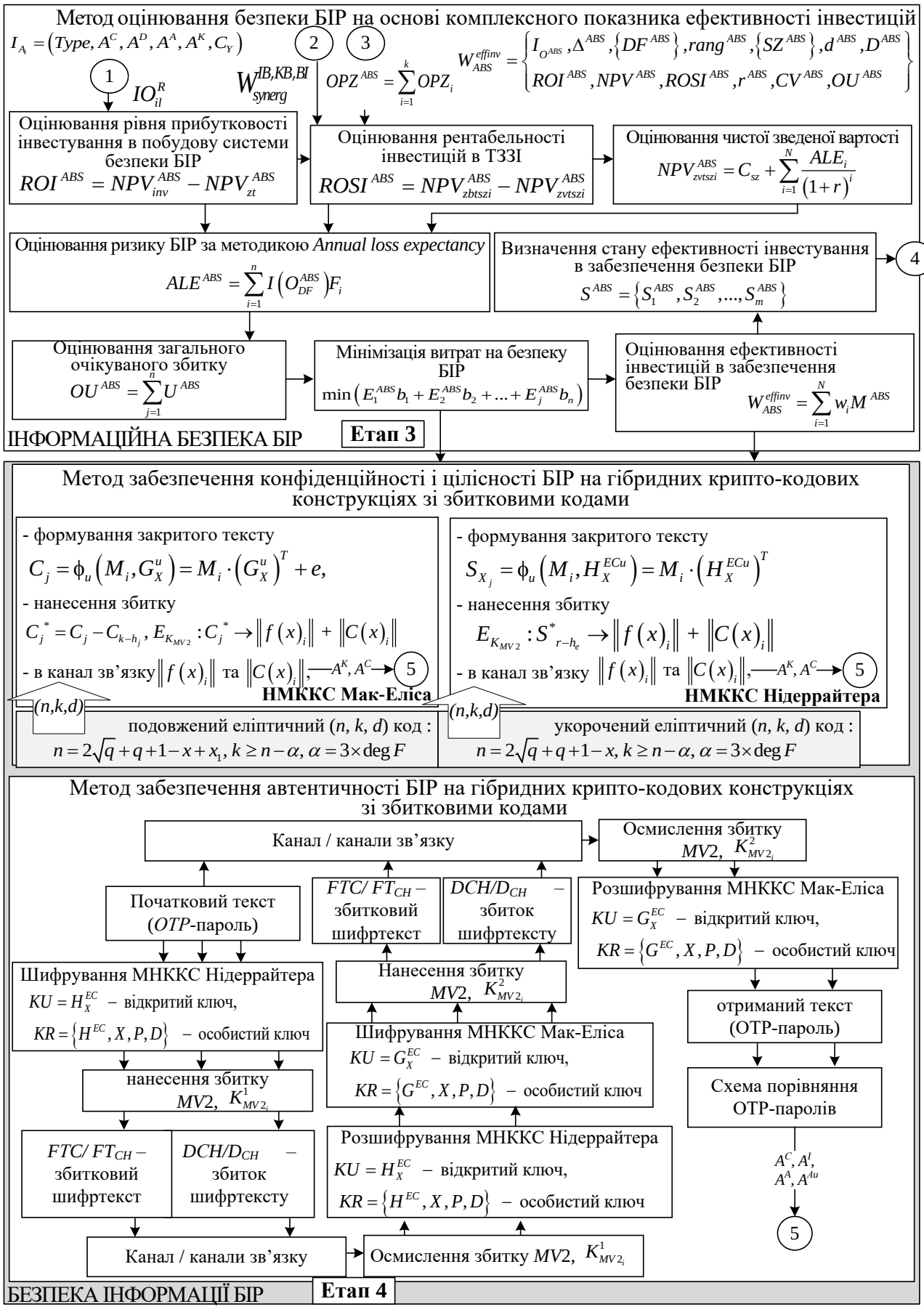


Рисунок 5.4 – Схема методології побудови системи безпеки банківських інформаційних ресурсів

Етап 1. Визначення ймовірності впливу загроз ІБ, КБ, БІ на безпеку БІР.

На першому етапі, зважаючи на те, що загрози ІБ, КБ, БІ мають можливість впливати на різні послуги безпеки (конфіденційність, цілісність, доступність, автентичність) з різною інтенсивністю експертами з ІБ вирішується завдання щодо нормування метричних коефіцієнтів загроз за послугами безпеки та формування класифікації загроз на основі запропонованого класифікатора [33]. Складовими класифікатора є:

– складова забезпечення безпеки БІР ОБС: ІБ (01), БІ (02), КБ (03);

– характер напрямків: нормативно-правовий (01), організаційний (02), інженерно-технічний (03);

– основні особливості інформації: конфіденційність (01), цілісність (02), доступність (03), автентичність (04);

– рівні ієрархії інфраструктури АБС: *FL* – фізичний рівень (01), *NL* – мережевий рівень (02), *OSL* – рівень операційних систем (ОС) (03), *DBL* – рівень систем управління базами даних (04), *BL* – рівень банківських технологічних застосунків і сервісів (05). Множину загроз ІБ, КБ, БІ на БІР запропоновано використовувати з ресурсу [61].

Для визначення вагових коефіцієнтів α_i, що визначають умови прояву *i*-ї загрози використовуються дані з табл. 5.1.

Таблиця 5.1 – Таблиця вибору вагових коефіцієнтів α_i прояву *i*-ї загрози залежно від умови її прояву

Вагові коефіцієнти α_i	Умови прояву загрози
0,067	загроза проявляється не частіше одного разу на 5 років
0,133	загроза проявляється не частіше одного разу на рік
0,2	загроза проявляється не частіше одного разу на місяць
0,267	загроза проявляється не частіше одного разу на тиждень
0,333	загроза проявляється щодня

Визначення реалізації кожної *i*-ї загрози з урахуванням імовірності прояву атаки її виникнення здійснюється за виразом:

$$w_i^j P_i^j = \frac{1}{K} P_i^j \sum_{k=1}^{N} w_{ik}^j.$$

Для кожної послуги безпеки та *i*-ї загрози:

$$w_i^C \alpha_i^C = \frac{1}{K} \alpha_i^C \sum_{k=1}^{K} w_{ik}^C \text{ – послуга конфіденційність;}$$

$$w_i^I \alpha_i^I = \frac{1}{K} \alpha_i^I \sum_{k=1}^{K} w_{ik}^I \text{ – послуга цілісність;}$$

$$w_i^A \alpha_i^A = \frac{1}{K} \alpha_i^A \sum_{k=1}^{K} w_{ik}^A \text{ – послуга доступність;}$$

$$w_i^{Au} \alpha_i^{Au} = \frac{1}{K} \alpha_i^{Au} \sum_{k=1}^{K} w_{ik}^{Au} \text{ – послуга автентичність,}$$

де $w_{ik}{}^C$, $w_{ik}{}^I$, $w_{ik}{}^A$, $w_{ik}{}^{Au}$ – експертні вагові коефіцієнти послуг безпеки: конфіденційності, цілісності, доступності, автентичності; α_i^C, α_i^I, α_i^A, α_i^{Au} – ваговий коефіцієнт послуги безпеки: конфіденційності, цілісності, доступності, автентичності прояву атаки *i*-ї загрози.

Визначення реалізації виникнення декількох загроз для обраної послуги розраховується за виразами:

$$W_{synerg}^C = \sum_{i=1}^{M} w_i^C \alpha_i^C \text{ – послуга конфіденційність;}$$

$$W_{synerg}^I = \sum_{i=1}^{M} w_i^I \alpha_i^I \text{ – послуга цілісність;}$$

$$W_{synerg}^A = \sum_{i=1}^{M} w_i^A \alpha_i^A \text{ – послуга доступність;}$$

$$W_{synerg}^{Au} = \sum_{i=1}^{M} w_i^{Au} \alpha_i^{Au} \text{ – послуга автентичність,}$$

де *M* – кількість декількох загроз, які вибрані експертом з ІБ банку з множини

$\{i\}_i^M$, що є підмножиною усієї множини загроз класифікатора, тобто $M \le N$.

Визначення сумарної загрози за складовими безпеки:

$$W_{synerg}^{IB} = \sum_{i=1}^{N} \left(w_i^C \cap w_i^I \cap w_i^A \cap w_i^{Au} \right) \alpha_i ,$$

$$W_{synerg}^{KB} = \sum_{i=1}^{N} \left(w_i^C \cap w_i^I \cap w_i^A \cap w_i^{Au} \right) \alpha_i ,$$

$$W_{synerg}^{BI} = \sum_{i=1}^{N} \left(w_i^C \cap w_i^I \cap w_i^A \cap w_i^{Au} \right) \alpha_i .$$

Визначення узагальненої синергетичної загрози проводиться згідно з виразом (рис. 5.3):

$$W_{synerg}^{IB,KB,BI} = W_{synerg}^{IB} \bigcup W_{synerg}^{KB} \bigcup W_{synerg}^{BI} .$$

Визначення узагальненої синергетичної загрози з урахуванням її гібридності розраховується: $W_{synerg}^{\text{hybrid } C,I,A,Au} = W_{synerg}^{C} \bigcap W_{synerg}^{\text{I}} \bigcap W_{synerg}^{A} \bigcap W_{synerg}^{Au}$.

Одержані за результатами аналізу комплексування загроз дані подаються на 3-й рівень моделі стратегічного управління банком для їх узагальнення при оцінюванні достатності технічних засобів захисту БІР. Результати досліджень загроз з максимальною частотою їх прояву на БІР наведені у табл. 5.2.

Таблиця 5.2 – Результати оцінки загроз на основі синергетичного підходу

Складові безпеки	Послуги безпеки				
	C, W_{synerg}^{C}	*I*, W_{synerg}^{I}	*A*, W_{synerg}^{I}	*Au*, W_{synerg}^{Au}	Підсумок
IB, W_{synerg}^{IB}	0,023	0,223	0,193	0,207	0,0002
KB, W_{synerg}^{KB}	0,222	0,234	0,197	0,134	0,0014
BI, W_{synerg}^{BI}	0,226	0,109	0,152	0,189	0,0007
Підсумок	0,471	0,566	0,542	0,53	
$W_{synerg}^{IB,KB,BI} = W_{synerg}^{IB} \bigcup W_{synerg}^{KB} \bigcup W_{synerg}^{BI} =$ =0,0002+0,0014+0,0007=**0,0223**			$W_{synerg}^{\text{hybrid } C,I,A,Au} = W_{synerg}^{\text{C}} \bigcap W_{synerg}^{\text{I}} \bigcap W_{synerg}^{A} \bigcap W_{synerg}^{Au}$ = =0,471×0,566×0,542×0,53=**0,0766**		

Етап 2. визначення узагальненого показника рівня захищеності БІР.

На основі сформованої множини загроз ІБ, КБ, БІ на БІР та моделі ієрархії АБС – G^{ABS} ={{O^{ABS}}, {L^{ABS}}, {I_A}} визначається залежність між інформаційними активами БІР і загрозами ІБ, КБ, БІ за такими діями:

– визначення зв'язку між інформаційними активами БІР $\{I_A\}$ та елементами інфраструктури АБС $A^{ABS} = \left\| a_{ij}^{ABS} \right\|$. Кожен елемент $I_{A_i} \in \{I_A\}$ описується вектором $I_{A_i} = \left(Type, A^C, A^I, A^A, A^{Au}, C_Y\right)$, *Type* – тип інформаційного активу, описується множиною базових значень *Type* = {*BT, PID, RrD, KT, StO, Ol, YI, PD*}, де *BT* – банківська таємниця; *PID* – платіжні документи; *KrD* – кредитні документи; *KT* – комерційна таємниця; *StO* – статистичні звіти; *Ol* – загальнодоступна інформація; *YI* – керівна інформація; *PD* – персональні дані. A^C – конфіденційність; A^I – цілісність; A^A – доступність; A^{Au} – автентичність; *CY* – безперервність – це властивості інформації, які необхідно забезпечувати. Вони набувають значення 1 – якщо властивість необхідно, 0 – в іншому випадку;

– визначення зв'язку між інформаційними активами $\{I_A\}$ і об'єктами середовища. Кожен елемент $O_l \in \{O^{ABS}\}$, описується вектором $O_l = \{Y^{ABS}, IO\}$, де Y^{ABS} – рівень ієрархії інформаційної структури, яка визначається множиною Y^{ABS} = {*FL, NL, OSL, DBL, BL*}, де *FL* – фізичний рівень; *NL* – мережевий рівень; *OSL* – рівень операційних систем (ОС); *DBL* – рівень систем управління базами даних; *BL* – рівень банківських технологічних застосунків і сервісів. Для визначення типу зв'язку та існуючого відношення I^{OR} між інформаційними активами БІР та об'єктами АБС використовується правило:

$$IO^R = \left\| IO_{il}^R \right\|,$$

де IO_{il}^R – відображає наявність і тип зв'язку між *i*-м інформаційним активом та *l*-м об'єктом середовища АБС.

На основі запропонованої синергетичної моделі загроз, маємо:

$$GR^{ABS} = \left\{ \left\{ DF^{ABS} \right\}, \left\{ T_{risk} \right\}, \left\{ T_P \right\}, \left\{ T_U \right\}, \left\{ VH \right\} \right\},$$

де $\left\{ DF^{ABS} \right\}$ – множина джерел загроз; $\left\{ T_{risk} \right\}$ – якісний показник ризику; $\left\{ T_P \right\}$ – множина базових термів ймовірності реалізації хоча б однієї загрози *j*-му активу; $\left\{ T_U \right\}$ – множина базових термів величини збитку від реалізації погрози; $\left\{ VH \right\}$ – множина деструктивних станів елементів АБС, і узагальненої моделі зловмисника:

$$G_{IA}^{ABS} = \left\{ aid_i, pur_i, T_{IA}, S_{\max_i}, pr_j, MS_i^{ABS} \right\} \forall i \in n, \forall j \in m,$$

де aid_i – ідентифікатор зловмисника (категорія зловмисника); pur_i – мета зловмисника; T_{IA} – час успішної реалізації загрози; $S_{\max_i}$ – ймовірнісний збиток системи; pr_j – ймовірність реалізації хоча б однієї загрози *j*-му активу; MS_i^{ABS} – рекомендації щодо виявлення, реагування ТЗЗІ, здійснюється комплексування множини загроз вигляду:

$$DF^{ABS} = \left\{ V^{NS} \right\} \bigcup \left\{ V^{AS} \right\}, \text{ де } \left\{ V^{AS} \right\} = \left\{ V^{ASBI} \right\} \bigcap \left\{ V^{ASIB} \right\} \bigcap \left\{ V^{ASKB} \right\}.$$

Такий підхід дозволяє визначити зв’язок між джерелами загроз і елементами АБС $A^{DF} = \left\| a_{ij}^{DF} \right\|$, що захищаються.

Визначення ціни повного ризику всіх активів БІР:

$$R_{повн} = \sum_{j=1}^{n} R_j,$$

де $R_j = pr_j \times q_j$, де pr_j – ймовірність реалізації хоча б однієї загрози *j*-му активу; q_j – збиток.

Ймовірність реалізації хоча б однієї загрози для кожного активу БІР:

$$p_{rj} = 1 - \prod_{i=1}^{m} \left(1 - pr_{ij}\right),$$

де pr_{ij} – ймовірність реалізації *i*-ї загрози *j*-му активу.

Визначення захищеності АБС від загроз ІБ, КБ, БІ на БІР пропонується здійснювати на основі удосконаленої моделі рівня захищеності банківських інформаційних ресурсів:

$$G_{OZ}^{ABS} = \begin{Bmatrix} \{I_A\}, \{O^{ABS}\}, \{DF^{ABS}\}, \{RR^{ABS}\}, \\ \{SZ^{ABS}\}, \{ROZ^{ABS}\}, \{UZ_r^{ABS}\} \end{Bmatrix},$$

де $\{I_A\}$ – множина елементів інформаційних активів; $\{O^{ABS}\}$ – множина елементів ієрархії АБС; $\{DF^{ABS}\}$ – множина джерел загроз безпеці АБС; $\{RR^{ABS}\}$ – множина вимог регуляторів до забезпечення безпеки БІР; $\{SZ^{ABS}\}$ – множина можливих ТСЗІ; $\{ROZ^{ABS}\}$ – дані обліку про результати оцінки захищеності АБС; $\{UZ_r^{ABS}\}$ – рівень захищеності АБС.

На основі зв'язку між джерелами загроз та елементами АБС визначається зв'язок між загрозами і технічними засобами системи захисту інформації (ТЗСЗІ) – $A^{DFSZ} = \left\| a_{ij}^{DFSZ} \right\|$.

У моделі використані такі типи зв'язку: *MZ* – є механізм захисту, що забезпечує протидію її деструктивному впливу $VH_i \in \{VH\}$; *NMZ* – немає механізму захисту для забезпечення протидії *i*-ій загрози.

Якщо для всіх $i = m$ $a_{mj}^{DFSZ} = NMZ$, то робиться висновок, що ТЗСЗІ АБС не здатні захистити БІР від певного деструктивного впливу, а тому для підвищення рівня захищеності АБС необхідно залучати додаткові кошти на механізми захисту.

Визначення множини вимог регуляторів $\{RR^{ABS}\}$, яка складається з вимог до забезпечення безпеки БІР – $\{R_{BBI}\}$, зазначених у міжнародних і

національних стандартах, множини оцінок ступеня виконання вимог безпеки $\{OV_{BBI}\}$ та множини підсумкового рівня відповідності безпеки БІР вимогам з множини $\{IU_{BBI}\}$:

$$\{RR^{ABS}\} = \{R_{BBI}\} \cup \{OV_{BBI}\} \cup \{IU_{BBI}\}.$$

Для оцінювання $\{RR^{ABS}\}$ використаємо вимоги з [65; 66], визначимо, що приватні показники поділяються на два типу:

перший – приватні показники, що відображають вимоги [66], виконання яких є обов'язковим в організації;

другий – приватні показники, що відображають положення [66], виконання яких рекомендується в ОБС.

Для часткових показників, виконання яких є обов'язковим (перший тип), встановлюється наступна шкала ступеня їх виконання:

"ні" – оцінці присвоюється значення, рівне нулю;

"частково" – оцінці присвоюється значення 0,25, 0,5 або 0,75;

"так" – оцінці присвоюється значення, рівне одиниці.

Якщо частковий показник призначений для оцінки вимог, які не належать до діяльності організації або на момент оцінки не є актуальними для організації, що зафіксовано документами організації, то даний частковий показник визначається як неоцінюваний (повинна бути заповнена графа "н/о" – немає оцінки) і не враховується у формуванні подальших результатів оцінки.

Для часткових показників, виконання яких рекомендується (другий тип), встановлюється наступна шкала ступеня їх виконання:

"так" – оцінці присвоюється значення, рівне одиниці;

"ні" – частковий показник визначається як неоцінюваний (повинна бути заповнена графа "н/о" – немає оцінки) і не враховується у формуванні подальших результатів оцінки. В табл. 5.3, 5.4 наведені рекомендовані критерії виставлення оцінок окремих показників ІБ за першим та другим типами часткових показників.

Таблиця 5.3 – Рекомендовані критерії виставлення оцінок окремих показників ІБ, в яких оцінюється як ступінь документованості, так і ступінь виконання вимог ІБ

оцінка приватного показника ІБ	Критерій виставлення оцінки приватного показника ІБ
0	Вимоги приватного показника ІБ не встановлені (визначені) у внутрішніх документах аудиту
0,25	Вимоги приватного показника ІБ встановлені (визначені) у внутрішніх документах аудиту, але не виконуються
0,5	Вимоги приватного показника ІБ встановлені (визначені) у внутрішніх документах аудиту, але не виконуються
0,75	Вимоги приватного показника ІБ встановлені (визначені) у внутрішніх документах аудиту і виконуються майже в повному обсязі
1,0	Вимоги приватного показника ІБ встановлені (визначені) у внутрішніх документах аудиту і виконуються в повному обсязі

Таблиця 5.4 – Рекомендовані критерії виставлення оцінок окремих показників ІБ, в яких оцінюється тільки ступінь документованості вимог ІБ

оцінка приватного показника ІБ	Критерій виставлення оцінки приватного показника ІБ
0	Вимоги приватного показника ІБ не встановлені у внутрішніх документах аудиту
1,0	Вимоги приватного показника ІБ повністю встановлені у внутрішніх документах аудиту

При проведенні оцінки часткових показників, для яких оцінюється тільки ступінь виконання (частковий показник категорії перевірки 3), використовується наступний загальний підхід (табл. 5.5):

Таблиця 5.5 – Рекомендовані критерії виставлення оцінок окремих показників ІБ, в яких оцінюється тільки ступінь виконання вимог ІБ

оцінка приватного показника ІБ	Критерій виставлення оцінки приватного показника ІБ
0	Вимоги приватного показника ІБ не виконуються
0,5	Вимоги приватного показника ІБ виконуються в неповному обсязі
1,0	Вимоги приватного показника ІБ виконуються в повному обсязі

У випадках, якщо при проведенні оцінки приватного показника використовується обмежений набір об’єктів, що входять в область оцінювання відповідності ІБ (наприклад, обмежена вибірка АБС), і за результатами оцінювання приватного показника отримані результати, що вказують на повне виконання або повне невиконання / повну документованість або відсутність документованості відповідних вимог ІБ, рекомендується розширити набір зазначених об’єктів (вибірку) для підтвердження або корекції отриманих результатів [66].

В табл. 5.6 частково наведені відповідні групові та часткові показниками ІБ, призначеними для перевірки реалізації даних вимог, повний перелік наведений у дод. Ж.

Визначимо наступні групові показники:

R_{BBI_1} – оцінка ступеня виконання вимог за напрямом “поточний рівень ІБ організації”;

R_{BBI_2} – оцінка ступеня виконання вимог за напрямом “менеджмент ІБ організації”;

R_{BBI_3} – оцінка ступеня виконання вимог за напрямом “рівень усвідомлення ІБ організації”;

OV_{ooIP} – оцінка ступеня виконання вимог, що регламентують обробку БІР;

$OV_{БІТП}$ – оцінка ступеня виконання вимог, що регламентують банківський інформаційний технологічний процес;

$OV_{БПТП}$ – оцінка ступеня виконання вимог, що регламентують банківський платіжний технологічний процес;

OV_{ozIP} – оцінка ступеня захисту БІР з використанням криптографічних ЗЗІ;

OV_{IU_i} – оцінка ступеня виконання вимог для групового показника;

$OV_{IU_{ij}}$ – оцінка ступеня виконання вимог для приватного показника;

де i – номер групового показника, j – номер приватного показника;

IU_{ij} – позначення приватного показника;

Групові показники ІБ утворюють структуру напрямків оцінки, деталізуючи оцінки поточного рівня ІБ організації, менеджменту і рівня усвідомлення ІБ.

Оцінки групових показників (OV_{IU_i}) використовуються для отримання оцінки за напрямами (R_{BBI_1}, R_{BBI_2} і R_{BBI_3}).

Приватні показники ІБ входять до складу групових показників і представлені у вигляді питань, відповіді на які дають можливість визначити оцінки $\left(OV_{IU_{ij}}\right)$, які потім формують оцінки OV_{IU_i} групових показників.

Таблиця 5.6 – Групові та часткові показниками ІБ, призначеними для перевірки реалізації даних вимог

Позначення ЧП	Частковий показник (ЧП)	Обов’язковість виконання	Категорія перевірки	Оцінка часткового показника ІБ					
				0	0,25	0,5	0,75	1	н/о
R_{BBI_2} – оцінка ступеня виконання вимог за напрямом “менеджмент ІБ організації”									
$IU_{1.1}$	упровадження процесного підходу до діяльності банку	обов’язковий	категорія 2						
...	...	...	...						
$IU_{1.20}$	застосувати заходи безпеки для захисту від атак на відмову в обслуговуванні та/або розподілених атак на відмову в обслуговуванні (*DoS/DDoS*-атак) на зовнішньому периметрі мережі банку	обов’язковий	категорія 3						
R_{BBI_3} – оцінка ступеня виконання вимог за напрямом “рівень усвідомлення ІБ організації”									
$IU_{2.1}$	визначати підходи (методики) оцінювання та оброблення ризиків інформаційної безпеки	рекомендований	категорія 1						
...	...	...	...						
$U_{2.25}$	визначити в посадових інструкціях працівників банку або організаційно-розпорядчих документах банку особисті функції та обов'язки з виявлення, класифікації, реагування і аналізу інцидентів безпеки інформації	обов’язковий	категорія 3						

Продовження таблиці 5.6

Позначення ЧП	Частковий показник (ЧП)	Обов'язковість виконання	Категорія перевірки	Оцінка часткового показника ІБ					
				0	0,25	0,5	0,75	1	н/о
OV_{ooIP} – оцінка ступеня виконання вимог, що регламентують обробку БІР									
$IU_{3.1}$	здійснити ідентифікацію змінних носіїв інформації за допомогою унікального ідентифікатора, який дозволить визначити тип носія та користувача змінного носія	обов'язковий	категорія 1						
...	...	...	...						
$IU_{3.30}$	використовувати сертифікати відкритих ключів, отримані в акредитованих/зареєстрованих ЦСК для ідентифікації та автентифікації, забезпечення конфіденційності інформації під час інформаційного обміну між інформаційними системами банку та Національного банку	обов'язковий	категорія 2						
$OV_{БІТП}$ – оцінка ступеня виконання вимог, що регламентують банківський інформаційний технологічний процес									

Продовження таблиці 5.6

Позначення ЧП	Частковий показник (ЧП)	Обов'язковість виконання	Категорія перевірки	Оцінка часткового показника ІБ					
				0	0,25	0,5	0,75	1	н/о
$IU_{4.1}$	забезпечується застосування багаторівневого (ешелонованого) підходу, за яким окремо за допомогою незалежних систем криптографічного захисту інформації захищається сеансовий рівень базової еталонної моделі взаємодії відкритих систем (*Open systems interconnection basic reference model, OSI/ISO*) та прикладний рівень моделі взаємодії відкритих систем інформаційних систем Національного банку	обов'язковий	категорія 2						
...	...	...	...						
$IU_{4.34}$	використовувати проміжний сервер для виконання функцій адміністрування чи супроводження інформаційних систем банку, мережевого обладнання та серверів	обов'язковий	категорія 2						

Кінець таблиці 5.6

Позначення ЧП	Частковий показник (ЧП)	Обов'язковість виконання	Категорія перевірки	Оцінка часткового показника ІБ					
				0	0,25	0,5	0,75	1	н/о
$OV_{БПТП}$ – оцінка ступеня виконання вимог, що регламентують банківський платіжний технологічний процес									
$IU_{5.1}$	забезпечити дотримання принципу надання мінімального рівня повноважень під час надання доступу до інформаційних систем банку (уключаючи доступ привілейованих користувачів)	обов'язковий	категорія 2						
...	...	...	...						
$IU_{5.15}$	використовувати механізми багатофакторної автентифікації під час надання доступу до САБ	обов'язковий	категорія 2						
OV_{ozIP} – оцінка захисту БІР з використанням криптографічних ЗЗІ									
$IU_{6.1}$	використовувати механізми багатофакторної автентифікації під час надання доступу для виконання функцій адміністрування або супроводження САБ	обов'язковий	категорія 1						
...	...	...	...						
$IU_{6.20}$	використовувати стандарти, документи та настанови відкритого проекту захисту веб-додатків "*Open web application security project*" (*OWASP*)	обов'язковий	категорія 2						

Оцінка групового показника (OV_{IU_i}) обчислюється з оцінок, що входять до нього часткових показників $\left(OV_{IU_{ij}}\right)$:

$$OV_{IU_i} = \frac{\sum_j IU_{ij}}{j}.$$

Оцінка ступеня виконання вимог за напрямом R_{BBI_1} "поточний рівень ІБ організації" здійснюється за виразом:

$$R_{BBI_1} = \min\left(OV_{БІТП}, OV_{БІТТП}, OV_{ooIP}, OV_{ozIP}\right),$$

де OV_{ooIP} – оцінка ступеня виконання вимог, що регламентують обробку БІР; $OV_{БІТП}$ – оцінка ступеня виконання вимог, що регламентують банківський інформаційний технологічний процес; $OV_{БІТТП}$ – оцінка ступеня виконання вимог, що регламентують банківський платіжний технологічний процес; OV_{ozIP} – оцінка ступеня захисту БІР з використанням криптографічних ЗЗІ.

Оцінка ступеня виконання вимог за напрямом "менеджмент ІБ організації" визначається виразом:

$$R_{BBI_2} = k_{R_{BBI_2}} \frac{\sum_{j=1}^{m} IU_{1j}}{j},$$

де $k_{R_{BBI_2}}$ – коригуючий коефіцієнт, визначений у табл. 5.7;

j – номер приватного показника, $j = \overline{1,...,m}$.

Оцінка ступеня виконання вимог за напрямом "рівень усвідомлення ІБ організації" визначається виразом:

$$R_{BBI_3} = k_{R_{BBI\,3}} \frac{\sum_{j=1}^{m} IU_{2j}}{j},$$

де $k_{R_{BBI\,3}}$ – коригуючий коефіцієнт, визначений у табл. 5.7;

j – номер приватного показника, $j = \overline{1,...,m}$.

Оцінка ступеня виконання вимог, що регламентують обробку БІР визначається виразом:

$$OV_{ooIP} = k_{ooIP} \frac{\sum_{j=1}^{m} IU_{3j}}{j},$$

де k_{ooIP} – коригуючий коефіцієнт, визначений у табл. 5.7;

j – номер приватного показника, $j = \overline{1,...,m}$.

Оцінка ступеня виконання вимог, що регламентують банківський інформаційний технологічний процес визначається виразом:

$$R_{OV_{БІТП}} = k_{OV_{БІТП}} \frac{\sum_{j=1}^{m} IU_{4j}}{j},$$

де $k_{OV_{БІТП}}$ – коригуючий коефіцієнт, визначений у табл. 5.7;

j – номер приватного показника, $j = \overline{1,...,m}$.

Оцінка ступеня виконання вимог, що регламентують банківський платіжний технологічний процес визначається виразом:

$$OV_{БІТТП} = k_{БІТТП} \frac{\sum_{j=1}^{m} IU_{5j}}{j},$$

де $k_{БІТТП}$ – коригуючий коефіцієнт, визначений у табл. 5.7;

j – номер приватного показника, $j = \overline{1,...,m}$.

Оцінка ступеня захисту БІР з використанням криптографічних ЗЗІ визначається виразом:

$$OV_{ozIP} = k_{ozIP} \frac{\sum_{j=1}^{m} IU_{6j}}{j},$$

де k_{ozIP} – коригуючий коефіцієнт, визначений у табл. 5.7;

j – номер приватного показника, $j = \overline{1,...,m}$.

Правила визначення коригувальних коефіцієнтів наведені у табл. 5.7.

Таблиця 5.7 – Правила визначення коригувальних коефіцієнтів

коригувальний коефіцієнт	Кількість часткових показників, оцінки яких дорівнюють нулю (Повністю не виконуються)		
$k_{R_{ВВІ_2}}$	0	1 – 15	більш 15
$k_{R_{ВВІ\,3}}$	0	1 –20	більш 20
k_{ooIP}	0	1 –25	більш 25
$k_{OV_{БІТП}}$	0	1 – 30	більш 30
$k_{БІТТП}$	0	1 – 10	більш 10
k_{ozIP}	0	1 – 15	більш 15
Значення коригуючого коефіцієнта	1	0,85	0,7

Узагальний показник рівня захищеності АБС дозволяє оцінити рівень відповідності ТЗСЗІ вимогам регуляторів та визначається:

$$OPZ^{ABS} = \sum_{i=1}^{k} OPZ_i ,$$

де k – кількість часткових показників безпеки, OPZ_i – частковий показник, що набуває значення з множини: OPZ_1 – відсутність неприпустимих ризиків, у разі якщо в ОБС при складанні моделі загроз / моделі зловмисника і оцінки ризиків (якщо виявлені неприпустимі за своїм рівнем ризики, то $OPZ_1 = 0$, в іншому випадку – $OPZ_1 = 1$); OPZ_2 – відсутність небезпечних загроз (якщо виявлені загрози “закриті” механізмами ТЗЗІ, то $OPZ_2 = 1$, у разі, якщо в ОБС при складанні моделі виявлені “незакриті” загрози – $OPZ_2 = 0$); OPZ_3 – рівень відповідності захищеності БІР вимогам регуляторів (якщо визнаний рекомендованим – $OPZ_3 = 1$, в разі, якщо визнано нерекомендованим – $OPZ_3 = 0$).

Етап 3. оцінювання ефективності інвестицій в забезпечення безпеки БІР.

На основі результатів узагальненого показника рівня захищеності OPZ^{ABS}, узагальненої синергетичної загрози $W_{synerg}^{IB,KB,BI}$, множини активів БІР

$I_{A_i} = \left(Type, A^C, A^I, A^A, A^{Au}, C_Y\right)$ та запропонованої моделі оцінювання безпеки банківських інформаційних ресурсів, яка враховує комплексний показник ефективності інвестицій, що виділяються на забезпечення безпеки БІР в умовах дії гібридних загроз визначається комплексний показник ефективності інвестицій в безпеку БІР ОБС. Формально модель оцінювання безпеки банківських інформаційних ресурсів, яка ґрунтується на комплексному показнику ефективності інвестицій, що виділяються на забезпечення безпеки БІР описується виразом:

$$W_{ABS}^{effinv} = \begin{Bmatrix} I_{O^{ABS}}, \Delta^{ABS}, \left\{DF^{ABS}\right\}, rang^{ABS}, \left\{SZ^{ABS}\right\}, d^{ABS}, D^{ABS} \\ ROI^{ABS}, NPV^{ABS}, ROSI^{ABS}, r^{ABS}, CV^{ABS}, OU^{ABS} \end{Bmatrix},$$

де $I_{O^{ABS}}$ – значення інформаційного активу; Δ^{ABS} – ознака ефективності витрат; $\left\{DF^{ABS}\right\}$ – множина джерел загроз безпеці БІР; $rang^{ABS}$ – вартість процесу розробки ТЗЗІ; $\left\{SZ^{ABS}\right\}$ – множина ТЗЗІ; d^{ABS} – зведена вартість грошового потоку; ROI^{ABS} – коефіцієнт повернення інвестицій; NPV^{ABS} – чиста зведена вартість; $ROSI^{ABS}$ – рентабельність інвестицій в ТЗЗІ; r^{ABS} – коефіцієнт рентабельності в безпеці БІР; CV^{ABS} – ступінь ризику на одиницю середнього прибутку; D^{ABS} – прибуток від використання ТЗЗІ; OU^{ABS} – оцінка прибутку від використання ТЗЗІ.

Стан моделі ефективності інвестицій в безпеку БІР ОБС (рис. 5.4):

Крок 1. Оцінювання рівня прибутковості інвестицій в побудову системи безпеки банківських інформаційних ресурсів:

$$ROI^{ABS} = NPV_{inv}^{ABS} - NPV_{zt}^{ABS},$$

де NPV_{inv}^{ABS} – прибуток від інвестицій в ТЗЗІ АБС;

NPV_{zt}^{ABS} – витрати в ТЗЗІ АБС;

ROI^{ABS} – прибутковість інвестицій в ТЗЗІ АБС.

Крок 2. Оцінювання рентабельності інвестицій в ТЗЗІ:

$$ROSI^{ABS} = NPV_{zbtszi}^{ABS} - NPV_{zvtszi}^{ABS},$$

де NPV_{zbtszi}^{ABS} – витрати на усунення компрометації безпеки без застосування ТЗЗІ;

NPV_{zvtszi}^{ABS} – витрати на усунення компрометації безпеки з застосуванням ТЗЗІ.

Крок 3. Оцінювання чистої зведеної вартості:

$$NPV_{zvtszi}^{ABS} = C_{sz} + \sum_{i=1}^{N} \frac{ALE_i}{(1+r)^i},$$

де N – кількість інтервалів інвестування;

ALE_i – очікувані витрати в i-му періоді;

r – ставка дисконтування;

C_{sz} – вартість засобів захисту.

Крок 4. Оцінювання ризику БІР за методикою розрахунку *Annual loss expectancy – ALE*, тобто очікуваних витрат у кожен період оцінки:

$$ALE^{ABS} = \sum_{i=1}^{n} I\left(O_{DF}^{ABS}\right) F_i,$$

де $\left\{O_{DF}^{ABS}\right\}$ – множина загроз; $I\left(O_{DF}^{ABS}\right)$ – вартісні наслідки реалізації загрози;

ALE^{ABS} – очікувана шкода від реалізації загрози;

F_i – частота (можливість) реалізації загрози.

Крок 5. Оцінювання потенційних збитків U^{ABS} інформаційного активу:

$$U^{ABS} = p_{rj} u_j,$$

де p_{rj} – ймовірність реалізації хоча б однієї загрози j-му активу;

u_j – цінність j-го активу.

Крок 6. Оцінювання потенційних збитків U^{ABS} інформаційного активу БІР:

$$OU^{ABS} = \sum_{j=1}^{n} U^{ABS}.$$

Отримані дані надходять на 1-й рівень моделі стратегічного управління банком для прийняття рішення щодо стану безпеки БІР $S^{ABS} = \left\{S_1^{ABS}, S_2^{ABS}, ..., S_m^{ABS}\right\}$.

Етап 4. Побудова інтегрованих механізмів забезпечення конфіденційності, цілісності, автентичності та достовірності БІР. На основі оцінок ефективності ТЗЗІ в АБС для забезпечення конфіденційності, цілісності БІР запропоновані нові механізми на основі гібридних крипто-кодових конструкцій на збиткових кодах, які дозволяють будувати несиметричні криптосистеми на основі МНККС Мак-Еліса з *MEC* (укороченими або подовженими), що забезпечують відповідний рівень безпеки та достовірність БІР (рис. 5.4). Використання збиткових кодів дозволяє зменшити енергетичні затрати при практичній реалізації МНККС Мак-Еліса шляхом зменшення потужності алфавіту *GF(q)* без зменшення загальної стійкості криптосистеми в цілому та використовувати багатоканальну криптографію.

Для модифікації еліптичного коду, що не зменшує мінімальну кодову відстань, використовується скорочення його довжини шляхом скорочення інформаційних символів.

$I=(I_1, I_2, \ldots, I_k)$ – інформаційний вектор (n, k, d) блокового коду, підмножина h інформаційних символів, $h=x$, $x \leq 1/2k$ визначає нульові символи.

При кодуванні інформаційного вектора символи множини h не застосовуються (вони нульові) і їх можна відкинути, а отримане кодове слово буде коротше на x кодових символів.

Другий спосіб модифікації використовує збільшення довжини шляхом формування вектора ініціалізації (визначення символів скорочення) і заміни нульових символів символами інформаційного вектора.

Для нанесення збитку використовуємо універсальний механізм нанесення збитку C_m:

$$CFT / CH_{FT} = E_1\left(M, KU^{EC}\right),$$
$$CHD / CH_D = E_2\left(M, KU^{EC}\right),$$
$$M = E_{1,2}^{-1}(CFT / CH_{FT}, CHD / CH_D, KU^{EC}),$$

де $CFT / CH_{FT} = CFT / CH_{FT}^i, \ldots, CFT / CH_{FT}^m,$

$KU^{EC} = \varphi(K_D^i, \ldots, K_D^m, KU_1^{EC}, \ldots, KU_m^{EC},$

$CHD / CH_D = CHD / CH_D^i, \ldots, CHD / CH_D^m$.

Таким чином, шифртекст вихідного повідомлення (*M*) в результаті має два шифртексти (збиток (*CHD*) і збитковий текст (*FTC*)), кожен з яких окремо не може відновити вихідний текст.

Основні властивості *МЕС* наведені у табл. 5.8, основні параметри МНККС в табл. 5.9. Протоколи обміну БІР з застосуванням ГКККЗК на укорочених та подовжених *МЕС* наведені на рис. 5.5, 5.6 відповідно.

Таблиця 5.8 – Основні *(n, k, d)* властивості *МЕС*

Властивість	Укорочені *МЕС*	Подовжені *МЕС*
(n, k, d) параметри коду, який побудований через відображення виду $\varphi: X \to P^{k-1}$	$n = 2\sqrt{q} + q + 1 - x$, $k \geq \alpha - x$, $d \geq n - \alpha$, $\alpha = 3 \times degF$, $k + d \geq n$	$n = 2\sqrt{q} + q + 1 - x + x_1$, $k \geq \alpha - x + x_1$, $d \geq n - \alpha$, $\alpha = 3 \times degF$
n, k, d) параметри коду, який побудований через відображення виду $\varphi: X \to P^{r-1}$	$n = 2\sqrt{q} + q + 1 - x$, $k \geq n - \alpha$, $d \geq \alpha$, $\alpha = 3 \times degF$, $k + d \geq n$	$n = 2\sqrt{q} + q + 1 - x + x_1$, $k \geq n - \alpha$, $d \geq \alpha$, $\alpha = 3 \times degF$

Таблиця 5.9 – Основні параметри МНККС Мак-Еліса на *МЕС*

Властивість	Укорочені *МЕС*	Подовжені *МЕС*
розмірність секретного ключа	$l_{K+} = x \times \left\lceil \log_2 \left(2\sqrt{q} + q + 1 \right) \right\rceil$	$l_{K+} = (x - x_1) \times \log_2 \left(2\sqrt{q} + q + 1 \right)$
розмірність інформаційного вектора	$l_I = (\alpha - x) \times m$	$l_I = (\alpha - x + x_1) \times m$
розмірність криптограми	$l_S = \left(2\sqrt{q} + q + 1 - x \right) \times m$	$l_S = \left(2\sqrt{q} + q + 1 - x + x_1 \right) \times m$
відносна швидкість передачі	$R = (\alpha - x) / \left(2\sqrt{q} + q + 1 - x \right)$	$R = (\alpha - x + x_1) / \left(2\sqrt{q} + q + 1 - x + x_1 \right)$

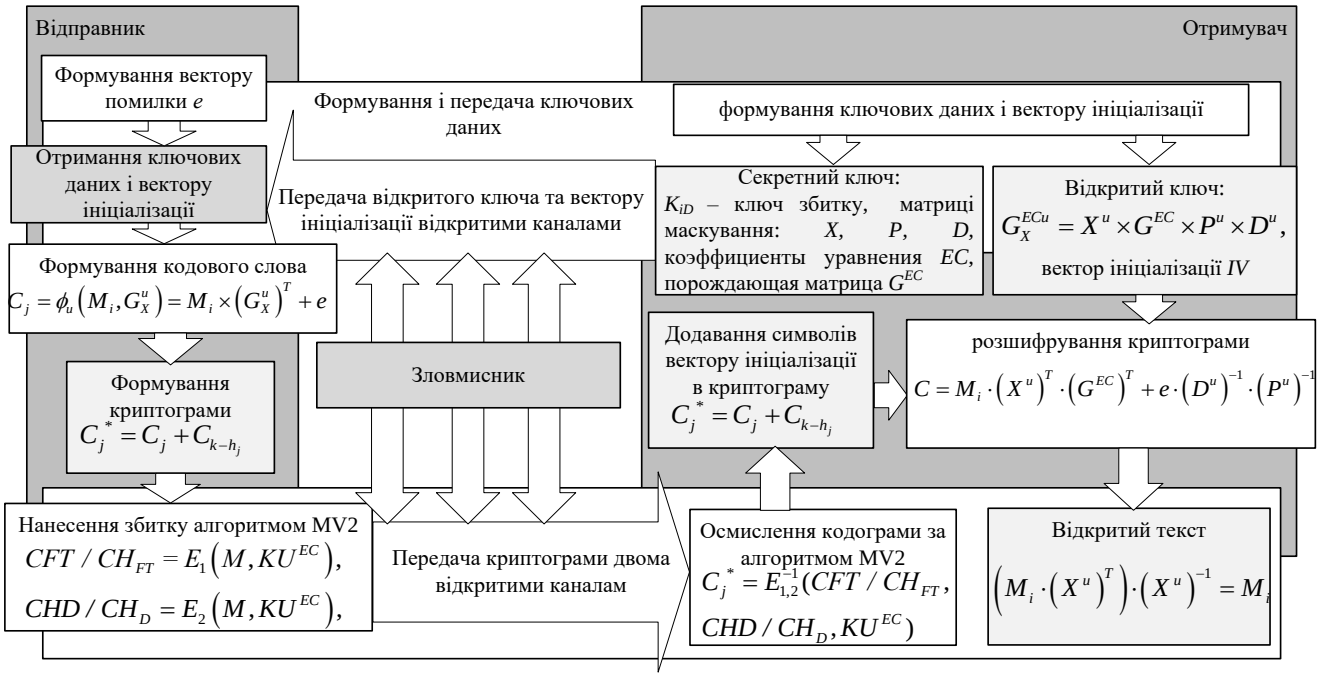


Рисунок 5.5 – Структурна схема протоколу забезпечення конфіденційності й цілісності БІР на основі ГКККЗК з укороченими *MEC*

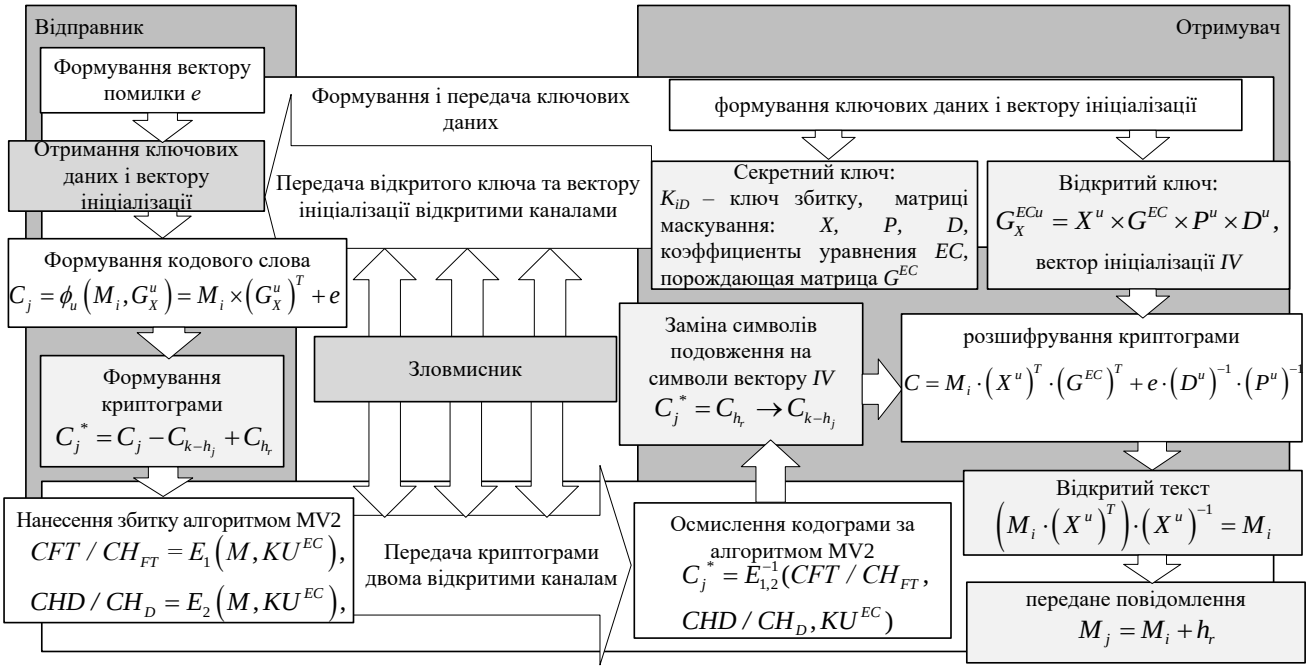


Рисунок 5.6 – Структурна схема протоколу забезпечення конфіденційності й цілісності БІР на основі ГКККЗК з подовженими *MEC*

Для забезпечення автентичності БІР пропонується використовувати модифіковану схему двофакторної автентифікації на основі *OTP*-паролів з використанням ГКККЗК на МНККС Мак-Еліса і Нідеррайтера.

Структурна схема протоколу вдосконаленого методу *OTP*-автентифікації на основі ГККККЗК наведена на рис. 5.7 [60].

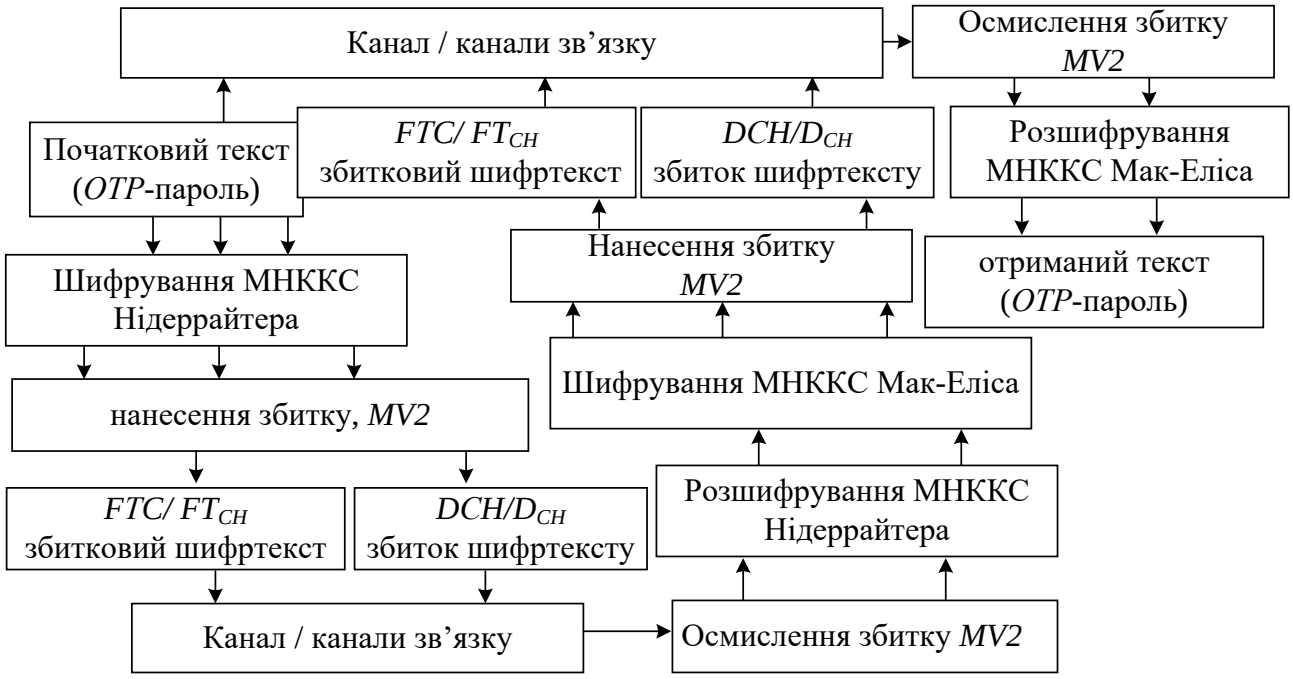


Рисунок 5.7 – Структурна схема протоколу вдосконаленого методу *OTP*-автентифікації на основі ГККККЗК

Використання гібридних крипто-кодових конструкцій на збиткових кодах дозволяє збільшувати кількість токенів автентифікатора, використовувати дві несиметричні крипто-кодові системи, два / чотири канали передачі збиткового тексту автентифікатора і збитку. Масштабованість програмного модуля шляхом зміни параметрів МНККС Нідеррайтера і / або Мак-Еліса залежно від висунутих вимог до комунікаційних каналах АБС, забезпечує його програмну реалізацію в мобільних гаджетах і сумісність з протоколами, що використовуються для передачі даних в Інтернет і мобільних мережах.

Етап 5. Визначення стану та формування стратегій безпеки БІР.

На заключному етапі реалізується трирівнева стратегія управління безпекою БІР (рис. 5.4).

Перший рівень описує загальну корпоративну стратегію банку та його функціональні стратегії. Корпоративна стратегія визначає перспективи розвитку та сприяє виконанню основної місії банку. На цьому рівні відповідно до

синергетичного підходу розглядається загальна концепція забезпечення безпеки інформаційних технологій АБС і формуються цілі і завдання забезпечення КБ, а також визначається стан безпеки БІР $S^{ABS} = \left\{ S_1^{ABS}, S_2^{ABS}, ..., S_m^{ABS} \right\}$.

Функціональні стратегії одного рівня мають горизонтальні зв'язки і узгоджуються на рівні цілей з подальшою деталізацією на наступному рівні стратегічного набору.

На *другому рівні* формується корпоративна стратегія безпеки БІР – $\left\{ RR^{ABS} \right\} = \left\{ R_{BBI} \right\} \cup \left\{ OV_{BBI} \right\} \cup \left\{ IU_{BBI} \right\}$, визначаються цілі та завдання основних бізнес-процесів, пов'язаних із захистом персональних даних юридичних і фізичних клієнтів банку.

Корпоративна стратегія безпеки описує, яким чином слід керувати і координувати зусилля за різними аспектами безпеки. Вона розвивається у формі функціональних стратегій: фінансової, економічної, фізичної та ІБ.

На *третьому рівні* проводиться деталізація функціональних стратегій другого рівня стратегічного набору, формується корпоративна стратегія безпеки інформації. Серед основних напрямків щодо захисту доцільно виділити кадрову безпеку, фізичну безпеку, мережеву та БІ. На цьому рівні визначається відповідність між застосованими ТЗСЗІ та загрозами ІБ, КБ, БІ на БІР – $OPZ^{ABS} = \sum_{i=1}^{k} OPZ_i$.

Стратегія ІБ є важливою функцією керівництва банку в сфері безпеки і повинна формуватися і проводиться вищим керівництвом банку.

Концепція стратегічного управління безпекою ІТ АБС України на основі трирівневої моделі і синергетичної моделі загроз на відміну від відомих охоплює всі основні напрямки розвитку діяльності банку щодо безпеки БІР.

Запропонована концепція ґрунтується на синергетичному підході до вибору найбільш ефективних напрямків досягнення поставлених цілей безпеки БІР з урахуванням величини ризику на кожному рівні моделі стратегічного управління

банком. Описаний підхід дозволяє комплексно проводити відбір альтернативних варіантів можливих стратегічних рішень з питань безпеки.

Запропонована методологія побудови системи безпеки БІР на відміну від відомих підходів реалізовує принципово нову концепцію протидії гібридним загрозам банківського сектору. Її сутність та зміст полягають в раціональній організації системи безпеки БІР в умовах одночасної дії на систему загроз інформаційній безпеці, кібербезпеці та безпеці інформації.

Методологія ґрунтується на вперше запропонованій трирівневій моделі стратегічного управління безпекою інформаційних технологій в АБС. Її основу складає вперше введена синергетична модель загроз безпеці БІР, що дозволила удосконалити відому модель зловмисника безпеки БІР.

На основі розробленої методології удосконалений класифікатор загроз безпеці в частині, що стосується одночасного урахування в ньому, крім загроз інформаційній безпеці, загроз кібербезпеці та загроз безпеці інформації БІР. Впровадження класифікатора дозволило зробити висновок про те, що для протидії гібридним загрозам БІР доцільно застосовувати нові інтегровані механізми забезпечення послуг на основі ГКККЗК, які також розробляються відповідно до запропонованої методології.

Запропоновані ГКККЗК ґрунтуються на криптографічних перетвореннях завадостійкого і збиткового кодування, що дозволило гарантувати послуги безпеки при заданих їх ймовірнісних показниках. Так, швидкість криптоперетворень забезпечено на рівні швидкості криптоперетворень БСШ, криптостійкість на рівні 10^{25}–10^{35} групових операцій, достовірність передачі БІР відкритими каналами зв’язку не нижче $P_{пом}$ 10^{-9}–10^{-12}.

Подана методологія є дієвим інструментом для розроблення практичних застосунків у вигляді програмних та програмно-апаратних засобів, що реалізують визначену системою безпеки БІР політику безпеки. Практичне зазначення методології підтверджено відповідними актами впровадження.

5.3. Експеримент

Експеримент здійснено з дотриманням основних вимог, що висуваються до його проведення, а саме: розроблено план експерименту, програму експерименту та приведено аналіз його результатів.

Розглянемо послідовно визначені пункти.

До плану експерименту включено:

1) мету експерименту;
2) завдання експерименту:
3) обґрунтування вибору множини загроз на БІР;

Метою експерименту є перевірка адекватності методики оцінювання ефективності функціонування АБС на основі комплексного показника оцінювання якості обслуговування об’єктів автоматизованої банківської системи щодо відбору альтернативних варіантів можливих стратегічних рішень з питань безпеки. *Об’єктом дослідження* визначено рівень загроз на складові безпеки (ІБ, КБ, БІ) БІР, що забезпечує мінімізацію інвестицій в побудову систем безпеки БІР.

Основними завданнями експерименту визначено такі:

– визначення ймовірності впливу загроз ІБ, КБ, БІ на безпеку БІР;

– визначення залежностей між елементами інфраструктури АБС, інформаційними активами БІР, загрозами ІБ, КБ, БІ та ТЗЗІ на основі удосконаленої моделі інфраструктури АБС, синергетичної моделі загроз, удосконаленої моделі зловмисника;

– визначення узагальненого показника рівня безпеки БІР на основі удосконаленої моделі оцінювання рівня захищеності БІР;

– оцінювання інвестицій в безпеку БІР, яка відрізняється від відомих комплексованих економічних показників інвестицій в безпеку БІР з урахуванням гібридності та синергізму атак на складові безпеки (ІБ, КБ, БІ);

– дослідження адекватності методики оцінювання ефективності функціонування АБС на основі комплексного показника оцінювання якості обслуговування об’єктів автоматизованої банківської системи щодо відбору альтернативних варіантів можливих стратегічних рішень з питань безпеки.

Обґрунтування вибору множини загроз на БІР. Керуючись створеною методологією побудови систем безпеки IP автоматизованих банківських систем (рис. 5.3, 5.4) як множину загроз на БІР виберемо загрози з веб-ресурсу (http://bdu.fstec.ru/threat) [61] рис. 5.8.

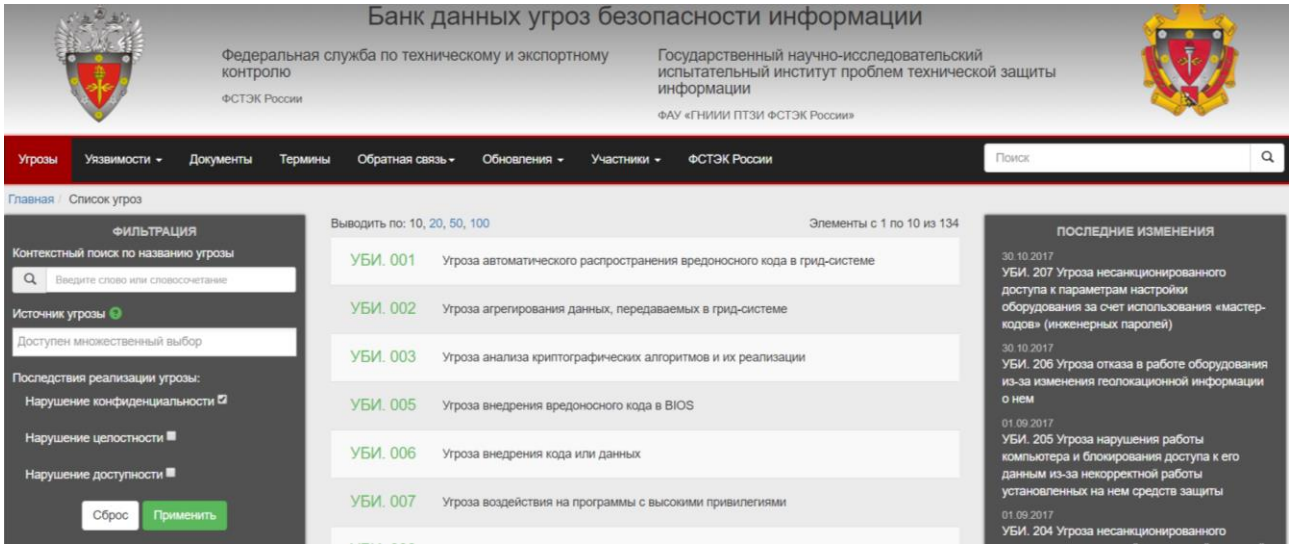


Рисунок 5.8 – Вибір множини загроз з ресурсу “Банк даних загроз безпеці інформації”

Розроблений **програмний ресурс експерименту** регламентує порядок його організації та проведення:

Етап 1. *Визначення ймовірності впливу загроз ІБ, КБ, БІ на безпеку БІР:*

Крок 1. Формування метричних коефіцієнтів загроз експертами за послугами безпеки:

$$w^j = \frac{1}{K}\sum_{i=1}^{N}\sum_{k=1}^{K} w_{ik}^j , \qquad (5.7)$$

де w_{ik}^j – значення метричного коефіцієнта, виставленого k-м експертом для i-ї загрози j-ї послуги безпеки; N – кількість загроз; K – кількість експертів.

На рис. 5.9 наведена таблиця побудови метричних коефіцієнтів за складовими послуг безпеки за всіма загрозами на БІР у програмному ресурсі (http://skl.hneu.edu.ua/).

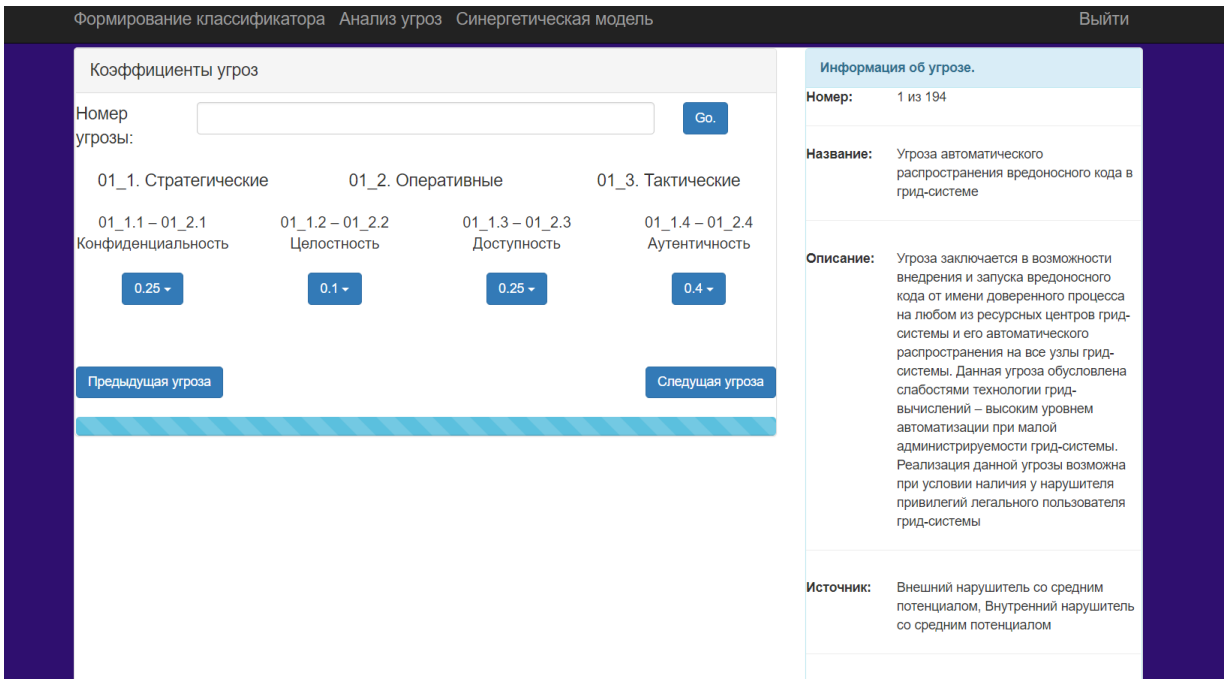


Рисунок 5.9 – Формування метричних коефіцієнтів загроз експертами

На основі введеної метрики розраховуються основні показники метрики загроз: математичне сподівання – μ i-ї загрози, $i \in [1; N]$, де N – кількість загроз у класифікаторі; дисперсія – σ i-ї загрози, $i \in [1; N]$. При розрахунках враховується можливість отримання в класифікаторі залежних загроз (коди загроз збігаються), тоді спочатку знаходиться повна ймовірність залежних загроз, а після цього обчислюються основні показники для незалежних загроз. У додатку Е наведені результати дослідження загроз БІР на основі запропонованого класифікатору, (рис. 5.10 – 5.13).

Крок 1.2. Формування ідентифікаторів загроз за складовими класифікатора. На даному кроці експерти формують цифрове значення (код) ідентифікатора загрози за відповідними складовими класифікатора. Складовими класифікатора є:

– складова безпеки БІР ОБС: ІБ (01), БІ (02), КБ (03);

– характер напрямків: нормативно-правовий (01), організаційний (02), інженерно-технічний (03);

– основні особливості інформації: конфіденційність (01), цілісність (02), доступність (03), автентичність (04);

– рівні ієрархії інфраструктури АБС: *FL* – фізичний рівень (01), *NL* – мережевий рівень (02), *OSL* – рівень операційних систем (ОС) (03), *DBL* – рівень систем управління базами даних (04), *BL* – рівень банківських технологічних застосунків і сервісів (05) (рис. 5.10).

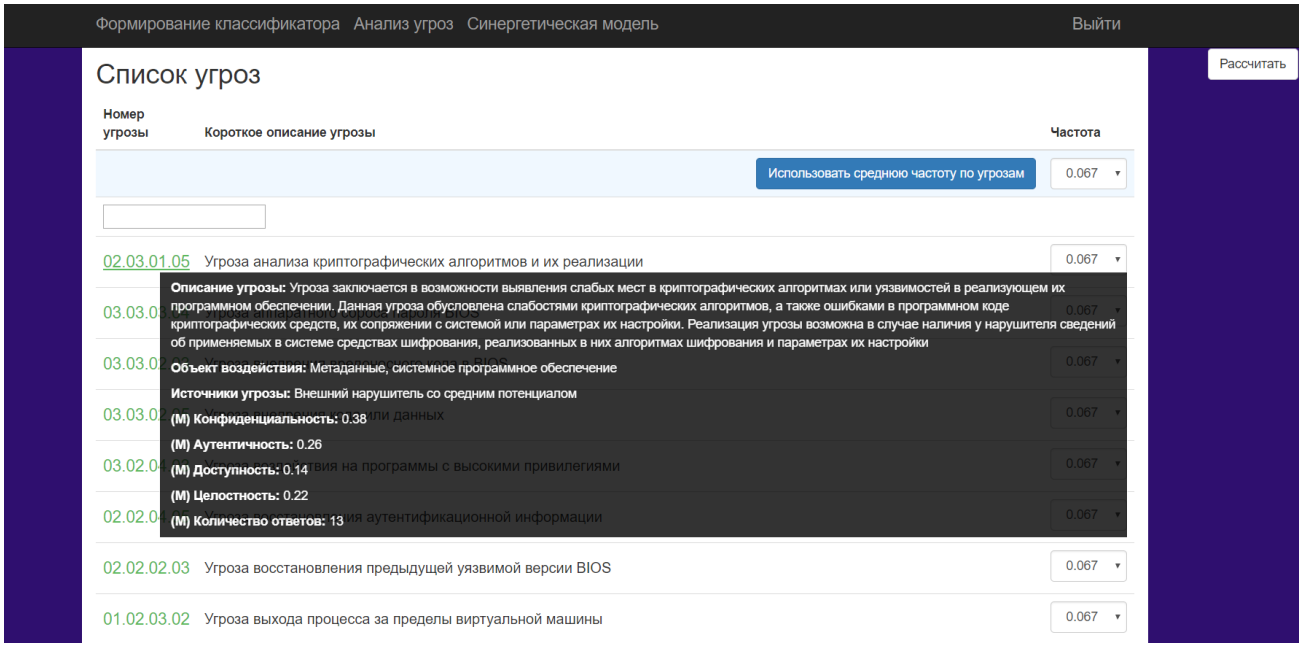


Рисунок 5.10 – Формування класифікатора за складовими

Крок 1.3 Вибір вагових коефіцієнтів α_i, що визначають умови прояву *i*-ї загрози (табл. 5.10), (рис. 5.11). Запропоноване значення вагових коефіцієнтів α_i виникнення *i*-ї загрози визначається на основі метрики експертів за кожною складовою послуги безпеки, з ранжуванням отриманого результату.

Таблиця 5.10 – Таблиця визначення ймовірності виникнення загроз залежно від частоти їх прояву

Вагові коефіцієнти α_i	Умови прояву загрози
0,067	загроза проявляється не частіше одного разу на 5 років
0,133	загроза проявляється не частіше одного разу на рік
0,2	загроза проявляється не частіше одного разу місяць
0,267	загроза проявляється не частіше одного разу на тиждень
0,333	загроза проявляється щодня

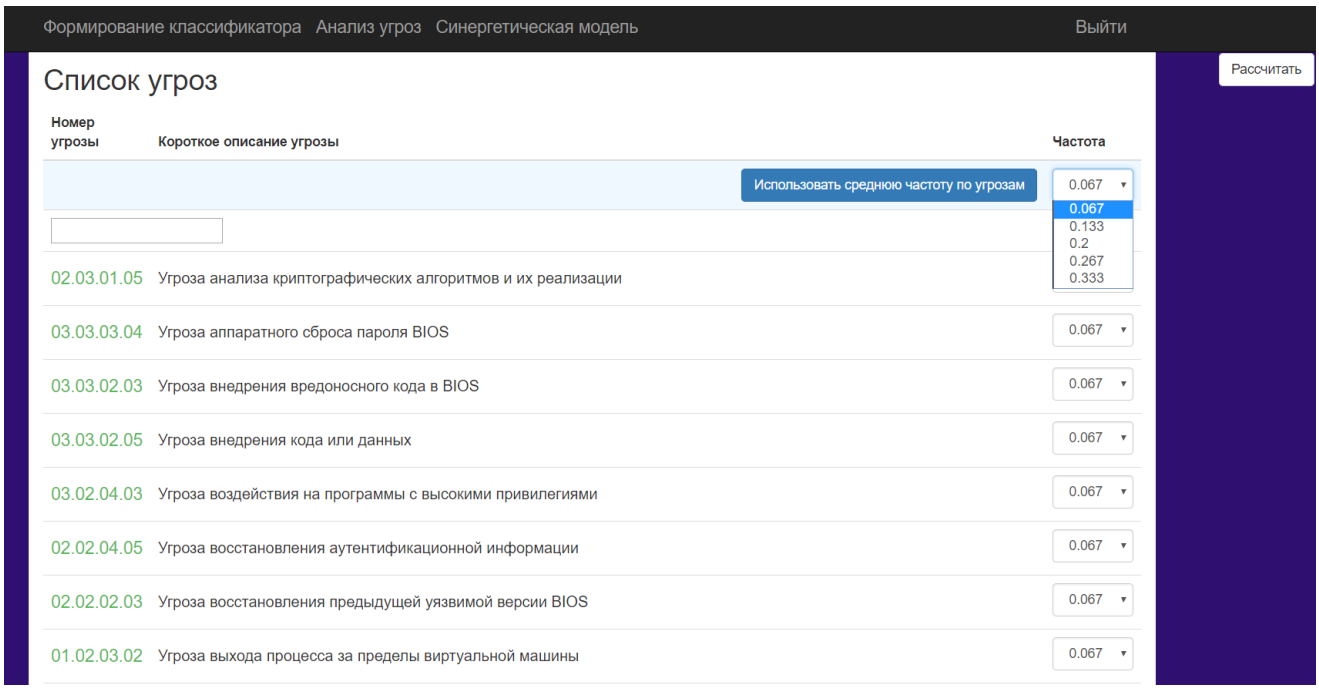


Рисунок 5.11 – Вибір вагових коефіцієнтів α_i, що визначають умови прояву *i*-ї загрози

Крок 1.4. Визначення реалізації кожної *i*-ї загрози з урахуванням імовірності прояву атаки її виникнення здійснюється за виразом:

$$w_i^j P_i^j = \frac{1}{K} P_i^j \sum_{k=1}^{N} w_{ik}^j. \tag{5.8}$$

Для кожної послуги безпеки та *i*-ї загрози:

$$w_i^C \alpha_i^C = \frac{1}{K} \alpha_i^C \sum_{k=1}^{K} w_{ik}^C \text{ – послуга конфіденційність;}$$

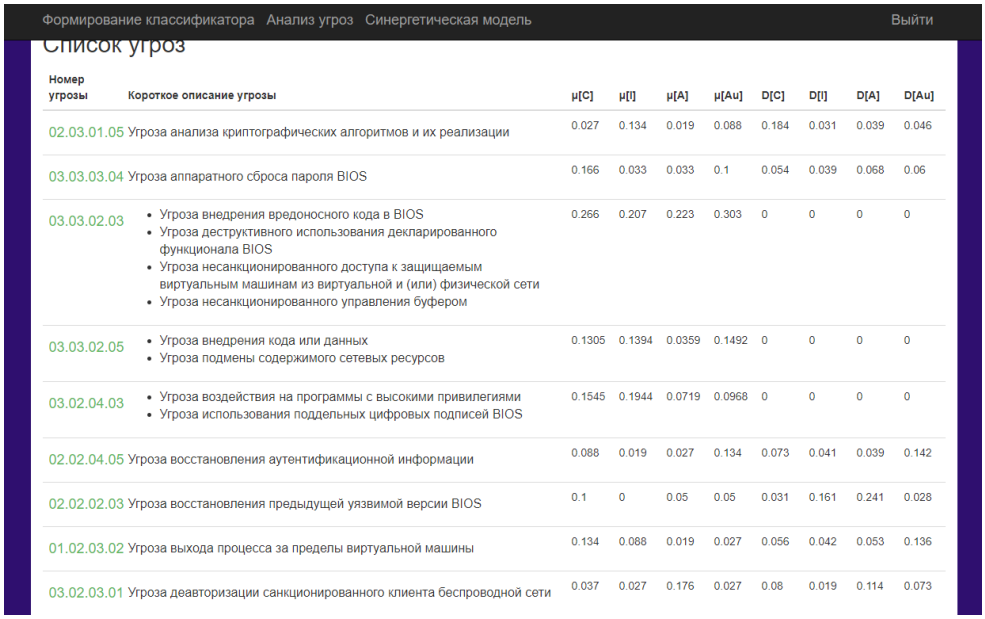
$$w_i^I \alpha_i^I = \frac{1}{K} \alpha_i^I \sum_{k=1}^{K} w_{ik}^I \text{ – послуга цілісність;}$$

$$w_i^A \alpha_i^A = \frac{1}{K} \alpha_i^A \sum_{k=1}^{K} w_{ik}^A \text{ – послуга доступність;}$$

$$w_i^{Au} \alpha_i^{Au} = \frac{1}{K} \alpha_i^{Au} \sum_{k=1}^{K} w_{ik}^{Au} \text{ – послуга автентичність,}$$

де w_{ik}^C, w_{ik}^I, w_{ik}^A, w_{ik}^{Au} – експертні вагові коефіцієнти послуг безпеки: конфіденційності, цілісності, доступності, автентичності; α_i^C, α_i^I, α_i^A, α_i^{Au} –

ваговий коефіцієнт послуги безпеки: конфіденційності, цілісності, доступності, автентичності прояву атаки *i*-ій загрози, (див. рис. 5.12).



Номер угрозы	Короткое описание угрозы	μ[C]	μ[I]	μ[A]	μ[Au]	D[C]	D[I]	D[A]	D[Au]
02.03.01.05	Угроза анализа криптографических алгоритмов и их реализации	0.027	0.134	0.019	0.088	0.184	0.031	0.039	0.046
03.03.03.04	Угроза аппаратного сброса пароля BIOS	0.166	0.033	0.033	0.1	0.054	0.039	0.068	0.06
03.03.02.03	• Угроза внедрения вредоносного кода в BIOS • Угроза деструктивного использования декларированного функционала BIOS • Угроза несанкционированного доступа к защищаемым виртуальным машинам из виртуальной и (или) физической сети • Угроза несанкционированного управления буфером	0.266	0.207	0.223	0.303	0	0	0	0
03.03.02.05	• Угроза внедрения кода или данных • Угроза подмены содержимого сетевых ресурсов	0.1305	0.1394	0.0359	0.1492	0	0	0	0
03.02.04.03	• Угроза воздействия на программы с высокими привилегиями • Угроза использования поддельных цифровых подписей BIOS	0.1545	0.1944	0.0719	0.0968	0	0	0	0
02.02.04.05	Угроза восстановления аутентификационной информации	0.088	0.019	0.027	0.134	0.073	0.041	0.039	0.142
02.02.02.03	Угроза восстановления предыдущей уязвимой версии BIOS	0.1	0	0.05	0.05	0.031	0.161	0.241	0.028
01.02.03.02	Угроза выхода процесса за пределы виртуальной машины	0.134	0.088	0.019	0.027	0.056	0.042	0.053	0.136
03.02.03.01	Угроза деавторизации санкционированного клиента беспроводной сети	0.037	0.027	0.176	0.027	0.08	0.019	0.114	0.073

Рисунок 5.12 – Результати оцінювання основних показників кожної загрози (μ, σ)

Крок 1.5. Визначення реалізації виникнення декількох загроз для обраної послуги розраховується з урахуванням виразу (5.8):

$$W_{synerg}^{C} = \sum_{i=1}^{M} w_i^C \alpha_i^C = 0.009 + 0.142 + 0.099 = 0.25 \text{ – послуга конфіденційність;}$$

$$W_{synerg}^{I} = \sum_{i=1}^{M} w_i^I \alpha_i^I = 0.112 + 0.155 + 0.061 = 0.328 \text{ – послуга цілісність;}$$

$$W_{synerg}^{A} = \sum_{i=1}^{M} w_i^A \alpha_i^A = 0.108 + 0.123 + 0.088 = 0.319 \text{ – послуга доступність;}$$

$$W_{synerg}^{Au} = \sum_{i=1}^{M} w_i^{Au} \alpha_i^{Au} = 0.126 + 0.047 + 0.141 = 0.314 \text{ – послуга автентичність,} \qquad (5.9)$$

де M – загальна кількість загроз в класифікаторі.

Крок. 1.6. Визначення узагальненої синергетичної загрози на БІР з урахуванням виразу (5.9) розраховується:

$$W_{synerg}^{IB} = \sum_{i=1}^{N} \left(w_i^C \cap w_i^I \cap w_i^A \cap w_i^{Au} \right) P_i = 0.009 \times 0.112 \times 0.108 \times 0.126 = 0.0000137,$$

$$W_{synerg}^{KB} = \sum_{i=1}^{N} \left(w_i^C \cap w_i^I \cap w_i^A \cap w_i^{Au} \right) P_i = 0.142 \times 0.155 \times 0.123 \times 0.047 = 0.0001272,$$

$$W_{synerg}^{BI} = \sum_{i=1}^{N}\left(w_i^C \cap w_i^I \cap w_i^A \cap w_i^{Au}\right)P_i = 0.099 \times 0.061 \times 0.088 \times 0.141 = 0.0000749. \quad (5.10)$$

Крок. 1.7. Визначення узагальненої синергетичної загрози на БІР:

$$W_{synerg}^{IB,KB,BI} = W_{synerg}^{IB} \bigcup W_{synerg}^{KB} \bigcup W_{synerg}^{BI} = 0,0002 + 0,0014 + 0,0007 = \mathbf{0.000216}. \quad (5.11)$$

Крок 1.8. Визначення узагальненої синергетичної загрози з урахуванням її гібридності розраховується, (рис. 5.13, табл. 5.11):

$$W_{synerg}^{\text{hybrid } C,I,A,Au} = W_{synerg}^{C} \bigcap W_{synerg}^{\text{I}} \bigcap W_{synerg}^{A} \bigcap W_{synerg}^{Au} = 0,471 \times 0,566 \times 0,542 \times 0,53 = \mathbf{0.008214}. \quad (5.12)$$

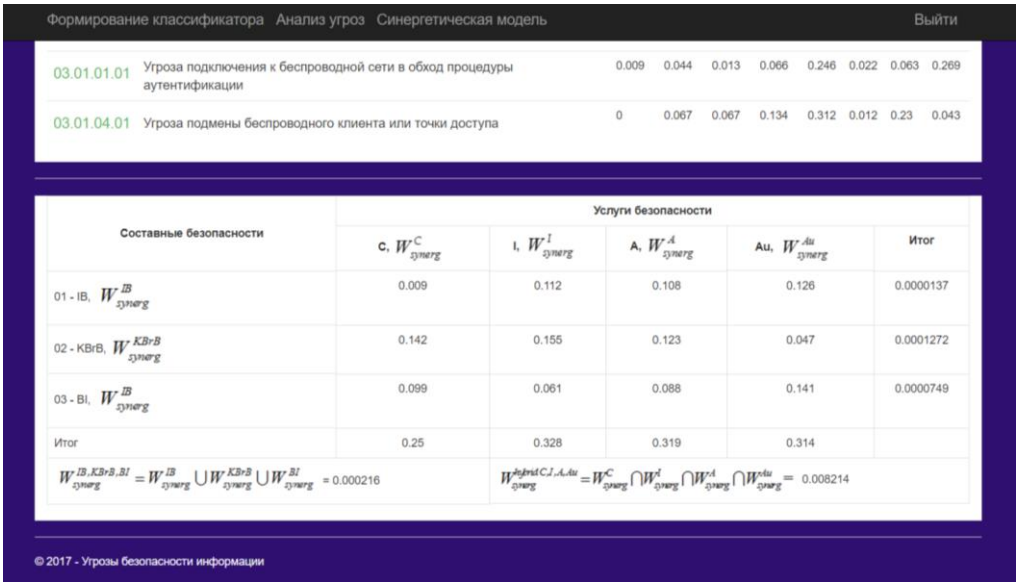


Рисунок 5.13 – Результати оцінки загроз на основі синергетичного підходу

Таблиця 5.11 – Результати оцінки загроз на основі синергетичного підходу

Складові безпеки	Послуги безпеки				
	C, W_{synerg}^{C}	*I*, W_{synerg}^{I}	*A*, W_{synerg}^{A}	*Au*, W_{synerg}^{Au}	Підсумок
IB, W_{synerg}^{IB}	0.009	0.112	0.108	0.126	0.0000137
KB, W_{synerg}^{KB}	0.142	0.155	0.123	0.047	0.0001272
BI, W_{synerg}^{BI}	0.099	0.061	0.088	0.141	0.0000749
Підсумок	0.25	0.328	0.319	0.314	
$W_{synerg}^{IB,KB,BI} = W_{synerg}^{IB} \bigcup W_{synerg}^{KB} \bigcup W_{synerg}^{BI} =$ =0,0002+0,0014+0,0007= **0.000216**			$W_{synerg}^{\text{hybrid } C,I,A,Au} = W_{synerg}^{C} \bigcap W_{synerg}^{I} \bigcap W_{synerg}^{A} \bigcap W_{synerg}^{Au} =$ = 0,471×0,566×0,542×0,53= **0.008214**		

Етап 2. *Визначення залежностей між елементами інфраструктури АБС, інформаційними активами БІР, загрозами ІБ, КБ, БІ та ТЗЗІ на основі удосконаленої моделі інфраструктури АБС, синергетичної моделі загроз, удосконаленої моделі зловмисника*:

На основі сформованої множини загроз ІБ, КБ, БІ на БІР та моделі ієрархії АБС – $G^{ABS}=\{\{O^{ABS}\},\{L^{ABS}\},\{I_A\}\}$, де $\{O^{ABS}\}$ – множина об'єктів середовища АБС, що описують елементи АБС і їх приналежність до рівнів ієрархії АБС, формується $\{L^{ABS}\}$ – множина зв'язків між елементами АБС; $\{I_A\}$ – множина інформаційних активів БІР (див. підрозд. 2.3.1, рис. 5.14).

Крок 2.1. Визначення зв'язку між інформаційними активами БІР $\{I_A\}$ та елементами інфраструктури АБС $A^{ABS}=\left\|a_{ij}^{ABS}\right\|$. Кожен елемент $I_{A_i}\in\{I_A\}$ описується вектором $I_{A_i}=\left(Type,A^C,A^I,A^A,A^{Au},C_Y\right)$, *Type* – тип інформаційного активу, описується множиною базових значень *Type* = {*BT, PID, RrD, KT, StO, Ol, YI, PD*}, де *BT* – банківська таємниця; *PID* – платіжні документи; *KrD* – кредитні документи; *KT* – комерційна таємниця; *StO* – статистичні звіти; *Ol* – загальнодоступна інформація; *YI* – керівна інформація; *PD* – персональні дані. Значення A^C – конфіденційність; A^I – цілісність; A^A – доступність; A^{Au} – автентичність; *CY* – безперервність – властивості інформації, які необхідно забезпечувати. Вони приймають значення 1 – якщо властивість необхідно, 0 – в іншому випадку (рис. 5.14);

Крок 2.2. Визначення зв'язку між інформаційними активами $\{I_A\}$ й об'єктами середовища (рис. 5.14, табл. 5.12, 5.13). Кожен елемент $O_l\in\left\{O^{ABS}\right\}$ описується вектором $O_l=\left\{Y^{ABS},IO\right\}$, де Y^{ABS} – рівень ієрархії інформаційної структури, яка визначається множиною Y^{ABS} = {*FL, NL, OSL, DBL, BL*}, де *FL* – фізичний рівень; *NL* – мережевий рівень; *OSL* – рівень операційних систем (ОС); *DBL* – рівень систем управління базами даних; *BL* – рівень банківських технологічних застосунків і сервісів. Для визначення типу зв'язку та існуючого відношення I^{OR} між інформаційними активами БІР і об'єктами АБС використовується правило:

$$IO^R=\left\|IO_{il}^R\right\|, \tag{5.13}$$

де IO_{il}^{R} – відображає наявність і тип зв'язку між *i*-м інформаційним активом та *l*-м об'єктом середовища АБС. При цьому $\forall i \in \{I_A\}$, а $\forall l \in \{O^{ABS}\}$:

$$IO_{il}^{R} = \begin{cases} 0 \ – \text{ зв'язок відсутній;} \\ cs – \text{включає і зберігає;} \\ pt – \text{обробляє або передає;} \\ so \ – \text{ підтримує функціонування.} \end{cases}.$$

Кожному параметру присвоюються вагові категорії за правилом Фішберна [64], заснованому на тому, що зміна вагових коефіцієнтів критеріїв підкоряється спадній арифметичній прогресії.

При цьому перший критерій (*i = 1*), розташований першим в строго упорядкованому за важливістю ранжируваному ряду критеріїв *i* = 1, 2, ..., *n*, є найбільш важливим і має найбільший ваговий коефіцієнт. Це правило задається виразом:

$$w_i = \frac{2(N - n + 1)}{N(N + 1)},$$

де w_i – ваговий коефіцієнт Фішберна;
N – загальна кількість параметрів;
n – порядковий номер параметра;
i – кількість параметрів.
Відповідно до виразу Фішберна маємо:

$$w_1 = \frac{2 \times N}{N(N + 1)}, \ w_N = \frac{2}{N(N + 1)}, \ \gamma = \frac{w_1}{w_N} = N,$$

де γ – кратність відмінності вагових коефіцієнтів один від одного.

Таким чином, $cs = 0.5, \quad pt = 0.22, \quad so = 0.17.$

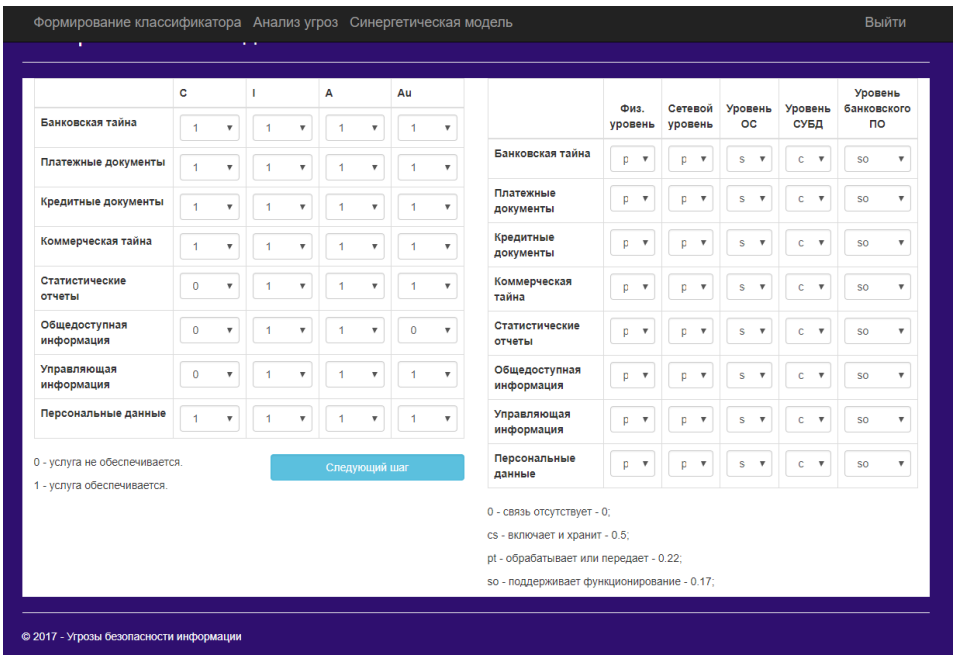


Рисунок 5.14 – Визначення взаємозв'язку між інформаційними активами БІР, послугами безпеки та елементами удосконаленої інфраструктури АБС

Крок. 2.3. Визначення комплексування множини загроз на основі синергетичної моделі загроз й удосконаленої моделі зловмисника.

Синергетична модель загроз формально описується виразом:

$$GR^{ABS} = \left\{ \left\{ DF^{ABS} \right\}, \left\{ T_{risk} \right\}, \left\{ T_P \right\}, \left\{ T_U \right\}, \left\{ VH \right\} \right\}, \tag{5.14}$$

де $\left\{ DF^{ABS} \right\}$ – множина джерел загроз; $\left\{ T_{risk} \right\}$ – якісний показник ризику; $\left\{ T_P \right\}$ – множина базових термів ймовірності реалізації хоча б однієї загрози *j*-му активу; $\left\{ T_U \right\}$ – множина базових термів величини збитку від реалізації погрози; $\left\{ VH \right\}$ – множина деструктивних станів елементів АБС.

Таблиця 5.12 – Надання послуг інформаційним активам БІР

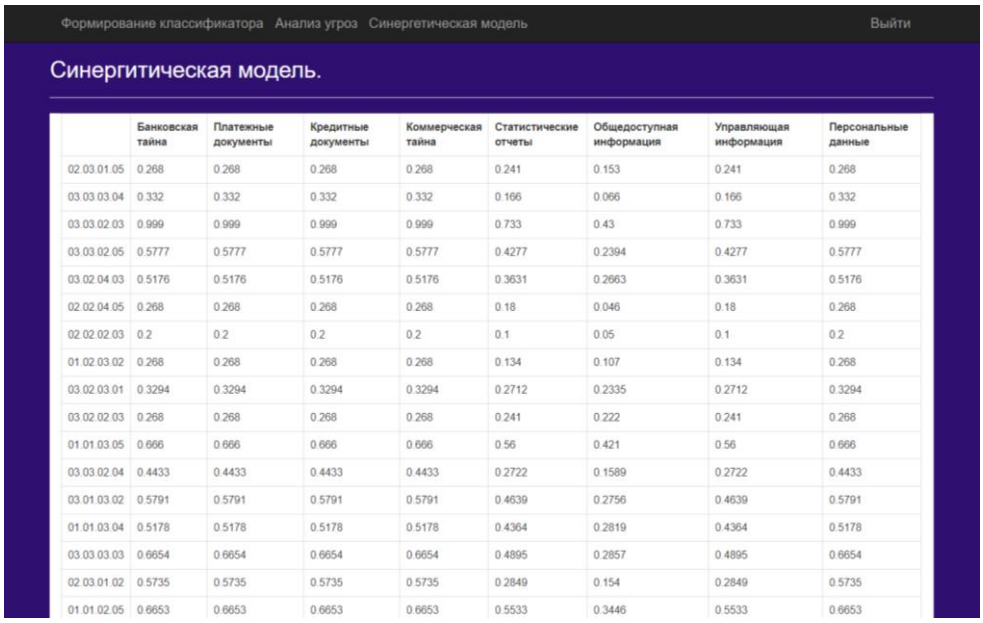
Назва, I_{A_i}	*C*	*I*	*A*	*Au*
BT	1	1	1	1
PID	1	1	1	1
KrD	1	1	1	1
KT	1	1	1	1
StO	0	1	1	1
Ol	0	1	1	0
YI	0	1	1	1
PD	1	1	1	1

Таблиця 5.13 – Взаємозв'язок інформаційних активів БІР з елементами узагальненої інфраструктури АБС

Назва, I_{A_i}	Фізичний рівень	Мережевий рівень	Рівень ОС	Рівень СУБД	Рівень банківського ПЗ
BT	*pt*	*pt*	*so*	*cs*	*so*
PID	*pt*	*pt*	*so*	*cs*	*so*
KrD	*pt*	*pt*	*so*	*cs*	*so*
KT	*pt*	*pt*	*so*	*cs*	*so*
StO	*pt*	*pt*	*so*	*cs*	*so*
Ol	*pt*	*pt*	*so*	*cs*	*so*
YI	*pt*	*pt*	*so*	*cs*	*so*
PD	*pt*	*pt*	*so*	*cs*	*so*

Удосконалена модель визначена п'ятьма категоріями зловмисника та формально описується виразом: $G_{IA}^{ABS} = \left\{ aid_i, pur_i, T_{IA}, S_{\max_i}, pr_j, MS_i^{ABS} \right\} \forall i \in n, \forall j \in m$, (5.15) де aid_i – ідентифікатор зловмисника (категорія зловмисника); pur_i – мета зловмисника; T_{IA} – час успішної реалізації загрози; $S_{\max_i}$ – ймовірнісний збиток системи; pr_j – ймовірність реалізації хоча б однієї загрози *j*-му активу; MS_i^{ABS} – рекомендації щодо виявлення, реагування ТЗЗІ.

На основі запропонованих моделей здійснюється комплексування множини загроз (рис. 5.15, табл. 5.14): $DF^{ABS} = \{V^{NS}\} \cup \{V^{AS}\}$, де $\{V^{AS}\} = \{V^{ASIB}\} \cap \{V^{ASKB}\} \cap \{V^{ASBI}\}$, де $\{V^{NS}\}$ – клас природних джерел загроз; $\{V^{AS}\}$ – клас антропогенних загроз, де $\{V^{ASIB}\}$ – множина загроз ІБ; $\{V^{ASKB}\}$ – множина загроз КБ; $\{V^{ASBI}\}$ – множина загроз БІ.



	Банковская тайна	Платежные документы	Кредитные документы	Коммерческая тайна	Статистические отчеты	Общедоступная информация	Управляющая информация	Персональные данные
02.03.01.05	0.268	0.268	0.268	0.268	0.241	0.153	0.241	0.268
03.03.03.04	0.332	0.332	0.332	0.332	0.166	0.066	0.166	0.332
03.03.02.03	0.999	0.999	0.999	0.999	0.733	0.43	0.733	0.999
03.03.02.05	0.5777	0.5777	0.5777	0.5777	0.4277	0.2394	0.4277	0.5777
03.02.04.03	0.5176	0.5176	0.5176	0.5176	0.3631	0.2663	0.3631	0.5176
02.02.04.05	0.268	0.268	0.268	0.268	0.18	0.046	0.18	0.268
02.02.02.03	0.2	0.2	0.2	0.2	0.1	0.05	0.1	0.2
01.02.03.02	0.268	0.268	0.268	0.268	0.134	0.107	0.134	0.268
03.02.03.01	0.3294	0.3294	0.3294	0.3294	0.2712	0.2335	0.2712	0.3294
03.02.02.03	0.268	0.268	0.268	0.268	0.241	0.222	0.241	0.268
01.01.03.05	0.666	0.666	0.666	0.666	0.56	0.421	0.56	0.666
03.03.02.04	0.4433	0.4433	0.4433	0.4433	0.2722	0.1589	0.2722	0.4433
03.01.03.02	0.5791	0.5791	0.5791	0.5791	0.4639	0.2756	0.4639	0.5791
01.01.03.04	0.5178	0.5178	0.5178	0.5178	0.4364	0.2819	0.4364	0.5178
03.03.03.03	0.6654	0.6654	0.6654	0.6654	0.4895	0.2857	0.4895	0.6654
02.03.01.02	0.5735	0.5735	0.5735	0.5735	0.2849	0.154	0.2849	0.5735
01.01.02.05	0.6653	0.6653	0.6653	0.6653	0.5533	0.3446	0.5533	0.6653

Рисунок 5.15 – Ймовірність виникнення *i*-ї загрози на інформаційні активи БІР

Крок 2.4. Визначення ціни повного ризику всіх активів БІР. Ціна повного ризику дорівнює сумі цін ризику всіх активів (табл. 5.11):

$$R_{повн} = \sum_{j=1}^{n} R_j, \tag{5.16}$$

де $R_j = pr_j \times q_j$, де pr_j – ймовірність реалізації хоча б однієї загрози *j*-му активу; q_j – збиток.

Крок 2.5. Визначення ймовірності реалізації хоча б однієї загрози для кожного активу БІР. Розрахунок ймовірності реалізації хоча б однієї загрози для кожного активу виконується за виразом (рис. 5.15, табл. 5.14):

$$p_{rj} = 1 - \prod_{i=1}^{m} (1 - pr_{ij}), \tag{5.17}$$

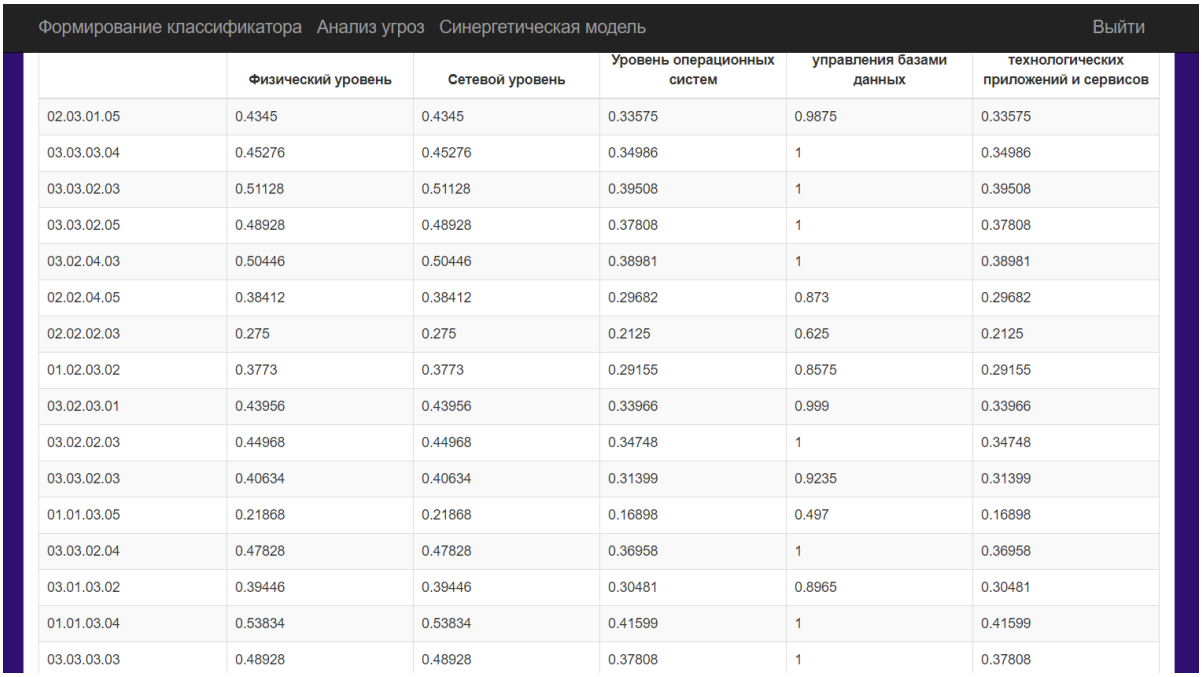
де pr_{ij} – ймовірність реалізації *i*-ї загрози *j*-му активу

Таблиця 5.14 – Визначення ймовірності реалізації хоча б однієї загрози для кожного активу БІР

ID загрози	*BT*	*PID*	*KrD*	*KT*	*StO*	*Ol*	*YI*	*PD*
02.03.01.05	0.268	0.268	0.268	0.268	0.241	0.153	0.241	0.268
03.03.03.04	0.332	0.332	0.332	0.332	0.166	0.066	0.166	0.332
03.03.02.03	0.332	0.332	0.332	0.332	0.249	0.166	0.249	0.332
03.03.02.05	0.333	0.333	0.333	0.333	0.223	0.113	0.223	0.333
03.02.04.03	0.332	0.332	0.332	0.332	0.222	0.189	0.222	0.332
02.02.04.05	0.268	0.268	0.268	0.268	0.18	0.046	0.18	0.268
02.02.02.03	0.2	0.2	0.2	0.2	0.1	0.05	0.1	0.2
01.02.03.02	0.268	0.268	0.268	0.268	0.134	0.107	0.134	0.268
03.02.03.01	0.267	0.267	0.267	0.267	0.23	0.203	0.23	0.267
03.02.02.03	0.268	0.268	0.268	0.268	0.241	0.222	0.241	0.268
…	…	…	…	…	…	…	…	…
03.03.02.03	0.267	0.267	0.267	0.267	0.2	0.112	0.2	0.267
01.01.03.05	0.133	0.133	0.133	0.133	0.114	0.101	0.114	0.133
03.03.02.04	0.332	0.332	0.332	0.332	0.199	0.116	0.199	0.332
03.01.03.02	0.267	0.267	0.267	0.267	0.182	0.094	0.182	0.267
01.01.03.04	0.332	0.332	0.332	0.332	0.299	0.189	0.299	0.332
3.01.01.01	0.2	0.2	0.2	0.2	0.186	0.086	0.186	0.2
03.01.04.01	0.132	0.132	0.132	0.132	0.132	0.066	0.132	0.132
03.01.04.05	0.268	0.268	0.268	0.268	0.249	0.115	0.249	0.268
03.01.04.05	0.268	0.268	0.268	0.268	0.228	0.094	0.228	0.268

Крок 2.6. Визначення зв’язку між джерелами загроз та елементами АБС, (рис. 5.16, табл. 5.15):

$$A^{DF} = \left\| a_{ij}^{DF} \right\|. \qquad (5.18).$$



	Физический уровень	Сетевой уровень	Уровень операционных систем	управления базами данных	технологических приложений и сервисов
02.03.01.05	0.4345	0.4345	0.33575	0.9875	0.33575
03.03.03.04	0.45276	0.45276	0.34986	1	0.34986
03.03.02.03	0.51128	0.51128	0.39508	1	0.39508
03.03.02.05	0.48928	0.48928	0.37808	1	0.37808
03.02.04.03	0.50446	0.50446	0.38981	1	0.38981
02.02.04.05	0.38412	0.38412	0.29682	0.873	0.29682
02.02.02.03	0.275	0.275	0.2125	0.625	0.2125
01.02.03.02	0.3773	0.3773	0.29155	0.8575	0.29155
03.02.03.01	0.43956	0.43956	0.33966	0.999	0.33966
03.02.02.03	0.44968	0.44968	0.34748	1	0.34748
03.03.02.03	0.40634	0.40634	0.31399	0.9235	0.31399
01.01.03.05	0.21868	0.21868	0.16898	0.497	0.16898
03.03.02.04	0.47828	0.47828	0.36958	1	0.36958
03.01.03.02	0.39446	0.39446	0.30481	0.8965	0.30481
01.01.03.04	0.53834	0.53834	0.41599	1	0.41599
03.03.03.03	0.48928	0.48928	0.37808	1	0.37808

Рисунок 5.16 – Визначення зв’язку між джерелами загроз і елементами АБС

Таблиця 5.15 – Визначення зв’язку між джерелами загроз і елементами АБС

ID загрози	Фізичний рівень	Мережевий рівень	Рівень ОС	Рівень СУБД	Рівень банківського ПЗ
02.03.01.05	0.4345	0.4345	0.33575	0.9875	0.33575
03.03.03.04	0.45276	0.45276	0.34986	1	0.34986
03.03.02.03	0.51128	0.51128	0.39508	1	0.39508
03.03.02.05	0.48928	0.48928	0.37808	1	0.37808
03.02.04.03	0.50446	0.50446	0.38981	1	0.38981
…	…	…	…	…	…
03.01.01.01	0.32076	0.32076	0.24786	0.729	0.24786
03.01.04.01	0.2178	0.2178	0.1683	0.495	0.1683
03.01.04.05	0.42966	0.42966	0.33201	0.9765	0.33201
03.01.04.05	0.4158	0.4158	0.3213	0.945	0.3213
02.03.02.03	0.28512	0.28512	0.22032	0.648	0.22032
03.02.03.01	0.10098	0.10098	0.07803	0.2295	0.07803

Етап 3. *Визначення узагальненого показника рівня захищеності БІР на основі удосконаленої моделі оцінювання рівня захищеності БІР.*

Визначення рівня захищеності АБС від загроз ІБ, КБ, БІ на БІР пропонується одержати на основі моделі:

$$G_{OZ}^{ABS} = \begin{Bmatrix} \{I_A\}, \{O^{ABS}\}, \{DF^{ABS}\}, \{RR^{ABS}\}, \\ \{SZ^{ABS}\}, \{ROZ^{ABS}\}, \{UZ_r^{ABS}\} \end{Bmatrix}, \quad (5.19)$$

де $\{I_A\}$ – множина елементів інформаційних активів; $\{O^{ABS}\}$ – множина елементів ієрархії АБС; $\{DF^{ABS}\}$ – множина джерел загроз безпеці АБС; $\{RR^{ABS}\}$ – множина вимог регуляторів безпеки БІР; $\{SZ^{ABS}\}$ – множина можливих ТЗЗІ; $\{ROZ^{ABS}\}$ – дані обліку про результати оцінки захищеності АБС; $\{UZ_r^{ABS}\}$ – рівень захищеності АБС.

Крок 3.1. Визначення зв’язку між загрозами і технічними засобами захисту інформації (рис. 5.17, табл. 5.16):

$$A^{DFSZ} = \left\| a_{ij}^{DFSZ} \right\|, \text{ при цьому } \forall j \in \{I_A\}, \text{ а } \forall i \in \{DF_i\}. \quad (5.20)$$

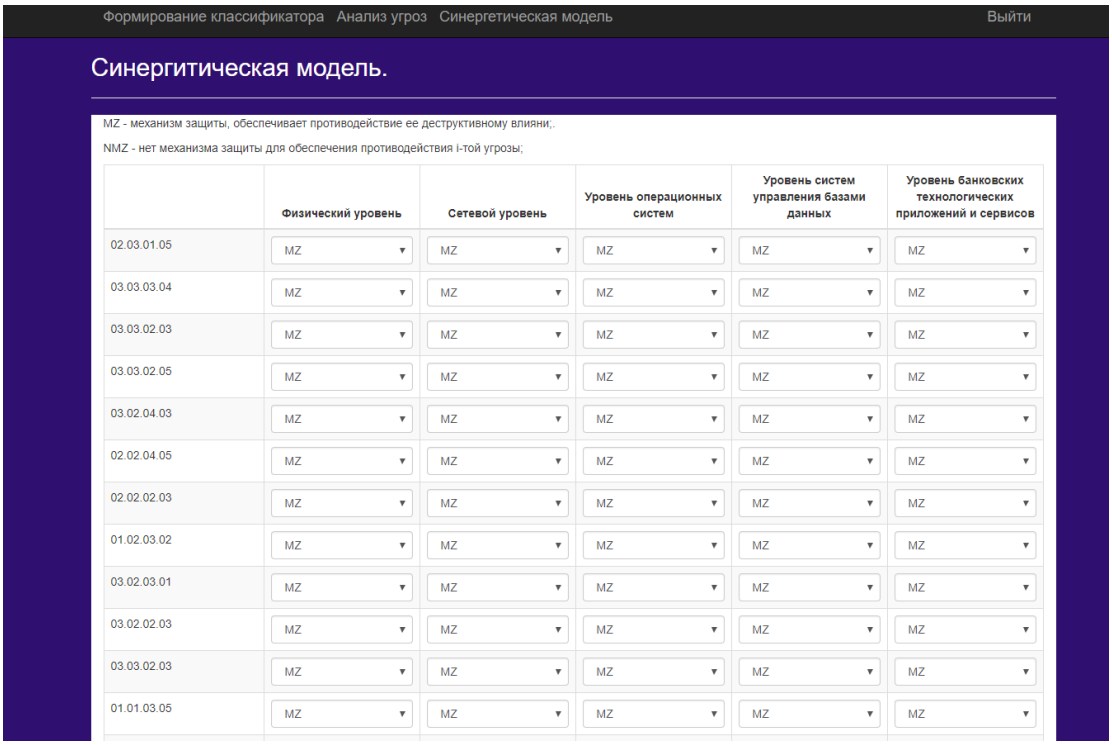


Рисунок 5.17 – Зв’язок між загрозами і ТЗЗІ

Таблиця 5.16 – Зв’язок між загрозами і ТЗЗІ

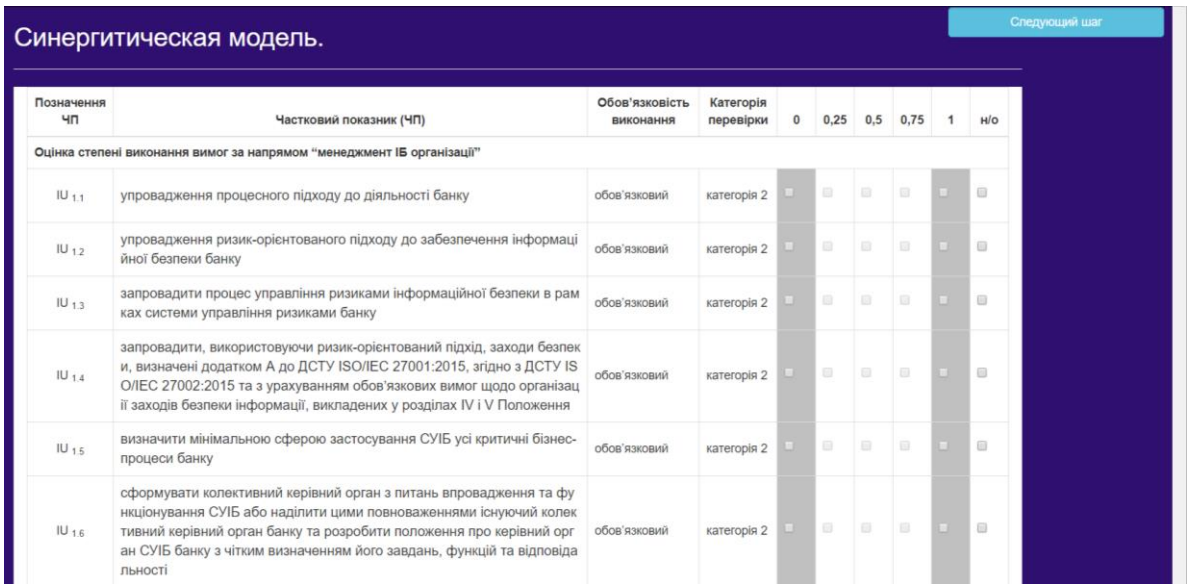
ID загрози	Фізичний рівень	Мережевий рівень	Рівень ОС	Рівень СУБД	Рівень банківського ПЗ
02.03.01.05	*MZ*	*MZ*	*MZ*	*MZ*	*MZ*
03.03.03.04	*MZ*	*MZ*	*MZ*	*MZ*	*MZ*
03.03.02.03	*MZ*	*MZ*	*MZ*	*MZ*	*MZ*
03.03.02.05	*MZ*	*MZ*	*MZ*	*MZ*	*MZ*
03.02.04.03	*MZ*	*MZ*	*MZ*	*MZ*	*MZ*
…	…	…	…	…	…
03.01.01.01	*MZ*	*MZ*	*MZ*	*MZ*	*MZ*
03.01.04.01	*MZ*	*MZ*	*MZ*	*MZ*	*MZ*
03.01.04.05	*MZ*	*MZ*	*MZ*	*MZ*	*MZ*
03.01.04.05	*MZ*	*MZ*	*MZ*	*MZ*	*MZ*
02.03.02.03	*MZ*	*MZ*	*MZ*	*MZ*	*MZ*
03.02.03.01	*MZ*	*MZ*	*MZ*	*MZ*	*MZ*

У моделі використані такі типи зв’язку: *MZ* – є механізм захисту, що забезпечує протидію її деструктивному впливу $VH_i \in \{VH\}$; *NMZ* – немає механізму захисту для забезпечення протидії *i*-ї загрози.

Якщо для всіх $i = m$ $a_{mj}^{DFSZ} = NMZ$, то робиться висновок що ТЗЗІ АБС не здатні захистити БІР від певного деструктивного впливу, а тому для підвищення рівня захищеності АБС необхідно залучати додаткові кошти на механізми захисту.

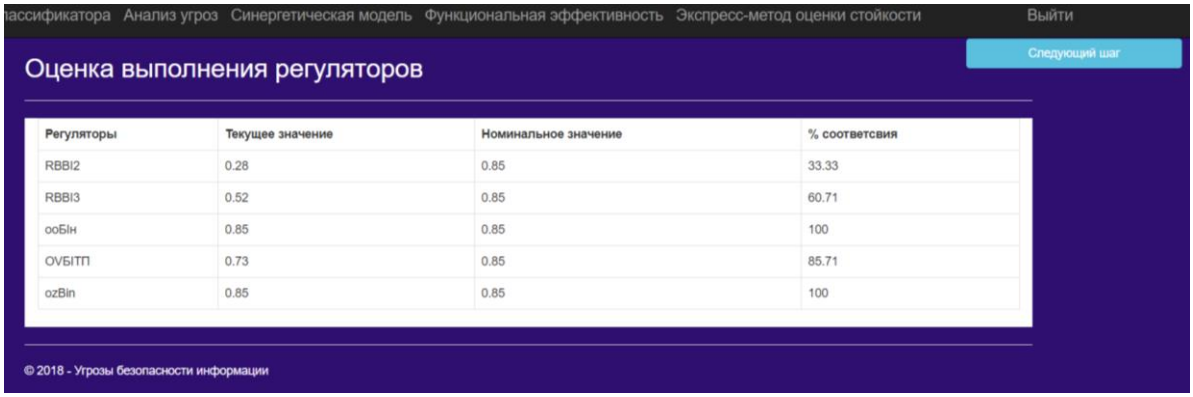
Крок 3.2. Визначення множини вимог регуляторів $\{RR^{ABS}\}$, яка складається з вимог до забезпечення безпеки БІР – $\{R_{BBI}\}$, зазначених у міжнародних і національних стандартах, множини оцінок ступеня виконання вимог безпеки $\{OV_{BBI}\}$ та множини підсумкового рівня відповідності безпеки БІР вимогам з множини $\{IU_{BBI}\}$ (рис. 5.18, 5.19):

$$\{RR^{ABS}\} = \{R_{BBI}\} \cup \{OV_{BBI}\} \cup \{IU_{BBI}\}. \qquad (5.20)$$



Позначення ЧП	Частковий показник (ЧП)	Обов'язковість виконання	Категорія перевірки	0	0,25	0,5	0,75	1	н/о
Оцінка степені виконання вимог за напрямом "менеджмент ІБ організації"									
IU 1.1	упровадження процесного підходу до діяльності банку	обов'язковий	категорія 2						
IU 1.2	упровадження ризик-орієнтованого підходу до забезпечення інформаційної безпеки банку	обов'язковий	категорія 2						
IU 1.3	запровадити процес управління ризиками інформаційної безпеки в рамках системи управління ризиками банку	обов'язковий	категорія 2						
IU 1.4	запровадити, використовуючи ризик-орієнтований підхід, заходи безпеки, визначені додатком А до ДСТУ ISO/IEC 27001:2015, згідно з ДСТУ ISO/IEC 27002:2015 та з урахуванням обов'язкових вимог щодо організації заходів безпеки інформації, викладених у розділах IV і V Положення	обов'язковий	категорія 2						
IU 1.5	визначити мінімальною сферою застосування СУІБ усі критичні бізнес-процеси банку	обов'язковий	категорія 2						
IU 1.6	сформувати колективний керівний орган з питань впровадження та функціонування СУІБ або наділити цими повноваженнями існуючий колективний керівний орган банку та розробити положення про керівний орган СУІБ банку з чітким визначенням його завдань, функцій та відповідальності	обов'язковий	категорія 2						

Рисунок 5.18 – Визначення вимог регуляторів



Регуляторы	Текущее значение	Номинальное значение	% соответсвия
RBBI2	0.28	0.85	33.33
RBBI3	0.52	0.85	60.71
ooБІн	0.85	0.85	100
OVБІТП	0.73	0.85	85.71
ozBIn	0.85	0.85	100

Рисунок 5.19 – Визначення вимог регуляторів

Припустимо що, цей показник виконується.

Крок 3.3. Визначення узагальненого показника рівня захищеності АБС, який дозволяє оцінити рівень відповідності ТЗЗІ вимогам регуляторів та розраховується (рис. 5.20):

$$OPZ^{ABS} = \sum_{i=1}^{k} OPZ_i , \qquad (5.21)$$

де k – кількість окремих показників безпеки, OPZ_i –окремий показник, що набуває значення з множини: OPZ_1 – відсутність неприпустимих ризиків, у разі якщо в ОБС при складанні моделі загроз / моделі зловмисника і оцінки ризиків (якщо виявлені неприпустимі за своїм рівнем ризики, то $OPZ_1 = 0$, в іншому випадку – $OPZ_1 = 1$); OPZ_2 – відсутність небезпечних загроз (якщо виявлені загрози "закриті"

механізмами ТЗЗІ, то OPZ_2 = 1, у разі, якщо в ОБС при складанні моделі виявлені “незакриті” загрози – OPZ_2 = 0); OPZ_3 – рівень відповідності захищеності БІР вимогам регуляторів (якщо визнаний рекомендованим – OPZ_3 = 1, в разі, якщо визнано нерекомендованим – OPZ_3 = 0).

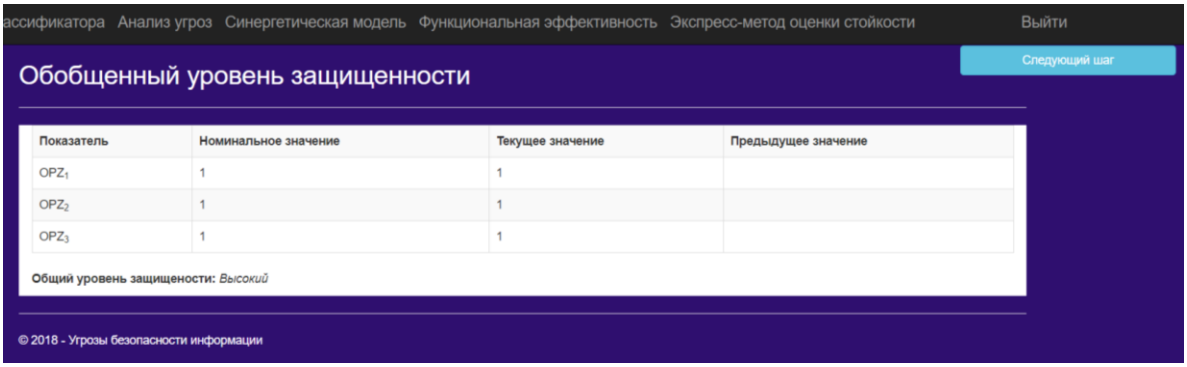


Рисунок 5.20 – Визначення узагальненого показника рівня захищеності БІР

На основі результатів узагальненого показника рівня захищеності OPZ^{ABS}, узагальненої синергетичної загрози $W_{synerg}^{IB,KB,BI}$, множини активів БІР $I_{A_i} = \left(Type, A^C, A^D, A^A, A^K, C_Y\right)$ та запропонованої моделі оцінювання безпеки БІР на основі комплексного показника ефективності інвестицій (див. підрозд. 4.1) визначається ефективність інвестицій в забезпечення безпеки БІР.

Вихідними даними для проведення оцінки є основні показники на основі даних консолідованої фінансової звітності за Міжнародними стандартами фінансової звітності та звіту незалежного аудитора банку “ГРУПИ ПРИВАТ” за 2015, 2016 рр. (https://bank.gov.ua/control/uk/publish/article?art_id=34661442), які наведені у табл. 5.17. При розрахунках враховуємо, що на забезпечення ІБ в АБС банком витрачається до 4% від річного прибутку, витрати на розробку ТЗЗІ складають до 2 % від річного прибутку, NPV_{zbtszi}^{ABS} – ймовірні витрати на усунення компрометації безпеки без застосування до 25% від річного прибутку, NPV_{zbtszi}^{ABS} – ймовірні витрати на усунення компрометації безпеки, що становить до 2% від річного прибутку, C_{sz} – вартість засобів захисту становить 30% від загальної вартості БІР.

Ставка дисконтування становить 13%. (http://bank-ua.com/%D0%9E%D0%B1%D0%BB%D1%96%D0%BA%D0%BE%D0%B2%D0%B0_%D1%81%D1%82%D0%B0%D0%B2%D0%BA%D0%B0_%D0%9D%D0%91%D0%A3), табл. 5.18.

Таблиця 5.17 – Вихідні дані, тис. грн.

Рік	$C_{приб}^{ABC}$	I_{nv}^{ABC}	N, (періоди)	r (%)
2015	7261000000	145220000	2	13
2016	2448000000	48960000	2	13

Таблиця 5.18 – Вихідні дані за інформаційними активами БІР, тис. грн.

Назва, I_{A_i} % від $C_{приб}^{ABC}$	u_j	NPV_{inv}^{ABS}	NPV_{zt}^{ABS}	ROI^{ABS}	C_{sz}
BT, (20%)	24480000	24480000	7344000	17136000	7344000
PID, (5%)	6120000	6120000	1836000	4284000	1836000
KrD, (30%)	36720000	36720000	11016000	25704000	11016000
KT, (20%)	24480000	24480000	734000	17136000	734000
StO, (3%)	3672000	3672000	1101600	2570400	1101600
Ol, (2%)	2448000	2448000	7344000	1713600	7344000
YI, (10%)	12240000	12240000	3672000	8568000	3672000
PD, (10%)	12240000	12240000	3672000	8568000	3672000

Оцінка безпеки БІР на основі комплексного показника ефективності інвестицій визначається за такими кроками:

Крок 1. Оцінювання рівня прибутковості інвестицій в побудову системи безпеки БІР:

$$ROI^{ABS} = NPV_{inv}^{ABS} - NPV_{zt}^{ABS}, \quad (5.22)$$

де NPV_{inv}^{ABS} – прибуток від інвестицій в ТЗЗІ АБС; NPV_{zt}^{ABS} – витрати в ТЗЗІ АБС; ROI^{ABS} –прибутковість інвестицій в ТЗЗІ АБС.

Результати розрахунку наведені у табл. 5.18.

Крок 2. Оцінювання рентабельності інвестицій в ТЗЗІ:

$$ROSI^{ABS} = NPV_{zbtszi}^{ABS} - NPV_{zvtszi}^{ABS}, \quad (5.23)$$

де NPV_{zbtszi}^{ABS} – витрати на усунення компрометації безпеки без застосування ТЗЗІ; NPV_{zvtszi}^{ABS} – витрати на усунення компрометації безпеки з застосуванням ТЗЗІ.

Результати розрахунку наведені у табл. 5.19.

Таблиця 5.19 – Результати оцінювання рентабельності інвестицій, тис. грн.

Назва, I_{A_i}	NPV_{zbtszi}^{ABS}	C_{sz}	ALE_i	NPV_{zvtszi}^{ABS}	$ROSI^{ABS}$
BT	122400000	7344000	16279200	34272000	88128000
PID	30600000	1836000	4069800	8568000	22032000
KrD	183600000	11016000	24418800	51408000	132192000
KT	122400000	734000	16279200	34272000	88128000
StO	18360000	1101600	1733184	5140800	13219200
Ol	12240000	7344000	682992	3427200	8812800
YI	61200000	3672000	5777280	17136000	44064000
PD	61200000	3672000	8139600	17136000	44064000

Крок 3. Оцінювання чистої зведеної вартості:

$$NPV_{zvtszi}^{ABS} = C_{sz} + \sum_{i=1}^{N} \frac{ALE_i}{(1+r)^i}, \quad (5.24)$$

де N – кількість інтервалів інвестування; ALE_i – очікувані витрати в i-му періоді; r – ставка дисконтування; C_{sz} – вартість засобів захисту. Результати наведені у табл. 5.19.

Крок 4. Оцінювання ризику БІР за методикою розрахунку *Annual loss expectancy – ALE*, тобто очікуваних втрат в кожен період оцінки:

$$ALE^{ABS} = \sum_{i=1}^{n} I\left(O_{DF}^{ABS}\right) F_i, \quad (5.25)$$

де $\left\{O_{DF}^{ABS}\right\}$ – множина загроз; $I\left(O_{DF}^{ABS}\right)$ – вартісні наслідки реалізації загрози; ALE^{ABS} – очікувана шкода від реалізації загрози; F_i – частота (можливість) реалізації загрози. Результати наведені у табл. 5.19.

Крок 5. Оцінювання потенційних збитків U^{ABS} інформаційного активу з урахуванням виразу (5.17) і табл. 5.14:

$$U^{ABS} = p_{rj} u_j, \tag{5.26}$$

де p_{rj} – ймовірність реалізації хоча б однієї загрози j-му активу; u_j – цінність j-го активу. Результати наведені у табл. 5.20.

Таблиця 5.20 – Результати оцінювання потенційних збитків U^{ABS}, тис. грн.

ID загрози	*BT*	*PID*	*KrD*	*KT*	*StO*	*Ol*	*YI*	*PD*
02.03.01.05	131212,8	32803,2	196819	131213	17699	7490,88	58997	65606
03.03.03.04	162547,2	40636,8	243821	162547	12191	3231,36	40637	81274
03.03.02.03	162547,2	243821	162547	18286,6	8127,36	8127,36	60955	81274
03.03.02.05	163036,8	40759,2	244555	163037	16377,1	5532,48	54590	81518
03.02.04.03	162547,2	40636,8	243821	162547	16303,7	9253,44	54346	81274
02.02.04.05	131212,8	131213	196819	131213	13219,2	2252,16	44064	65606
03.02.02.03	131212,8	32803,2	196819	131213	17699	10869,12	58997	65606
…	…	…	…	…	…	…	…	…
03.03.02.03	130723,2	32680,8	196085	130723	14688	5483,52	48960	65362
01.01.03.05	65116,8	16279,2	97675,2	65116,8	8372,16	4944,96	27907	32558
03.03.02.04	162547,2	40636,8	243821	162547	14614,6	5679,36	48715	81274
03.01.03.02	130723,2	32680,8	196085	130723	13366,1	4602,24	44554	65362
3.01.01.01	97920	24480	146880	97920	13659,8	4210,56	45533	48960
03.01.04.01	64627,2	16156,8	96940,8	64627,2	9694,08	3231,36	32314	32314
03.01.04.05	131212,8	32803,2	196819	131213	18286,6	5630,4	60955	65606
03.01.04.05	131212,8	32803,2	196819	131213	19681,9	4602,24	55814	65606

Крок 6. Оцінювання загального очікуваного збитку:

$$OU^{ABS} = \sum_{j=1}^{n} U^{ABS} . \quad (5.27)$$

Результати наведені у табл. 5.21.

Крок 7. Оцінювання сукупної вартості витрат ліквідації наслідків реалізації загрози та інших причин виведення з ладу ТЗЗІ:

$$M^{ABS} = \sum_{i=1}^{m} C_i , \quad (5.28)$$

де C_i – вартість i-го заходу; m – загальна кількість вжитих заходів. Результати наведені у табл. 5.21.

Таблиця 5.21 – Результати загального очікуваного збитку, наслідків виведення з ладу ТЗЗІ, тис. грн.

Назва I_{A_i}	OU^{ABS}	M^{ABS}	Вагові коефіцієнти Фішберна				W_{ABS}^{effinv} за складовими послуг безпеки			
			w_i^C	w_i^I	w_i^A	w_i^{Au}	*C*	*I*	*A*	*Au*
BT	16279200	122400000	0,4	0,3	0,2	0,1	48960000	36720000	244800000	12240000
PID	4069800	30600000	0,4	0,3	0,2	0,1	12240000	9180000	55080000	36720000
KrD	24418800	183600000	0,4	0,3	0,2	0,1	73440000	55080000	36720000	183600000
KT	16279200	122400000	0,4	0,3	0,2	0,1	48960000	36720000	244800000	12240000
StO	1733184	18360000	0,4	0,3	0,2	0,1	7344000	5508000	3672000	18360000
Ol	682992	12240000	0,4	0,3	0,2	0,1	4896000	3672000	24480000	1224000
YI	5777280	61200000	0,4	0,3	0,2	0,1	24480000	18360000	12240000	6120000
PD	8139600	61200000	0,4	0,3	0,2	0,1	24480000	18360000	12240000	6120000

Крок 8. Визначення комплексного показника ефективності інвестицій в забезпечення безпеки БІР:

$$W_{ABS}^{effinv} = \sum_{i=1}^{N} w_i M^{ABS} , \quad (5.29)$$

де $w_i \in [0;1]$, $W_{\Phi}^{ABS} = \sum_{i=1}^{N} w_i$ – система вагових коефіцієнтів Фішберна, $i \in [1;N]$.

Кожному параметру присвоюються вагові категорії за правилом Фішберна [65], заснованому на тому, що зміна вагових коефіцієнтів критеріїв підкоряється спадній арифметичній прогресії.

При цьому перший критерій (*i = 1*), розташований першим в строго упорядкованому за важливістю ранжируваному ряду критеріїв *i* = 1, 2, ..., *n*, є найбільш важливим і має найбільший ваговий коефіцієнт. Це правило задається виразом:

$$w_i = \frac{2\left(N - n + 1\right)}{N\left(N + 1\right)},$$

де w_i – ваговий коефіцієнт Фішберна; N – загальна кількість параметрів; n – порядковий номер параметра; i – кількість параметрів.

Відповідно до виразу Фішберна маємо:

$$w_1 = \frac{2 \times N}{N\left(N + 1\right)},\ w_N = \frac{2}{N\left(N + 1\right)},\ \gamma = \frac{w_1}{w_N} = N,$$

де γ – кратність відмінності вагових коефіцієнтів один від одного.

Таким чином, $w_i^C = 0.4, \quad w_i^I = 0.3, \quad w_i^A = 0.2, \quad w_i^{Au} = 0.1.$

Для нормування отриманих значень показника W_{ABS}^{effinv} розділимо отримані результати на 10^8 та використаємо підхід формування загального показника $W_{synerg}^{IB,KB,BI}$, результати наведені у табл. 5.22.

$W_{ABS_{загI_{A_i}}}^{effinv \quad C} = \sum_{i=1}^{A_i} W_{ABS}^{effinv\,C}$ – загальний показник за послугою конфіденційність;

$W_{ABS_{загI_{A_i}}}^{effinv \quad I} = \sum_{i=1}^{A_i} W_{ABS}^{effinv\,I}$ – загальний показник за послугою цілісність;

$W_{ABS_{загI_{A_i}}}^{effinv \quad A} = \sum_{i=1}^{A_i} W_{ABS}^{effinv\,A}$ – загальний показник за послугою доступність;

$W_{ABS_{загI_{A_i}}}^{effinv \quad Au} = \sum_{i=1}^{A_i} W_{ABS}^{effinv\,Au}$ – загальний показник за послугою автентичність.

Загальний показник визначається за виразом:

$$W_{ABS_{заг}}^{effinv} = W_{ABS_{загI_{A_i}}}^{effinv \quad C} \bigcap W_{ABS_{загI_{A_i}}}^{effinv \quad I} \bigcap W_{ABS_{загI_{A_i}}}^{effinv \quad A} \bigcap W_{ABS_{загI_{A_i}}}^{effinv \quad Au}.$$

Таблиця 5.22 – Результати загального показника ефективності

Назва, I_{A_i}	W_{ABS}^{effinv} за складовими послуг безпеки			
	C	*I*	*A*	*Au*
BT	0,04896	0,03672	0,02448	0,01224
PID	0,01224	0,00918	0,05508	0,00367
KrD	0,07344	0,05508	0,03672	0,01836
KT	0,04896	0,03672	0,02448	0,01224
StO	0,007344	0,005508	0,003672	0,001836
Ol	0,04896	0,03672	0,02448	0,01224
YI	0,02448	0,01836	0,01224	0,00612
PD	0,02448	0,01836	0,01224	0,00612
$W_{ABS_{загI_{A_i}}}^{effinv}$	0,2448	0,1836	0,1224	0,0612
$W_{ABS_{заг}}^{effinv} = W_{ABS_{загI_{A_i}}}^{effinv\ C} \bigcap W_{ABS_{загI_{A_i}}}^{effinv\ I} \bigcap W_{ABS_{загI_{A_i}}}^{effinv\ A} \bigcap W_{ABS_{загI_{A_i}}}^{effinv\ Au} = 0{,}00034$				

Для оцінювання якості обслуговування об’єктів АБС щодо забезпечення безпеки БІР використаємо запропоновану методику оцінки функціональної ефективності обміну даними в мережі АБС, яка ґрунтується на простому багатофакторному аналізі, в якій враховуються як технічні показники мережі (швидкість передачі даних, імовірність і час доставки пакета і ін.), показники безпеки технічних засобів захисту інформації, так і економічні параметри (вартість масштабування, обслуговування мережі, ефективність інвестицій в безпеку і т.п.).

Методика містить 4 етапи: 1) визначення стійкості криптосистем методом експрес-аналізу на основі ентропійного методу оцінки випадковості вихідної послідовності; 2) визначення впливу загроз на складові безпеки (ІБ, КБ, БІ) з урахуванням їх гібридності і синергізму; 3) визначення інвестицій в безпеку БІР; 4) визначення ефективності обміну даними в АБС на основі комплексного показника.

1 етап. Визначення стійкості криптосистем методом експрес-аналізу на основі ентропійного методу оцінки випадковості вихідної послідовності (див. підр. 4.2, 5.1). Результатом досліджень є таблиця оцінки максимального криптографічного захисту БІР (табл. 5.23).

Таблиця 5.23 – Оцінка максимального криптографічного захисту інформації

№	Шифр	Ентропія відкр. тексту (H_M)	Ентропія криптограми (H_C)	Різниця $H_{Cypher} = H_C - H_M$	Ймовірність криптозахисту, P_c
1.	Клітинні автомати, правило “60”	0,5023775 (5,023775)	0,6820179 (6,820179)	0,1796404 (1,796404)	0,637079949
2.	генератор ПВП *Secure Random*	0,5023767 (5,023767)	0,7999982 (7,999982)	0,2976215 (2,976215)	0,747287753
3.	*DES*	0,469276	0,812043	0,342767	0,812043
4.	*3DES*	0,469276	0,812043	0,342767	0,812043
5.	ГОСТ 28147-2009	0,469276	0,811348	0,342072	0,811348
6.	Калина-256	0,469276	0,954519	0,485243	0,954519
7.	*AES*-256	0,469276	0,95454	0,485264	0,95454
8	*RSA*	0,469276	1,000	0,530724	1,000
9	ГККККЗК з *МЕС* (*HCCDC*)	0,469276	0,98764	0,518364	0,98764
10	Ідеальний шифр		1,000		1,000

2 етап. *Визначення ступеня впливу загроз на складові безпеки (ІБ, КБ, БІ) з урахуванням їх гібридності і синергізму*.

На основі класифікатора, з урахуванням виразів (5.8) – (5.12) визначається узагальнена синергетична ймовірність реалізації атаки на БІР $W_{synerg}^{IB,KB,BI}$.

Стійкість системи безпеки в АБС до можливих дій зловмисника визначається таким чином:

$$B = P_c \times W_{synerg}^{IB,KB,BI}, \tag{5.30}$$

де B – стійкість системи безпеки в АБС; P_c.– ймовірність криптозахисту ТЗЗІ в АБС.

3 етап. *Визначення комплексного показника ефективності інвестицій в забезпечення безпеки БІР*.

На основі виразів (5.22) – (5.29) і запропонованої методики визначається комплексний показник ефективності інвестицій в забезпечення безпеки БІР – W_{effinv} .

4. етап. *Визначення ефективності обміну даними в АБС на основі комплексного показника.*

Оцінка ефективності обміну даними здійснюється на основі комплексного показника за виразом:

$$W(u_i) = \frac{n^{(u_i)} - t^{(u_i)}}{n^{(u_i)}} \times B^{(u_i)} \times P_{np.n}{}^{(u_i)} \times W_{effinv} \times W_{norm}, \quad (5.31)$$

де $W(u_i)$ – показник ефективності мережі для обраної стратегії u_i; $n^{(ui)}$ – кількість інформаційних розрядів пакета для обраної стратегії u_i; $t^{(ui)}$ – час доставки пакета t для обраної стратегії u_i; $B^{(ui)}$ – стійкість системи безпеки в АБС; $P_{np\,n}{}^{(ui)}$ – достовірність правильної доставки пакета для обраної стратегії; U – множина допустимих стратегій (методів підвищення достовірності доставки пакетів); $W_{eff}{}^{(ui)}$ – комплексний показник ефективності інвестицій в забезпечення безпеки банківських інформаційних ресурсів; W_{norm} – нормований багатофакторний показник ефективності.

Вихідними даними мережі АБС є результати в умовних балах табл. 5.24 на основі опорних таблиць з параметрами систем передачі даних, які враховуються в інтегральному показнику функціональної ефективності *IP*-мережі АБС W_{norm} (див. підр. 4.2).

Таблиця 5.24 – Узагальнена ефективність мереж передачі даних

Технологія	Умовні бали							
	група						Узагальнений індекс ефективності	Відносна ефективність,%
	1	2	3	4	5	6		
X.25	3	1	3	1	1	1	9	0,25
Frame Relay	3	2	1	5	3	3	270	7,37
Ethernet	3	1	2	4	3	3	216	5,89
Fast Ethernet	3	2	2	4	3	3	432	11,79
Gigabit Ethernet	2	3	4	4	3	3	864	23,59
10 Gb Ethernet	2	4	4	4	3	3	1152	31,45
40 Gb Ethernet	1	5	4	4	3	3	720	19,66
Всього:							3663	100

Група: 1 – вартість розгортання мережі; 2 – швидкість передачі даних; 3 – ймовірність доставки пакету; 4 – час доставки пакету; 5 – затримка пакету; 6 – продуктивність мережі.

На рис. 5.21 наведені результати досліджень функціональної ефективності передачі БІР в АБС.

Вихідними даними для проведення досліджень є: технології *Frame Relay*, 100 *Mbit Ethernet*, 10 *Gbit Ethernet*, 40 *Gbit Ethernet* з розв'язувальним зворотним зв'язком і *ARQ* "Повернення-на-*N*", $W_{synerg}^{IB,KB,BI} = 0.0022839$, БСШ *Gost* – $t_{ш,\,рш} = 0{,}033$ с, *RSA* – $t_{ш,\,рш} = 0{,}2$ с, ГККЗК з *MEC* – $t_{ш,\,рш} = 0{,}0015$ с, $P_C^{Gost} = 0{,}95454$, $P_C^{HCCDC} = 0{,}98764$, $P_C^{RSA} = 1{,}0000$, $n = 1518$, $C = 36000$, $P_{пр.п} = 0{,}9999$, $s = 32$, $w = 300000000$.

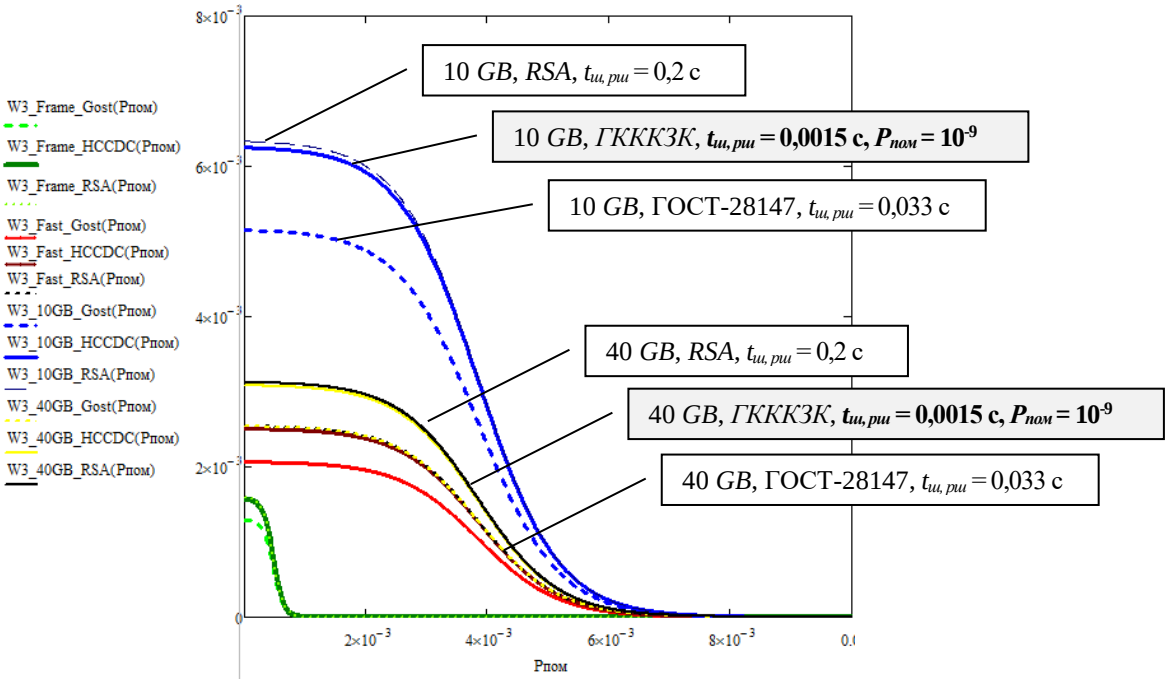


Рисунок 5.21 – Результати досліджень функціональної ефективності АБС з протоколом *ARQ* "Повернення-на-*N*"

Аналіз результатів рис. 5.21 показав, що запропонована методика оцінювання функціональної ефективності АБС дозволяє без значних часових і експертних витрат дослідити стан якості обслуговування користувачів АБС, використовувати результати оцінки для її масштабування, поліпшення технічних показників АБС та рівня захищеності БІР.

Таким чином, усі сформульовані науково-прикладні висновки підтверджено результатами експерименту.

5.4. Висновки до п’ятого розділу

У заключному розділі дисертації запропоновано методологію побудови системи безпеки БІР, яка дає можливість забезпечити підвищення рівня безпеки БІР в умовах дії гібридних загроз на організації банківського сектору, раціональну організацію системи безпеки банківських інформаційних ресурсів, в умовах одночасної дії на систему загроз інформаційній безпеці, кібербезпеці та безпеці інформації. У результаті цього отримані такі результати:

1. Виконано верифікацію та дослідження адекватності запропонованих методу оцінювання безпеки банківських інформаційних ресурсів, який враховує комплексний показник ефективності інвестицій, які виділяються на забезпечення безпеки БІР, методики оцінювання функціональної ефективності передачі даних в АБС з урахуванням умов протидії гібридним загрозам ІБ, КБ, БІ на БІР.

2. Розроблено методологію побудови системи безпеки банківських інформаційних ресурсів, яка, на відміну від відомих підходів, реалізує принципово нову концепцію протидії гібридним загрозам банківському сектору держави. Її сутність та зміст полягають в раціональній організації системи безпеки банківських інформаційних ресурсів в умовах одночасної дії на систему загроз інформаційній безпеці, кібербезпеці та безпеці інформації. Такий підхід дозволяє одержати повноцінну та адекватну оцінку рівня захищеності банківських інформаційних ресурсів, що суттєво впливає на величину інвестицій в забезпечення безпеки банківського сектору та відкриває шляхи до прийняття обґрунтованих управлінських рішень з питань забезпечення безпеки банківських інформаційних ресурсів. Практичне використання методології дозволяє забезпечити виконання всього функціоналу системи управління інформаційною безпекою банку на принципово новому підході до оцінювання ймовірності впливу загроз інформаційній безпеці, кібербезпеці та безпеці інформації на безпеку банківських інформаційних ресурсів, без значних часових та експертних витрат на проведення їх оцінювання і аналіз, забезпечити раціональне інвестування в інформаційну безпеку організацій банківського сектору.

Таким чином, запропонована методологія дозволяє забезпечити підвищення рівня захищеності банківських інформаційних ресурсів, отримати максимальну кількість емерджентних властивостей ***в умовах протидії гібридним загрозам інформаційній безпеці, кібербезпеці та безпеці інформації*** а саме: оцінювання синергізму і гібридності загроз складових безпеки (інформаційній безпеці, кібербезпеці, безпеці інформації) на банківські інформаційні ресурси, мінімізація витрат на інвестування в забезпечення безпеки банківських інформаційних ресурсів, висока швидкість криптоперетворень та доказовий рівень стійкості в інтегрованих механізмах забезпечення цілісності, конфіденційності, автентичності і достовірності банківських інформаційних ресурсів при використанні відкритих каналів зв'язку, оцінювання функціональної ефективності передачі банківських інформаційних ресурсів в автоматизованих банківських системах.

Список використаних джерел у п'ятому розділі

1. С. П. Евсеев, Д. В. Сумцов, О. Г. Король, и Б. П. Томашевский, "Анализ эффективности передачи данных в компьютерных системах с использованием интегрированных механизмов обеспечения надежности и безопасности", *Восточно-европейский журнал передовых технологий*, № 2/2(44), с. 45 – 49, 2010.

2. О. Г. Король, "Оцінка якості обслуговування глобальної мережі на основі технологій Ethernet за допомогою комплексного показника", *Системи обробки інформації*, – № 2(148), с. 88 – 94. 2017.

3. С. П. Євсеєв, С. Е. Остапов, Х. Н. Рзаєв, та В. І. Ніколаєнко, "Оцінка обміну даними в глобальних обчислювальних мережах на основі комплексного показника якості обслуговування мережі", *Науковий журнал Радіоелектроніка, інформатика, управління*, № 1(40). – 2017. – С. 115 – 128.

4. О. О. Кузнецов, С. П. Євсеєв, С. В. Кавун, та О. Г. Король *Сигнали і коди. Алгебраїчні методи синтезу*. Монографія. Харків, Україна: Вид. ХНЕУ, 2009.

5. Р. Блейхут, *Теория и практика кодов, контролирующих ошибки*: пер. с англ., М.: Мир, 1986.

6. Дж.-мл. Кларк, *Кодирование с исправлением ошибок в системах цифровой связи*: пер. с англ. / под ред. Б. С. Цыбакова, М.: Радио и связь, 1987.

7. Ф. Дж. Мак-Вильямс, и Н. Дж. А. Слоэн, *Теория кодов, исправляющих ошибки*, М. : Связь, 1979.

8. В. М. Мутер, *Основы помехоустойчивой телепередачи информации*, Л.: Энергоатомиздат. Ленингр. отд-ние, 1990.

9. Т. Касами, Н. Токура, Е. Ивадари, и Я. Инагаки, *Теория кодирования*: пер. с япон. под ред. Б. С. Цыбакова и С. И. Гельфанда, М.: Мир, 1978.

10. Р. Грищук, та О. Корченко, "Методологія синтезу та аналізу диференціально-ігрових моделей та методів моделювання процесів кібернападу на державні інформаційні ресурси", *Науково-практичний журнал "Захист інформації"*, № 3, с.115 – 122, 2012.

11. Г. Баранов, М. Захарова, та Д. Горніцька, "Методологія синтезу систем оцінки рівня захищеності державних інформаційних ресурсів від соціотехнічних атак", *Науково-практичний журнал "Захист інформації"*, № 3, с.98 – 103, 2012.

12. О. Корченко, М. Луцький, М. Захарова, та Ю. Дрейс, "Методологія синтезу та програмна реалізація системи оцінювання шкоди національній безпеці у сфері охорони державної таємниці", Захист інформації, Т. 15, №1, с. 14 – 20, 2013.

13. S. Rajba, M. Karpinski, and O. Korchenko, "Generalized models, construction methodology and the application of secure wireless sensor networks with random network parameters", *Інформаційна безпека*, № 2(20), с. 120 – 125, 2014.

14. О. Юдін, та С. Бучик, "Методологія захисту державних інформаційних ресурсів. порівняльний аналіз основних термінів та визначень", *Науково-практичний журнал "Захист інформації"*, т. 17, № 3, с.218 – 225, 2015.

15. Б. Журиленко, "Методология построения и анализа состояния комплекса технической защиты информации с вероятностной надежностью и учетом временных попыток взлома", *Науково-практичний журнал "Захист інформації"*, т. 17, № 3, с.196 – 204, 2015.

16. С. Бучик, “Методологія аналізу ризиків дерева ідентифікаторів державних інформаційних ресурсів”, *Науково-практичний журнал “Захист інформації”*, т. 18, № 1, с.81 – 89, 2016.

17. А. Корченко, В. Щербина, и Н. Вишневская, “Методология построения систем выявления аномлий порожденных кибератаками”, *Захист інформації*, Т. 18, №1, с. 30 – 38, 2016.

18. Е. Иванченко, С. Казмирчук, и А. Гололобов, “Методология синтеза систем анализа и оценки рисков потерь информационных ресурсов”, *Захист інформації*, Т. 14, № 2, с. 24 – 28, 2012.

19. А. Шиян, “Методологія комплексного захисту людини та соціальних груп від негативного інформаційно-психологічного впливу”, *Інформаційна безпека*, № 1(22), с. 94 – 98, 2016.

20. А. Корченко, С. Казмирчук, и Е. Иванченко, “Методология синтеза адаптивных систем оценивания рисков безопасности ресурсов информационных систем”, Науково-практичний журнал “Захист інформації”, т. 19, № 3, с.198 – 204, 2017.

21. Доктрина інформаційної безпеки України, затверджено Указом Президента України від 25 лютого 2017 року № 47/2017. [Електронний ресурс]. Доступно: http://zakon3.rada.gov.ua/laws/show/47/2017/paran2#n2.

22. Указ Президента України від 15 березня 2016 року № 96 “Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року “Про Стратегію кібербезпеки України”. [Електронний ресурс]. Доступно: http://zakon3.rada.gov.ua/laws/show/96/2016/paran11#n11.

23. Указ Президента України від 12 лютого 2007 року № 105 “Про Стратегію національної безпеки України”. [Електронний ресурс]. Доступно: http://zakon3.rada.gov.ua/laws/show/105/2007.

24. Р. В. Грищук, та Ю. Г. Даник, “Синергія інформаційних та кібернетичних дій”, *Труди університету. НУОУ*, № 6 (127), с. 132–143. 2014.

25. В. Л. Бурячок, Р. В. Грищук, та В. О. Хорошко, під заг. ред. проф. В. О. Хорошка, *“Політика інформаційної безпеки”*, ПВП “Задруга”,. 2014.

26. Ю. Г. Даник та ін., "*Основи захисту інформації*" навч. пос., Житомир : ЖВІ ДУТ, 2015.

27. О. К. Юдін, "*Інформаційна безпека. Нормативно-правове забезпечення*", К. : НАУ, 2011.

28. Р. В. Грищук, та Ю. Г. Даник; за заг. ред. проф. Ю. Г. Даника, *"Основи кібербезпеки"*, Житомир : ЖНАЕУ, 2016.

29. І. С. Іванченко, В. О. Хорошко, Ю. Е.Хохлачова, та Д. В. Чирков під заг. ред. проф. В. О. Хорошка, *"Забезпечення інформаційної безпеки держави"*, К: ПВП "Задруга", 2013.

30. О. Г. Корченко, О. Є. Архипов, та Ю. О. Дрейс, *"Оцінювання шкоди національній безпеці України у разі витоку державної таємниці"*, монографія, К: наук.-вид.центр НА СБУ України, 2014.

31. А. О. Корченко, Л. М. Скачек, та В. О. Хорошко, під заг. ред. проф. В. О. Хорошка, *"Банківська безпека"* підручник, К: ПВП "Задруга", 2014.

32. В. И. Ярочкин, *"Безопасность банковских систем"*, М.: Издательство: Ось-89, 416 с., 2012.

33. А. Потий, та Д. Пилипенко, "Концепция стратегического управления информационной безопасностью", *Радіоелектронні і комп'ютерні системи*. № 6 (47). с. 53 – 58, 2010.

34. М. Барилюк, "Методичний підхід до формування організаційно-економічного забезпечення управління фінансовою безпекою комерційного банку", *Бізнесінформ*, № 6, с.191 – 200, 2017.

35. С. Евсеев, "Анализ защиты в национальной системе масовых электронных платежей", *Інформаційна безпека*, № 3(15), № 4 (16), с. 15 – 28, 2014.

36. С. Евсеев, О. Король, и Г. Коц, "Анализ законодательной базы к системе управления информационной безопасностью НСМЭП", *Восточно-европейский журнал передовых технологий*, вып. 5/3(77), с. 48 – 59, 2015.

37. С. Евсеев, "Методология оценивания безопасности информационных технологий автоматизированных банковских систем Украины", *Науково-технічний журнал "Захист інформації"*, том. 22, № 2, с. 297 – 309, 2016.

38. Briones, P. Chamoso, and A. Barriuso, “Review of the Main Security Problems with Multi-Agent Systems used in E-commerce Applications”, *ADCAIJ, Regular Issue,* Vol. 5, N. 3, pp. 55-61, 2016.

39. W. Simpson, “Securing Information Systems in an Uncertain World Enterprise Level Security”, *Systemics, Cybernetics and Informatics*, Vol. 14, № 2, pp. 83 – 90, 2016.

40. С. Евсеев, О. Король, и А. Сочнева, “Анализ оценки рисков кибербезопасности банковской информации”, *Сборник научных трудов НАУ “Защита информации”*, вып 23, с. 109 – 129, 2016.

41. Р. Грищук, и С. Евсеев, “The synergetic approach for providing bank information security: the problem formulation”, *“Безпека інформації”*, № 22(1), с. 64 – 74, 2016.

42. С. Евсеев, “Модель нарушителя прав доступа в автоматизированной банковской системе на основе синергетического подхода”, *Науково-технічний журнал “Інформаційна безпека”*, № 2 (26), с. 110 – 120, 2017.

43. Ю. Малий, “Методические подходы к анализу угроз безопасности информации и рисков в банковской сфере”, Вестник БУКЭП, № 1, с. 135 – 140, 2013.

44. З. Васильченко, “Деякі аспекти методологічної основи моделювання фінансової безпеки банку”, *Економіка*, № 6(147), с.15 – 19, 2013.

45. С. Евсеев, “Синергетическая модель оценки безопасности банковской информации”, *Науково-технічний журнал “Інформаційна безпека”,* № 4 (24), с. 104 – 118, 2016.

46. С. Евсеев, “Оценка эффективности инвестиций в безопасность организаций банковского сектора на основе синергетической модели угроз”, *Системи обробки інформації*, № 2(148), с. 88 – 94, 2017.

47. О. Маркова, “Совершенствование информационной безопасности электронных расчетов в коммерческих банках России”, *Финансовая аналитика: проблемы и решения*, 31, с. 38 – 49, 2015.

48. С. Евсеев, С. Остапов, Х. Рзаев, та В. Николаенко, “Оцінка обміну даними в глобальних обчислювальних мережах на основі комплексного показника якості обслуговування мережі”, Науковий журнал Радіоелектроніка, інформатика, управління, № 1(40), с. 115 – 128, 2017.

49. С. Евсеев, О. Король, Х. Рзаев, и З. Иманова, “Разработка модифицированной несимметричной крипто-кодовой системы Мак-Элиса на укороченных эллиптических кодах”, *Восточно-европейский журнал передовых технологий*, том 4. 9(82), с. 18 – 26, 2016.

50. С. Евсеев, Х. Рзаев, и А. Цыганенко, “ Анализ программной реализации прямого и обратного преобразования по методу недвоичного равновесного кодирования”, *Науково-технічний журнал “Безпека інформації”*, том.22, № 2, с. 196 – 203, 2016.

51. С. Евсеев, О. Король, и Г. Коц, “Construction of hybrid security systems based on the crypto-code structures and flawed codes”, *Восточно-европейский журнал передовых технологий*, 4/9(88), с. 4 – 21, 2017.

52. С. Евсеев, “Использование ущербных кодов в крипто-кодовых системах”, *Системи обробки інформації*, № 5 (151) , с. 109 – 121, 2017.

53. С. Евсеев, А. Андрощук, та В. Федорченко, “Побудова систем безпеки інформаційно-телекомунікаційних систем на основі комплексного крипто-графічного підходу”, Збірник наукових праць Нац. академії Держ. прикор. служби України ім. Богдана Хмельницького, № 2(72), с. 258 – 268, 2017.

54. C. Scheau, A. Arsene, and G. Dinca, “Phishing and e-commerce: an information security management problem”, Journal of Defence Resources Management, vol.7, № 1 (12), pp. 129 – 140, 2016.

55. Ab. Alhothaily, A. Alrawais, T. Song, B. Lin, and X. Cheng, “QuickCash: Secure Transfer Payment Systems”, *Sensors*, № 17, 1376, pp.1 – 20, 2017. doi:10.3390/s17061376.

56. О. Юсупова, “Безопасность транзакций при использовании интернет-банкинга”, *Финансовая аналитика: проблемы и решения*, № 35, с. 26 – 40, 2016.

57. С. Евсеев, и О. Король, “Исследование методов двухфакторной аутентификации”, *Системи обробки інформації*, № 2(118), с. 81– 87, 2014.

58. С. Евсеев, и В. Абдулаев, “Алгоритм мониторинга метода двухфакторной аутентификации на основе системы Passwindow”, *Восточно-европейский журнал передовых технологий*, вып. 2/2(74), с. 9 – 15, 2015.

59. С. Евсеев, Г. Коц, и Е. Лекарев, “Developing of multi-factor authentication method based on Niederreiter-McEliece modified crypto-code system”, *Восточно-европейский журнал передовых технологий*, 6/4(84), с. 11 – 23, 2016.

60. С. Евсеев, О. Король, Г. Коц, С. Минухин, и А. Холодкова, “The development of the method of multifactor authentication based on hybrid crypto-code constructions on defective codes”, *Восточно-европейский журнал передовых технологий*, 5/9(89), с. 19 – 36, 2017.

61. Банк данных угроз безопасности информации. [Электроний ресурс]. Доступно : http://bdu.fstec.ru/vul. Дата обращения: Декабрь, 5.2017

62. S. Yevseiev, V. Ponomarenko, and O. Rayevnyeva, “Evaluation of the functional efficiency of the corporate scientific-educational network based on complex quality of service indicators”, *Восточно-европейский журнал передовых технологий*, 6/2 (90), с. 4 – 15, 2017. *Scopus*

63.Р. Грищук, та С. Євсеєв, “Методологія побудови системи забезпечення інформаційної безпеки банківської інформації в автоматизованих банківських системах”, *Науково-технічний журнал “Безпека інформації”*, том 23, № 3, с. 204 – 214, 2017.

64. В. М. Постников, и С. Б. Спиридонов, “Методы выбора весовых коэффициентов локальных критериев”, *Издатель ФГБОУ ВПО “МГТУ им. Н.Э. Баумана”. Эл, № ФС 77 – 48211*, Вып. № 3, с.267 – 287, 2016.

65. Постанова НБУ28.09.2017 № 95, “Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України”, [Электроний ресурс]. Доступно : http://zakon2.rada.gov.ua/laws/show/en/v0095500-17/page. Дата звернення: Груд., 5,2017.

66. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0-2014 [Електронний ресурс]. Доступно: www.cbr.ru/credit/gubzi_docs/st-12-14.pdf. Дата звернення: Груд. 7.2017.

ВИСНОВКИ

У дисертації вирішена актуальна науково-прикладна проблема створення методології побудови системи безпеки банківських інформаційних ресурсів для підвищення рівня їх захищеності від загроз безпеці гібридного характеру, що має важливе значення для подальшого розвитку галузі інформаційної безпеки держави.

У процесі виконання дисертаційної роботи отримані такі основні результати:

1. Проведено аналіз сучасних моделей, методів та систем безпеки банківських інформаційних ресурсів організацій банківського сектору як складової систем з критичною кібернетичною інфраструктурою держави. Встановлено, що переважна більшість відомих досліджень орієнтована на розробку або загальних підходів до безпеки банківських інформаційних ресурсів, або створення методів, моделей та засобів забезпечення на основі моделі *CIA*, що не повною мірою враховує сучасні вимоги й підходи до побудови системи безпеки банківських інформаційних ресурсів. Невирішеними аспектами загальної проблеми захисту банківських інформаційних ресурсів залишаються питання розробки цілісної науково-обґрунтованої методології побудови на практиці системи безпеки банківських інформаційних ресурсів, розробка та впровадження в комплексну систему захисту інформації інтегрованих механізмів *CIA* із забезпеченням вимог до швидкодії та достовірності циркуляції банківських інформаційних ресурсів в автоматизованих банківських системах. Результати проведеного аналізу дали можливість чітко визначити завдання дисертаційного дослідження щодо розробки методології побудови системи безпеки банківських інформаційних ресурсів.

2. Вперше розроблено концепцію побудови синергетичної моделі загроз безпеки банківських інформаційних ресурсів, базис якої становить трирівнева модель стратегічного управління безпекою банківських інформаційних технологій. Концепція охоплює всі основні напрямки розвитку діяльності банку щодо безпеки банківських інформаційних ресурсів, ґрунтується на синергетичному підході до вибору найбільш ефективних напрямків досягнення цілей безпеки банківських інформаційних ресурсів на кожному з рівнів моделі управління стратегічним

управлінням безпеки банківських інформаційних технологій з урахуванням величини ризику на кожному рівні та забезпеченням дієвого контролю за виконанням функцій системи управління інформаційною безпекою організацій банківського сектору.

3. Удосконалено класифікатор загроз безпеці банківських інформаційних ресурсів, який, на відміну від існуючих, ґрунтується на синергетичній моделі загроз, що дозволяє класифікувати загрози за складовими безпеки, видами послуг та рівнями ієрархії інфраструктури автоматизованих банківських систем, оцінювати синергію та гібридність загроз інформаційній безпеці, кібербезпеці, безпеці інформації, ймовірність їх впливу на безпеку банківських інформаційних ресурсів. Розроблено програмний засіб, що реалізує удосконалений класифікатор. Практична реалізація класифікатора дозволяє в он-лайн режимі формувати експертну оцінку рівня загроз банківських інформаційних ресурсів, аналізувати їх синергію та гібридність, оцінювати ймовірність впливу загроз інформаційній безпеці, кібербезпеці, безпеці інформації на безпеку банківських інформаційних ресурсів без значних витрат інвестицій та людських ресурсів (електронний доступ до ресурсу: http://skl.hneu.edu.ua/).

4. Вперше розроблено метод оцінювання узагальненого показника рівня захищеності банківських інформаційних ресурсів. Розроблено практичну методику для оцінювання рівня захищеності банківських інформаційних ресурсів на основі синергетичної моделі загроз, удосконалених класифікатора загроз та моделі зловмисника, моделі оцінки захищеності банківських інформаційних ресурсів та моделі інфраструктури автоматизованих банківських систем, що дозволяє оптимізувати витрати коштів на побудову системи безпеки банківських інформаційних ресурсів. Практична значимість полягає у можливості своєчасного оцінювання взаємозв’язків між активами банківських інформаційних ресурсів, елементами інфраструктури, технічними засобами захисту автоматизованих банківських систем і можливими проявами загроз інформаційній безпеці, кібербезпеці та безпеці інформації, що дозволяє своєчасно корегувати керівні документи банку з інформаційної безпеки, планувати інвестування в технічні засоби

захисту інформації, формувати превентивні заходи для недопущення реалізації загроз.

5. Вперше розроблено метод забезпечення конфіденційності та цілісності банківських інформаційних ресурсів на гібридних крипто-кодових конструкціях зі збитковими кодами. Метод базується на модифікованій крипто-кодовій системі Мак-Еліса на модифікованих алгеброгеометричних кодах, що інтегровано (одним механізмом) забезпечує безпеку банківських інформаційних ресурсів (безпечний час – $T_Б$> 200 р., стійкість до криптоаналізу P_K <10^{25}–10^{35} групових операцій), достовірність передачі банківських інформаційних ресурсів в автоматизованих банківських системах ($P_{пом}$ <10^{-9}) та зменшення енергетичних витрат на їх практичну реалізацію в 10 – 12 разів (шифрування, розшифрування) за рахунок зменшення порядку *GF (q)*. Впровадження запропонованого методу дозволяє підвищити рівень захищеності банківських інформаційних ресурсів та забезпечити своєчасне реагування на вимоги міжнародних і національних регуляторів безпеки банківських інформаційних ресурсів за рахунок зміни окремих параметрів та модифікації застосування модифікованих крипто-кодових систем Мак-Еліса і Нідеррайтера з системами багатоканальної криптографії на збиткових кодах.

6. Вперше розроблено метод двофакторної автентифікації на гібридних крипто-кодових конструкціях зі збитковими кодами на основі модифікованих крипто-кодових систем Мак-Еліса і Нідеррайтера з *MEC*, що дозволяє забезпечити рівень стійкості *OTP*-паролів при передачі відкритими каналами зв’язку та зберегти можливість подальшого використання протоколу двофакторної автентифікації на основі *SMS*-повідомлень. Не зважаючи на зменшення потужності поля Галуа до $GF(2^6)$ для модифікованих крипто-кодових систем і $GF(2^4)$ для гібридних крипто-кодових конструкцій на збиткових кодах, статистичні характеристики таких крипто-кодових конструкцій виявилися, як мінімум, не гірше традиційних схем Мак-Еліса над $GF(2^{10})$. Всі криптосистеми пройшли 100% тестів, причому найкращий результат показала гібридна крипто-кодова конструкція на укорочених *MEC*: 155 з 189 тестів пройдено на рівні 0,99, що становить 82% від усієї кількості

тестів. При цьому традиційна схема Мак-Еліса на $GF(2^{10})$ показала 149 тестів на рівні 0,99.

7. Набув подальшого розвитку метод оцінювання безпеки банківських інформаційних ресурсів, що на, відміну від відомих, враховує комплексний показник ефективності інвестицій, які виділяються на забезпечення безпеки банківських інформаційних ресурсів, що дозволяє оптимізувати витрати коштів на її побудову в умовах впливу гібридних загроз при одночасному забезпеченні заданого рівня їх безпеки. Практична реалізація методу дозволяє комплексно оцінювати основні показники інвестування в забезпечення безпеки банківських інформаційних ресурсів з урахуванням синергетичного оцінювання загроз інформаційній безпеці, кібербезпеці та безпеці інформації.

8. Вперше розроблено методологію побудови системи безпеки банківських інформаційних ресурсів, яка, на відміну від відомих підходів, реалізує принципово нову концепцію протидії гібридним загрозам банківському сектору держави. Її сутність та зміст полягають в раціональній організації системи безпеки банківських інформаційних ресурсів в умовах одночасної дії на систему загроз інформаційній безпеці, кібербезпеці та безпеці інформації. Такий підхід дозволяє одержати повноцінну та адекватну оцінку рівня захищеності банківських інформаційних ресурсів, що суттєво впливає на величину інвестицій в забезпечення безпеки банківського сектору та відкриває шляхи до прийняття обґрунтованих управлінських рішень з питань забезпечення безпеки банківських інформаційних ресурсів. Практичне використання методології дозволяє забезпечити виконання всього функціоналу системи управління інформаційною безпекою банку на принципово новому підході до оцінювання ймовірності впливу загроз інформаційній безпеці, кібербезпеці та безпеці інформації на безпеку банківських інформаційних ресурсів, без значних часових та експертних витрат на проведення їх оцінювання і аналіз, забезпечити раціональне інвестування в інформаційну безпеку організацій банківського сектору.

Таким чином, запропонована методологія дозволяє забезпечити підвищення рівня захищеності банківських інформаційних ресурсів, отримати максимальну

кількість емерджентних властивостей ***в умовах протидії гібридним загрозам інформаційній безпеці, кібербезпеці та безпеці інформації*** а саме: оцінювання синергізму і гібридності загроз складових безпеки (інформаційній безпеці, кібербезпеці, безпеці інформації) на банківські інформаційні ресурси, мінімізація витрат на інвестування в забезпечення безпеки банківських інформаційних ресурсів, висока швидкість криптоперетворень та доказовий рівень стійкості в інтегрованих механізмах забезпечення цілісності, конфіденційності, автентичності і достовірності банківських інформаційних ресурсів при використанні відкритих каналів зв'язку, оцінювання функціональної ефективності передачі банківських інформаційних ресурсів в автоматизованих банківських системах.

9. Розроблено алгоритмічне забезпечення та програмні застосунки, що дозволило верифікувати запропоновані методи, моделі та методологію і підтвердити їх ефективність у контексті безпеки банківських інформаційних ресурсів. Результати дисертації впроваджено в діяльність ТОВ "Сайфер БІС" – реалізовані програмні бібліотеки криптографічних перетворень інформації на основі модифікованих крипто-кодових систем Нідеррайтера – Мак-Еліса на еліптичних кодах з відкритим ключем на основі збиткових кодів. Розроблені програмні бібліотеки криптографічних перетворень інформації використано у підсистемі автентифікації Інтернет-банкінгу "*ELPay*" (Акт від 18.05.2017), "Мікрокріпт Технолоджіс" – розроблені бібліотеки криптографічних перетворень інформації використано у програмному комплексі захисту миттєвих повідомлень "*Crypto-IM+*" (акт впровадження від 30.11.2017), планується використання в банківській установі у складі перспективного протоколу 2*FA* спільно з ТОВ "ТАНТАРІУМ" (Акт від 14.06.2017), та "МЕГАБАНК" Публічне акціонерне товариство (Акт від 9.06.2017). Результати дисертаційної роботи використовуються у навчальному процесі Харківського національного економічного університету ім. С. Кузнеця, Харківського національного університету "ХПІ", Чернівецького національного університету ім. Ю. Федьковича для підвищення рівня ефективності підготовки фахівців з інформаційної безпеки, безпеки інформації.

ДОДАТКИ

Додаток А

Відомості щодо впровадження результатів роботи

«МЕГАБАНК»
ПУБЛІЧНЕ АКЦІОНЕРНЕ ТОВАРИСТВО

вул. Алчевських, 30, м. Харків, 61002, Україна
тел.: +38 (057) 714 20 05
тел./факс: +38 (057) 714 21 41

megabank
Стабільність від європейських гарантів

№ 02-4795 від «09» 06 20 17 р.

на № ..... від «.....» ..... 20.....р.

Банк ознайомився з результатами наукових досліджень дисертаційної роботи докторанта Євсеєва Сергія Петровича щодо формування 2FA на основі використання багатоканальної автентифікації з обов'язковим шифруванням інформації у кожному каналі на основі крипто-кодових систем з відкритим ключем на ущербних кодах дозволяють забезпечити необхідний рівень безпеки в протоколі двофакторної автентифікації. Для ознайомлення банку були надані програмні бібліотеки модифікованих крипто-кодових систем Мак-Еліса та Нідеррайтера на модифікованих еліптичних кодах. Встановлено, що бібліотеки дозволяють забезпечити високу швидкість криптоперетворень, а доказовий рівень криптостійкості – забезпечує необхідний рівень захисту банківської інформації.

Запропоновані докторантом наукові результати, дозволяють врахувати динаміку розвитку та зміни механізмів можливих несанкціонованих втручань і їх варіацій, в автоматизовані банківські системи.

Банк вважає, що використання запропонованих бібліотек у складі перспективного 2FA протоколу для автентифікації користувачів Інтернет-банкінгу для фізичних осіб, у банківській установі можливо за умови отримання автором експертного висновку, наданого Державною службою спеціального зв'язку та захисту інформації України, у встановленому чинним законодавством порядку, та відповідно до Наказу Міністерства фінансів України від 08.06.2011 № 692 потрібно надати запропонованим бібліотекам та матеріалам дисертаційної роботи докторанта гриф "Конфіденційна" (інформація з обмеженим доступом, крім службової інформації та таємної інформації).

Голова Правління Шипілов О.О.

ПУБЛІЧНЕ АКЦІОНЕРНЕ ТОВАРИСТВО "МЕГАБАНК" megabank № 09804119 № 2 Україна * місто Харків

001886

ЗАТВЕРДЖУЮ:
Виконавчий директор ТОВ «Сайфер БІС»
_____ О.В. Зацепін
«___» _____ 2017 р.

АКТ

про впровадження результатів дисертаційної роботи докторанта кафедри інформаційних систем Харківського національного економічного університету ім. С. Кузнеця Євсеєва Сергія Петровича

Цей акт складено комісією у складі: голови комісії заступника директора з виробництва, ктн Ковтуна В.Ю., провідного розробника Белясника Л.В., старшим розробником Веремеєнко Я.В., про те, що запропонований протокол «2FA» багатофакторної автентифікації на основі модифікованих крипто-кодових систем Нідеррайтера – Мак-Еліса задовольняють основним ймовірносно-часовим вимогам до використання в системах Інтернет-банкінгу, забезпечує конфіденційність за рахунок шифрування двома криптосистемами з відкритим ключем за кожним каналу передачі, забезпечує додатковий рівень ентропії (криптостійкості) за рахунок перетворень на ущербних кодах та забезпечує передачу ущербного зашифрованого тексту в режимі прямого виправлення помилок, що забезпечує вимоги щодо оперативності, які досліджені у дисертаційній роботі Євсеєва Сергія Петровича, а саме:

програмні бібліотеки криптографічних перетворень інформації на основі модифікованих крипто-кодових систем Нідеррайтера – Мак-Еліса на еліптичних кодах з відкритим ключем на основі ущербних кодів, що дозволяють забезпечити високу швидкість криптоперетворень та доказовий рівень криптостійкості, бібліотеку формування ущербу, яка забезпечує зниження енергетичної ємності несиметричної криптосистеми Мак-Еліса, без зниження рівня безпеки.

Розроблені програмні бібліотеки криптографічних перетворень інформації використано у підсистемі автентифікації Інтернет-банкінгу «ELPay».

Вважаємо, що при використання запропонованих бібліотек у складі Інтернет-банкінгу, який розгорнуто у банківській установі, відповідно до

Наказу Міністерства фінансів України від 08.06.2011 № 692, для забезпечення безпеки інформаційних банківських системи, потрібно надати запропонованим бібліотекам та матеріалам дисертаційної роботи докторанта гриф «Конфіденційна» (інформація з обмеженим доступом, крім службової інформації та таємної інформації).

Голова комісії: _____ В.Ю. Ковтун

Члени комісії:

_____ Л.В. Белясник

_____ Я.В. Веремеєнко

ЗАТВЕРДЖУЮ:
Генеральний директор
ТОВ «Мікрокрипт Текнолоджіс»
"30" листопада 2017 р.

АКТ

про впровадження результатів дисертаційної роботи докторанта кафедри інформаційних систем Харківського національного економічного університету імені Семена Кузнеця
Євсеєва Сергія Петровича

Цей акт складено генеральним директором ТОВ «Мікрокрипт Текнолоджіс» Головашичем Сергієм Олександровичем, про те, що запропоновані гібридні крипто-кодові конструкції зі збитковими кодами можуть застосовуватися для забезпечення послуг конфіденційності, автентичності та цілісності інформації в автоматизованих банківських системах, в умовах дії загроз кібербезпеки. Запропонована модифікована крипто-кодова система Мак-Еліса на модифікованих еліптичних кодах забезпечує підвищення криптостійкості зазначених послуг при фіксованих (заданих) значеннях ймовірності виправлення помилок у блоці криптограми.

Модифікована крипто-кодова система Мак-Еліса, які досліджена у дисертаційній роботі Євсеєва Сергія Петровича була втілена у програмній бібліотеці криптографічних перетворень інформації на основі гібридних крипто-кодових конструкцій зі збитковими кодами на основі модифікованих крипто-кодових систем Нідеррайтера – Мак-Еліса на модифікованих еліптичних кодах, що дозволяють забезпечити високу швидкість криптоперетворень та доказовий рівень криптостійкості, а також бібліотеці формування ущербного коду, яка забезпечує зниження енергетичної ємності несиметричної криптосистеми Мак-Еліса, без зниження рівня безпеки.

Розроблені програмні бібліотеки криптографічних перетворень інформації використано у програмному комплексі захисту миттєвих повідомлень “Crypto-IM+”.

Вважаю, що при використанні запропонованих бібліотек у складі автоматизованої банківської системи, відповідно до Наказу Міністерства фінансів України від 08.06.2011 № 692, для забезпечення безпеки інформаційних банківських систем, потрібно надати запропонованим бібліотекам та матеріалам дисертаційної роботи докторанта гриф “Конфіденційно” (інформація з обмеженим доступом, крім службової інформації та таємної інформації).

Генеральний директор
ТОВ «Мікрокрипт Технолоджіс» Головашич С.О.

ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ * м. Харків * "МІКРОКРИПТ ТЕХНОЛОДЖІС" код 38281163

Продовження додатку А

ЗАТВЕРДЖУЮ:
директор
ТОВ «ТАЛАНТАРІУМ»
_____Кулик Є.Ю.
«14» червня 2017 р.

АКТ
про реалізацію наукових досліджень Євсеєва Сергія Петровича

Комісія у складі: голови комісії – Войткова К.Л. та членів комісії Висоцького В.В., Орлова М.В. розглянула запропоновані особисто Євсеєвим С.П. несиметричні криптосистеми на основі модифікованих крипто-кодових систем з ущербними кодами Мак-Еліса і Нідеррайтера на еліптичних кодах, які задовольняють основним вимогам, що приділяються безпеці банківської інформації в автоматизованих банківських системах.

Запропоновані протоколи модифікованих крипто-кодових систем дозволяють забезпечити швидкість криптоперетворень на рівні сучасних блочних симетричних шифрів (ДСТУ ГОСТ 28147:2009, AES, ДСТУ 7624:2014) з рівнем безпеки доказової стійкості. Реалізація запропонованого протоколу, у вигляді бібліотеки, дозволяє підвищити рівень безпеки при використанні в мобільному програмному забезпеченні за рахунок скорочення довжини тексту за межами не надлишковості, що веде до спотворення смислу повідомлення.

Розроблені програмні бібліотеки криптографічних перетворень інформації використано у підсистемі автентифікації Інтернет-банкінгу «Digital Bank».

Комісія вважає, що при використання запропонованих бібліотек у складі Інтернет-банкінгу «Digital Bank», відповідно до Наказу Міністерства фінансів України від 08.06.2011 № 692, для забезпечення безпеки інформаційних банківських системи, потрібно надати запропонованим бібліотекам та матеріалам дисертаційної роботи докторанта гриф “Конфіденційна” (інформація з обмеженим доступом, крім службової інформації та таємної інформації).

Голова комісії:

Войтков К.Л. _____

Члени комісії:

Висоцький В.В. _____

Орлов М.В. _____

Кінець додатку А

ЗАТВЕРДЖУЮ
Проректор з наукової роботи
Кіровоградського національного
технічного університету

_____ О.М. Левченко
“ ” _____ 2016 р.

АКТ
про впровадження результатів дисертаційної роботи
докторанта кафедри інформаційних систем Харківського національного
економічного університету ім. С. Кузнеця
Євсеєва Сергія Петровича

Цей акт складено у тому, що під час роботи над держбюджетною темою № 36Б115 “Розробка методів синтезу тестових моделей поведінки програмних об’єктів, підвищення оперативності передачі та захисту інформації у телекомунікаційних системах”, (д.р. № 0115U003103), яка виконується у Кіровоградському національному технічному університеті, реалізовано наступний результат наукового дослідження Євсеєва С.П.:

Запропонована, у результаті виконання наукових досліджень Євсеєва Сергія Петровича програмна реалізація методології оцінки безпеки банківської інформації на основі синергетичного підходу дозволяє на основі виявлення емерджентних властивостей забезпечити комплексірований підхід щодо оцінки ризиків в автоматизованих банківських системах організацій банківського сектору.

Керівник ДБ № 36Б115 “Розробка методів синтезу тестових моделей поведінки програмних об’єктів, підвищення оперативності передачі та захисту інформації у телекомунікаційних системах”

доктор технічних наук, професор О.А. Смірнов

Додаток Б

Вихідні дані побудови алгеброгеометричних кодів

Таблиця Б.1 – Конструктивні кодові характеристики еліптичних кодів, побудованих через відображення $\varphi: EC \to P^{k-1}$ над $GF(q)$, $q = 2^m$, $m = \overline{2,6}$

degF	α	*(n, k, d)*				
		GF(4)	*GF(8)*	*GF(16)*	*GF(32)*	*GF(64)*
1	3	9, 3, 6	14, 3, 11	25, 3, 22	44, 3, 41	81, 3, 78
2	6	9, 6, 3	14, 6, 8	25, 6, 19	44, 6, 38	81, 6, 75
3	9	–	14, 9, 5	25, 9, 16	44, 9, 35	81, 9, 72
4	12	–	14, 12, 2	25, 12, 13	44, 12, 32	81, 12, 69
5	15	–	–	25, 15, 10	44, 15, 29	81, 15, 66
6	18	–	–	25, 18, 7	44, 18, 26	81, 18, 63
7	21	–	–	25, 21, 4	44, 21, 23	81, 21, 60
8	24	–	–	–	44, 24, 20	81, 24, 57
9	27	–	–	–	44, 27, 17	81, 27, 54
10	30	–	–	–	44, 30, 14	81, 30, 51
11	33	–	–	–	44, 33, 11	81, 33, 48
12	36	–	–	–	44, 36, 8	81, 36, 45
13	39	–	–	–	44, 39, 5	81, 39, 42
14	42	–	–	–	44, 42, 2	81, 42, 39
15	45	–	–	–	–	81, 45, 36
16	48	–	–	–	–	81, 48, 33
17	51	–	–	–	–	81, 51, 30
18	54	–	–	–	–	81, 54, 27
19	57	–	–	–	–	81, 57, 24
20	60	–	–	–	–	81, 60, 21
21	63	–	–	–	–	81, 63, 18
22	66	–	–	–	–	81, 66, 15
23	69	–	–	–	–	81, 69, 12
24	72	–	–	–	–	81, 72, 9
25	75	–	–	–	–	81, 75, 6
26	78	–	–	–	–	81, 78, 3

Продовження додатку Б

Таблиця Б.2 – Конструктивні кодові характеристики модифікованих еліптичних кодів (укорочені МЕС), побудованих через відображення $\varphi: EC \to P^{k-1}$ над $GF(q)$, $q = 2^m$, $m = \overline{2,6}$

degF	α	*(n, k, d)*				
		GF(4)	*GF(8)*	*GF(16)*	*GF(32)*	*GF(64)*
1	2	7, 2, 5	11, 2, 9	20, 2, 18	32, 2, 30	56, 2, 54
2	4	7, 4, 3	11, 4, 7	20, 4, 16	32, 4, 28	56, 4, 52
3	6	–	11, 6, 5	20, 6, 14	32, 6, 26	56, 6, 50
4	8	–	11, 8, 3	20, 8, 12	32, 8, 24	56, 8, 48
5	10	–	–	20, 10, 10	32, 10, 22	56, 10, 46
6	12	–	–	20, 12, 8	32, 12, 20	56, 12, 44
7	14	–	–	20, 14, 6	32, 14, 18	56, 14, 42
8	16	–	–	–	32, 16, 16	56, 16, 40
9	18	–	–	–	32, 18, 14	56, 18, 38
10	20	–	–	–	32, 20, 12	56, 20, 36
11	22	–	–	–	32, 22, 10	56, 22, 34
12	24	–	–	–	32, 24, 8	56, 24, 32
13	26	–	–	–	32, 26, 6	56, 26, 30
14	28	–	–	–	32, 28, 4	56, 28, 28
15	30	–	–	–	–	56, 30, 26
16	32	–	–	–	–	56, 32, 24
17	34	–	–	–	–	56, 34, 22
18	36	–	–	–	–	56, 36, 20
19	38	–	–	–	–	56, 38, 18
20	40	–	–	–	–	56, 40, 16
21	42	–	–	–	–	56, 42, 14
22	44	–	–	–	–	56, 44, 12
23	46	–	–	–	–	56, 46, 10
24	48	–	–	–	–	56, 48, 8
25	50	–	–	–	–	56, 50, 6
26	52	–	–	–	–	56, 52, 4

Кінець додатку Б

Таблиця Б.3 – Конструктивні кодові характеристики модифікованих еліптичних кодів (подовжені МЕС), побудованих через відображення $\varphi: EC \to P^{k-1}$ над $GF(q)$, $q = 2^m$, $m = \overline{2,6}$

degF	α	*(n, k, d)*				
		GF(4)	*GF(8)*	*GF(16)*	*GF(32)*	*GF(64)*
1	4	11, 4, 7	18, 4, 14	30, 4, 26	52, 4, 41	108, 4, 104
2	8	11, 8, 3	18, 8, 10	30, 8, 22	52, 8, 38	108, 8, 100
3	12	–	18, 12, 6	30, 12, 18	52, 12, 35	108, 12, 96
4	16	–	18, 16, 2	30, 16, 14	52, 18, 32	108, 16, 92
5	20	–	–	30, 20, 10	52, 20, 29	108, 20, 88
6	24	–	–	30, 24, 6	52, 24, 26	108, 24, 84
7	28	–	–	30, 28, 2	52, 28, 23	108, 28, 80
8	32	–	–	–	52, 32, 20	108, 32, 76
9	36	–	–	–	52, 34, 17	108, 36, 72
10	40	–	–	–	52, 40, 14	108, 40, 68
11	44	–	–	–	52, 42, 11	108, 44, 64
12	48	–	–	–	52, 48, 8	108, 48, 60
13	52	–	–	–	–	108, 52, 56
14	56	–	–	–	–	108, 56, 52
15	60	–	–	–	–	108, 60, 48
16	64	–	–	–	–	108, 64, 44
17	68	–	–	–	–	108, 68, 40
18	72	–	–	–	–	108, 72, 36
19	76	–	–	–	–	108, 76, 32
20	80	–	–	–	–	108, 80, 28
21	84	–	–	–	–	108, 84, 24
22	88	–	–	–	–	108, 88, 20
23	92	–	–	–	–	108, 92, 16
24	96	–	–	–	–	108, 96, 12
25	100	–	–	–	–	108, 100, 8
26	104	–	–	–	–	108, 104, 4

Додаток В

Приклади протоколів обміну БІР на основі ГККЗК на *MEC*

Протокол забезпечення конфіденційності обміну БІР з прямим виправленням помилок на основі МНККС Мак Еліса з модифікованим еліптичним кодом (укорочений код)

Алгоритм створення шифрування для відправки повідомлень від абонента *A* до абонента *B*.

Крок 1. Формування закритого ключа абонентом *B* (KR_B)

Вихідні дані: Алгебраїчна крива $x^3+y^2z+yz^2=0$ над полем $GF(2^2)$, точки кривої:

	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9
X	0	0	0	1	2	3	1	2	3
Y	1	0	1	2	2	2	3	3	3
Z	0	1	1	1	1	1	1	1	1

$$H^{EC} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 2 & 3 & 1 & 2 & 3 \\ 0 & 1 & 2 & 2 & 2 & 3 & 3 & 3 \\ 0 & 0 & 1 & 3 & 2 & 1 & 3 & 2 \\ 0 & 0 & 2 & 3 & 1 & 3 & 1 & 2 \\ 0 & 1 & 3 & 3 & 3 & 2 & 2 & 2 \end{bmatrix} \quad G^{EC} = \begin{bmatrix} 2 & 2 & 3 & 0 & 1 & 3 & 0 & 1 \\ 3 & 3 & 2 & 1 & 0 & 2 & 1 & 0 \end{bmatrix}$$

Матриці маскування: *X*, *P*, *D*:

$$X = \begin{bmatrix} 1 & 2 \\ 3 & 0 \end{bmatrix} \quad X^{-1} = \begin{bmatrix} 0 & 2 \\ 3 & 1 \end{bmatrix}$$

$$D = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 3 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 3 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \quad D^{-1} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 3 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

$$P = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} \quad P^{-1} = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{bmatrix}$$

i = 11 – відкритий текст, e = 00000200 – вектор помилки (сеансовий ключ)

Крок 2. Формування відкритого ключа абонентом B (KU_B)

Знаходимо відкритий ключ $G_x^{MEC} = X \times G^{EC} \times P \times D$

$$G_x^{MEC} = \begin{bmatrix} 1 & 2 \\ 3 & 0 \end{bmatrix} \times \begin{bmatrix} 2 & 2 & 3 & 0 & 1 & 3 & 0 & 1 \\ 3 & 3 & 2 & 1 & 0 & 2 & 1 & 0 \end{bmatrix} \times \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} \times$$

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 3 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 3 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 2 & 1 & 3 & 0 & 1 & 1 & 1 & 0 \\ 0 & 2 & 2 & 2 & 2 & 0 & 3 & 2 \end{bmatrix}$$

Крок 3. Шифрування IP АБС абонентом A.

Знаходимо $C_x^* = i \times G_x^{MEC} \oplus e = 11 \times \begin{bmatrix} 2 & 1 & 3 & 0 & 1 & 1 & 1 & 0 \\ 0 & 2 & 2 & 2 & 2 & 0 & 3 & 2 \end{bmatrix} \oplus 00000200 =$

23023322;

Формуємо вектор ініціалізації *IV* = 00100000 на стороні абонентів *A* і *B*

Вектор ініціалізації показує місце скорочення кодової послідовності.

C_x^* = 2323322– в *MV*2;

Крок 4. Нанесення збитку алгоритмом *MV*2.

Таблиця перетворень *MV*2

Слово (перемішується)	Довжина залишку	*C(x)*	*F(x)*
000	2	00	1
001	2	01	1
010	2	10	1
011	2	11	1
100	2	00	0
101	2	01	0
110	2	10	0
111	2	11	0

Початковий текст (слово): $C_x^* = 2323322_{10} = 010\ 011\ 000\ 010\ 011\ 011\ 010\ 010_2$

Крок 5. Відправлення збитку (флагу) першим каналом абоненту *B*, відправлення збиткового коду (залишку) другим каналом абоненту *B*.

Отримуємо C_x^*: 1011001011111010_2

Переводимо в десяткову систему числення: 545750_{10}

В перший канал АБС поступає – 545750

Отримані флаги *F(x)*: 111111111_2

При переведені в десяткову систему числення отримуємо: 777_{10}

В другий канал АБС поступає – 777.

На стороні абонента *B*:

Крок 1. Відновлення отриманого тексту в *MV*2

Отримуємо з першого каналу – $C(x) = 545750_{10}$

з другого отримуємо флаги – $F(x) = 777_{10}$

Переводимо все в двійкову систему числення:

$$C_x^* = 545750_{10} = 1011001011111010_2$$
$$F(x) = 777_{10} = 111111111_2$$

Крок 2. Відновлення збитку алгоритмом *MV*2

За допомогою таблицы перетворень алгоритму *MV*2 отримуємо кодове слово:

Таблиця перетворень *MV*2

Слово (перемішується)	Довжина залишку	*C(x)*	*F(x)*
000	2	00	1
001	2	01	1
010	2	10	1
011	2	11	1
100	2	00	0
101	2	01	0
110	2	10	0
111	2	11	0

Отримуємо текст (кодове слово) – $C_x^* = 010\ 011\ 000\ 010\ 011\ 011\ 010\ 010_2$

Переводимо в десяткову систему числення:

$010\ 011\ 000\ 010\ 011\ 011\ 010\ 010_2 = 2323322_{10}$

Крок 3. Для відновлення закритого тексту уповноважений користувач додає нульові інформаційні символи в місце, на яке вказує вектор ініціалізації *IV*.

IV = 00100000

$C_x^* = 2323322 – 23023322$

Крок 4. З відновленого закритого тексту C_x знімаємо дію секретних перестановочної і діагональної матриць.

Знаходимо $C_x^* = C_x \times D^{-1} \times P^{-1}$

$$C_x^* = 23123322 \times \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 3 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \times \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{bmatrix} =$$

= 22102221

$$C_x^* = 22102221$$

Крок 5. Знаходимо синдром і многочлен локаторів помилок.

Знаходимо $S = C_x^* \times H^{EC^T}$,

$$S = 22102221 \times \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 2 & 3 & 1 & 2 & 3 \\ 0 & 1 & 2 & 2 & 2 & 3 & 3 & 3 \\ 0 & 0 & 1 & 3 & 2 & 1 & 3 & 2 \\ 0 & 0 & 2 & 3 & 1 & 3 & 1 & 2 \\ 0 & 1 & 3 & 3 & 3 & 2 & 2 & 2 \end{bmatrix}$$

Знаходимо синдром

S_{00}= 1

S_{10}= 2+1+2+3+3=1

S_{01}= 2+3+3+1+1+3=1

S_{20}= 2+3+2+1+2=0

S_{11}= 3+2+1+2+2=0

S_{02}= 2+1+1+3+3+2=0

$$S = (1,1,1,0,0,0);$$

Знаходимо многочлен локаторів помилок $\Lambda(x) = a_{00}+a_{10}x+y = 0$

$$\begin{bmatrix} S_{00} & S_{10} \\ S_{10} & S_{20} \end{bmatrix} \times \begin{bmatrix} a_{00} \\ a_{01} \end{bmatrix} = \begin{bmatrix} S_{01} \\ S_{11} \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \end{bmatrix} \qquad a_{00}=0; \quad a_{10}=1;$$

$\Lambda\ (xy) = x+y= 0$ – многочлен локаторів помилок

Крок 6. Знаходимо локатори помилок за процедурою Ченя.

$P_1(0,0,1)\ \Lambda\ (x,y) = 0+0=0$ – помилка

$P_2(0,1,1)\ \Lambda\ (x,y) = 0+1=1$

$P_3(1,2,1)\ \Lambda\ (x,y) = 1+2=3$

$P_4(2,2,1)\ \Lambda\ (x,y) = 2+2=0$ – помилка

$P_5(3,2,1)\ \Lambda\ (x,y) = 3+2=1$

$P_6(1,3,1)\ \Lambda\ (x,y) = 1+3=2$

$P_7(2,3,1)\ \Lambda\ (x,y) = 2+3=1$

$P_8(3,3,1)\ \Lambda\ (x,y) = 3+3=0$ – помилка

$$e^* = e_1 00 e_4 000 e_8$$

Знаходимо: $e^* \times H^{EC^T} = S$, вирішивши систему рівнянь отримаємо

$e_1 = 0$, $e_4 = 2$, $e_8 = 3$

$$e^* = 00020003$$

Знаходимо $i^* = e^* + C_x^*$

$i^* = 00020003 \oplus 22102221 = 22;$

Крок 7. Знаходимо відкритий текст

$$i = i^* \times X^{-1},\ i = 22 \times \begin{bmatrix} 0 & 2 \\ 3 & 1 \end{bmatrix} = 11$$

Протокол забезпечення конфіденційності обміну БІР з прямим виправленням помилок на основі МНККС Мак Еліса з модифікованим еліптичним кодом (подовжений код)

Алгоритм створення шифрування для відправки повідомлень від абонента *A* до абонента *B*.

Крок 1. Формування закритого ключа абонентом *B* (KR_B)

Вихідні дані: Алгебраїчна крива $x^3+y^2z+yz^2=0$ над полем $GF(2^2)$, точки кривої:

	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9
X	0	0	0	1	2	3	1	2	3
Y	1	0	1	2	2	2	3	3	3
Z	0	1	1	1	1	1	1	1	1

$$H^{EC} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 2 & 3 & 1 & 2 & 3 \\ 0 & 1 & 2 & 2 & 2 & 3 & 3 & 3 \\ 0 & 0 & 1 & 3 & 2 & 1 & 3 & 2 \\ 0 & 0 & 2 & 3 & 1 & 3 & 1 & 2 \\ 0 & 1 & 3 & 3 & 3 & 2 & 2 & 2 \end{bmatrix} \quad G^{EC} = \begin{bmatrix} 2 & 2 & 3 & 0 & 1 & 3 & 0 & 1 \\ 3 & 3 & 2 & 1 & 0 & 2 & 1 & 0 \end{bmatrix}$$

Матриці маскування: *X*, *P*, *D*:

$$X = \begin{bmatrix} 1 & 2 \\ 3 & 0 \end{bmatrix} \quad X^{-1} = \begin{bmatrix} 0 & 2 \\ 3 & 1 \end{bmatrix}$$

$$D = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 3 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 3 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \quad D^{-1} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 3 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

$$P = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} \quad P^{-1} = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{bmatrix}$$

i = 11 – відкритий текст, e = 00000200 – вектор помилки (сеансовий ключ)

Крок 2. Формування відкритого ключа абонентом B (KU_B)

Знаходимо відкритий ключ $G_x^{MEC} = X \times G^{EC} \times P \times D$

$$G_x^{MEC} = \begin{bmatrix} 1 & 2 \\ 3 & 0 \end{bmatrix} \times \begin{bmatrix} 2 & 2 & 3 & 0 & 1 & 3 & 0 & 1 \\ 3 & 3 & 2 & 1 & 0 & 2 & 1 & 0 \end{bmatrix} \times \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} \times$$

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 3 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 3 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 2 & 1 & 3 & 0 & 1 & 1 & 1 & 0 \\ 0 & 2 & 2 & 2 & 2 & 0 & 3 & 2 \end{bmatrix}$$

Крок 3. Шифрування IP АБС абонентом A.

Знаходимо $C_x^* = i \times G_x^{MEC} \oplus e = 11 \times \begin{bmatrix} 2 & 1 & 3 & 0 & 1 & 1 & 1 & 0 \\ 0 & 2 & 2 & 2 & 2 & 0 & 3 & 2 \end{bmatrix} \oplus 00000200 =$

23023322;

Формуємо вектор ініціалізації *IV* = 00100000 на стороні абонентів *A* і *B*

Вектор ініціалізації показує місце подовження кодової послідовності.

$$C_x^* = 23123322_{10} \text{– в } MV2;$$

Крок 4. Нанесення збитку алгоритмом *MV*2.

Таблиця

Таблиця перетворень *MV*2

Слово (перемішується)	Довжина залишку	*C(x)*	*F(x)*
000	2	00	1
001	2	01	1
010	2	10	1
011	2	11	1
100	2	00	0
101	2	01	0
110	2	10	0
111	2	11	0

Початковий текст (слово): $C_x^* = 23123322_{10} = 010\ 011\ 001\ 000\ 010\ 011\ 011\ 010\ 010_2$

Крок 5. Відправлення збитку (флагу) першим каналом абоненту *B*, відправлення збиткового коду (залишку) другим каналом абоненту *B*.

Отримуємо $C_x^* = 100111001011111010_2$

При переведені в десяткову систему числення отримуємо: 471372_{10}

В перший канал АБС поступає – 471372_{10}

Отримані флаги: $F(x) = 111111111_2$

При переведені в десяткову систему числення отримуємо: 777_{10}

В другий канал АБС поступає – 777.

На стороні абонента В:

Крок 1. Відновлення отриманого тексту в MV2

Отримуємо з першого каналу – $C(x) = 471372_{10}$

з другого отримуємо флаги – $F(x) = 777_{10}$

Переводимо все в двійкову систему числення:

$$C_x^* = 471372_{10} – 1001110010111110_{2}$$

$$F(x) = 777_{10}\text{-}111111111_{2}$$

Крок 2. Відновлення збитку алгоритмом *MV*2

Таблиця

Таблиця перетворень *MV*2

Слово (перемішується)	Довжина залишку	*C(x)*	*F(x)*
000	2	00	1
001	2	01	1
010	2	10	1
011	2	11	1
100	2	00	0
101	2	01	0
110	2	10	0
111	2	11	0

Отримуємо текст (слово) – $C_x^* = 010\ 011\ 001\ 000\ 010\ 011\ 011\ 010\ 010_2$
Переводимо в десяткову систему числення:

$C_x^* = 010\ 011\ 001\ 000\ 010\ 011\ 011\ 010\ 010_2 = 23123322_{10}$

Крок 3. Для відновлення закритого тексту уповноважений користувач за допомогою вектору ініціалізації *IV* відновлює ключову послідовність

$IV = 00100000$

$C_x^* = 23123322_{10} – 23023322_{10}$

Крок 4. З відновленого закритого тексту C_x знімаємо дію секретних перестановочної і діагональної матриць.

Знаходимо $C_x* = C_x \times D^{-1} \times P^{-1}$

$$C_x* = 23023322 \times \begin{bmatrix} 1&0&0&0&0&0&0&0 \\ 0&3&0&0&0&0&0&0 \\ 0&0&2&0&0&0&0&0 \\ 0&0&0&1&0&0&0&0 \\ 0&0&0&0&3&0&0&0 \\ 0&0&0&0&0&2&0&0 \\ 0&0&0&0&0&0&1&0 \\ 0&0&0&0&0&0&0&1 \end{bmatrix} \times \begin{bmatrix} 0&0&0&1&0&0&0&0 \\ 1&0&0&0&0&0&0&0 \\ 0&0&0&0&1&0&0&0 \\ 0&0&1&0&0&0&0&0 \\ 0&1&0&0&0&0&0&0 \\ 0&0&0&0&0&0&1&0 \\ 0&0&0&0&0&0&0&1 \\ 0&0&0&0&0&1&0&0 \end{bmatrix} =$$

$$= 22102221$$

$$C_x* = 22102221$$

Крок 5. Знаходимо синдром і многочлен локаторів помилок.

Знаходимо $S = C_x^* \times H^{EC^T}$,

$$S = 22102221 \times \begin{bmatrix} 1&1&1&1&1&1&1&1 \\ 0&0&1&2&3&1&2&3 \\ 0&1&2&2&2&3&3&3 \\ 0&0&1&3&2&1&3&2 \\ 0&0&2&3&1&3&1&2 \\ 0&1&3&3&3&2&2&2 \end{bmatrix}$$

Знаходимо синдром

S_{00}= 1

S_{10}= 2+1+2+3+3=1

S_{01}= 2+3+3+1+1+3=1

S_{20}= 2+3+2+1+2=0

S_{11}= 3+2+1+2+2=0

S_{02}= 2+1+1+3+3+2=0

$$S = (1,1,1,0,0,0);$$

Знаходимо многочлен локаторів помилок $\Lambda(x) = a_{00}+a_{10}x+y = 0$

$$\begin{bmatrix} S_{00} & S_{10} \\ S_{10} & S_{20} \end{bmatrix} \times \begin{bmatrix} a_{00} \\ a_{01} \end{bmatrix} = \begin{bmatrix} S_{01} \\ S_{11} \end{bmatrix} \quad \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \end{bmatrix} \qquad a_{00}=0; \quad a_{10}=1;$$

$\Lambda(xy) = x+y= 0$ – многочлен локаторів помилок

Крок 6. Знаходимо локатори помилок за процедурою Ченя.

$P_1(0,0,1)$ $\Lambda(x,y) =0+0=0$– помилка

$P_2(0,1,1)$ $\Lambda(x,y) =0+1=1$

$P_3(1,2,1)$ $\Lambda(x,y) =1+2=3$

$P_4(2,2,1)$ $\Lambda(x,y) =2+2=0$– помилка

$P_5(3,2,1)$ $\Lambda(x,y) =3+2=1$

$P_6(1,3,1)$ $\Lambda(x,y) =1+3=2$

$P_7(2,3,1)$ $\Lambda(x,y) =2+3=1$

$P_8(3,3,1)$ $\Lambda(x,y) =3+3=0$– помилка

$$e^* = e_1 00 e_4 000 e_8$$

Знаходимо : $e^* \times H^{EC^T} = S$, вирішивши систему рівнянь отримаємо

$e_1 =0,\ e_4 = 2,\ e_8 =3$

$$e^* = 00020003$$

Знаходимо $i^* = e^* + C_x^*$

$i^* = 00020003 \oplus 22102221 = 22;$

Крок 7. Знаходимо відкритий текст

$i = i^* \times X^{-1}$

$$\text{i} = 22 \times \begin{bmatrix} 0 & 2 \\ 3 & 1 \end{bmatrix} = 11$$

Додаток Д

Лістинг гібридних крипто-кодових конструкцій з збитковими кодами

```
void clearStatisticsData() {
	sumCount = 0;
	subtractCount = 0;
	multiplyCount = 0;
	divideCount = 0;
	compareCount = 0;
}

void printStatisticsData() {
	cout << "\n";
	cout << "Sum count: " << sumCount << "\n";
	cout << "Subtract count: " << subtractCount << "\n";
	cout << "Multiply count: " << multiplyCount << "\n";
	cout << "Divide count: " << divideCount << "\n";
	cout << "Compare count: " << compareCount << "\n";
	cout << "All count: " << sumCount + subtractCount + multiplyCount +
divideCount + compareCount << "\n";
}

vector<bool> convertFxToDK(int r, int n, int fx) {
	vector<bool> vectorDK;
	compareCount++;
	if (fx > 0 && fx <= (n - r + 1)) {
		compareCount++;
		if (fx == (n - r + 1)) {
			for (int i = 0; i < fx - 1; ++i) {
				compareCount++;
				sumCount++;
				vectorDK.push_back(false);
			}
		}
		else {
			for (int i = 0; i < fx - 1; ++i) {
				compareCount++;
				sumCount++;
				vectorDK.push_back(false);
			}
			vectorDK.push_back(true);
		}
	}
	return vectorDK;
}

int convertDKToFx(vector<bool> dk) {
	int s = dk.size();
	compareCount++;
	if (dk[s - 1]) {
		subtractCount++;
		s--;
	}
	sumCount++;
	return s+1;
}

vector<bool> convertBase10To2(int dec, int length) {
	vector<bool> res;
	while (length != 0) {
		compareCount++;
		subtractCount++;
```

```
                length--;
                divideCount++;
                res.push_back(dec % 2);
                divideCount++;
                dec /= 2;
        }
        reverse(begin(res), end(res));
        return res;
}

int convertBase2To10(vector<bool> base2, int start, int size) {
        int result = 0;
        for (int i = start; i < start+size; ++i) {
                sumCount++;
                compareCount += 2;
                if (base2[i]) {
                        sumCount++;
                        subtractCount += 3;
                        result += pow(2, size - (i - start) - 1);
                }
        }
        return result;
}

int convertBase2To10(vector<bool> base2) {
        return convertBase2To10(base2, 0, base2.size());
}

void printVectorRow(vector<bool> v) {
        for (int i = 0; i < v.size(); ++i) {
                if (v[i]) {
                        cout << 1;
                }
                else {
                        cout << 0;
                }
        }
}

void printVectorRow(vector<char> v) {
        for (int i = 0; i < v.size(); ++i) {
                cout << v[i];
        }
}


struct SubstitutionRow
{
        int ostLength;
        vector<bool> ost;
        int flagFx;
};

class SubstitutionTable {
public:
        vector<SubstitutionRow> tableData;
        vector<int> wordsArray;

        void init(int r, int n) {
                multiplyCount += 2;
                int twoPowN = pow(2, n);
                int twoPowR = pow(2, r);
```

```
                subtractCount++;
                sumCount++;
                int lastPhase = twoPowN - twoPowR + 1;
                int ostValue = 0;
                int ostLength = r;
                subtractCount++;
                int flagFx = n - r;
                multiplyCount++;
                int next2powOstLen = pow(2, ostLength);
                //when ostLength++ then flagFx--
                for (int i = 1; i < lastPhase; ++i) {
                        sumCount++;
                        compareCount++;
                        SubstitutionRow substitutionRow;
                        substitutionRow.flagFx = flagFx;
                        substitutionRow.ostLength = ostLength;
                        substitutionRow.ost = convertBase10To2(ostValue,
ostLength);
                        tableData.push_back(substitutionRow);

                        sumCount++;
                        ostValue++;
                        compareCount++;
                        if (ostValue >= next2powOstLen) {
                                ostValue = 0;
                                sumCount++;
                                ostLength++;
                                subtractCount++;
                                flagFx--;
                                multiplyCount++;
                                next2powOstLen = pow(2, ostLength);
                        }
                }
                ostLength = r;
                sumCount++;
                subtractCount++;
                flagFx = n - r + 1;
                ostValue = 0;
                for (int i = lastPhase; i <= twoPowN; ++i) {
                        sumCount++;
                        compareCount++;
                        SubstitutionRow substitutionRow;
                        substitutionRow.flagFx = flagFx;
                        substitutionRow.ostLength = ostLength;
                        substitutionRow.ost = convertBase10To2(ostValue,
ostLength);
                        sumCount++;
                        ostValue++;
                        tableData.push_back(substitutionRow);
                }
                multiplyCount++;
                int powOfTwo = pow(2, n);
                for (int i = 0; i < powOfTwo; ++i) {
                        sumCount++;
                        compareCount++;
                        wordsArray.push_back(i);
                }
                random_shuffle(wordsArray.begin(), wordsArray.end());
        }

        int indexOfRowByWord(int word) {
```

```
                for (int i = 0; i < wordsArray.size(); ++i) {
                        sumCount++;
                        compareCount += 2;
                        if (wordsArray[i] == word) {
                                return i;
                        }
                }
                throw std::invalid_argument("This (int) word [" + to_string(word) +
"] does not exist in table!!");
        }

        void printTable() {
                for (int i = 0; i < tableData.size(); ++i) {
                        cout << wordsArray[i] << " | ";
                        cout << tableData[i].ostLength << " | ";
                        printVectorRow(tableData[i].ost);
                        cout << " | ";
                        cout << tableData[i].flagFx;
                        cout << "\n";
                }
        }
};

struct EncodedData
{
        vector<bool> osts;
        vector<bool> flags;
};

EncodedData encodeString(int r, int n, string strMsg, SubstitutionTable
substitutionTable) {
        EncodedData encodedData;
        compareCount++;
        if (n != 8) {
                //get words
                throw std::invalid_argument("This realisation works only with N ==
8 !!! But you use: " + to_string(n));
        }
        for (int i = 0; i < strMsg.size(); ++i) {
                sumCount++;
                compareCount++;
                int wordRowIndex = substitutionTable.indexOfRowByWord((int)
strMsg.at(i));
                encodedData.osts.insert(encodedData.osts.end(),
                        substitutionTable.tableData[wordRowIndex].ost.begin(),
                        substitutionTable.tableData[wordRowIndex].ost.end());
                vector<bool> flag = convertFxToDK(r, n,
substitutionTable.tableData[wordRowIndex].flagFx);
                encodedData.flags.insert(encodedData.flags.end(),
                        flag.begin(),
                        flag.end());
        }
        return encodedData;
}

vector<bool> decodeData(int r, int n, EncodedData encodedData, SubstitutionTable
substitutionTable) {
        vector<int> flags;
        int zeroInRow = 0;
        for (int i = 0; i < encodedData.flags.size(); ++i) {
                sumCount++;
```

```
                compareCount += 2;
                if (!encodedData.flags[i]) {
                        sumCount++;
                        zeroInRow++;
                }
                else {
                        sumCount++;
                        flags.push_back(zeroInRow + 1);
                        zeroInRow = 0;
                        continue;
                }
                compareCount++;
                subtractCount++;
                if (zeroInRow == n - r) {
                        subtractCount++;
                        sumCount++;
                        flags.push_back(n - r + 1);
                        zeroInRow = 0;
                }
        }

        vector<bool> res;

        for (int i = 0; i < flags.size(); ++i) {
                sumCount++;
                compareCount++;
                subtractCount += 2;
                int d = n - r - flags[i];
                sumCount++;
                int s = r + d;
                compareCount++;
                if (s < r) {
                        s = r;
                }
                vector<bool> ostV;
                for (int j = 0; j < s; ++j) {
                        sumCount++;
                        compareCount++;
                        ostV.push_back(encodedData.osts[j]);
                }
                sumCount++;
                encodedData.osts.erase(encodedData.osts.begin(),
encodedData.osts.begin() + s);

                for (int j = 0; j < substitutionTable.tableData.size(); ++j) {
                        compareCount+=2;
                        sumCount++;
                        if (substitutionTable.tableData[j].flagFx == flags[i]) {
                                pair<vector<bool>::iterator, vector<bool>::iterator
> mypair;
                                mypair = mismatch(ostV.begin(), ostV.end(),
substitutionTable.tableData[j].ost.begin());
                                compareCount++;
                                if (mypair.first == ostV.end()) {
                                        vector<bool> r =
convertBase10To2(substitutionTable.wordsArray[j], n);
                                        res.insert(res.end(), r.begin(), r.end());
                                        break;
                                }
                        }
                }
```

```
        }

        return res;
}

vector<char> boolsToChars(vector<bool> data) {
        vector<char> res;
        for (int i = 0; i < data.size() / 8; ++i) {
                compareCount++;
                sumCount++;
                divideCount++;
                multiplyCount++;
                res.push_back((char) convertBase2To10(data, i * 8, 8));
        }
        return res;
}

void genRandomString(char *s, const int len) {
        static const char alphanum[] =
                "0123456789"
                "ABCDEFGHIJKLMNOPQRSTUVWXYZ"
                "abcdefghijklmnopqrstuvwxyz";

        for (int i = 0; i < len; ++i) {
                s[i] = alphanum[rand() % (sizeof(alphanum) - 1)];
        }

        s[len] = 0;
}



int highest_degree(unsigned int a)
{
        int i=63;
        for ( ; i >= 0; --i)
        {
                if((a>>i&1)==1) return i;
        }

        return i;
}

static unsigned int galois_div(unsigned int dividor, unsigned int divisor)
{

        int highest_a=highest_degree(dividor), highest_b=highest_degree(divisor);
        unsigned int quotient=0;
        int diff=0, loop=0;
        while(highest_a>=highest_b)
        {
                loop++;
                if (loop>30)
                {
                        break;
                }
                diff=highest_a-highest_b;
                quotient^=(0x00000001<<diff);
                dividor^=(divisor<<diff);
                highest_a=highest_degree(dividor);
        }
```

```
        return quotient;
}


static unsigned int mul(unsigned int a, unsigned int b)
{
        unsigned int output=0;
        for (int i = 0; i <=31; ++i)
        {
                if(((b>>i)&1)==1) output^=(a<<i);
        }
        return output;
}

unsigned int galois_mul(unsigned int a, unsigned int b, unsigned int P_x)
{
        unsigned int output = mul(a,b);
        return modp(output, P_x);
}

//This gives you the inverse in GF(2^8);
unsigned int inverse(unsigned int input, unsigned int P_x)
{
        unsigned int r0=P_x, r1=input, t0=0,t1=1;
        unsigned int q=0, temp=0;
        while(r1>0)
        {
                q=galois_div(r0,r1);
                temp=r0;
                r0=r1;
                r1=temp^mul(q,r1);

                temp=t0;
                t0=t1;
                t1=temp^mul(q,t1);
        }
        return modp(t0, P_x);
}

unsigned int modp(unsigned int input, unsigned int P_x)
{
        input^=mul(galois_div(input,P_x),P_x);
        return input;
}

unsigned int galois_pow(unsigned input, int power, unsigned int P_x)
{
        unsigned int output = 1;
        for (int i = 0; i < power; ++i)
        {
                output = galois_mul(output,input,P_x);
        }
        return output;
}

Poly_t Euclidean_add_p(Poly_t oprand_1, Poly_t oprand_2, const Field_t GF){
    if(oprand_1.degree > oprand_2.degree){
        for(unsigned i = oprand_2.degree + 1; i < oprand_1.degree + 1; i++){
            oprand_2.coefficient[i] = 0;
        }
```

```
        oprand_2.degree = oprand_1.degree;
    }else{
        for(unsigned i = oprand_1.degree + 1; i < oprand_2.degree + 1; i++){
            oprand_1.coefficient[i] = 0;
        }
        oprand_1.degree = oprand_2.degree;
    }

    Poly_t result;
    result.degree = oprand_1.degree;
    for(unsigned i = 0; i < result.degree + 1; i++){
        result.coefficient[i] = Euclidean_add_c(oprand_1.coefficient[i],
oprand_2.coefficient[i]);
    }
    while((result.coefficient[result.degree] == 0)&&(result.degree > 0)){
        result.degree--;
    }
    return result;
}

unsigned Euclidean_mult_cc(unsigned oprand_1, unsigned oprand_2, const Field_t
GF){
    unsigned result;
    if((oprand_1%GF.max_ele == 0)||(oprand_2%GF.max_ele == 0)){
        result = 0;
    }else{
        result = GF.gen[((GF.gen_inv[oprand_1%GF.max_ele] - 1) +
(GF.gen_inv[oprand_2%GF.max_ele] - 1))%(GF.max_ele - 1) + 1];
    }
    return result;
}

Poly_t Euclidean_mult_pc(Poly_t oprand_1, unsigned oprand_2, const Field_t GF){
    Poly_t result;
    result.degree = oprand_1.degree;
    for(unsigned i = 0; i < result.degree + 1; i++){
        result.coefficient[i] = Euclidean_mult_cc(oprand_1.coefficient[i],
oprand_2, GF);
    }
    if(oprand_2 == 0){
        result.degree = 0;
    }
    return result;
}

Poly_t Euclidean_mult_pz(Poly_t oprand, unsigned time, const Field_t GF){
    Poly_t result;
    result.degree = oprand.degree + time;
    for(unsigned i = 0; i < time; i++){
        result.coefficient[i] = 0;
    }
    for(unsigned i = time; i < result.degree + 1; i++){
        result.coefficient[i] = oprand.coefficient[i - time];
    }
    return result;
}

Poly_t Euclidean_mult_pp(Poly_t oprand_1, Poly_t oprand_2, const Field_t GF){
    Poly_t result;
    result.degree = oprand_1.degree + oprand_2.degree;
    for(unsigned i = 0; i < result.degree + 1; i++){
```

```
        result.coefficient[i] = 0;
    }

    for(unsigned i = 0; i < oprand_2.degree + 1; i++){
        result = Euclidean_add_p(result,
Euclidean_mult_pz(Euclidean_mult_pc(oprand_1, oprand_2.coefficient[i], GF), i,
GF), GF);
    }
    return result;
}

Poly_t Euclidean_div_pp(Poly_t divider, Poly_t divisor, const Field_t GF){
    Poly_t result;
    if(divisor.degree == 0){
        result.degree = divider.degree;
        for(unsigned i = 0; i < result.degree + 1; i++){
            if(divider.coefficient[i] != 0){
                result.coefficient[i] =
GF.gen[(GF.gen_inv[divider.coefficient[i]%GF.max_ele] -
GF.gen_inv[divisor.coefficient[0]%GF.max_ele] + (GF.max_ele - 1))%(GF.max_ele - 1)
+ 1];
            }
        }
    }else if(divider.degree < divisor.degree){
        result.degree = 0;
        result.coefficient[0] = 0;
    }else{
        result.degree = divider.degree - divisor.degree;
        for(unsigned i = 0; i < result.degree + 1; i++){
            result.coefficient[i] = 0;
        }
        while((divider.degree >= divisor.degree)&&(divider.degree > 0)){
            result.coefficient[divider.degree - divisor.degree] =
GF.gen[(GF.gen_inv[divider.coefficient[divider.degree]%GF.max_ele] -
GF.gen_inv[divisor.coefficient[divisor.degree]%GF.max_ele] + (GF.max_ele -
1))%(GF.max_ele - 1) + 1];
            divider = Euclidean_add_p(divider,
Euclidean_mult_pz(Euclidean_mult_pc(divisor, result.coefficient[divider.degree -
divisor.degree], GF), divider.degree - divisor.degree, GF), GF);
        }
    }
    return result;
}

Poly_t Euclidean_modp(Poly_t oprand, Poly_t modulo, const Field_t GF){
    return Euclidean_add_p(oprand, Euclidean_mult_pp(Euclidean_div_pp(oprand,
modulo, GF), modulo, GF), GF);
}

Poly_t Euclidean_pow(Poly_t oprand, Poly_t modulo, unsigned power, const Field_t
GF){
    Poly_t result;
    result.degree = 0;
    result.coefficient[0] = 1;
    for(unsigned i = 0; i < power; i++){
        result = Euclidean_modp(Euclidean_mult_pp(result, oprand, GF), modulo,
GF);
    }
    return result;
}
```

```
Poly_t Euclidean_inv(Poly_t oprand, Poly_t modulo, const Field_t GF){
    Poly_t r_1, r_0, u_1, u_0, v_1, v_0;
    u_1.degree = 0;
    u_1.coefficient[0] = 1;
    u_0.degree = 0;
    u_0.coefficient[0] = 0;
    v_1.degree = 0;
    v_1.coefficient[0] = 0;
    v_0.degree = 0;
    v_0.coefficient[0] = 1;
    if(oprand.degree >= modulo.degree){
        r_1 = oprand;
        r_0 = modulo;
    }else{
        r_1 = modulo;
        r_0 = oprand;
    }
    while((r_0.degree != 0)||(r_0.coefficient[0] != 0)){
        Poly_t quotient = Euclidean_div_pp(r_1, r_0, GF);
        Poly_t remainder = Euclidean_add_p(r_1, Euclidean_mult_pp(r_0, quotient,
GF), GF);
        Poly_t temp_u = Euclidean_add_p(u_1, Euclidean_mult_pp(u_0, quotient, GF),
GF);
        Poly_t temp_v = Euclidean_add_p(v_1, Euclidean_mult_pp(v_0, quotient, GF),
GF);
        r_1 = r_0;
        r_0 = remainder;
        u_1 = u_0;
        u_0 = temp_u;
        v_1 = v_0;
        v_0 = temp_v;
    }
    Poly_t result;
    if(oprand.degree >= modulo.degree){
        result = u_1;
    }else{
        result = v_1;
    }
    result = Euclidean_mult_pc(result, GF.gen[GF.max_ele -
GF.gen_inv[r_1.coefficient[0]] + 1], GF);
    return result;
}


mat MyMatrixMul(mat A, mat B, unsigned int p_x)
{
        mat C = zeros(A.n_rows,B.n_cols);
        unsigned int temp;
        for (unsigned int i = 0; i < C.n_rows; ++i)
        {
                for (unsigned int j = 0; j < C.n_cols; ++j)
                {
                        temp = 0;
                        for (unsigned int k = 0; k < A.n_cols; ++k)
                        {
                                temp^= galois_mul((unsigned int)A(i,k),(unsigned
int)B(k,j),p_x);
                        }
                        C(i,j) = temp;
                }
```

```
        }
        return C;
}

mat int2vec(unsigned int input, int length)
{
        mat output=zeros<mat>(length,1);
        for (int i = 0; i < length; ++i)
        {
                if(((input>>i)&0x00000001) == 0x00000001)
                        output(i,0) = 1;
        }
        return output;
}

unsigned int vec2int(mat A, int length)
{
        unsigned int output = 0;
        unsigned int power = 1;
        for (int i = 0; i < length; ++i)
        {
                if(A(i,0)==1)
                        output+= power;
                power*=2;
        }
        return output;
}

unsigned int G_z(unsigned int alpha, unsigned int P_x, unsigned int g_z[],int
degree)
{
        unsigned output = 0;
        unsigned power = 1;
        for (int i = 0; i < degree+1; ++i)
        {
                output ^= galois_mul(power,g_z[i],P_x);
                power = galois_mul(power,alpha,P_x);

        }
        return output;
}

mat JoinMatrix(mat h,int length)
//wirte H in 0 1 form
{
        if(h.n_cols == 1)
        {
                mat temp = int2vec(h(0,0),length);
                for (unsigned int i = 1; i < h.n_rows; ++i)
                {
                        temp = join_cols(temp,int2vec(h(i,0),length));
                }
                return temp;
        }
        else
        {
                mat mycol = int2vec(h(0,0),length);
                for (unsigned int i = 1; i < h.n_rows; ++i)
                {
                        mycol = join_cols(mycol,int2vec(h(i,0),length));
                }
```

```
                return
                join_rows(mycol,JoinMatrix(h(span(0,h.n_rows - 1),span(1,h.n_cols-
1)),length));
        }
}

bool rowequal(mat &a, mat &b)
{
        bool result = 1;
        for (unsigned int i = 0; i < a.n_cols; ++i)
                if (a(0,i)!=b(0,i))
                        return false;
        return result;
}

mat findnullspace(const mat &H)
{
    mat temp(H.n_cols, H.n_cols);
    temp.eye();
    // join 2 matrices
    temp = join_vert(H, temp);
    // rearrage columns
    for(unsigned int i = 0; i < H.n_rows; i++){
        unsigned int j = i;
        while(!temp(i, j)&&(j < H.n_cols)) j++;
        vec temp_v = temp.col(i);
        temp.col(i) = temp.col(j);
        temp.col(j) = temp_v;
        // elimination
        for(j = 0; j < H.n_cols; j++){
            if(temp(i, j)&&(i != j)){
                for(unsigned int k = 0; k < temp.n_rows; k++){
                    temp(k, j) = ((unsigned int)temp (k, j) + (unsigned int)temp
(k, i))%2;
                }
            }
        }
    }
    unsigned int max_j = 0;
    for(unsigned int i = 0; i < H.n_rows; i++){
        for(unsigned int j = 0; j < H.n_cols; j++){
            if(temp(i, j)&&(j > max_j)) max_j = j;
        }
    }
    // get generator matrix
    mat G_t = temp(span(H.n_rows, temp.n_rows - 1), span(max_j + 1, H.n_cols -
1));
    return G_t.t();
}

void mykeygen(mat& H, mat& G, mat& S, mat& P, mat& Ghat, bool random)
{
        unsigned int p_x = 0x0000012b;
        int N = 256;
        unsigned int a[256]={0};
        for (int i = 1; i < 256; ++i)
        {
                a[i] = galois_pow(2,i-1,p_x);
        }
```

```
    unsigned int g_z[14]={0};
    g_z[0] = 53;
g_z[1] = 100;
g_z[2] = 17;
g_z[3] = 229;
g_z[4] = 248;
g_z[5] = 45;
g_z[6] = 120;
g_z[7] = 152;
g_z[8] = 113;
g_z[9] = 131;
g_z[10] = 133;
g_z[11] = 197;
g_z[12] = 103;
g_z[13] = 129;
    int degree = 13;
    if (random)
    {
            int N = 0;
            srand (time(NULL));
            while(N<256)
            {
                    N = 0;
                    g_z[degree] = a[rand() % 255 + 1];

                    for (int i = 0; i < degree; ++i)
                    //the rest of coefficient from 0 to 255
                    g_z[i] = a[rand() % 255];

                    for (int i = 0; i < 256; ++i)
                            if(G_z(a[i],p_x,g_z,degree)!=0)
                                    N++;
            }
    }


    for (int i = 1; i < N; ++i)
            a[i] = galois_pow(2,i-1,p_x);

    mat Y = zeros(N,N);
    mat C = zeros(degree,degree);
    mat X = zeros(degree,N);

    for (int i = 0; i < N; ++i)
            Y(i,i) = inverse(G_z(a[i],p_x,g_z,degree),p_x);


    for (int i = 0; i < degree; ++i)
    {
            for (int j = i; j < degree; ++j)
            {
                    C(i,j) = g_z[degree + i - j];
            }
    }


    for (int i = 0; i < degree; ++i)
    {
            for (int j = 0; j < N; ++j)
            {
                    X(i,j) = galois_pow(a[j], degree - i - 1, p_x);
```

```
                }
        }

        mat temp = MyMatrixMul(C,MyMatrixMul(X,Y,p_x),p_x);

        H = JoinMatrix(temp, 8);
        G = findnullspace(H);
        if(!random)
                srand(13);//lucky number

        S = zeros(G.n_rows,G.n_rows);
        vec temp_v = randu<vec>(G.n_rows);
    uvec temp_v_p = sort_index(temp_v);
    for(unsigned int i = 0; i < G.n_rows; i++)
        S(i, temp_v_p(i)) = 1;

        P = zeros(G.n_cols,G.n_cols);
        temp_v = randu<vec>(G.n_cols);
    temp_v_p = sort_index(temp_v);
    for(unsigned int i = 0; i < G.n_cols; i++)
        P(i, temp_v_p(i)) = 1;

        Ghat = S*G*P;
        for (unsigned int i = 0; i < Ghat.n_rows; ++i)
        {
                for (unsigned int j = 0; j < Ghat.n_cols; ++j)
                        Ghat(i,j)=((unsigned int)Ghat(i,j))%2;
        }
}

void adderror(mat& cipher, int weight)
{
        srand(time(NULL));
        vec temp_v =randu<vec>(cipher.n_rows);
        uvec temp_v_e = sort_index(temp_v);
        mat e = zeros(cipher.n_rows,1);
        for (int i = 0; i < weight; ++i)
        {
                e(temp_v_e(i),0) = 1;
        }
        cipher = cipher + e;
        for (unsigned int i = 0; i < cipher.n_rows; ++i)
        {
                cipher(i,0) = ((unsigned int)cipher(i,0))%2;
        }
}

mat decrypt_one(mat H, mat G, mat S, mat P, mat ciphertext, const Poly_t g_z,
const Field_t GF){
    Poly_t z;
    z.degree = 1;
    z.coefficient[0] = 0;
    z.coefficient[1] = 1;

    mat error_codeword = ciphertext*P.t();
    mat syndrome = H*error_codeword.t();
    for(unsigned int i = 0; i < H.n_rows; i++) syndrome(i, 0) = ((int)syndrome(i,
0))%2;

    // express syndrome s(z) as an array of coefficients of a polynomial of degree
degree
```

```
    Poly_t s_z;
    s_z.degree = g_z.degree - 1;
    for(unsigned i = 0; i < s_z.degree + 1; i++) s_z.coefficient[i] =
vec2int(syndrome.rows(8*i, 8*(i + 1) - 1), 8);
    while(s_z.coefficient[s_z.degree] == 0){
        s_z.degree--;
    }

    // calculate sigma(z)
    Poly_t h_z = Euclidean_inv(s_z, g_z, GF);
    Poly_t d_2_z = Euclidean_add_p(h_z, z, GF);
    for(unsigned i = 0; i < 8*g_z.degree - 1; i++){
        d_2_z = Euclidean_pow(d_2_z, g_z, 2, GF);
    }
    Poly_t d_z = d_2_z;

    Poly_t a_z;
    Poly_t b_z;
    Poly_t d_i_z = Euclidean_inv(d_z, g_z, GF);
    if(g_z.degree%2){
        if(d_i_z.degree == (g_z.degree - 1)/2){
            a_z.degree = 0;
            a_z.coefficient[0] = 1;
            b_z = d_i_z;
        }else if(d_i_z.degree < (g_z.degree - 1)/2){
            a_z = Euclidean_pow(z, g_z, (g_z.degree - 1)/2 - d_i_z.degree, GF);
            b_z = Euclidean_mult_pp(d_i_z, a_z, GF);
        }else{
            Poly_t r_1, r_0, u_1, u_0, v_1, v_0;
            u_1.degree = 0;
            u_1.coefficient[0] = 1;
            u_0.degree = 0;
            u_0.coefficient[0] = 0;
            v_1.degree = 0;
            v_1.coefficient[0] = 0;
            v_0.degree = 0;
            v_0.coefficient[0] = 1;
            r_1 = g_z;
            r_0 = d_i_z;
            while((r_0.degree != 0)||(r_0.coefficient[0] != 0)){
                Poly_t quotient = Euclidean_div_pp(r_1, r_0, GF);

                Poly_t remainder = Euclidean_add_p(r_1, Euclidean_mult_pp(r_0,
quotient, GF), GF);
                Poly_t temp_u = Euclidean_add_p(u_1, Euclidean_mult_pp(u_0,
quotient, GF), GF);
                Poly_t temp_v = Euclidean_add_p(v_1, Euclidean_mult_pp(v_0,
quotient, GF), GF);
                r_1 = r_0;
                r_0 = remainder;
                u_1 = u_0;
                u_0 = temp_u;
                v_1 = v_0;
                v_0 = temp_v;
                if(r_1.degree == (g_z.degree - 1)/2){
                    b_z = r_1;
                    a_z = Euclidean_modp(Euclidean_mult_pp(d_z, b_z, GF), g_z,
GF);
                    break;
                }
            }
```

```
        }
    }else{
        if(d_z.degree == g_z.degree/2){
            b_z.degree = 0;
            b_z.coefficient[0] = 1;
            a_z = d_z;
        }else if(d_z.degree < g_z.degree/2){
            b_z = Euclidean_pow(z, g_z, g_z.degree/2 - d_z.degree, GF);
            a_z = Euclidean_mult_pp(d_z, b_z, GF);
        }else{
            Poly_t r_1, r_0, u_1, u_0, v_1, v_0;
            u_1.degree = 0;
            u_1.coefficient[0] = 1;
            u_0.degree = 0;
            u_0.coefficient[0] = 0;
            v_1.degree = 0;
            v_1.coefficient[0] = 0;
            v_0.degree = 0;
            v_0.coefficient[0] = 1;
            r_1 = g_z;
            r_0 = d_z;
            while((r_0.degree != 0)||(r_0.coefficient[0] != 0)){
                Poly_t quotient = Euclidean_div_pp(r_1, r_0, GF);

                Poly_t remainder = Euclidean_add_p(r_1, Euclidean_mult_pp(r_0,
quotient, GF), GF);
                Poly_t temp_u = Euclidean_add_p(u_1, Euclidean_mult_pp(u_0,
quotient, GF), GF);
                Poly_t temp_v = Euclidean_add_p(v_1, Euclidean_mult_pp(v_0,
quotient, GF), GF);
                r_1 = r_0;
                r_0 = remainder;
                u_1 = u_0;
                u_0 = temp_u;
                v_1 = v_0;
                v_0 = temp_v;
                if(r_1.degree == g_z.degree/2){
                    a_z = r_1;
                    b_z = Euclidean_modp(Euclidean_mult_pp(d_i_z, b_z, GF), g_z,
GF);
                    break;
                }
            }
        }
    }

    // get the location of errors
    Poly_t sigma_z = Euclidean_add_p(Euclidean_mult_pp(a_z, a_z, GF),
Euclidean_mult_pp(Euclidean_mult_pp(b_z, b_z, GF), z, GF), GF);
    mat codeword = error_codeword;
    for(unsigned i = 0; i < GF.max_ele; i++){
        unsigned sum = 0;
        unsigned multiplier = 1;
        for(unsigned j = 0; j < sigma_z.degree + 1; j++){
            sum = Euclidean_add_c(sum, Euclidean_mult_cc(multiplier,
sigma_z.coefficient[j], GF));
            multiplier = Euclidean_mult_cc(multiplier, GF.gen[i], GF);
        }
        if(sum == 0){
            codeword(0, i) = ((unsigned)codeword(0, i) + 1)%2;
        }
```

```
    }

    // get m
    mat temp_g = join_horiz(G.t(), codeword.t());
    for(unsigned int j = 0; j < G.n_rows; j++){
        unsigned int i = j;
        while(!temp_g(i, j)&&(i < G.n_cols)) i++;
        temp_g.swap_rows(i, j);
        // elimination
        for(i = 0; i < G.n_cols; i++){
            if(temp_g(i, j)&&(i != j)){
                for(unsigned int k = 0; k < G.n_rows + 1; k++){
                    temp_g(i, k) = ((unsigned int)temp_g (i, k) + (unsigned
int)temp_g (j, k))%2;
                }
            }
        }
    }
    mat retrieve = temp_g(span(0, G.n_rows - 1), span(G.n_rows,
G.n_rows)).t()*S.t();

    for(unsigned i = 0; i < retrieve.n_cols; i++){
        retrieve(0, i) = ((unsigned)retrieve(0, i))%2;
    }
    return retrieve;
}

bool SpecialCase(unsigned int part[])
{
        unsigned int temp[64] = {98, 51 ,164 ,116, 177, 120, 87, 72, 47, 249 ,105,
39, 255, 91 ,14, 216, 1, 100, 152, 182, 84, 176, 90 ,85, 154, 78, 10, 240, 12,
205, 252, 65, 161, 27, 248, 178, 101, 49, 197, 10, 141, 45, 35, 195, 185, 30, 223
,127, 64, 76, 13, 150, 113, 48, 26, 60, 93, 254, 168, 88, 30, 244, 180, 139};
        bool flag1 = true;
        for (int i = 0; i < 32; ++i)
        {
                if (part[i] != temp[i])
                {
                        flag1 = false;
                        break;
                }
        }

        bool flag2 = true;
        for (int i = 0; i < 32; ++i)
        {
                if (part[i] != temp[32+i])
                {
                        flag2 = false;
                        break;
                }
        }

        return (flag1 || flag2);
}

int main(int argc, char const *argv[])
{
        if ((string)argv[1] == "key")
        {
                mat G,S,P,Ghat,H;
```

```
        mykeygen(H,G,S,P,Ghat,true);
        Ghat.save("RandomPublicKey", raw_ascii);
        G.save("RandomPrivateG",raw_ascii);
        S.save("RandomPrivateS",raw_ascii);
        P.save("RandomPrivateP",raw_ascii);
        cout << "random key generating done !" << endl;
        return 0;
}

if((string)argv[1] == "encrypt")
{
        mat G,S,P,Ghat,H;

        mykeygen(H,G,S,P,Ghat,false);
        ifstream myfile;
        myfile.open (argv[2]);
        if (!myfile)
        {
                cout << "no file!" << endl;
                exit(-1);
        }
        string plaintext = "";
        getline(myfile,plaintext);
        if (plaintext.length()!=38)
        {
                cout << "illegal plaintext!" << endl;
                exit(-1);
        }
        myfile.close();

        string plaintext1 = plaintext.substr(0,19);
        string plaintext2 = plaintext.substr(19,38);
        char temp = (char)plaintext1[0];
        mat blk1 = int2vec((unsigned int)temp,8);
        for (int i = 1; i < 19; ++i)
        {
                temp = (char)plaintext1[i];
                blk1 = join_cols(blk1, int2vec((unsigned int)temp,8));
        }

        temp = (char)plaintext2[0];
        mat blk2 = int2vec((unsigned int)temp,8);
        for (int i = 1; i < 19; ++i)
        {
                temp = (char)plaintext2[i];
                blk2 = join_cols(blk2, int2vec((unsigned int)temp,8));
        }

        mat cipher1 = trans(blk1)*Ghat;
        mat cipher2 = trans(blk2)*Ghat;
        cipher1 = trans(cipher1);
        cipher2 = trans(cipher2);
        adderror(cipher1, 13);
        adderror(cipher2, 13);
        mat cipher = join_cols(cipher1,cipher2);

        unsigned int ciphertext[64];
        for (int i = 0; i < 64; ++i)
                ciphertext[i] = vec2int(cipher(span(8*i,8*i+7),0),8);

        ofstream output ("cipher");
```

```
        if (output.is_open())
                {
                for (int i = 0; i < 64; ++i)
                        output << ciphertext[i] << " ";
                output.close();
        }
        cout << "encryption done !" << endl;
                return 0;
        }

        if((string)argv[1] == "decrypt")
        {
                mat G,S,P,Ghat,H;
                unsigned int
g_z[14]={53,100,17,229,248,45,120,152,113,131,133,197,103,129};
                mykeygen(H,G,S,P,Ghat,false);
                ifstream myfile;
                myfile.open(argv[2]);
                if (!myfile)
                {
                        cout << "no file!" << endl;
                        exit(-1);
                }

                unsigned int part1[32] = {0}, part2[32]= {0};
                for (int i = 0; i < 32; ++i)
                        myfile >> part1[i];
                for (int i = 0; i < 32; ++i)
                        myfile >> part2[i];

                myfile.close();

                if (SpecialCase(part1)||SpecialCase(part2))
                {
                        cout << "original plaintext! " << endl;
                        return -1;
                }

                mat blk1 = int2vec(part1[0],8);
                for (int i = 1; i < 32; ++i)
                        blk1 = join_cols(blk1, int2vec(part1[i],8));
                blk1=trans(blk1);

                mat blk2 = int2vec(part2[0],8);
                for (int i = 1; i < 32; ++i)
                        blk2 = join_cols(blk2, int2vec(part2[i],8));
                blk2=trans(blk2);


                //decode
                Field_t GF;
                GF.P_x = 0453;
            GF.max_ele = 256;
            GF.gen[0] = 0;
            GF.gen_inv[0] = 0;
                GF.gen[1] = 1;
                GF.gen_inv[1] = 1;
            for(unsigned i = 2; i < GF.max_ele; i++){
            GF.gen[i] = galois_mul(GF.gen[i - 1], 2, GF.P_x);
            GF.gen_inv[GF.gen[i]] = i;
```

Кінець додатку Д

```
                }

                Poly_t GZ;
                GZ.degree = 13;
                for (int i = 0; i <= 13; ++i)
                        GZ.coefficient[i] = g_z[i];

                mat plain1 = decrypt_one(H, G, S, P, blk1, GZ, GF);
                mat plain2 = decrypt_one(H, G, S, P, blk2, GZ, GF);
                cout << "decryption success" << endl;

                for (int i = 0; i < 152; ++i)
                {
                        plain1(0,i) = ((unsigned int)plain1(0,i))%2;
                        plain2(0,i) = ((unsigned int)plain2(0,i))%2;
                }
                plain2 = trans(plain2);
                plain1 = trans(plain1);

                string text1 = "";
                string text2 = "";
                unsigned int temp;
                for (int i = 0; i < 19; ++i)
                {
                        temp = vec2int(plain1(span(i*8,i*8+7),0),8);
                        text1 = text1 + (char)temp;
                        temp = vec2int(plain2(span(i*8,i*8+7),0),8);
                        text2 = text2 + (char)temp;
                }

                string text = text1+text2;
                cout << "decryption done!" << endl;
                cout << text << endl;
                return 0;

        }
        return 0;
}
```

Додаток Е

Результати дослідження загроз безпеки банківських інформаційних ресурсів на основі запропонованого класифікатору

Номер загрози	Короткий опис загрози	μ[C]	μ[I]	μ[A]	μ[Au]	D[C]	D[I]	D[A]	D[Au]
02.03.01.05	Загроза аналізу криптографічних алгоритмів і їх реалізації	0.027	0.134	0.019	0.088	0.184	0.031	0.039	0.046
03.03.03.04	Загроза апаратного скидання пароля BIOS	0.166	0.033	0.033	0.1	0.054	0.039	0.068	0.06
03.03.02.03	• Загроза застосування шкідливого коду в BIOS • Загроза деструктивного використання декларованого функціоналу BIOS • Загроза несанкціонованого доступу до віртуальних машин, що захищаються, з віртуальної і (або) фізичної мережі • Загроза несанкціонованого управління буфером	0.266	0.207	0.223	0.303	0	0	0	0
03.03.02.05	• Загроза впровадження коду або даних • Загроза підміни вмісту мережевих ресурсів	0.1305	0.1394	0.0359	0.1492	0	0	0	0
03.02.04.03	• Загроза впливу на програми з високими привілеями • Загроза використання підроблених цифрових підписів BIOS	0.1545	0.1944	0.0719	0.0968	0	0	0	0
02.02.04.05	Загроза відновлення автентифікаційної інформації	0.088	0.019	0.027	0.134	0.073	0.041	0.039	0.142
02.02.02.03	Загроза відновлення попередньої вразливої версії BIOS	0.1	0	0.05	0.05	0.031	0.161	0.241	0.028
01.02.03.02	Загроза виходу процесу за межі віртуальної машини	0.134	0.088	0.019	0.027	0.056	0.042	0.053	0.136
03.02.03.01	Загроза деавторізації санкціонованого клієнта бездротової мережі	0.037	0.027	0.176	0.027	0.08	0.019	0.114	0.073
03.02.02.03	Загроза деструктивної зміни конфігурації/середовища оточення програм	0.027	0.134	0.088	0.019	0.02	0.101	0.147	0.036

Продовження додатку Е

Номер загрози	Короткий опис загрози	μ[C]	μ[I]	μ[A]	μ[Au]	D[C]	D[I]	D[A]	D[Au]
01.01.03.05	• Загроза тривалого утримання обчислювальних ресурсів користувачами • Загроза зміни компонентів системи • Загроза спотворення вводиться і виводиться, що вводиться та виводиться на периферійні пристрої інформації • Загроза неможливості міграції образів віртуальних машин через несумісність апаратного та програмного забезпечення • Загроза неузгодженості політик безпеки елементів хмарної інфраструктури	0.172	0.223	0.266	0.205	0	0	0	0
03.03.02.04	• Загроза доступу до файлів, що захищаються, з використанням обхідного шляху • Загроза несанкціонованого відновлення видаленої інформації, що захищається	0.1711	0.1133	0.0456	0.1133	0	0	0	0
03.01.03.02	• Загроза доступу до локальних файлів сервера за допомогою URL • Загроза зловживання можливостями, наданими споживачам хмарних послуг	0.1152	0.1416	0.134	0.1883	0	0	0	0
01.01.03.04	• Загроза доступу / перехоплення / зміни HTTP cookies • Загроза неузгодженості правил доступу до великих даних	0.0649	0.1852	0.066	0.1394	0	0	0	0
03.03.03.03	• Загроза завантаження нештатної операційної системи • Загроза надлишкового виділення оперативної пам'яті • Загроза перехоплення управління гіпервізором	0.1599	0.06	0.1978	0.1819	0	0	0	0
02.03.01.02	• Загроза зараження DNS-кешу • Загроза використання слабкостей протоколів мережевого/локального обміну даними	0.2886	0.0562	0.0978	0.1309	0	0	0	0

Продовження додатку Е

Номер загрози	Короткий опис загрози	μ[C]	μ[I]	μ[A]	μ[Au]	D[C]	D[I]	D[A]	D[Au]
01.01.02.05	• Загроза зловживання довіроюспоживачів хмарних послуг • Загроза переповнення цілочисельних змінних • Загроза підробки записів журналу реєстрації подій	0.101	0.112	0.1509	0.1709	0	0	0	0
03.03.03.01	• Загроза зміни режимів роботи апаратних елементів комп'ютера • Загроза несанкціонованого доступу до системи по бездротових каналах • Загроза відключення контрольних датчиків	0.1748	0.1509	0.1529	0.1878	0	0	0	0
02.03.03.05	• Загроза зміни системних і глобальних змінних • Загроза несанкціонованого доступу до активного і (або) пасивного віртуального і (або) фізичного мережевого обладнання з фізичної та (або) віртуальної мережі • Загроза несанкціонованого копіювання інформації, що захищається • Загроза несанкціонованого управління покажчиками	0.231	0.216	0.154	0.265	0	0	0	0
03.03.03.05	• Загроза спотворення XML-схеми • Загроза дослідження додатку через звіти про помилки	0.1295	0.1126	0.1463	0.129	0	0	0	0
02.03.02.03	• Загроза використання альтернативних шляхів доступу до ресурсів • Загроза несанкціонованого використання привілейованих функцій BIOS • Загроза перезавантаження апаратних і програмно-апаратних засобів обчислювальної техніки • Загроза підміни резервної копії програмного забезпечення BIOS	0.159	0.2	0.232	0.172	0	0	0	0

Продовження додатку Е

Номер загрози	Короткий опис загрози	μ[C]	μ[I]	μ[A]	μ[Au]	D[C]	D[I]	D[A]	D[Au]
01.02.03.03	• Загроза використання обчислювальних ресурсів суперкомп'ютера «паразитними» процесами • Загроза неможливості управління правами користувачів BIOS • Загроза перевантаження ГРІД-системи обчислювальними завданнями	0.1229	0.118	0.1818	0.1769	0	0	0	0
01.02.04.05	• Загроза використання інформації ідентифікації / автентифікації, заданої за замовчуванням • Загроза міжсайтовій підробки запиту • Загроза некоректної реалізації політики ліцензування в хмарі • Загроза неправомірного ознайомлення з інформацією, що захищається • Загроза несанкціонованого видалення інформації, що захищається	0.419	0.187	0.284	0.375	0	0	0	0
03.02.03.03	• Загроза використання механізмів авторизації для підвищення привілеїв • Загроза порушення ізоляції середовища виконання BIOS • Загроза несанкціонованого доступу до віртуальних пристроїв, що захищаються, з віртуальної і (або) фізичної мережі	0.092	0.117	0.1499	0.1749	0	0	0	0
01.01.04.05	• Загроза використання слабкостей кодування вхідних даних • Загроза конфлікту юрисдикцій різних країн • Загроза порушення цілісності даних кешу • Загроза невизначеності в розподілі відповідальності між ролями в хмарі • Загроза несанкціонованого створення облікового запису користувача	0.267	0.309	0.274	0.283	0	0	0	0

Продовження додатку Е

Номер загрози	Короткий опис загрози	μ[C]	μ[I]	μ[A]	μ[Au]	D[C]	D[I]	D[A]	D[Au]
01.01.03.03	Загроза використання слабких криптографічних алгоритмів BIOS	0.033	0.044	0.023	0.033	0.078	0.353	0.007	0.016
02.03.03.03	• Загроза дослідження механізмів роботи програми • Загроза безперервної модернізації хмарної інфраструктури • Загроза несанкціонованого редагування реєстру • Загроза опосередкованого управління групою програм через спільно використовувані дані • Загроза відмови в обслуговуванні системою зберігання даних суперкомп'ютера • Загроза помилки поновлення гіпервізора • Загроза передачі заборонених команд на обладнання з числовим програмним управлінням	0.356	0.348	0.403	0.278	0	0	0	0
01.03.02.04	Загроза вичерпання обчислювальних ресурсів сховища великих даних	0.018	0.05	0.066	0.066	0.015	0.246	0.028	0.245
02.03.02.04	• Загроза вичерпання запасу ключів, необхідних для відновлення BIOS • Загроза неможливості відновлення сесії роботи на ПЕОМ при виведенні з проміжних станів харчування • Загроза неконтрольованого копіювання даних усередині сховища великих даних • Загроза неконтрольованого знищення інформації сховищем великих даних • Загроза несанкціонованого доступу до даних за межами зарезервованого адресного простору, в тому числі виділеного під віртуальне апаратне забезпечення	0.265	0.194	0.194	0.214	0	0	0	0

Продовження додатку Е

Номер загрози	Короткий опис загрози	μ[C]	μ[I]	μ[A]	μ[Au]	D[C]	D[I]	D[A]	D[Au]
01.03.02.05	• Загроза міжсайтового скриптинга • Загроза несумлінного виконання зобов'язань постачальниками хмарних послуг	0.1154	0.1637	0.1883	0.1127	0	0	0	0
02.03.03.02	Загроза порушення доступності хмарного сервера	0.021	0.017	0.022	0.007	0.023	0.014	0.741	0.002
01.03.03.03	Загроза порушення ізоляції призначених для користувача даних всередині віртуальної машини	0.05	0.05	0.05	0.02	0.014	0.031	0.021	0.31
01.01.04.04	Загроза порушення процедури автентифікації суб'єктів віртуальної інформаційної взаємодії	0.017	0.011	0.017	0.022	0.072	0.006	0.014	0.559
03.02.03.04	• Загроза порушення працездатності ГРІД-системи при нетиповому мережевому навантаженні • Загроза неконтрольованого зростання кількості віртуальних машин	0.064	0.0918	0.0865	0.02	0	0	0	0
02.02.03.04	Загроза порушення технології обробки інформації шляхом несанкціонованого внесення змін до образів віртуальних машин	0.05	0.05	0.066	0.034	0.112	0.287	0.021	0.059
02.02.02.05	Загроза невірного визначення формату вхідних даних, що надходять в сховище великих даних	0.043	0.044	0.033	0.013	0.021	0.374	0.013	0.26
02.02.03.05	Загроза незахищеного адміністрування хмарних послуг	0.024	0.088	0.067	0.088	0.241	0.059	0.173	0.019
01.02.02.05	• Загроза неякісного перенесення інфраструктури в хмару • Загроза невизначеності відповідальності за забезпечення безпеки хмари	0.0649	0.0755	0.0755	0.0446	0	0	0	0
03.01.04.04	Загроза неконтрольованого зростання числа зарезервованих обчислювальних ресурсів	0.006	0.017	0.022	0.022	0.002	0.269	0.037	0.32

Продовження додатку Е

Номер загрози	Короткий опис загрози	μ[C]	μ[I]	μ[A]	μ[Au]	D[C]	D[I]	D[A]	D[Au]
03.02.04.04	Загроза некоректного завдання структури даних транзакції	0.11	0.03	0.083	0.11	0.121	0.132	0.219	0.021
02.01.04.02	Загроза некоректного використання прозорого проксі-сервера за рахунок плагінів браузера	0.034	0.05	0.05	0.066	0.366	0.021	0.134	0.02
02.03.02.05	• Загроза некоректного використання функціоналу програмного забезпечення • Загроза несанкціонованого виключення або обходу механізму захисту від запису в BIOS • Загроза несанкціонованого доступу до інформації, що захищається, яка зберігається в віртуальному просторі	0.2068	0.1739	0.103	0.2485	0	0	0	0
03.02.03.05	• Загроза неправомірного/некоректного використання інтерфейсу взаємодії з додатком • Загроза виявлення хостів	0.0823	0.0975	0.1127	0.0978	0	0	0	0
03.03.01.02	• Загроза неправомірних дій у каналах зв’язку • Загроза несанкціонованого доступу до віртуальних каналів передачі • Загроза перехоплення даних, переданих по обчислювальній мережі	0.11	0.065	0.054	0.105	0	0	0	0
01.01.04.03	• Загроза несанкціонованого доступу до автентифікаційної інформації • Загроза перехоплення привілейованого процесу	0.1394	0.1104	0.0755	0.1305	0	0	0	0
03.03.03.02	• Загроза несанкціонованого доступу до гіпервізору з віртуальної машини і (або) фізичної мережі • Загроза несанкціонованого віддаленого за смуговим доступом до апаратних засобів • Загроза перехоплення управління середовищем віртуалізації	0.2256	0.1509	0.1459	0.2097	0	0	0	0

Продовження додатку Е

Номер загрози	Короткий опис загрози	μ[C]	μ[I]	μ[A]	μ[Au]	D[C]	D[I]	D[A]	D[Au]
02.02.03.02	Загроза несанкціонованого доступу до віртуальних машин, що захищаються, з боку інших віртуальних машин	0.067	0.045	0.067	0.088	0.019	0.057	0.235	0.226
03.02.04.05	Загроза несанкціонованого доступу до локального комп'ютера через клієнта ГРІД-системи	0.066	0.048	0.02	0.066	0.238	0.134	0.255	0.021
02.03.03.04	Загроза несанкціонованого доступу до сегментів обчислювального поля	0.044	0.012	0.033	0.044	0.022	0.138	0.491	0.022
02.02.02.04	Загроза несанкціонованого доступу до системи зберігання даних з віртуальної і (або) фізичної мережі	0.05	0.05	0.034	0.066	0.062	0.359	0.071	0.021
02.03.04.05	Загроза несанкціонованої зміни автентифікаційної інформації	0.033	0.044	0.013	0.043	0.264	0.074	0.004	0.124
01.02.03.05	Загроза несанкціонованого управління синхронізацією та станом	0.005	0.022	0.007	0.034	0.001	0.276	0.387	0.055
03.02.03.02	• Загроза виявлення відкритих портів та ідентифікації прив'язаних до нього мережевих служб • Загроза визначення топології обчислювальної мережі	0.0347	0.0603	0.0545	0.0485	0	0	0	0
02.03.04.04	Загроза обходу некоректно налаштованих механізмів автентифікації	0.044	0.033	0.012	0.044	0.198	0.013	0.089	0.146
02.02.04.04	Загроза загальнодоступності хмарної інфраструктури	0.066	0.05	0.018	0.066	0.021	0.062	0.497	0.028
02.01.03.05	Загроза визначення типів об'єктів захисту	0.05	0.05	0.05	0.05	0.062	0.237	0.134	0.071
03.01.04.05	• Загроза відмови в завантаженні вхідних даних невідомого формату сховищем великих даних • Загроза підміни дії користувача шляхом обману • Загроза підміни довіреного користувача • Загроза підміни суб'єкта мережевого доступу	0.091	0.132	0.116	0.263	0	0	0	0

Кінець додатку Е

Номер загрози	Короткий опис загрози	μ[C]	μ[I]	μ[A]	μ[Au]	D[C]	D[I]	D[A]	D[Au]
03.02.01.05	• Загроза перебору всіх налаштувань і параметрів програми • Загроза передачі даних по прихованим каналам	0.0993	0.0269	0.0709	0.0662	0	0	0	0
02.03.03.01	Загроза перехоплення на периферійні пристрої інформації, що вводиться і виводиться	0.044	0.033	0.013	0.043	0.426	0.068	0.004	0.02
03.03.04.03	• Загроза перехоплення привілейованого потоку • Загроза підвищення привілеїв	0.065	0.0289	0.0494	0.0543	0	0	0	0
02.02.03.03	Загроза пошкодження системного реєстру	0.085	0.088	0.067	0.027	0.024	0.236	0.134	0.014
03.01.04.03	Загроза підбору пароля BIOS	0.027	0.067	0.067	0.088	0.22	0.035	0.029	0.021
03.01.01.01	Загроза підключення до бездротової мережі в обхід процедури автентифікації	0.009	0.044	0.013	0.066	0.246	0.022	0.063	0.269
03.01.04.01	Загроза підміни бездротового клієнта або точки доступу	0	0.067	0.067	0.134	0.312	0.012	0.23	0.043

Додаток Ж

Групові та часткові показниками ІБ

Позначення ЧП	Частковий показник (ЧП)	Обов'язковість виконання	Категорія перевірки	Оцінка часткового показника ІБ					
				0	0,25	0,5	0,75	1	н/о
R_{BBI_2} – оцінка степені виконання вимог за напрямом "менеджмент ІБ організації"									
$IU_{1.1}$	упровадження процесного підходу до діяльності банку	обов'язковий	категорія 2						
$IU_{1.2}$	упровадження ризик-орієнтованого підходу до забезпечення інформаційної безпеки банку	обов'язковий	категорія 2						
$IU_{1.3}$	запровадити процес управління ризиками інформаційної безпеки в рамках системи управління ризиками банку	обов'язковий	категорія 2						
$IU_{1.4}$	запровадити, використовуючи ризик-орієнтований підхід, заходи безпеки, визначені додатком А до ДСТУ ISO/IEC 27001:2015, згідно з ДСТУ ISO/IEC 27002:2015 та з урахуванням обов'язкових вимог щодо організації заходів безпеки інформації, викладених у розділах IV і V Положення	обов'язковий	категорія 2						
$IU_{1.5}$	визначити мінімальною сферою застосування СУІБ усі критичні бізнес-процеси банку	обов'язковий	категорія 2						
$IU_{1.6}$	сформувати колективний керівний орган з питань впровадження та функціонування СУІБ або наділити цими повноваженнями існуючий колективний керівний орган банку та розробити положення про керівний орган СУІБ банку з чітким визначенням його завдань, функцій та відповідальності	обов'язковий	категорія 2						

Продовження додатку Ж

Позначення ЧП	Частковий показник (ЧП)	Обов'язковість виконання	Категорія перевірки	Оцінка часткового показника ІБ					
				0	0,25	0,5	0,75	1	н/о
$IU_{1.7}$	включити до складу керівного органу СУІБ голову правління банку та/або його заступника, що відповідає за інформаційну безпеку банку, керівників підрозділів банку – власників критичних бізнес-процесів банку та керівника підрозділу банку з управління ризиками	обов'язковий	категорія 2						
$IU_{1.8}$	сформувати підрозділ з інформаційної безпеки не менше як із двох працівників зі складу штатних працівників банку.	обов'язковий	категорія 2						
$IU_{1.9}$	розробити та затвердити внутрішній документ, який установлює вимоги до забезпечення захисту від зловмисного коду та описує організацію захисту від зловмисного коду в банку	обов'язковий	категорія 2						
$IU_{1.10}$	обробляти виявлені атаки або вторгнення до мережі банку в рамках процесу управління інцидентами безпеки інформації	обов'язковий	категорія 2						
$IU_{1.11}$	виконувати перевірку ефективності заходів щодо захисту периметра мережі банку шляхом виконання періодичних тестів на проникнення	обов'язковий	категорія 1						
$IU_{1.12}$	ознайомити своїх працівників із документами, які встановлюють вимоги щодо безпеки інформації, технічного обслуговування та експлуатації факсимільних апаратів, багатофункціональних пристроїв для друку, телефонів та/або телефонних систем.	обов'язковий	категорія 1						

Продовження додатку Ж

Позначення ЧП	Частковий показник (ЧП)	Обов'язковість виконання	Категорія перевірки	Оцінка часткового показника ІБ					
				0	0,25	0,5	0,75	1	н/о
$IU_{1.13}$	визначити та задокументувати вимоги безпеки інформації для інформаційних систем банку під час їх розроблення, модернізації (у тому числі їх компонентів) або в разі придбання	обов'язковий	категорія 2						
$IU_{1.14}$	використовувати тестову програмно-апаратну платформу, яка підключена до окремого (тестового) виділеного сегмента мережі банку	обов'язковий	категорія 2						
$IU_{1.15}$	на стадії експлуатації інформаційних систем задокументувати положення щодо: 1) контролю функціонування реалізованих в інформаційних системах банку заходів безпеки інформації, уключаючи контроль реалізації організаційних заходів та контроль складу і параметрів налагодження технічних засобів безпеки інформації; 2) контролю вразливостей в обладнанні та програмному забезпеченні інформаційних систем банку; 3) контролю конфігурації програмного забезпечення інформаційних систем банку; 4) відновлення всіх реалізованих заходів щодо забезпечення безпеки інформації в інформаційних системах банку після збоїв у роботі внаслідок інцидентів безпеки інформації.	обов'язковий	категорія 3						

Позначення ЧП	Частковий показник (ЧП)	Обов'язковість виконання	Категорія перевірки	Оцінка часткового показника ІБ					
				0	0,25	0,5	0,75	1	н/о
$IU_{1.16}$	упровадити процес управління інцидентами безпеки інформації та розробити і затвердити документи, які містять описи дій стосовно: 1) виявлення інцидентів; 2) інформування про інциденти, у тому числі відповідальної особи за інформаційну безпеку, підрозділу з безпеки інформації та працівників банку; 3) класифікації інцидентів та оцінки негативного впливу (збитку), нанесеного банку інцидентом; 4) реагування на інциденти; 5) аналізу причин, що призвели до інцидентів та оцінки результатів реагування на інциденти; 6) зберігання інформації щодо інцидентів, аналізу інцидентів та результатів реагування на інциденти.	обов'язковий	категорія 3						
$IU_{1.17}$	забезпечити документування інформації щодо інцидентів безпеки інформації та її зберігання не менше ніж один рік	обов'язковий	категорія 3						
$IU_{1.18}$	створити та підтримувати в актуальному стані (в електронному або паперовому вигляді) перелік змінних носіїв інформації банку	обов'язковий	категорія 3						
$IU_{1.19}$	упровадити системи виявлення несанкціонованого доступу до мережі (*Intrusion detection system*, IDS) та системи запобігання несанкціонованому доступу до мережі (*Intrusion prevention system*, IPS) для захисту периметра мережі банку	обов'язковий	категорія 3						

Позначення ЧП	Частковий показник (ЧП)	Обов'язковість виконання	Категорія перевірки	Оцінка часткового показника ІБ					
				0	0,25	0,5	0,75	1	н/о
$IU_{1.20}$	застосувати заходи безпеки для захисту від атак на відмову в обслуговуванні та/або розподілених атак на відмову в обслуговуванні (DoS/DDoS-атак) на зовнішньому периметрі мережі банку	обов'язковий	категорія 3						
R_{BBI_3} – оцінка степені виконання вимог за напрямом "рівень усвідомлення ІБ організації"									
$IU_{2.1}$	визначати підходи (методики) оцінювання та оброблення ризиків інформаційної безпеки	рекомендований	категорія 1						
$IU_{2.2}$	розширити сферу застосування СУІБ банку відповідно до особливостей його діяльності, характеру та обсягу банківських, фінансових послуг та інших видів діяльності	рекомендований	категорія 1						
$IU_{2.3}$	здійснювати перевірку стану впровадження СУІБ банку та повноту виконання заходів безпеки інформації	рекомендований	категорія 1						
$IU_{2.4}$	розробити та впровадити політику інформаційної безпеки	обов'язковий	категорія 2						
$IU_{2.5}$	забезпечити підтримку політики інформаційної безпеки в актуальному стані та її перегляд не рідше ніж один раз на рік	обов'язковий	категорія 2						
$IU_{2.6}$	затвердити політику інформаційної безпеки і довести її зміст до відома всього персоналу банку та, за необхідності, представникам третіх сторін	обов'язковий	категорія 1						
$IU_{2.7}$	розробити та затвердити стратегію розвитку інформаційної безпеки	обов'язковий	категорія 2						

Продовження додатку Ж

Позначення ЧП	Частковий показник (ЧП)	Обов'язковість виконання	Категорія перевірки	Оцінка часткового показника ІБ					
				0	0,25	0,5	0,75	1	н/о
$IU_{2.8}$	розробити та затвердити план забезпечення безперервності діяльності банку, у якому враховано безперервність функціонування заходів інформаційної безпеки в рамках процесу управління безперервністю діяльності банку	обов'язковий	категорія 2						
$IU_{2.9}$	ознайомити працівників під час прийому на роботу з політикою інформаційної безпеки банку. Працівник банку зобов'язаний ознайомитися з політикою інформаційної безпеки банку під підпис та надати зобов'язання про дотримання конфіденційності.	обов'язковий	категорія 2						
$IU_{2.10}$	включити до трудового контракту/договору працівника та/або посадової інструкції працівника обов'язки працівника банку щодо виконання вимог із забезпечення безпеки інформації.	обов'язковий	категорія 2						
$IU_{2.11}$	ознайомити працівників банку з внутрішніми документами банку, які встановлюють вимоги щодо безпеки інформації	обов'язковий	категорія 2						
$IU_{2.12}$	упровадити програму підвищення обізнаності/навчання працівників банку з питань безпеки інформації з урахуванням досвіду, отриманого за результатами вирішення інцидентів безпеки інформації	обов'язковий	категорія 1						
$IU_{2.13}$	розробити та затвердити внутрішні документи, які встановлюють вимоги щодо безпеки інформації під час використання змінних носіїв інформації	обов'язковий	категорія 1						

Позначення ЧП	Частковий показник (ЧП)	Обов'язковість виконання	Категорія перевірки	Оцінка часткового показника ІБ					
				0	0,25	0,5	0,75	1	н/о
$IU_{2.14}$	розробити та затвердити внутрішні документи, які встановлюють вимоги щодо використання, надання, скасування та контролю доступу до інформаційних систем банку	обов'язковий	категорія 1						
$IU_{2.15}$	розробити та впровадити політику використання криптографічних засобів для захисту інформації	обов'язковий	категорія 1						
$IU_{2.16}$	розробити та затвердити внутрішні документи, які містять опис процесу управління оновленнями (описи дій щодо отримання, тестування, розповсюдження та застосування оновлень операційних систем, прикладного програмного забезпечення та драйверів)	обов'язковий	категорія 2						
$IU_{2.17}$	забезпечити централізоване управління мережею банку (єдине місце управління)	обов'язковий	категорія 2						
$IU_{2.18}$	забезпечити підтримання в актуальному стані документації мережі банку (в електронному та/або паперовому вигляді), документування всіх змін у конфігурації мережі банку та зберігання попередніх версій документації мережі строком не менше ніж один рік. Документація мережі банку має бути погоджена відповідальною особою за інформаційну безпеку банку	обов'язковий	категорія 2						
$IU_{2.19}$	задокументувати порядок контролю змін у конфігурації мережі, у якому мають зазначатися вимоги щодо перегляду конфігурації мережі не рідше ніж один раз на рік з документуванням результатів перегляду	обов'язковий	категорія 2						

Позначення ЧП	Частковий показник (ЧП)	Обов’язковість виконання	Категорія перевірки	Оцінка часткового показника ІБ					
				0	0,25	0,5	0,75	1	н/о
$IU_{2.20}$	розробити та затвердити внутрішні документи, які встановлюють вимоги щодо безпеки інформації, технічного обслуговування, експлуатації факсимільних апаратів, багатофункціональних пристроїв, телефонів та/або телефонних систем та мають містити такі положення щодо: 1) функцій та обов'язків персоналу банку стосовно підключення, технічного обслуговування та експлуатації систем та пристроїв зв’язку; 2) категорій інформації за критерієм конфіденційності, що може передаватися пристроями зв’язку; 3) обов’язковості очищення оперативної та постійної пам’яті факсимільних апаратів і багатофункціональних пристроїв перед передаванням їх третім сторонам або перед виведенням з експлуатації.	обов’язковий	категорія 2						
$IU_{2.\ 21}$	розробити та затвердити документ щодо використання електронної пошти, який має містити положення щодо: 1) обмежень під час пересилання інформації банку; 2) категорії інформації, яка може надсилатись засобами електронної пошти; 3) обмежень використання сторонніх сервісів електронної пошти, які не пов’язані з виконанням функціональних обов’язків персоналом банку	обов’язковий	категорія 3						

Позначення ЧП	Частковий показник (ЧП)	Обов'язковість виконання	Категорія перевірки	Оцінка часткового показника ІБ					
				0	0,25	0,5	0,75	1	н/о
$IU_{2.22}$	розробити документацію для інформаційних систем банку та/або їх компонентів з обов'язковим описом реалізованих в інформаційних системах банку організаційних та технічних заходів безпеки інформації, якщо така документація не надана розробником інформаційних систем банку	обов'язковий	категорія 3						
$IU_{2.23}$	визначити функції та обов'язки, пов'язані з експлуатацією інформаційних систем і впроваджених в них заходів безпеки інформації, уключаючи внесення змін до параметрів їх налаштування	обов'язковий	категорія 3						
$IU_{2.24}$	задокументувати та впровадити порядок виведення з експлуатації обладнання інформаційних систем банку, який має містити опис процесу видалення інформації з таких систем, використовуючи алгоритми та/або методи, що забезпечать неможливість її відновлення	обов'язковий	категорія 3						
$IU_{2.25}$	визначити в посадових інструкціях працівників банку або організаційно-розпорядчих документах банку особисті функції та обов'язки з виявлення, класифікації, реагування і аналізу інцидентів безпеки інформації	обов'язковий	категорія 3						
OV_{ooIP} – оцінка степені виконання вимог, що регламентують обробку БІн									

Позначення ЧП	Частковий показник (ЧП)	Обов'язковість виконання	Категорія перевірки	Оцінка часткового показника ІБ					
				0	0,25	0,5	0,75	1	н/о
$IU_{3.1}$	здійснити ідентифікацію змінних носіїв інформації за допомогою унікального ідентифікатора, який дозволить визначити тип носія та користувача змінного носія	обов'язковий	категорія 1						
$IU_{3.2}$	розробити та затвердити документи, що описують процес управління ключами	обов'язковий	категорія 1						
$IU_{3.3}$	при використанні алгоритму RSA для цифрових підписів і ключів шифрування сеансу або аналогічних ключів, зобов'язаний використовувати різні ключові пари для передавання ключів шифрування сеансу (або аналогічних ключів) та для цифрових підписів.	обов'язковий	категорія 2						
$IU_{3.4}$	використовувати останню версію протоколу захисту на транспортному рівні та реалізацію цього протоколу, що підтримує безпечне повторне погодження з'єднання для захисту з'єднань, які управляються протоколом *Transmission control protocol* (TCP). Якщо безпечне повторне погодження з'єднання не підтримується, то ця процедура має бути відключена	обов'язковий	категорія 2						
$IU_{3.5}$	забороняється використання анонімного (без автентифікації) алгоритму DH	обов'язковий	категорія 2						
$IU_{3.6}$	при застосуванні стандартів для шифрування "*Secure multipurpose internet mail extension*" (S/MIME), зобов'язаний використовувати цей стандарт не нижче версії 3.0	обов'язковий	категорія 2						

Позначення ЧП	Частковий показник (ЧП)	Обов'язковість виконання	Категорія перевірки	Оцінка часткового показника ІБ					
				0	0,25	0,5	0,75	1	н/о
$IU_{3.7}$	використовувати набір протоколів для забезпечення захисту даних, що передаються за допомогою протоколу Інтернету (набір протоколів *Internet protocol security*, IPsec) у режимі ESP (*Encapsulating security payload*) (якщо банк не використовує криптографічний протокол захисту на транспортному рівні).	обов'язковий	категорія 2						
$IU_{3.8}$	використовувати кабелі типу "вита пара" не нижче категорії 5E та/або оптично-волоконні кабелі для організації структурованої кабельної системи (далі - СКС).	обов'язковий	категорія 2						
$IU_{3.9}$	здійснювати централізоване управління захистом від зловмисного коду	обов'язковий	категорія 2						
$IU_{3.10}$	використовувати операційні системи, для яких не припинено підтримку виробника	обов'язковий	категорія 2						
$IU_{3.11}$	використовувати офіційні стабільні версії прикладного програмного забезпечення та драйверів, для яких не припинено підтримку виробника	обов'язковий	категорія 2						
$IU_{3.12}$	визначити стандартне еталонне джерело часу та забезпечити синхронізацію з ним операційних систем	обов'язковий	категорія 2						
$IU_{3.13}$	забезпечити блокування або перейменування облікових записів користувачів операційних систем, що встановлюються за замовчуванням, та відключення гостьових облікових записів	обов'язковий	категорія 2						

Позначення ЧП	Частковий показник (ЧП)	Обов'язковість виконання	Категорія перевірки	Оцінка часткового показника ІБ					
				0	0,25	0,5	0,75	1	н/о
$IU_{3.14}$	здійснювати налаштування програмного забезпечення систем управління базами даних (СУБД) для роботи під окремим обліковим записом з дотриманням принципу надання мінімального рівня повноважень (необхідних для виконання функцій СУБД)	обов'язковий	категорія 2						
$IU_{3.15}$	здійснити розподіл мережі банку на фізичному та/або логічному рівні (сегментацію мережі) і обмежити доступ між сегментами мережі з використанням міжмережевих екранів.	обов'язковий	категорія 2						
$IU_{3.16}$	забезпечити ідентифікацію обладнання (наприклад, за ідентифікатором управління доступом до обладнання, MAC-адреса), що підключається до мережі банку, та вжиття заходів, які унеможливлюють роботу обладнання в мережі без відповідної ідентифікації	обов'язковий	категорія 2						
$IU_{3.17}$	забезпечити синхронізацію всіх активних мережевих пристроїв з еталонним джерелом часу банку	обов'язковий	категорія 2						
$IU_{3.18}$	створити та підтримувати в актуальному стані перелік факсимільних апаратів і багатофункціональних пристроїв (в електронному або паперовому вигляді), який містить унікальні ідентифікатори обладнання та місце його розташування	обов'язковий	категорія 2						

Позначення ЧП	Частковий показник (ЧП)	Обов'язковість виконання	Категорія перевірки	Оцінка часткового показника ІБ					
				0	0,25	0,5	0,75	1	н/о
$IU_{3.19}$	розміщувати обладнання телефонної мережі (сервери, комутаційне та абонентське обладнання) в окремому сегменті мережі банку, захищеному за допомогою міжмережевого екрана.	обов'язковий	категорія 2						
$IU_{3.20}$	запровадити такі заходи безпеки в разі використання телефонного зв'язку на основі протоколу Інтернет (IP-телефонії): 1) активувати вбудовані алгоритми шифрування трафіку між шлюзами, які забезпечують роботу телефонної системи банку, або між шлюзом та кінцевим абонентським обладнанням (телефоном); 2) здійснювати розподіл унікальних ідентифікаторів мережевого рівня (IP-адрес) у телефонній мережі банку відповідно до стандарту RFC 1918 "Розподіл адрес у приватних IP-мережах".	обов'язковий	категорія 3						
$IU_{3.21}$	розробити та впровадити заходи безпеки інформації для сервера електронної пошти, які включають: 1) додаткові заходи безпеки операційної системи, на якій встановлено сервер застосувань електронної пошти; 2) заходи безпеки сервера застосувань електронної пошти; 3) налаштування правил доступу до сервера електронної пошти.	обов'язковий	категорія 3						

Позначення ЧП	Частковий показник (ЧП)	Обов'язковість виконання	Категорія перевірки	Оцінка часткового показника ІБ					
				0	0,25	0,5	0,75	1	н/о
$IU_{3.22}$	забезпечити перевірку програмними або апаратними засобами захисту всіх повідомлень, що обробляються сервером застосувань електронної пошти, на наявність зловмисного коду	обов'язковий	категорія 3						
$IU_{3.23}$	впровадити періодичне тестування захищеності та перегляд налаштувань параметрів безпеки операційної системи сервера застосувань електронної пошти та безпосередньо сервера застосувань електронної пошти	обов'язковий	категорія 3						
$IU_{3.24}$	розміщувати сервер застосувань електронної пошти на окремому фізичному або віртуальному сервері	обов'язковий	категорія 2						
$IU_{3.25}$	використання віддаленого доступу до сервера застосувань електронної пошти банк зобов'язаний запровадити такі заходи безпеки інформації: 1) сервер має бути розміщений в демілітаризованій зоні мережі банку з обмеженням доступу до нього з публічної мережі за допомогою міжмережевого екрана або пристрою уніфікованого управління загрозами; 2) доступ до сервера електронної пошти має надаватись лише шифрованими каналами зв'язку.	обов'язковий	категорія 2						

Продовження додатку Ж

Позначення ЧП	Частковий показник (ЧП)	Обов'язковість виконання	Категорія перевірки	Оцінка часткового показника ІБ					
				0	0,25	0,5	0,75	1	н/о
$IU_{3.26}$	заходи безпеки інформації для сервера електронної пошти: 1) використовувати міжмережевий екран операційної системи сервера електронної пошти для обмеження доступу до сервера; 2) заблокувати отримання вхідних повідомлень від серверів мережі Інтернет, що розсилають спам; 3) упровадити процес постійного моніторингу вразливостей сервера застосувань електронної пошти та клієнтського програмного забезпечення доступу до сервера застосувань електронної пошти, забезпечити встановлення відповідних оновлень, що усувають виявлені вразливості.	обов'язковий	категорія 2						
$IU_{3.27}$	використовувати виключно ідентифіковані змінні носії інформації в інформаційних системах банку	обов'язковий	категорія 2						
$IU_{3.28}$	автоматизувати процес контролю за використанням змінних носіїв інформації в інформаційних системах банку	обов'язковий	категорія 2						
$IU_{3.29}$	використовувати досконалу пряму секретність (Perfect forward secrecy, PFS) для з'єднань на основі протоколу захисту на транспортному рівні	обов'язковий	категорія 2						
$IU_{3.30}$	використовувати сертифікати відкритих ключів, отримані в акредитованих/зареєстрованих ЦСК для ідентифікації та автентифікації, забезпечення конфіденційності інформації під час інформаційного обміну між інформаційними системами банку та Національного банку	обов'язковий	категорія 2						

Позначення ЧП	Частковий показник (ЧП)	Обов'язковість виконання	Категорія перевірки	Оцінка часткового показника ІБ					
				0	0,25	0,5	0,75	1	н/о
$OV_{БІТП}$ – оцінка степені виконання вимог, що регламентують банківський інформаційний технологічний процес									
$IU_{4.1}$	забезпечується застосування багаторівневого (ешелонованого) підходу, за яким окремо за допомогою незалежних систем криптографічного захисту інформації захищається сеансовий рівень базової еталонної моделі взаємодії відкритих систем (*Open systems interconnection basic reference model*, OSI/ISO) та прикладний рівень моделі взаємодії відкритих систем інформаційних систем Національного банку	обов'язковий	категорія 2						
$IU_{4.2}$	для захисту сеансового рівня моделі взаємодії відкритих систем інформаційних систем Національного банку використовується криптографічний протокол захисту на транспортному рівні (*Transport layer security*, TLS), забезпечуються контроль цілісності та конфіденційність інформації.	обов'язковий	категорія 2						
$IU_{4.3}$	для захисту прикладного рівня моделі взаємодії відкритих систем інформаційних систем Національного банку використовуються такі механізми захисту: ідентифікація/автентифікаці підписувача, контроль цілісності та конфіденційність на всіх етапах оброблення інформації	обов'язковий	категорія 3						

Позначення ЧП	Частковий показник (ЧП)	Обов'язковість виконання	Категорія перевірки	Оцінка часткового показника ІБ					
				0	0,25	0,5	0,75	1	н/о
$IU_{4.4}$	для забезпечення ідентифікації та автентифікації, використовується односпрямований (криптографічний ключ лише на стороні сервера, сувора криптографічна автентифікація сервера) або двоспрямований достовірний канал захисту на транспортному рівні (криптографічний ключ на стороні клієнта і на стороні сервера, сувора криптографічна автентифікація обох сторін з'єднання)	обов'язковий	категорія 3						
$IU_{4.5}$	інформаційні системи Національного банку підтримують роботу криптографічного протоколу захисту на транспортному рівні останньої версії, але не нижче версії 1.2	обов'язковий	категорія 3						
$IU_{4.6}$	здійснювати протоколювання всіх дій щодо надання, скасування чи зміни доступу до інформаційних систем банку, які безпосередньо забезпечують автоматизацію банківської діяльності, у захищених від несанкціонованої модифікації електронних журналах із забезпеченням їх збереження не менше ніж протягом трьох років	обов'язковий	категорія 2						
$IU_{4.7}$	забезпечити протоколювання, збереження та захист від модифікації інформації про події доступу до інформаційних систем банку, які безпосередньо забезпечують автоматизацію банківської діяльності, та зберігання її не менше ніж протягом одного року	обов'язковий	категорія 2						

Продовження додатку Ж

Позначення ЧП	Частковий показник (ЧП)	Обов'язковість виконання	Категорія перевірки	Оцінка часткового показника ІБ					
				0	0,25	0,5	0,75	1	н/о
$IU_{4.8}$	забезпечити персоналізований та контрольований доступ до комутаційних вузлів СКС	обов'язковий	категорія 2						
$IU_{4.9}$	забезпечити перевірку програмними та/або програмно-апаратними засобами захисту від зловмисного коду: 1) усіх вхідних та вихідних повідомлень корпоративної електронної пошти, уключаючи вкладення до них; 2) усього вхідного Інтернет-трафіку; 3) усіх змінних носіїв інформації, що підключаються до робочих станцій або іншого обладнання інформаційних систем банку	обов'язковий	категорія 2						
$IU_{4.10}$	зберігати електронні журнали роботи засобів захисту від зловмисного коду не менше ніж три місяці	обов'язковий	категорія 2						
$IU_{4.11}$	заблокувати вбудовані облікові записи локального адміністратора операційних систем або (якщо немає технічної можливості на рівні фунціоналу операційної системи) перейменувати такі вбудовані облікові записи та змінювати їх пароль не рідше ніж один раз на 30 діб	обов'язковий	категорія 2						
$IU_{4.12}$	забезпечити автоматичне блокування робочого стола операційної системи на робочій станції або сервері, якщо немає активності користувача протягом 15 хвилин, з наступною повторною автентифікацією користувача під час розблокування (за винятком робочих станцій або серверів, на яких блокування неможливе або потребує більшого інтервалу часу відсутності активності за технологією використання)	обов'язковий	категорія 2						

Позначення ЧП	Частковий показник (ЧП)	Обов'язковість виконання	Категорія перевірки	Оцінка часткового показника ІБ					
				0	0,25	0,5	0,75	1	н/о
$IU_{4.13}$	забезпечити централізоване розповсюдження налаштувань параметрів безпеки та інших параметрів конфігурації операційних систем (наприклад, за допомогою використання групових політик контролера домену "*Active Directory*")	обов'язковий	категорія 2						
$IU_{4.14}$	забезпечити блокування можливості здійснення працівниками банку, яким не надано адміністративних прав у операційних системах, таких дій (налаштувань): 1) самостійного встановлення програмного забезпечення, яке не внесено до переліку програмного забезпечення, що використовується в банку; 2) автоматичного запуску програм із зовнішніх пристроїв та носіїв інформації; 3) самостійного видалення встановленого програмного забезпечення, оновлень безпеки.	обов'язковий	категорія 2						
$IU_{4.15}$	забезпечити блокування облікових записів адміністраторів СУБД, установлених за замовчуванням (або зміну їх паролів) та використання облікових записів адміністраторів СУБД виключно для вирішення адміністративних завдань	обов'язковий	категорія 2						
$IU_{4.16}$	забезпечити фізичне або віртуальне функціональне розділення серверів СУБД та серверів застосувань інформаційних систем банку	обов'язковий	категорія 2						

Позначення ЧП	Частковий показник (ЧП)	Обов'язковість виконання	Категорія перевірки	Оцінка часткового показника ІБ					
				0	0,25	0,5	0,75	1	н/о
$IU_{4.17}$	зобов'язаний розміщувати сервери баз даних в окремому сегменті мережі банку, захищеному за допомогою міжмережевого екрана	обов'язковий	категорія 2						
$IU_{4.18}$	визначити привілейовані облікові записи для інформаційних систем банку, мережевого обладнання та серверів	обов'язковий	категорія 2						
$IU_{4.19}$	забезпечити розташування робочих станцій, з яких виконуються дії щодо адміністрування та супроводження інформаційних систем банку, мережевого обладнання та серверів банку, використовуючи привілейовані облікові записи, в окремому сегменті мережі банку, захищеному за допомогою міжмережевого екрана	обов'язковий	категорія 2						
$IU_{4.20}$	забезпечити надання доступу до портів адміністрування та супроводження інформаційних систем, мережевого обладнання та серверів банку виключно з IP-адрес (робочих станцій), які визначені банком для адміністрування та супроводження таких систем або обладнання	обов'язковий	категорія 2						
$IU_{4.\ 21}$	забезпечити використання адміністраторами інформаційних систем банку, мережевого обладнання та серверів банку облікових записів без привілейованих повноважень для автентифікації на робочих станціях, які визначені банком для адміністрування та супроводження таких систем чи обладнання	обов'язковий	категорія 2						

Позначення ЧП	Частковий показник (ЧП)	Обов'язковість виконання	Категорія перевірки	Оцінка часткового показника ІБ					
				0	0,25	0,5	0,75	1	н/о
$IU_{4.22}$	визначити та запровадити посилені вимоги щодо парольної політики для привілейованих облікових записів (довжина та складність паролів, частота зміни) або застосовувати багатофакторну автентифікацію для таких облікових записів	обов'язковий	категорія 2						
$IU_{4.23}$	забезпечити програмне відключення портів на активних мережевих пристроях мережі банку, які не використовуються	обов'язковий	категорія 2						
$IU_{4.24}$	використовувати облікові записи та паролі за замовчуванням на активних мережевих пристроях, які підключені до мережі банку	обов'язковий	категорія 2						
$IU_{4.25}$	забороняється використовувати протокол Інтернету версії 6 (IPv6) у мережі банку	обов'язковий	категорія 2						
$IU_{4.26}$	забороняється використовувати версії 1 або 2 простого протоколу керування мережею (*Simple network management protocol*, SNMP) для управління пристроями в мережі.	обов'язковий	категорія 2						
$IU_{4.27}$	розробити та впровадити заходи безпеки інформації у разі використання бездротових мереж передавання даних	обов'язковий	категорія 1						
$IU_{4.28}$	розмістити бездротові мережі банку в окремій зоні безпеки мережі банку (сегмент або набір сегментів мережі зі спільним рівнем безпеки) та розмежувати доступ із зони безпеки бездротових мереж до мережі банку з використанням міжмережевих екранів	обов'язковий	категорія 2						

Позначення ЧП	Частковий показник (ЧП)	Обов'язковість виконання	Категорія перевірки	Оцінка часткового показника ІБ					
				0	0,25	0,5	0,75	1	н/о
$IU_{4.29}$	встановити ідентифікатори бездротових мереж (SSID), відмінні від встановлених виробником або інсталятором обладнання за замовчуванням	обов'язковий	категорія 2						
$IU_{4.30}$	забезпечити розмежування доступу між мережею банку і публічною мережею з використанням міжмережевих екранів та/або пристроїв уніфікованого управління загрозами	обов'язковий	категорія 2						
$IU_{4.31}$	використовувати централізовані системи управління обліковими записами	обов'язковий	категорія 2						
$IU_{4.32}$	використовувати інструменти централізованого моніторингу та застосування оновлень безпеки для операційних систем	обов'язковий	категорія 2						
$IU_{4.33}$	забезпечити шифрування каналів передавання даних між серверами СУБД і серверами застосувань або шифрування даних, що передаються між серверами СУБД і серверами застосувань банку	обов'язковий	категорія 2						
$IU_{4.34}$	використовувати проміжний сервер для виконання функцій адміністрування чи супроводження інформаційних систем банку, мережевого обладнання та серверів	обов'язковий	категорія 2						
$OV_{БПТП}$ – оцінка степені виконання вимог, що регламентують банківський платіжний технологічний процес									

Позначення ЧП	Частковий показник (ЧП)	Обов'язковість виконання	Категорія перевірки	Оцінка часткового показника ІБ					
				0	0,25	0,5	0,75	1	н/о
$IU_{5.1}$	забезпечити дотримання принципу надання мінімального рівня повноважень під час надання доступу до інформаційних систем банку (уключаючи доступ привілейованих користувачів)	обов'язковий	категорія 2						
$IU_{5.2}$	запровадити такі заходи контролю доступу до інформаційних систем банку: 1) перевірку наявності у користувача дозволу керівництва та власника ІС на такий доступ; 2) заборону одноосібного ініціювання заявки, підтвердження та надання доступу; 3) перевірку відповідності рівня наданого доступу принципу мінімально необхідного рівня повноважень; 4) періодичну перевірку відповідності наданих прав доступу користувачеві тим, що діють на момент перевірки.	обов'язковий	категорія 1						
$IU_{5.3}$	забезпечити блокування облікових записів користувачів в інформаційних системах банку в таких випадках: 1) п'яти невдалих спроб автентифікації поспіль (автоматичне блокування); 2) відсутності реєстрації користувача в інформаційних системах банку протягом 90 календарних днів; 3) звільнення користувача.	обов'язковий	категорія 2						
$IU_{5.4}$	запровадити заходи, що забезпечують захист від несанкціонованого видалення, відключення та скасування оновлень засобів захисту від зловмисного коду, а також від зміни їх налаштувань та конфігурації	обов'язковий	категорія 1						

Позначення ЧП	Частковий показник (ЧП)	Обов'язковість виконання	Категорія перевірки	Оцінка часткового показника ІБ					
				0	0,25	0,5	0,75	1	н/о
$IU_{5.5}$	обробляти факти ураження інформаційних систем банку зловмисним кодом в рамках процесу управління інцидентами безпеки інформації	обов'язковий	категорія 1						
$IU_{5.6}$	здійснювати перевірку всіх переносних та/або стаціонарних носіїв інформації засобами захисту від зловмисного коду, які окремо або в складі пристрою були повернуті після їх використання третіми сторонами	обов'язковий	категорія 1						
$IU_{5.7}$	створити та підтримувати в актуальному стані перелік програмного забезпечення, що використовується в банку (в електронному або паперовому вигляді)	обов'язковий	категорія 2						
$IU_{5.8}$	забезпечити видалення/блокування неперсоналізованих і гостьових облікових записів користувачів СУБД та персоналізацію технологічних облікових записів СУБД	обов'язковий	категорія 2						
$IU_{5.9}$	забезпечити використання виключно персоналізованих облікових записів для виконання адміністрування чи супроводження інформаційних систем банку, мережевого обладнання та серверів	обов'язковий	категорія 2						

Позначення ЧП	Частковий показник (ЧП)	Обов’язковість виконання	Категорія перевірки	Оцінка часткового показника ІБ					
				0	0,25	0,5	0,75	1	н/о
$IU_{5.10}$	застосовувати такі заходи безпеки інформації для організації віддаленого доступу до інформаційних систем банку: 1) розміщення сервера (серверів) віддаленого доступу до інформаційних систем банку в демілітаризованій зоні (DMZ) мережі банку, з обмеженням доступу до нього з публічної мережі за допомогою міжмережевого екрана або пристрою уніфікованого управління загрозами; 2) шифрування каналів зв’язку для доступу до сервера віддаленого доступу до інформаційних систем банку; 3) багатофакторна автентифікація користувачів	обов’язковий	категорія 2						
$IU_{5.11}$	забезпечити доступ з публічної мережі до мережі банку виключно із застосуванням захищених з’єднань	обов’язковий	категорія 2						
$IU_{5.12}$	забезпечити розміщення в демілітаризованій зоні мережі банку серверів та обладнання, що забезпечує функціонування сервісів або банківських продуктів, які відкриті для доступу клієнтів з публічної мережі. З'єднання серверів та обладнання, що розміщено в демілітаризованій зоні, з серверами та обладнанням мережі банку захищаються міжмережевим екраном	обов’язковий	категорія 2						

Продовження додатку Ж

Позначення ЧП	Частковий показник (ЧП)	Обов'язковість виконання	Категорія перевірки	Оцінка часткового показника ІБ					
				0	0,25	0,5	0,75	1	н/о
$IU_{5.13}$	здійснювати маркування та документування елементів СКС відповідно до рекомендацій міжнародного стандарту ANSI/TIA/EIA-606	обов'язковий	категорія 3						
$IU_{5.14}$	здійснити функціональний розподіл серверів банку на мережевому рівні та забезпечити між ними мінімально необхідний зв'язок, що дозволить працювати серверам незалежно один від одного	обов'язковий	категорія 2						
$IU_{5.15}$	використовувати механізми багатофакторної автентифікації під час надання доступу до САБ	обов'язковий	категорія 2						
OV_{ozIP} – оцінка захисту БІн з використанням криптографічних ЗЗІ									
$IU_{6.1}$	використовувати механізми багатофакторної автентифікації під час надання доступу для виконання функцій адміністрування або супроводження САБ	обов'язковий	категорія 1						
$IU_{6.2}$	використовувати алгоритм Діффі – Геллмана (DH) для узгодження сеансових ключів шифрування	обов'язковий	категорія 2						
$IU_{6.3}$	використовувати алгоритм цифрового підпису (DSA) для цифрових підписів	обов'язковий	категорія 2						
$IU_{6.4}$	використовувати алгоритм Діффі – Геллмана на еліптичних кривих (ECDH) для узгодження сеансових ключів шифрування	обов'язковий	категорія 2						
$IU_{6.5}$	використовувати алгоритм цифрового підпису на еліптичних кривих (ECDSA) для цифрових підписів	обов'язковий	категорія 2						

Позначення ЧП	Частковий показник (ЧП)	Обов'язковість виконання	Категорія перевірки	Оцінка часткового показника ІБ					
				0	0,25	0,5	0,75	1	н/о
$IU_{6.6}$	використовувати алгоритм Ривест – Шаміра – Адлемана (RSA) для цифрових підписів і узгодження сеансових ключів шифрування або аналогічних ключів	обов'язковий	категорія 2						
$IU_{6.6}$	використовувати алгоритм цифрового підпису [ДСТУ 4145-2002 "Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння", затверджений наказом Державного комітету України з питань технічного регулювання та споживчої політики від 28 грудня 2002 року № 31 (ДСТУ 4145-2002)] для цифрових підписів	обов'язковий	категорія 2						
$IU_{6.6}$	використовувати алгоритми безпеки гешування SHA-224, SHA-256, SHA-384, SHA-512, "Купина" (ДСТУ 7564:2014 "Інформаційні технології. Криптографічний захист інформації. Функція гешування", прийнятий наказом Міністерства економічного розвитку і торгівлі України від 02 грудня 2014 року № 1431) або більш криптостійкі	обов'язковий	категорія 2						
$IU_{6.7}$	алгоритм "*Advanced encryption standard*" (*AES*) із використанням довжини ключа 128, 192 і 256 біт або більше	обов'язковий	категорія 2						

Позначення ЧП	Частковий показник (ЧП)	Обов'язковість виконання	Категорія перевірки	Оцінка часткового показника ІБ					
				0	0,25	0,5	0,75	1	н/о
$IU_{6.8}$	алгоритм криптографічного перетворення (ДСТУ ГОСТ 28147:2009 "Система оброблення інформації. Захист криптографічний. Алгоритм криптографічного перетворення", прийнятий наказом Державного комітету України з питань технічного регулювання та споживчої політики від 22 грудня 2008 року № 495)	обов'язковий	категорія 2						
$IU_{6.9}$	алгоритм "Калина" (ДСТУ 7624:2014 "Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення", прийнятий наказом Міністерства економічного розвитку і торгівлі України від 29 грудня 2014 року № 1484)	обов'язковий	категорія 2						
$IU_{6.10}$	при застосуванні алгоритму DH для узгодження сеансових ключів шифрування, зобов'язаний використовувати розмір модуля не менше ніж 2048 біт	обов'язковий	категорія 2						
$IU_{6.11}$	при застосуванні алгоритму DSA для цифрових підписів, зобов'язаний використовувати розмір модуля не менше ніж 2048 біт	обов'язковий	категорія 2						
$IU_{6.12}$	при застосуванні алгоритму на еліптичних кривих, зобов'язаний використовувати еліптичні криві з ДСТУ 4145-2002 або з Федерального стандарту оброблення інформації (США) (*Federal information processing standards, FIPS186-4*)	обов'язковий	категорія 2						

Позначення ЧП	Частковий показник (ЧП)	Обов’язковість виконання	Категорія перевірки	Оцінка часткового показника ІБ					
				0	0,25	0,5	0,75	1	н/о
$IU_{6.13}$	при застосуванні алгоритму ECDH для узгодження сеансових ключів шифрування, зобов’язаний використовувати розмір поля/ключа не менший, ніж 160 біт	обов’язковий	категорія 2						
$IU_{6.14}$	при застосуванні алгоритмів ECDSA, ДСТУ 4145-2002 для цифрових підписів, зобов'язаний використовувати розмір поля/ключа не менший, ніж 160 біт	обов’язковий	категорія 2						
$IU_{6.15}$	при застосуванні алгоритму RSA для цифрових підписів і ключів шифрування сеансу або аналогічних ключів, зобов'язаний використовувати розмір модуля не менше ніж 2048 біт.	обов’язковий	категорія 2						
$IU_{6.16}$	використовувати виключно актуальні версії ліцензійних засобів захисту від зловмисного коду, для яких не припинено підтримку виробника	обов’язковий	категорія 2						
$IU_{6.17}$	забезпечити використання в бездротових мережах банку режиму безпеки WPA2-Enterprise (корпоративний режим у наборі алгоритмів і протоколів *Wireless protected access* версії 2) та використання режиму безпеки WPA2-Personal (персональний режим у наборі алгоритмів і протоколів *Wireless protected access* версії 2) для реалізації гостьових підключень	обов’язковий	категорія 2						

Кінець додатку Ж

Позначення ЧП	Частковий показник (ЧП)	Обов'язковість виконання	Категорія перевірки	Оцінка часткового показника ІБ					
				0	0,25	0,5	0,75	1	н/о
$IU_{6.18}$	забороняється використовувати радіотелефони та/або радіоподовжувачі телефонної лінії без активованих у них алгоритмів шифрування сигналу, який передається радіоканалом.	обов'язковий	категорія 2						
$IU_{6.19}$	застосовувати комбінацію програмних та програмно-апаратних засобів захисту від зловмисного коду	обов'язковий	категорія 2						
$IU_{6.20}$	використовувати стандарти, документи та настанови відкритого проекту захисту веб-додатків "*Open web application security project*" (OWASP) для розроблення безпечних веб-додатків	обов'язковий	категорія 2						

Додаток К

Список публікацій здобувача за темою дисертації

Наукові праці, в яких опубліковані основні результати дисертації

Монографії

1. О. О. Кузнецов, С. П. Євсеєв, С. В. Кавун, та О. Г. Король, *Сигнали і коди. Алгебраїчні методи синтезу*. Монографія. Харків, Україна: Вид. ХНЕУ, 2009.

2. О. О. Кузнецов, С. П. Євсеєв, та С. В. Кавун, *Захист інформації та економічна безпека підприємства*. Монографія. Харків, Україна: Вид. ХНЕУ, 2009.

3. С. П. Євсеєв, О. Ю. Йохов, та О. Г. Король, *Гешування даних в інформаційних системах*. Монографія. Харків, Україна: Вид. ХНЕУ, 2013.

Колективні монографії за результатами конференцій

4. С. П. Евсеев, и О. Г. Король, “Исследование коллизионных свойств кодов аутентификации сообщений UMAC”. *Информационные технологии и системы в управлении, образовании, науке*. Коллективная монография [под. редакцией В. С. Пономаренко]. Харків, Україна: Цифрова друкарня, с. 25 – 38, 2013.

5. С. П. Евсеев, и Т. А. Свердло, “Исследование угроз методов двухфакторной аутентификации”. *Информационные технологии и защита информации в информационно-коммуникационных системах*: Коллективная монография [под. редакцией В. С. Пономаренка]. Харків, Україна: Вид-во ТОВ “Щедра садиба плюс”, с. 141 – 154, 2015.

6. С. П. Евсеев, и О. Г. Король, “Синергетические модели оценки безопасности в автоматизированных банковских системах”. *Інформаційні технології: проблеми та перспективи*. Коллективная монография [за заг. ред. В. С. Пономаренка]. Харків, Україна: Вид. Рожко С. Г., с. 203 – 221, 2017.

7. С. П. Евсеев, Г. П. Коц, и И. П. Отенко, “Методология построения модифицированной системы электронного документооборота в университете на основе электронной цифровой подписи стандарта X.509”. *Моделирование процессов управления в информационной экономике*. Колективна монографія

[Под ред. докт. экон. наук, проф. В. С. Пономаренка, докт. экон. наук, проф. Т. С. Клебановой] – Бердянск, Україна: издатель Ткачук А. В., с. 264 – 295, 2017.

У міжнародних рецензованих виданнях, що входять до баз даних Scopus та Web of Science:

8. С. Евсеев, и А. Дорохов, “Информационные угрозы и безопасность в банковских платежных системах Украины”, *Криминологический журнал БГУЭП*, вип. 2, с. 68 – 75, 2011. *(Scopus)*

9. С. Евсеев, и В. Абдулаев, “Алгоритм мониторинга метода двухфакторной аутентификации на основе системы Passwindow”, *Восточно-европейский журнал передовых технологий*, вып. 2/2(74), с. 9 – 15, 2015. *(Scopus)*

10. С. Евсеев, О. Король, и Г. Коц, “Анализ законодательной базы к системе управления информационной безопасностью НСМЭП”, *Восточно-европейский журнал передовых технологий*, вып. 5/3(77), с. 48 – 59, 2015. *(Scopus)*

11. С. Евсеев, О. Король, Х. Рзаев, и З. Иманова, “Разработка модифицированной несимметричной крипто-кодовой системы Мак-Элиса на укороченных эллиптических кодах”, *Восточно-европейский журнал передовых технологий*. том 4, 9(82), с. 18 – 26, 2016. *(Scopus)*

12. S. Yevseiev, H. Kots, and Y. Liekariev, “Developing of multi-factor authentication method based on Niederreiter-McEliece modified crypto-code system”, *Восточно-европейский журнал передовых технологий*, 6/4(84), с. 11 – 23, 2016 *(Scopus)*

13. С. Євсеєв, С. Остапов, Х. Рзаєв, та В. Ніколаєнко, “Оцінка обміну даними в глобальних обчислювальних мережах на основі комплексного показника якості обслуговування мережі”, *Науковий журнал Радіоелектроніка, інформатика, управління*, № 1(40), с. 115 – 128, 2017. *(Web of Science)*

14. S. Yevseiev, O. Korol, and H. Kots, “Construction of hybrid security systems based on the crypto-code structures and flawed codes”, *Восточно-европейский журнал передовых технологий*, 4/9(88), с. 4 – 20, 2017. *(Scopus)*

15. S. Yevseiev, H. Kots, S. Minukhin, O. Korol, and A. Kholodkova, “The development of the method of multifactor authentication based on hybrid crypto-code

constructions on defective codes", *Восточно-европейский журнал передовых технологий*, 5/9(89), с. 19 – 35, 2017. *(Scopus)*

16. S. Yevseiev, V. Ponomarenko, and O. Rayevnyeva, "Assessment of functional effectiveness of the corporate scientific-educational network based on comprehensive indicators of service quality", *Восточно-европейский журнал передовых технологий*, 6/2 (90), с. 4 – 15, 2017. *(Scopus)*

В іноземних наукових періодичних виданнях:

17. С. Евсеев, и О. Король, "Результаты статистического тестирования безопасности и продуктивности хеш-алгоритмов-претендентов конкурса по отбору стандартного алгоритма SHA-3", *Известия Высших технических учебных заведений Азербайджана*. том.14, № 2 (78), с. 73 – 78, 2012.

18. S. Yevseiev, T. Sverdlo, and O. Korol, "Mécanismes intégrés de sécurité et de fiabilité des données dans les systèmes d'information basés sur la théorie des codes correcteurs d'erreurs", *French Journal of Science and Education*, № 2(12), p. 358 – 368, 2014.

19. С. Евсеев, А. Сочнева, О. Король, и В. Абдулаев, "Анализ методик оценки рисков нарушения безопасности банковской информации", *Известия Высших технических учебных заведений Азербайджана*. том. 19, № 2 (106), с. 77 – 86, 2017.

20. С. Евсеев, и О. Король, "Метод каскадного формирования МАС-кодов на основе модулярных преобразований", *Известия Высших технических учебных заведений Азербайджана*, № 1 (89), с. 71 – 78, 2014.

У наукових фахових виданнях України, які входять до інших міжнародних наукометричних баз даних (Index Copernicus, EBSCO , Inspec тощо)

21. С. Евсеев, О. Король, и А. Жученко, "Защита информации в интернет-платежных системах", *Восточно-европейский журнал передовых технологий*, 5/2(35), с. 34 – 37. 2008.

22. С. Евсеев, О. Король, и Л. Пархуць, “Разработка модели и метода каскадного формирования МАС с использованием модулярных преобразований” *Захист інформації: науково-технічний журнал*, том 15, № 3, с. 186 – 196, 2013.

23. S. Evseev, “International legislation on personal data protection”, *Системи обробки інформації*, № 9(107), с. 140 – 144, 2012.

24. S. Evseev, and B. Tomashevsky, “Two-factor authentication methods threats analysis”, *Радіоелектроніка, інформатика, управління*, вип. 1(32), с. 52 – 59, 2015.

25. С. Евсеев, “Синергетический подход к оценке безопасности банковских систем”, *Системи обробки інформації*, № 4(141), с. 90 – 103, 2016.

26. R. Hryshchuk, and S. Yevseiev, “The synergetic approach for providing bank information security: the problem formulation”, *Безпека інформації*, № 22 (1), с. 64 – 74. 2016.

27. С. Евсеев, Х. Рзаев, и А. Цыганенко, “Анализ программной реализации прямого и обратного преобразования по методу недвоичного равновесного кодирования”, *Науково-технічний журнал “Безпека інформації”*, том 22, № 2, с. 196 – 203, 2016.

28. С. Евсеев, “Методология оценивания безопасности информационных технологий автоматизированных банковских систем Украины”, *Науково-технічний журнал “Безпека інформації”*, том. 22, № 3, с. 297 – 309, 2016.

29. С. Евсеев, “Модель нарушителя прав доступа в автоматизированной банковской системе на основе синергетического подхода”, *Науково-технічний журнал “Інформаційна безпека”*, № 2 (26), с. 110 – 119, 2017.

30. С. Евсеев, “Оценка эффективности инвестиций в безопасность организаций банковского сектора на основе синергетической модели угроз”, *Системи обробки інформації*, № 2 (148), с. 88 – 94, 2017.

31. С. Євсеєв, С. Остапов, та Р. Королев, “Використання міні-версій для оцінки стійкості блоково-симетричних шифрів”, *Науково-технічний журнал “Безпека інформації”,* том 23, № 2, с. 100 – 108, 2017.

32. Р. Грищук, та С. Євсеєв, “Методологія побудови системи забезпечення інформаційної безпеки банківської інформації в автоматизованих банківських системах”, *Науково-технічний журнал “Безпека інформації”*, том 23, № 3, с. 204 – 214, 2017.

У наукових фахових виданнях України

33. С. Євсеєв, “Анализ методов построения универсальных классов хеш-функций”, *Вісник Державного університету інформаційно-комунікаційних технологій*, том 7 (№ 4), с. 337 – 345, 2009.

34. С. Евсеев, О. Король, и А. Гончарова, “Построение моделей атак на внутриплатежные банковские системы”, *Радіоелектроніка, інформатика, управління*, вип. 1(22), с. 56 – 66, 2010.

35. С. Евсеев, и Б. Томашевский, “Исследование теоретико-кодовых схем для комплексного обеспечения безопасности и достоверности данных в информационных системах”, *Науковий вісник Чернівецького університету. Серія: Комп’ютерні системи та компоненти*, том 2, вип.1, с. 6 – 14, 2011.

36. А. Кузнецов, О. Король и С. Евсеев, “Исследование коллизионных свойств кодов аутентификации сообщений UMAC”, *Прикладная радиоэлектроника*, том 11, № 2, с. 171 – 183, 2012.

37. С. Евсеев, О. Король и Н. Суханова, “Анализ угроз и механизмов защиты во внутриплатежных системах коммерческого банка”, *Науково-практичний журнал “Сучасна спеціальна техніка”*, 1(24), с. 49 – 60, 2011.

38. С. Евсеев, “Анализ защиты в национальной системе массовых электронных платежей”, *Інформаційна безпека*, № 3(15), с. 15 – 28, 2014.

39. С. Евсеев, О. Король, и А. Сочнева, “Анализ оценки рисков кибербезопасности банковской информации”, *Сборник научных трудов НАУ “Защита информации”*, вып. 23, с. 109 – 128, 2016.

40. С. Евсеев, “Синергетическая модель оценки безопасности банковской информации”, *Науково-технічний журнал “Інформаційна безпека”*, № 4 (24), с. 104 – 118, 2016.

41. С. Євсеєв, О. Андрощук, та В. Федорченко, “Побудова систем безпеки інформаційно-телекомунікаційних систем на основі комплексного крипто-графічного підходу”, *Збірник наукових праць Нац. академії Держ. прикор. служби України ім. Богдана Хмельницького. Серія : військові та технічні науки* [гол. ред. Олексієнко Б. М.], № 2 (72), с. 258 – 268, 2017.

42. С. Євсеєв, та О. Король, “Дослідження загроз методів двофакторній автентифікації”, *Вісник національного університету “Львівська політехніка”*, № 806, с. 62 – 71, 2014.

43. С. Евсеев, Ю. Хохлачева, и О. Король, “Оценка обеспечения непрерывности бизнес-процессов в организациях банковского сектора на основе синергетического подхода, ч.1”, *Сучасна спеціальна техніка. Науково-практичний журнал*, № 1(48), с. 17 – 25. 2017.

44. С. Евсеев, Ю. Хохлачева, и О. Король, “Оценка обеспечения непрерывности бизнес-процессов в организациях банковского сектора на основе синергетического подхода, ч. 2”, *Сучасна спеціальна техніка. Науково-практичний журнал*, № 2(49), с. 10 – 17, 2017.

Наукові праці, які засвідчують апробацію матеріалів дисертації

45. С. Евсеев, Р. Грищук, и О. Король, “Анализ современных методов выявления кибератак на ресурсы коммуникационных систем”, *Науково-практична конференція “Проблеми науково-технічного та правового забезпечення кібербезпеки у сучасному світі”*, Харків, 2016, с. 9.

46. С. Евсеев, и И. Белодед, “Крипто-кодовая система на модифицированных кодах”, *V Міжнародна науково-технічна конференція “Методи та засоби кодування, захисту й ущільнення інформації”*, Вінниця, 2016, с. 47 – 50.

47. С. Евсеев, “Методология оценивания безопасности информационных технологий автоматизированных банковских систем”, *III Міжнародна науково-практична конференція “Актуальні питання забезпечення кібербезпеки та захисту інформації”*, Київ, 2017, с. 75 – 76.

48. С. Евсеев, и О. Король, “Модель нарушителя прав доступа в автоматизированной банковской системе на основе синергетического подхода”, *Друга Міжнародна науково-практична конференція “Проблеми науково-технічного та правового забезпечення кібербезпеки у сучасному світі”*, Харків, 2017, с. 23.

49. С. Євсеєв, та О. Король, “Комплексний показник ефективності інвестицій в безпеку банківської інформації на основі синергетичної моделі загроз”, *VI Міжнародна наукова конференція “Інформація, комунікація, суспільство 2017”*, Славське, 2017, с. 18 – 19.

50. С. Евсеев, и О. Король, “Классификатор угроз на основе синергетического подхода”, *VII міжнародна науково-технічна конференція “ITSEC: Безпека інформаційних технологій”*, Київ, 2017, с. 83 – 84.

51. С. Євсеєв, “Математичні моделі модифікованої несиметричної крипто-кодової системи Мак-Еліса на модифікованих еліптичних кодах”, *Міжнародна науково-практична конференція “Інформаційні технології та комп’ютерне моделювання”*, Івано-Франківськ, 2017, с. 192 – 196.

52. С. Евсеев, и О. Король, “Математическая модель протокола обмена данными на основе модифицированных несимметричных крипто-кодовых систем Мак-Элиса и Нидеррайтера на ущербных кодах”, *VII міжнародна науково-технічна конференція “Захист інформації і безпека інформаційних систем”*, Львів, 2017, с. 89 – 90.

53. С. Євсеєв, та І. Білодід, “Використання збиткових кодів в гібридних крипто-кодових конструкціях”, *П’ята міжнародна науково-технічна конференція “Проблеми інформатизації”*, Черкаси – Баку – Бельсько-Бяла – Полтава, 2017, с. 11.

54. С. Євсеєв, та О. Андрощук, “Система безпеки інформаційно-телекомунікаційних систем на основі комплексного криптографічного підходу”, *X Всеукраїнська науково-практична конференція “Освітньо-наукове забезпечення діяльності складових сектору безпеки і оборони України”,* Хмельницький, 2017, року, с. 268 – 269.

Таблиця К.1 – Апробація результатів дисертаційної роботи

№ з/п	Тип конференції	Назва конференції	Місце і дата проведення	Тип участі
1.	Міжнародна науково-технічна конференція	“Проблеми науково-технічного та правового забезпечення кібербезпеки у сучасному світі”	Харків, 30.03 – 1.04.2016	очна
2.	Міжнародна науково-практична конференція	“Методи та засоби кодування, захисту й ущільнення інформації”	Вінниця, 19 – 21.04.2016	заочна
3.	Міжнародна науково-практична конференція	“Актуальні питання забезпечення кібербезпеки та захисту інформації”	Київ, 22 – 25.02.2017	заочна
4.	Міжнародна науково-практична конференція	“Проблеми науково-технічного та правового забезпечення кібербезпеки у сучасному світі”	Харків, 10 – 12.04.2017	очна
5.	Міжнародна науково-практична конференція	“Інформація, комунікація, суспільство 2017”	Славське, 18 – 20.05.2017	заочна
6.	Міжнародна науково-практична конференція	“ITSEC: Безпека інформаційних технологій”	Київ, 16 – 18.05.2017	очна
7.	Міжнародна науково-практична конференція	“Інформаційні технології та комп’ютерне моделювання”	Івано-Франківськ, 15 – 20.05.2017	заочна
8.	Міжнародна науково-практична конференція	“Захист інформації і безпека інформаційних систем”	Львів, 1 – 2.06.2017	очна
9.	Міжнародна науково-технічна конференція	“Проблеми інформатизації”	Черкаси, 13 – 15.11.2017	заочна
10.	Всеукраїнська науково-практична конференція	“Освітньо-наукове забезпечення діяльності складових сектору безпеки і оборони України”	Хмельницький, 2.11.2017	очна