НАЦІОНАЛЬНА АКАДЕМІЯ ДЕРЖАВНОЇ ПРИКОРДОННОЇ СЛУЖБИ
УКРАЇНИ ІМЕНІ БОГДАНА ХМЕЛЬНИЦЬКОГО,
ДЕРЖАВНА ПРИКОРДОННА СЛУЖБА УКРАЇНИ

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ,
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Кваліфікаційна наукова
праця на правах рукопису

Стрельбіцький Михайло Анатолійович

Прим. № 1
УДК 623.618 : 351.746.1

ДИСЕРТАЦІЯ
«ТЕХНОЛОГІЯ ЗАБЕЗПЕЧЕННЯ ФУНКЦІОНАЛЬНОЇ БЕЗПЕКИ ІНТЕГРОВАНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ ДЕРЖПРИКОРДОНСЛУЖБИ НА СТАДІЇ МОДЕРНІЗАЦІЇ»

Спеціальність 05.13.06 – інформаційні технології
Галузь знань 12 – 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

М. А. Стрельбіцький

Науковий консультант: Юдін Олександр Костянтинович, доктор технічних наук, професор

Київ – 2018

АНОТАЦІЯ

Стрельбіцький М. А. Технологія забезпечення функціональної безпеки інтегрованої інформаційної системи Держприкордонслужби на стадії модернізації – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.13.06 – інформаційні технології. Національна академія Державної прикордонної служби України імені Б. Хмельницького, захист відбудеться в Національному авіаційному університеті, м. Київ, 2018.

У дисертаційній роботі вирішувалась науково-прикладна проблема забезпечення функціональної безпеки відомчої інтегрованої інформаційної системи на стадії модернізації.

Теоретичні дослідження виконані на підставі фундаментальних положень теорії ймовірностей, теорії ефективності, теорії графів, теорії інформації, теорії захисту інформації, а також загальні теоретико-множинні, алгебраїчні методи. Експертне оцінювання здійснювалось відповідно до апробованих методик у цій галузі з обов’язковим оцінюванням ступеня узгодженості думок експертів. Обробка експериментальних даних виконана із застосуванням методів математичного аналізу, комп’ютерного моделювання, числових методів та елементів математичної статистики.

Аналіз існуючих підходів до проблеми забезпечення функціональної безпеки інформаційних систем показав наявність циклічного процесу їх вдосконалення, що вимагає структурованого аналізу та декомпозиції факторів, які впливають на дотримання властивостей інформаційних систем на стадії модернізації.

Опис процесу модернізації інформаційних системи (ІС) дозволив сформулювати стратегію забезпечення функціональної безпеки, яка полягає у такій сукупності заходів по заміні складових інформаційної системи, за якої рівень функціональної безпеки відповідав нормативному. Проведений аналіз критеріїв забезпечення функціональної безпеки та особливостей

функціонування інтегрованої інформаційної системи дозволив сформувати раціональні стратегії модернізації.

Сформована загальна концепція забезпечення функціональної безпеки на стадії модернізації як інструментально-методологічна база, що забезпечує виконання розглянутих стратегій. Концепцією передбачено три завдання узгодження спільного функціонування: спеціального програмного забезпечення, програмних та технічних (апаратних) засобів забезпечення функціональної безпеки, а також визначення величини уразливості ІС при проведенні заходів з модернізації та оцінювання ефективності системи забезпечення функціональної безпеки ІС на стадії модернізації. Результатом є отримання оцінки ефективності проведених заходів, яка використовується власником системи для прийняття рішення з проведення модернізації та визначення організаційних заходів щодо особливості проведення самого процесу оновлення складових ІС.

Дослідження моделі інформаційних потоків інтегрованої інформаційної системи на стадії модернізації показало, що основним принципом послідовності модернізації елементів ІС, який знижує ймовірність порушення властивостей ІС, є модернізація за величиною вихідного потоку та ймовірності порушення властивостей елементів ІС при невідповідності версій спеціального програмного забезпечення (СПЗ). При однаковій ймовірності порушення властивостей елементів ІС з причини невідповідності версій СПЗ двох елементів модернізується перший той, в кого вхідний потік менший.

Аналіз особливостей функціонування різних ІС дозволив сформувати три види показників: за максимально можливим значенням ймовірності порушення властивостей ІС під час модернізації, за середнім значенням ймовірності порушення властивостей ІС у процесі модернізації та середньозваженим значення ймовірності. Визначено, що пріоритетним показником ефективності процесу модернізації є максимальне значення ймовірності порушення властивостей ІС у процесі модернізації. Чим менше

цей показник, тим ефективніше провадиться заміна спеціального програмного забезпечення на елементах ІС.

Проведені дослідження вирішили завдання аналізу та синтезу системи забезпечення функціональної безпеки при прийнятій гіпотезі щодо найбільш несприятливої ситуації про порушення, яке полягає в тому, що воно може відбуватись через будь-який канал інформаційного дестабілізаційного впливу та в будь-який момент часу.

Наукова новизна роботи полягає в таких основних положеннях.

Уперше розроблена математична модель інформаційних потоків ІС на стадії модернізації та метод визначення раціональної послідовності модернізації елементів інформаційних систем, що дозволило раціоналізувати процес модернізації елементів інформаційних систем довільної структури за обраною стратегією модернізації.

Уперше розроблені моделі каналу інформаційного дестабілізаційного впливу і функціональної захищеності інформаційної системи та метод розподілу засобів забезпечення функціональної безпеки інформаційних систем на стадії модернізації, що дозволило забезпечити нормативний рівень функціональної безпеки системи в цілому.

Отримав подальший розвиток метод оцінювання уразливості ІС в інтегрованій інформаційній системі на стадії модернізації на базі розроблених аналітичних моделей порушення властивостей ІС, що дозволило визначити інтегральну величину уразливості ІС. Відмінність наведених моделей від існуючих полягає у врахуванні дестабілізаційних факторів, викликаних стадією модернізації, та визначенні ймовірності потреби у забезпеченні дотримання властивостей інформаційного ресурсу інформаційних систем, яка ґрунтується на функції розподілу Гомперца-Мейкгама.

Уперше розроблено комплекс методів узгодження систем розмежування доступу в інформаційних системах на стадії модернізації, а саме: метод узгодження решіток рівнів конфіденційності систем мандатного розмежування доступу, метод узгодження матриць доступу систем

дискреційного розмежування доступу, метод узгодження систем рольового розмежування доступу. Така сукупність методів дозволила сформувати методологічний базис узгодження моделей розмежування доступу інформаційних систем на стадії модернізації. У рамках методів сформульовані та доказані базові теореми безпеки. Розроблені методологічний базис та методи узгодження систем розмежування доступу дозволяють забезпечити функціональну безпеку інформаційних систем в рамках систем розмежування доступу.

Отримала подальший розвиток модель інформаційних дестабілізаційних факторів на стадії модернізації та метод оцінювання ефективності забезпечення функціональної безпеки інформаційних систем на стадії модернізації, що дозволило визначити ймовірність виконання системою функціональних завдань в умовах впливу як зовнішніх, так і внутрішніх дестабілізуючих факторів. Відмінність розробленого методу полягає у двоетапному формуванні переліку інформаційних дестабілізаційних впливів із визначення ступеня їх реалізації.

Уперше розроблено інформаційну технологію забезпечення функціональної безпеки інтегрованої інформаційної системи на стадії модернізації, що дозволить здійснювати поетапне вдосконалення інформаційних систем реального часу критичного застосування.

Практичне значення одержаних результатів.

Використання розробленої моделі інформаційних потоків ІС на стадії модернізації та методу визначення раціональної послідовності модернізації елементів інформаційних систем дозволило зменшити ймовірність порушення властивостей ІС за обраною стратегією модернізації до восьми разів від максимального та до трьох разів від середнього значення.

Використання методу розподілу засобів забезпечення функціональної безпеки інформаційних систем на стадії модернізації, складовими якого є моделі каналу інформаційного дестабілізаційного впливу та функціональної захищеності інформаційної системи, дозволило визначити необхідну

сукупність додаткових засобів за умови дотримання нормативного рівня функціональної безпеки системи в цілому.

Розроблений метод оцінювання уразливості ІС в інтегрованій інформаційній системі на стадії модернізації на базі аналітичних моделей порушення властивостей ІС дозволив врахувати фактори, які викликані процесом модернізації інформаційної системи та до двох разів підвищити точність порівняно з існуючими методами.

Розроблений комплекс методів узгодження систем розмежування доступу в інформаційних системах на стадії модернізації забезпечує безпечне функціонування ІС на спільному полі даних при дотриманні базових методологічних засад. Разом із тим, у рамках методології розроблена методика оцінювання ефективності узгодження систем розмежування доступу за наявності недозволених інформаційних потоків. Проведене оцінювання ефективності узгодження систем розмежування доступу на прикладі взаємодії двох ІС у складі інтегрованої інформаційної системи "Гарт-1" та "Гарт-5" показало ймовірність порушення властивостей хоча б одного елементу даних під час модернізації на рівні до 0,0003.

Розроблений програмний комплекс, що базується на створених моделях, методах та технології, дозволив до трьох разів підвищити оперативність формування практичних рекомендацій із адаптації засобів забезпечення функціональної безпеки інформаційних систем на стадії модернізації.

Розроблена інформаційна технологія забезпечення функціональної безпеки інтегрованої інформаційної системи на стадії модернізації дозволила забезпечити нормативний рівень порушення функціональної безпеки при модернізації ІС "Гарт-1/П" на рівні до 0,005.

Ключові слова: інформаційна система, технологія, модернізація, ефективність, розмежування доступу, функціональна безпека.

Основні результати дисертаційних досліджень опубліковані в 39 наукових працях.

ABSTRACT

Strelbitsky M.A. Technology of providing functional safety of the integrated information system of the State Border Service at the stage of modernization - Qualifying scientific work on the rights of the manuscript.

Dissertation for the degree of Doctor of Technical Sciences in specialty 05.13.06 - Information Technologies. National Academy of the State Border Guard Service of Ukraine named after B. Khmelnytsky, promulgation and public defense will be held at the National Aviation University, Kyiv, 2018.

In the dissertation, the scientific and applied problem of ensuring the functional security of the departmental integrated information system at the stage of modernization was solved.

Theoretical studies are performed on the basis of the fundamental provisions of the theory of probability, the theory of efficiency, the theory of graphs, the theory of information, the theory of information security, as well as general theorem-plural, algebraic methods. The expert evaluation was carried out in accordance with proven methods in the field with the obligatory assessment of the degree of consistency of expert opinions. The processing of experimental data is performed using mathematical analysis, computer simulation, numerical methods and elements of mathematical statistics.

The analysis of existing approaches to the problem of providing functional security of information systems showed the existence of a cyclic process of their improvement, which requires structured analysis and decomposition of factors that affect the compliance of the properties of information systems at the stage of modernization.

The description of the process of modernization of the information system (IS) allowed formulating a strategy for providing functional security, consisting in such a set of measures to replace the components of the information system in which the level of functional security was in line with the normative. The analysis of the criteria for ensuring functional safety and the features of the functioning of the

integrated information system made it possible to form rational strategies for modernization.

The general concept of providing functional safety at the stage of modernization is formed, as an instrumental and methodological framework that ensures the implementation of the considered strategies. The concept provides three tasks for the coordination of the joint operation: special software, software and hardware (hardware) means of providing functional security, as well as determining the magnitude of the vulnerability of IS in the course of modernization and evaluation of the efficiency of the system for ensuring functional security of IS at the stage of modernization. The result is an assessment of the effectiveness of the measures taken by the system owner to decide on the modernization and definition of organizational measures regarding the peculiarities of the process of updating the components of the IS itself.

The research of the model of information flows of the integrated information system at the stage of modernization showed that the basic principle of the sequence of IS elements upgrading, which reduces the probability of breaking IS properties, is the modernization of the magnitude of the output stream and the probability of breaking the properties of the IS elements in case of non-compliance of special software versions (SS). At the same probability of violation of the properties of the elements of IS due to discrepancy versions of SS of the two elements is modernized the first one in whom the input flow is smaller.

The analysis of the peculiarities of the functioning of different ISs allowed to form three types of indicators: the maximum possible value of the probability of breaking the properties of IS during the upgrade, the average value of the probability of breaking the properties of IS in the process of modernization and the weighted average probability. It is determined that the priority indicator of the efficiency of the modernization process is the maximum value of the probability of breaking the properties of the IS during the modernization process. The lower this figure, the more effective the replacement of special software on the elements of the IS.

The conducted researches have solved the problem of analysis and synthesis of the system of providing functional safety, with the hypothesis adopted, about the most unfavorable violation situation, which is that it can occur through any channel of information destabilizing influence and at any given time.

The scientific novelty of the work is in the following basic provisions.

For the first time, a mathematical model and method for determining the rational sequence of modernization of elements of information systems were developed, which allowed streamlining the process of modernization of elements of information systems of an arbitrary structure according to the chosen strategy of modernization.

For the first time, models of the channel of information destabilizing influence and functional security of the information system and the method of distribution of means of providing functional security of information systems at the stage of modernization have been developed, which allowed providing the normative level of functional security of the system as a whole.

The method of evaluating the vulnerability of IS in the integrated information system at the modernization stage has been further developed on the basis of developed analytical models for the components of IS properties, which allowed to determine the integral value of IS vulnerability. The difference between the above models from the existing ones is to take into account the destabilizing factors caused by the stage of modernization and the determination of the probability of the need to ensure compliance with the properties of the information resource of information systems, based on the Gompetz-Makeham distribution function.

For the first time, a set of methods for reconciling access systems in information systems at the stage of modernization has been developed, namely: the method of matching the lattices of the levels of confidentiality of the credential access differentiation systems, the method of reconciling the matrices of access to the systems of discretionary access differentiation, the method of reconciling the systems of role access separation. This set of methods allowed to form a methodological basis for the harmonization of the models for the differentiation of

access information systems at the stage of modernization. In the framework of the methods, basic security theorems are formulated and proved. The developed methodological basis and methods of harmonization of access differentiation systems allow providing functional security of information systems within the systems of access differentiation.

The model and method for assessing the effectiveness of providing functional security of information systems at the stage of modernization have been further developed, which has allowed determining the probability of a system performing functional tasks under conditions of an influence of both external and internal destabilizing factors. The difference between existing the developed method consists in the two-stage formation of the list of information destabilizing influences on determining the degree of their implementation.

For the first time, the information technology for ensuring the functional security of integrated information systems at the stage of modernization was developed, which will allow to carry out a step-by-step improvement of real-time critical information systems.

The practical value of the results.

The use of the developed method for determining the rational sequence of modernization of elements of information systems and the model of information flows has reduced the likelihood of violations of IS properties by the chosen strategy of upgrading up to 8 times from the maximum and up to 3 times the average.

The use of the method of distribution of means of providing functional security of information systems at the stage of modernization, which are components of the channel information destabilizing effect and functional security of the information system, allowed to determine the necessary set of additional funds, provided that the regulatory level of functional security of the system as a whole is observed.

The developed method of evaluating the vulnerability of IS in the integrated information system at the stage of modernization based on analytical models on the components of IS properties allowed to take into account the factors caused by the

process of modernization of the information system and up to 2 times increase the accuracy compared with existing methods.

The developed complex of methods of harmonization of systems of access differentiation in information systems at the stage of modernization provides safe operation of IS on a common field of data with the observance of basic methodological principles. At the same time, within the framework of the methodology, a method for evaluating the effectiveness of the harmonization of access differentiation systems in the presence of unauthorized information flows has been developed. The evaluation of the efficiency of the coordination of access differentiation systems on the example of the interaction of two ISs in the integrated information system "Gart-1" and "Gart-5" has shown the probability of breaking the properties of at least one data element during the upgrade at the level of 0.0003.

The developed software complex, based on the created models, methods and technology, has allowed to 3 times increase the efficiency of the formation of practical recommendations for the adaptation of means of ensuring the functional security of information systems at the stage of modernization.

The developed information technology for ensuring the functional security of the integrated information system at the stage of modernization has allowed providing the normative level of a functional security breach during the modernization of the "Gart-1 / P" IS at the level of 0,005.

Keywords: information system, technology, modernization, efficiency, access delimitation, functional safety.

Публікація основних наукових результатів дисертації

1. Підходи до оцінювання ефективності захисту інформації в інформаційно-телекомунікаційних системах на стадії модернізації / О. К. Юдін, М. А. Стрельбіцький // Наукоємні технології в інфокомунікаціях: обробка інформації, кібербезпека, інформаційна боротьба : Монографія / під заг. ред. В. М. Безрука, В. В. Баранника. – Х. : Вид. "Лидер", 2017. – С. 582–599.

2. Технологія забезпечення функціональної безпеки інтегрованої інформаційної системи Держприкордонслужби на стадії модернізації : Монографія / О. К. Юдін, М. А. Стрельбіцький – К. : ТОВ «СІК ГРУП Україна», 2017. – 312 с.

3. Стрельбіцький М. А. Прикордонний інформаційний ресурс: визначення поняття / М. А. Стрельбіцький // Сучасні інформаційні технології у сфері безпеки та оборони: наук. збірник. – К.: НУОУ, 2016. – № 1(25). – С. 205–208.

4. Barannik V. Method of Ciphergrams Coding for Increasing the Effectiveness of Selective Cyber-Protection Technologies / Barannik V., Barannik D., Hahanova A., Medvedev D., Strelbtskiy M. // Radioelectronics & Informatics. – Kharkiv: 2016. – № 4 (75) – P. 34–40.

5. Юдін О.К. Ієрархічний класифікатор автоматизованих систем прикордонного відомства / О. К. Юдін, М. А. Стрельбіцький // Радіоелектроніка і інформатика. –Харків: 2017. – № 1 (76). – С. 57–60.

6. Юдін О.К. Спосіб визначення кількості інформації з урахуванням фактору її старіння / О. К. Юдін, М. А. Стрельбіцький // Наукоємні технології. – К.: 2017. – № 1 (33). – С. 8–12.

7. Стрельбіцький М. А. Метод узгодження матриць доступу систем дискреційного розмежування доступу інформаційно-телекомунікаційних систем на стадії модернізації / М. А. Стрельбіцький // Сучасні інформаційні технології у сфері безпеки та оборони. – К.: НУОУ, 2017. – № 1 (28). – С. 58–62.

8. Юдін О.К. Технологія забезпечення функціональної безпеки інформаційних систем на стадії модернізації / О. К. Юдін, М. А. Стрельбіцький // Наукоємні технології. – К.: 2017. – № 4 (36). – С. 323–328.

9. Стрельбіцький М. А. Обґрунтування та вибір цільової функції системного захисту інформації в інтегрованій інформаційно-телекомунікаційній системі Державної прикордонної служби України /

М. А. Стрельбіцький // Збірник наукових праць Національної академії Державної прикордонної служби України: зб. наук. праць. – Хмельницький: НАДПСУ, 2011. – № 56. – С. 63–64.

10. Стрельбіцький М. А. Аналіз і систематизація причин виникнення збитків від реалізації загроз в інтегрованій інформаційно-телекомунікаційній системі Державної прикордонної служби України / М. А. Стрельбіцький // Збірник наукових праць Національної академії Державної прикордонної служби України: зб. наук. праць. –Хмельницький: НАДПСУ, 2012. – № 58. – С. 151–153.

11. Стрельбіцький М. А. Декомпозиція технології захисту інформації в корпоративих системах / М. А. Стрельбіцький // Збірник наукових праць Національної академії Державної прикордонної служби України: зб. наук. праць. –Хмельницький: НАДПСУ, 2013. – № 1(59). – С. 296–301.

12. Стрельбіцький М. А. Окремі питання синтезу системного захисту інформації в інтегрованій інформаційно-телекомунікаційній системі прикордонного відомства на стадії модернізації / М. А. Стрельбіцький // Збірник наукових праць Національної академії Державної прикордонної служби України: зб. наук. праць. –Хмельницький: НАДПСУ, 2014. – № 3 (65). – С. 353–361.

13. Стрельбіцький М. А. Класифікація загроз інформації в інтегрованій інформаційно-телекомунікаційній системі прикордонного відомства на етапі модернізації / М. А. Стрельбіцький // Збірник наукових праць Військового інституту Київського національного університету ім. Т. Шевченка: зб. наук. праць. –К.: ВІКНУ, 2015. – № 50. – С. 248–252.

14. Стрельбіцький М. А. Визначення показника уразливості даних в інформаційно-телекомунікаційних системах на стадії модернізації / М. А. Стрельбіцький // Збірник наукових праць Військового інституту Київського національного університету ім. Т. Шевченка. – К. : ВІКНУ. 2016. – № 51. – С. 208 –213.

15. Юдін О.К. Класифікація загроз інформаційному ресурсу ДПСУ на стадії модернізації / О. К. Юдін, М. А. Стрельбіцький // Вісник інженерної академії України. – К. 2016. – вип 4. – С.166–170.

16. Стрельбіцький М. А. Визначення залишкового ризику загроз інформації на стадії модернізації інформаційно-телекомунікаційних систем / М. А. Стрельбіцький // Збірник наукових праць Національної академії Державної прикордонної служби України: зб. наук. праць. –Хмельницький: НАДПСУ, 2016. – № 3 (69). – С.308–321.

17. Стрельбіцький М. А. Аналіз спільного функціонування моделей розмежування доступу на стадії модернізації інформаційно-телекомунікаційних систем на стадії модернізації / М. А. Стрельбіцький // Збірник наукових праць Національної академії Державної прикордонної служби України: зб. наук. праць. –Хмельницький: НАДПСУ, 2016. – № 4 (70). – С. 276–287.

18. Стрельбіцький М. А. Формування множини допустимих значень показника якості системи захисту інформації інформаційно-телекомунікаційних систем на стадії модернізації / М. А. Стрельбіцький // Збірник наукових праць Національної академії Державної прикордонної служби України: зб. наук. праць. –Хмельницький: НАДПСУ, 2017. – Вип. 1 (29). – С. 27–32.

19. Кузавков В.В. Метод узгодження решіток рівнів конфіденційності систем мандатного розмежування доступу інформаційно-телекомунікаційних систем на стадії модернізації / В. В. Кузавков, М. А. Стрельбіцький, В. О. Данько // Збірник наукових праць Військового інституту телекомунікацій та інформатизації: зб. наук. праць. – К.: ВІТІ, 2017. – № 1. – С. 56–60.

20. Стрельбіцький М. А. Аналіз загроз інформаційної безпеки при використанні у Державній прикордонній службі України геоінформаційних систем/ М. А. Стрельбіцький, Р. В. Рачок, Д. А. Мул, Є. В. Прокопенко // Збірник наукових праць Національної академії Державної прикордонної

служби України: зб. наук. праць. –Хмельницький: НАДПСУ, 2017. – № 1 (71). – С 394–403.

21. Стрельбіцький М. А. Обґрунтування показника ефективності функціонування системи захисту інформації на стадії модернізації / М. А. Стрельбіцький // Збірник наукових праць Військового інституту Київського національного університету ім. Т. Шевченка: зб. наук. праць. – К.: 2017. – № 56. – С. 166–177.

22. Стрельбіцький М. А. Метод узгодження систем рольового розмежування доступу інформаційно-телекомунікаційних систем на стадії модернізації / М. А. Стрельбіцький, Д. А. Мул, Є. В. Прокопенко // Збірник наукових праць Національної академії Державної прикордонної служби України: зб. наук. праць. –Хмельницький: НАДПСУ, 2017. – №2 (72). – С 330–339.

23. Стрельбіцький М. А. Методологічний базис узгодження моделей розмежування доступу інформаційно-телекомунікаційних систем на стадії модернізації / М. А. Стрельбіцький // Збірник наукових праць Національної академії Державної прикордонної служби України: зб. наук. праць. – Хмельницький: НАДПСУ, 2017. – № 3 (73). – С 370–379.

24. Стрельбіцький М. А. Перспективні напрямки розвитку системи висвітлення надводної обстановки в Азово-Чорноморському басейні на сучасному етапі / М. А. Стрельбіцький, В. І. Кривий // Збірник наукових праць Військового інституту Київського національного університету ім. Т. Шевченка: зб. наук. праць. – К.: ВІКНУ, 2006. – № 4. – С 130 –133.

25. Шевченко В.Л. Перспективи застосування волоконно-оптичних системи у системі інформаційного забезпечення Державної прикордонної служби України / В. Л. Шевченко, М. А. Стрельбіцький, М. І. Лисий // Збірник наукових праць Національної академії Державної прикордонної служби України: зб. наук. праць. –Хмельницький: НАДПСУ, 2008. – № 42. – С. 70–72.

26. Стрельбіцький М. А. Оцінка ефективності методів отримання та обробки діагностичної інформації / М. А. Стрельбіцький, В. В. Кузавков // Збірник наукових праць Національної академії Державної прикордонної служби України: зб. наук. праць. –Хмельницький: НАДПСУ, 2014. – № 2 (62). – С. 277–289.

27. Юдін О.К. Зміст та ієрархія реєстру інформаційних ресурсів Держприкордонслужби України / О. К. Юдін, М. А. Стрельбіцький // Проблеми інформатизації та управління. – К.: НАУ, 2016. – № 4 (56). – С. 85–91

28. Стрельбіцький М. А. Шляхи захисту інформації в корпоративній мережі Державної прикордонної служби України на стадії модернізації / М. А. Стрельбіцький, Д. А. Купрієнко // Пріоритетні напрямки розвитку телекомунікаційних систем спеціального призначення: Труди III науково-практичної конференції. – К. : ВІНІ НТУУ "КПІ", 2006 – С. 247–249

29. Стрельбіцький М. А. Конструктивні елементи моделі системного захисту інформації в інтегрованій інформаційно-телекомунікаційній системі Державної прикордонної служби України / М. А. Стрельбіцький, Д. А. Мул // Освітньо-наукове забезпечення діяльності правоохоронних органів і військових формувань України: II Всеукраїнська науково-практична конф. 20 листопала 2009 р.: тези доп. – Хмельницький. – 2009. – С. 111.

30. Стрельбіцький М. А. Декомпозиція технології захисту сенсорної інформації в корпоративних системах. / М. А. Стрельбіцький, Т. О. Прищепа // Проблеми телекомунікацій : 7-ма міжнародна науково–технічна конф. 16-19 квітня 2013 р.: тези доп. – К. – 2013. – С 278–280

31. Стрельбіцький М. А. Конструктивні елементи моделі системного захисту інформації в рамках сучасних концепцій / М. А. Стрельбіцький, О. А. Ваврічен // Освітньо-наукове забезпечення діяльності правоохоронних органів і військових формувань України: Матеріали V всеукраїнської науково-практичної конф. 7 грудня 2012 р.: тези доп. – Хмельницький. – 2012. – С. 115–116.

32. Стрельбіцький М. А. Системний захист інформації як складова забезпечення національної безпеки в інформаційній сфері / М. А. Стрельбіцький, В. А. Кириленко // Освітньо-наукове забезпечення діяльності правоохоронних органів і військових формувань України: Матеріали VI всеукраїнської науково-практичної конф. 15 листопада 2013 р.: тези доп. – Хмельницький. – 2013. – С. 240 – 241.

33. Стрельбіцький М. А. Нечіткий пошук інформації у базі даних програмно–технічного комплексу "Гарт–1/П" / М. А. Стрельбіцький, Р. В. Рачок, Д. А. Мул // Освітньо-наукове забезпечення діяльності правоохоронних органів і військових формувань України: Матеріали VII всеукраїнської науково-практичної конф. 21 листопада 2014 р.: тези доп. – Хмельницький. – 2014. – С. 139.

34. Стрельбіцький М. А. Прикордонний інформаційний ресурс: визначення поняття / М. А. Стрельбіцький // Історія, сучасність та перспективи розвитку ДПСУ та охорони державного кордону: Матеріали міжнародної науково-практичної конф. 26 травня 2015 р.: тези доп. – К. – 2015. – С. 297–299.

35. Стрельбіцький М. А. Класифікація загроз інформації в інтегрованій інформаційно-телекомунікаційній системі прикордонного відомства на етапі модернізації / М. А. Стрельбіцький // Військова освіта і наука: сьогодення та майбутнє: Матеріали XI міжнародної науково-практичної конф. 27 листопада 2015 р.: тези доп. – К. – 2015. – С. 78.

36. Стрельбіцький М. А. Окремі питання синтезу системного захисту інформації в інформаційно-телекомунікаційній системі прикордонного відомства на стадії модернізації / М. А. Стрельбіцький // Освітньо–наукове забезпечення діяльності правоохоронних органів і військових формувань України: Матеріали VIII всеукраїнської науково-практичної конф. 10 грудня 2015 р.: тези доп. – Хмельницький. – 2015. – С. 524–525.

37. Стрельбіцький М. А. Аналіз і систематизація причин виникнення збитків від реалізації загроз у відомчих інформаційно-телекомунікаційних

системах / М. А. Стрельбіцький // Перспективи розвитку озброєння та військової техніки сухопутних військ: Матеріали міжнародної науково-технічної конф. 18-20 травня 2016 р.: тези доп. – Львів. –2016. – С. 227.

38. Стрельбіцький М. А. Приховані канали витоку інформації в інформаційно-телекомунікаційних системах Державної прикордонної служби України та шляхи їх ліквідації / М. А. Стрельбіцький, О. А. Ваврічен // Кібербезпека в Україні: правові та організаційні питання: Матеріали всеукраїнської науково-практичної конф. 21 жовтня 2016 р.: тези доп. – Одеса. – 2016. – С. 140–142.

39. Стрельбицкий М. А. Информационный ресурс пограничной службы– составляющая национальной безопасности Украины / М. А. Стрельбицкий // Материалы международной заочной научно-практической конф. Государственного учреждения образования "Институт пограничной службы Республики Беларусь". – Минск. – 2017. – С. 452–454.

40. Стрельбіцький М. А. Методологія узгодження моделей розмежування доступу інформаційно–телекомунікаційних систем на стадії модернізації / М. А. Стрельбіцький // Освітньо–наукове забезпечення діяльності правоохоронних органів і військових формувань України: Матеріали X всеукраїнської науково-практичної конф. 2 листопада 2017 р.: тези доп. – Хмельницький. – 2017. – С. 620–621.

41. Стрельбіцький М. А. Вплив процесів інформатизації прикордонного відомства на складові національної безпеки України / М. А. Стрельбіцький // Наукове забезпечення службово-бойової діяльності Національної гвардії України: VII науково-практична конф. 31 березня 2016 р.: тези доп. – Харків. – 2016. – С. 137–138.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ 24
ВСТУП 26
РОЗДІЛ І. ПРОБЛЕМА ЗАБЕЗПЕЧЕННЯ ФУНКЦІОНАЛЬНОЇ БЕЗПЕКИ ІНТЕГРОВАНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ ДЕРЖАВНОЇ ПРИКОРДОННОЇ СЛУЖБИ УКРАЇНИ НА СТАДІЇ МОДЕРНІЗАЦІЇ 39
1.1. Аналіз потреб у забезпеченні функціональної безпеки на сучасному етапі еволюції відомчої інформаційної системи Державної прикордонної служби України 39
1.1.1. Аналіз особливостей функціонування інтегрованої інформаційної системи Державної прикордонної служби України 40
1.1.2. Аналіз інформаційних дестабілізаційних факторів викликаних стадією модернізації 45
1.1.3. Аналіз і систематизація причин виникнення збитків від реалізації дестабілізаційних чинників процесу модернізації 47
1.2. Аналіз підходів до забезпечення функціональної безпеки в інтегрованих інформаційних системах на стадії модернізації 49
1.3. Вплив процесів інформатизації прикордонного відомства на складові національної безпеки України 52
1.4. Сучасні підходи до проблеми забезпечення функціональної безпеки в інформаційних системах 56
1.5. Аналіз моделей розмежування доступу в інформаційних системах 61
1.6. Обґрунтування напрямку дослідження 68
1.7. Висновки до розділу 1 71
Список використаних джерел у першому розділі 73
РОЗДІЛ 2. КОНЦЕПТУАЛЬНІ ОСНОВИ ТЕХНОЛОГІЇ ЗАБЕЗПЕЧЕННЯ ФУНКЦІОНАЛЬНОЇ БЕЗПЕКИ В ІНТЕГРОВАНІЙ ІНФОРМАЦІЙНІЙ СИСТЕМІ НА СТАДІЇ МОДЕРНІЗАЦІЇ 88

2.1. Основні теоретичні аспекти технології забезпечення функціональної безпеки в інтегрованих інформаційних системах на стадії модернізації 88
2.2. Обґрунтування об’єкта системи функціональної безпеки в інтегрованій інформаційній системі Держприкордонслужби 95
2.3. Декомпозиція структури та інформаційних потоків інтегрованої інформаційної системи прикордонного відомства 101
2.4. Метод визначення раціональної послідовності модернізації елементів інформаційної системи 113
2.4.1. Модель інформаційних потоків інформаційної системи на стадії модернізації 114
2.4.2. Обґрунтування показників ефективності процесу модернізації . 122
2.4.3. Структура методу визначення раціональної послідовності модернізації елементів інформаційної системи 124
2.5. Висновки до розділу 2 132
Список використаних джерел у другому розділі 135
РОЗДІЛ 3. РОЗПОДІЛ ЗАСОБІВ ЗАБЕЗПЕЧЕННЯ ФУНКЦІОНАЛЬНОЇ БЕЗПЕКИ ТА ОЦІНЮВАННЯ УРАЗЛИВОСТІ ІНФОРМАЦІЙНОЇ СИСТЕМИ НА СТАДІЇ МОДЕРНІЗАЦІЇ..... 143
3.1. Метод розподілу засобів забезпечення функціональної безпеки в інформаційних системах на стадії модернізації 143
3.1.1. Аналітична модель методу розподілу засобів забезпечення функціональної безпеки в інформаційних системах на стадії модернізації 145
3.1.2. Структурна схема методу розподілу засобів забезпечення функціональної безпеки в інтегрованих інформаційних системах на стадії модернізації 159
3.2. Метод оцінювання уразливості інформаційної системи на стадії модернізації 162
3.2.1. Введення показників уразливості інформаційної системи 162

3.2.2. Модель оцінювання уразливості інформаційної системи на стадії модернізації 164
3.2.3. Вплив доданих функцій узгодження на оцінку уразливості інформаційної системи..... 172
3.2.4. Структурна схема методу оцінювання уразливості інформаційної системи на стадії модернізації..... 180
3.3. Висновки до розділу 3 182
Список використаних джерел у третьому розділі 184
РОЗДІЛ 4. ТЕОРЕТИЧНІ ОСНОВИ УЗГОДЖЕННЯ МОДЕЛЕЙ РОЗМЕЖУВАННЯ ДОСТУПУ ІНФОРМАЦІЙНИХ СИСТЕМ НА СТАДІЇ МОДЕРНІЗАЦІЇ 190
4.1. Визначення критерію якості системи розмежування доступу інформаційної системи на стадії модернізації..... 192
4.2. Спільне функціонування моделей розмежування доступу на загальному полі даних при модернізації інформаційних систем 196
4.2.1. Спільне функціонування моделей дискреційного розмежування доступу..... 196
4.2.2. Спільне функціонування моделей рольового розмежування доступу..... 197
4.2.3. Спільне функціонування моделей мандатного розмежування доступу..... 198
4.2.4. Спільне функціонування моделей тематичного розмежування доступу..... 198
4.2.5. Спільне функціонування моделей безпеки інформаційних потоків..... 200
4.2.6. Спільне функціонування суб’єктно-орієнтованих моделей ізольованого програмного середовища 201
4.3. Метод узгодження решіток рівнів конфіденційності систем мандатного розмежування доступу інформаційних систем на стадії модернізації 202

4.4. Метод узгодження матриць доступу систем дискреційного розмежування доступу інформаційних систем на стадії модернізації . 207
4.5. Метод узгодження систем рольового розмежування доступу інформаційних систем на стадії модернізації..... 215
4.6. Методологічний базис узгодження моделей розмежування доступу інформаційних систем на стадії модернізації..... 221
4.7. Оцінювання ефективності узгодження систем розмежування доступу..... 226
4.8. Висновки до розділу 4..... 230
Список використаних джерел у четвертому розділі..... 233
РОЗДІЛ 5. ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ ФУНКЦІОНАЛЬНОЇ БЕЗПЕКИ ІНФОРМАЦІЙНИХ СИСТЕМ НА СТАДІЇ МОДЕРНІЗАЦІЇ..... 243
5.1. Підходи до оцінювання ефективності систем функціональної безпеки..... 244
5.2. Семантичні аспекти методу оцінювання ефективності функціональної безпеки..... 255
5.3. Обґрунтування показника ефективності функціонування системи функціональної безпеки..... 263
5.4. Методика формування моделі інформаційних дестабілізаційних факторів на стадії модернізації..... 266
5.5. Формування множини допустимих значень показника якості системи функціональної безпеки..... 273
5.6. Розробка методу оцінювання ефективності функціональної безпеки на стадії модернізації..... 279
5.6.1. Структурний опис методу оцінювання ефективності..... 279
5.6.2. Аналітичний опис методу оцінювання ефективності..... 281
5.7. Висновки до розділу 5..... 293
Список використаних джерел у п’ятому розділі..... 297

РОЗДІЛ 6. ЗАСТОСУВАННЯ ІНФОРМАЦІЙНОЇ ТЕХНОЛОГІЇ ЗАБЕЗПЕЧЕННЯ ФУНКЦІОНАЛЬНОЇ БЕЗПЕКИ В ІНТЕГРОВАНІЙ ІНФОРМАЦІЙНІЙ СИСТЕМІ НА СТАДІЇ МОДЕРНІЗАЦІЇ 303
6.1. Створення інформаційної технології забезпечення функціональної безпеки інтегрованої інформаційної системи на стадії модернізації 303
6.2. Застосування методу визначення раціональної послідовності модернізації елементів інформаційної системи 306
6.3. Застосування методу розподілу засобів забезпечення функціональної безпеки інформаційних систем на стадії модернізації . 311
6.4. Методика експертного оцінювання ступеня впливу дестабілізаційних факторів на інформаційні системи на стадії модернізації 318
6.5. Визначення уразливості інформаційних систем на стадії модернізації 325
6.6. Визначення ефективності узгодження систем розмежування доступу інформаційних систем "Гарт-1" та "Гарт-5" 327
6.7. Застосування методу оцінювання ефективності функціональної безпеки в інформаційних системах на стадії модернізації..... 330
6.8. Висновки до розділу 6 345
Список використаних джерел у шостому розділі 347
ВИСНОВКИ 349
ДОДАТКИ 352

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

АПК – автоматизація прикордонного контролю

АПС – автоматизація прикордонної служби

АРМ – автоматизоване робоче місце

АС – автоматизована система

АСОД – автоматизована система обробки даних

БД – база даних

ВПС – відділ прикордонної служби

ДПСУ – державна прикордонна служба

ДФ – дестабілізаційний фактор

ЗЗФБ – засоби забезпечення функціональної безпеки

ЗОТ – засоби обчислювальної техніки

ІДФ – інформаційний дестабілізаційний фактор

ІІДФ – інтегрований інформаційний дестабілізаційний фактор

ІІС – інтегрована інформаційна система

ІС – інформаційна система

ІнР – інформаційний ресурс

ІКС – інформаційно-комунікаційна система

КІДВ – канал інформаційного дестабілізаційного впливу

НБУ – національна безпека України

НСД – несанкціонований доступ

ОІД – об’єкт інформаційної діяльності

ООДК – орган охорони державного кордону

ОСД – оперативно-службова діяльність

ПЗ – програмні засоби

ПІР – прикордонний інформаційний ресурс

ПС – підсистема

ПТК – програмно-технічний комплекс

РУ – регіональне управління

СФБ – система функціональної безпеки

СПА – система програмного адміністрування

СПЗ – спеціальне програмне забезпечення

СРД – системи розмежування доступу

СУБД – система управління базою даних

ТТХ – тактико-технічні характеристики

ЦСД – центральне сховище даних

ЦСПД – центральний сервер передачі даних

ВСТУП

Актуальність теми. Захист національних інтересів України в умовах глобалізації суспільно-політичних процесів потребує надійного контролю прикордонним відомством за повітряним, надводним, сухопутним просторами, контролю транспортних та міграційних потоків, забезпечення прикордонної безпеки та виконання заходів визначених концепцією інтегрованого управління кордонами.

Значну роль у забезпеченні безпеки в Європі відіграє геополітичне розташування України. Державна прикордонна служба України (ДПСУ) постійно здійснює заходи щодо вдосконалення системи охорони державного кордону, технології пропуску транспортних засобів та осіб через державний кордон, координує дії органів виконавчої влади з питань забезпечення безпеки кордонів держави.

Активізація протиправної та терористичної діяльності на державному кордоні, значна територіальна розосередженість органів і підрозділів Державної прикордонної служби, їх маневреність, комплексне застосування різнорідних сил і засобів, широке залучення до охорони кордону місцевого населення, різка зміна обстановки ставлять високі вимоги до оперативності управління та зумовлюють необхідність удосконалення системи забезпечення безпеки на державному кордоні України.

У цих умовах необхідна розвинена, гнучка та високоефективна система управління, яка повинна збирати різнопланову і значну за обсягом інформацію, швидко її обробляти, готувати рішення і в найкоротші терміни доводити їх до підпорядкованих органів (підрозділів).

Одним із основних завдань з реалізації системи управління є створення загального інформаційного простору суб’єктів забезпечення прикордонної безпеки. Його якісна реалізація потребує від ДПСУ наявності сучасних систем збирання, обробки і аналізу даних про обстановку різного типу, великих обсягів та з великої кількості джерел та їх здатність до ефективного

отримання з них інформації, а також її висвітленням в інформаційних системах з метою прийняття рішень персоналом прикордонного відомства.

Реалізація систем такого класу потребує застосування сучасних підходів до формування її архітектури, врахування можливості інтеграції з іншими інформаційними системами, відкритості до модернізації, забезпечення функціональної безпеки інформаційних систем при великій їх територіальній розосередженості, наявності аналітичних центрів та засобів забезпечення ефективного висвітлення обстановки. Особливо важливим критерієм також є здатність таких систем ефективно функціонувати у гетерогенному інформаційному середовищі.

Інтенсивний розвиток інформаційних технологій спричинив в Україні створення на державному та відомчих рівнях великої кількості взаємно не пов’язаних інформаційних, комунікаційних та інформаційно-комунікаційних систем, спрямованих здебільшого на накопичення даних та різноманітної інформації довідкового, інформаційного, управлінського, статистичного характеру, та використання їх лише за напрямами діяльності суб’єктів національної безпеки. Спроба на державному рівні забезпечити інтегрованість їх функціонування для забезпечення інформаційних потреб правоохоронних органів у сфері загальнодержавного значення на сьогодні не має успіху.

Обмежена кількість досліджень з питань розробки підходів до функціонування відомчих інформаційних систем збору, аналізу та висвітлення обстановки в аспекті ефективного обміну державними інформаційними ресурсами між суб’єктами забезпечення прикордонної безпеки знижує ефективність функціонування органів державної влади з питань забезпечення національної безпеки в цілому.

Значний внесок у розвиток інформаційних технологій створення гарантоздатних автоматизованих систем управління критичного застосування та дослідженню моделей і методів забезпечення функціональної безпеки та надійності інформації внесли відомі вчені В. В. Бараннік, В. М. Богуш, В. А. Герасименко, Ю. І. Грицюк, А. А. Грушо, В. Б. Дудикевич,

І. С. Катеринчук, Б. Я. Корнієнко, О. Г. Корченко, Г. Ф. Конахович, В. В. Ліпаєв, О. В. Потій, В. В. Скляр, В. С. Харченко, В. О. Хорошко, К. Шеннон, О. К. Юдін, Leonard J. LaPadula, D. Elliot Bell, Harrison M., Hoffman J. та інші.

Проведений аналіз підходів до забезпечення функціональної безпеки показав достатньо глибоке опрацювання досліджень окремо за кожною інформаційною системою. Однак залишаються невивченими особливості взаємодії цих систем, зокрема при модернізації окремих інформаційних систем з точки зору забезпечення функціональної безпеки загалом.

Виконання завдань з ефективної охорони державного кордону вимагає створення в Держприкордонслужбі єдиного інформаційного простору – сукупності баз та банків даних, технологій їх ведення та використання, інформаційних систем та комунікаційних мереж, що функціонують на основі єдиних принципів та правил. З цією метою в Адміністрації Державної прикордонної служби України створено центральне сховище даних, в органах та підрозділах кордону розгортаються інформаційні системи та програмно-технічні комплекси різного призначення; забезпечується обмін інформацією між ними та центральним сховищем даних, надано віддалений доступу до нього посадовими особами органів, підрозділів охорони кордону та персоналу прикордонних нарядів, запроваджуються сучасні засоби перевірки (у тому числі і біометричної) осіб, паспортних документів, визначення «ризиків», аналіз міграційних потоків, дієва взаємодія між різнорідними силами та засобами охорони кордону, іншими правоохоронними органами.

Виходячи з цього, розвиток інформаційних систем у Державній прикордонній службі України сьогодні є об’єктивною потребою і здійснюється з урахуванням світової тенденції побудови та інтеграції мереж, засобів та послуг зв’язку. Ця тенденція вимагає запровадження обладнання і технологій, що відповідають сучасним міжнародним стандартам та рекомендаціям. Разом із тим, оперативне реагування на загрози в прикордонній сфері вимагає адаптації інформаційних систем до змін

функціональних завдань прикордонного відомства. Це спричиняє потребу в постійному вдосконаленні складових інтегрованої інформаційної системи ДПСУ, тобто модернізації системи, яка здійснюється поелементно.

Інформаційні системи суб'єктів національної безпеки України мають велику кількість підсистем, які розподілені на всій території держави. Особливістю таких систем є вимога функціонування в реальному масштабі часу та оперування критичною інформацією щодо прийняття рішень, при чому навіть незначний збій, зупинка або порушення властивостей інформаційного ресурсу може призвести до серйозних збитків національного масштабу.

Аналіз такого типу систем показав, з одного боку, сталу тенденцію до зростання множини інформаційних дестабілізуючих факторів, які впливають на функціональну безпеку, що спричинено:

– розширенням умов застосування та функціонування цих систем;

– збільшенням кола користувачів системи;

– зростанням кількості складових інтегрованих інформаційних систем;

– потребою у взаємодії з міжвідомчими та міжнародними інформаційними ресурсами;

– збільшенням обсягів інформації яка циркулює в ІС;

– збільшенням числа дестабілізуючих інформаційних впливів;

– запровадженням нових інформаційних технологій.

З іншого боку, захист життєво важливих інтересів держави вимагає від таких систем:

– забезпечення підвищених вимог до властивостей інформації, яка циркулює у них;

– оперативності доступу до інформаційних ресурсів;

– реалізації розширених можливостей щодо аналізу та узагальнення інформації;

– скорочення часу для прийняття рішень;

– контроль за виконанням розпоряджень.

Відомча інтегрована інформаційна система ДПСУ оперує критичною інформацією щодо прийняття рішень, від надійності якої залежить функціональна безпека системи в цілому. Разом з цим, постійне вдосконалення засобів обчислювальної техніки, спеціального програмного забезпечення передбачає якісні та кількісні їх зміни, що потребує постійної модернізації відомчих систем та призводить до спільного функціонування на загальному полі даних старих, модернізованих та нових версій інформаційних систем, як складових ІІС. Це спричиняє ***протиріччя*** між наявною теоретичною базою забезпечення функціональної безпеки та потребою у постійній модернізації ІС у складі інтегрованої інформаційної системи.

Вищенаведене дозволяє стверджувати про існування науково-прикладної проблеми, суть якої полягає у забезпеченні функціональної безпеки відомчої інтегрованої інформаційної системи на стадії модернізації, що і визначає ***актуальність*** дослідження.

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційна робота виконана згідно із Стратегією розвитку ДПСУ, з планами науково-дослідної роботи Національної академії Державної прикордонної служби України імені Б. Хмельницького. Дисертаційні дослідження проводились в рамках науково-дослідної роботи «Периметр» - 216-0008 І "Методичні рекомендації підрозділам Державної прикордонної служби України щодо порядку визначення зон виявлення сигналу з метою визначення захищеного периметра використання об'єкта інформаційної діяльності". Автором проведено дослідження основних засад забезпечення функціональної безпеки об'єкта інформаційної діяльності, розроблені методи розподілу засобів забезпечення функціональної безпеки та оцінки уразливості інформації на об'єкті інформаційної діяльності".

Дисертаційні дослідження проводились в рамках науково–дослідної роботи 217-0012 І "Системний захист інформації у інтегрованій інформаційно-телекомунікаційній системі "Гарт" на стадії модернізації". Автором проведено дослідження з визначення проблеми, пов'язаних із

забезпеченням безперервного функціонування і сумісності функціональних характеристик систем забезпечення функціональної безпеки в інтегрованій інформаційно-телекомунікаційній системі на стадії модернізації, проведено аналіз моделей, що описують суттєві аспекти структури та технології забезпечення функціональної безпеки в інтегрованій інформаційно-телекомунікаційній системі на стадії модернізації, обґрунтовано вибір критеріїв і способів раціональної адаптації структури та технології функціонування інформаційної систем при спряженні різнорідних засобів обчислювальної техніки, розроблено методологію узгодження систем розмежування доступу в умовах спільного функціонування різних версій спеціального програмного забезпечення інформаційних систем.

Дисертаційні дослідження проводились в рамках науково–дослідної роботи № 217-0015І "Інформаційні технології в діяльності військових формувань та правоохоронних органів України". Автором проведено дослідження з питань застосування інформаційних технологій у Державній прикордонній службі України, а саме аналізу систем обробки інформації, здійснена верифікація розроблених в роботі моделей та їх оцінювання.

Мета і завдання дослідження. Метою роботи є забезпечення функціональної безпеки інтегрованої інформаційної системи Держприкордонслужби на стадії модернізації.

Для досягнення поставленої мети в роботі необхідно вирішити наступні ***завдання***:

1. Провести аналіз потреб забезпечення функціональної безпеки на сучасному етапі еволюції відомчої інтегрованої інформаційної системи ДПСУ та сформувати концептуальні основи технології забезпечення функціональної безпеки в інтегрованих інформаційних системах на стадії модернізації.

2. Розробити модель інформаційних потоків ІС на стадії модернізації та метод формування раціональної послідовності модернізації елементів інформаційної системи.

3. Розробити моделі каналу інформаційного дестабілізуючого впливу і функціональної захищеності інформаційної системи та метод розподілу засобів забезпечення функціональної безпеки інформаційних систем на стадії модернізації.

4. Розробити моделі порушення властивостей ІС та метод оцінювання уразливості інформаційної системи на стадії модернізації.

5. Розробити теоретичні основи та сукупність моделей і методів узгодження різних версій систем розмежування доступу в інформаційних системах на стадії модернізації та сформувати їх методологічний базис.

6. Розробити модель інформаційних дестабілізаційних факторів на стадії модернізації та метод оцінювання ефективності забезпечення функціональної безпеки інформаційних систем на стадії модернізації.

7. Розробити інформаційну технологію забезпечення функціональної безпеки інтегрованої інформаційної системи на стадії модернізації.

8. На основі розроблених технології, моделей та методів розробити програмний комплекс забезпечення функціональної безпеки інтегрованої інформаційної системи на стадії модернізації.

З огляду на визначений напрям **об'єктом дослідження** є процеси забезпечення функціональної безпеки інформаційних систем Держприкордонслужби на стадії модернізації.

Предметом дослідження є моделі, методи та інформаційні технології забезпечення функціональної безпеки інформаційних систем Держприкордонслужби на стадії модернізації.

Науково-прикладна проблема дисертаційного дослідження полягає у розробці інформаційної технології забезпечення функціональної безпеки відомчої інтегрованої інформаційної системи на стадії модернізації.

Методи дослідження. Теоретичні дослідження виконані на базі фундаментальних положень теорії ймовірностей, теорії ефективності, теорії графів, теорії інформації, теорії захисту інформації, а також загальні теоретико-множинні, алгебраїчні методи. Експертне оцінювання здійснювалось відповідно до апробованих методів у цій галузі з

обов’язковим оцінюванням ступеня узгодженості думок експертів. Обробка експериментальних даних виконана із застосуванням методів математичного аналізу, комп’ютерного моделювання, числових методів та елементів математичної статистики.

Наукова новизна одержаних результатів

1. *Уперше* розроблена математична модель інформаційних потоків ІС на стадії модернізації та метод визначення раціональної послідовності модернізації елементів інформаційних систем, що дозволило раціоналізувати процес модернізації елементів інформаційних систем довільної структури за обраною стратегією модернізації.

2. *Уперше* розроблені моделі каналу інформаційного дестабілізаційного впливу і функціональної захищеності інформаційної системи та метод розподілу засобів забезпечення функціональної безпеки інформаційних систем на стадії модернізації, що дозволило забезпечити нормативний рівень функціональної безпеки системи в цілому.

3. *Отримав подальший розвиток* метод оцінювання уразливості ІС в інтегрованій інформаційній системі на стадії модернізації на базі розроблених аналітичних моделей порушення властивостей ІС, що дозволило визначити інтегральну величину уразливості ІС. Відмінність наведених моделей від існуючих полягає у врахуванні дестабілізаційних факторів, викликаних стадією модернізації та визначенні ймовірності потреби у забезпеченні дотримання властивостей інформаційного ресурсу інформаційних систем, яка ґрунтується на функції розподілу Гомперца-Мейкгама.

4. *Уперше* розроблено комплекс методів узгодження систем розмежування доступу в інформаційних системах на стадії модернізації, а саме: метод узгодження решіток рівнів конфіденційності систем мандатного розмежування доступу, метод узгодження матриць доступу систем дискреційного розмежування доступу, метод узгодження систем рольового розмежування доступу. Зазначена сукупність методів дозволила сформувати методологічний базис узгодження моделей розмежування доступу

інформаційних систем на стадії модернізації. У рамках методів сформульовані та доказані базові теореми безпеки. Розроблені методологічний базис та методи узгодження систем розмежування доступу дозволяють забезпечити функціональну безпеку інформаційних систем в рамках систем розмежування доступу.

5. *Отримали подальший розвиток* модель інформаційних дестабілізаційних факторів на стадії модернізації та метод оцінювання ефективності забезпечення функціональної безпеки інформаційних систем на стадії модернізації, що дозволило визначити ймовірність виконання системою функціональних задач в умовах впливу як зовнішніх, так і внутрішніх дестабілізаційних факторів. Відмінність розробленого методу полягає у двоетапному формуванні переліку інформаційних дестабілізаційних впливів із визначення ступеня їх реалізації.

6. *Уперше* розроблено інформаційну технологію забезпечення функціональної безпеки інтегрованої інформаційної системи на стадії модернізації, що дозволить здійснювати поетапне вдосконалення інформаційних систем реального часу критичного застосування.

Практичне значення одержаних результатів

1. Використання розробленої моделі інформаційних потоків ІС на стадії модернізації та методу визначення раціональної послідовності модернізації елементів інформаційних систем дозволило зменшити ймовірність порушення властивостей ІС за обраною стратегією модернізації до восьми разів від максимального та до трьох разів від середнього значення.

2. Використання методу розподілу засобів забезпечення функціональної безпеки інформаційних систем на стадії модернізації, складовими якого є моделі каналу інформаційного дестабілізаційного впливу та функціональної захищеності інформаційної системи дозволило визначити необхідну сукупність додаткових засобів за умови дотримання нормативного рівня функціональної безпеки системи в цілому.

3. Розроблений метод оцінювання уразливості ІС в інтегрованій інформаційній системі на стадії модернізації на базі аналітичних моделей

порушення властивостей ІС дозволив врахувати фактори, які викликані процесом модернізації інформаційної системи та до двох разів підвищити точність порівняно з існуючими методами.

4. Розроблений комплекс методів узгодження систем розмежування доступу в інформаційних системах на стадії модернізації забезпечує безпечне функціонування ІС на спільному полі даних при дотриманні базових методологічних засад. Разом із тим, у рамках методології розроблена методика оцінювання ефективності узгодження систем розмежування доступу при наявності недозволених інформаційних потоків. Проведене оцінювання ефективності узгодження систем розмежування доступу на прикладі взаємодії двох ІС у складі інтегрованої інформаційної системи "Гарт-1" та "Гарт-5" показало ймовірність порушення властивостей хоча б одного елементу даних під час модернізації на рівні до 0,0003.

5. Розроблений програмний комплекс, що базується на створених моделях, методах та технології, дозволив до трьох разів підвищити оперативність формування практичних рекомендацій із адаптації засобів забезпечення функціональної безпеки інформаційних систем на стадії модернізації.

6. Використання розробленої інформаційної технології забезпечення функціональної безпеки інтегрованої інформаційної системи на стадії модернізації дозволило забезпечити дотримання нормативного рівня порушення функціональної безпеки під час модернізації ІС "Гарт-1/П" не вище 0,005.

Основні результати дисертаційного дослідження впроваджено в діяльність: Головного центру зв’язку, автоматизації та захисту інформації ДПСУ (акт реалізації від 26.12.2017 р.); Східного регіонального управління ДПСУ (акт реалізації від 26.12.2017 р.); Національної академії Державної прикордонної служби імені Богдана Хмельницького (акт реалізації від 12.12.2017 р.); акціонерного товариства «Банкомзв’язок» (акт реалізації від 03.01.2018 р.).

Особистий внесок здобувача. Основні наукові й теоретичні положення та практичні результати дисертаційної роботи, які виносяться на захист, одержані здобувачем особисто. Без співавторів опубліковано наукові праці – [3, 7, 9–14, 16–18, 21, 23, 34–37, 39–41]. З наукових праць, опублікованих у співавторстві, використовуються результати, отримані особисто здобувачем, а саме: проведено оцінювання ефективності захисту інформації в інформаційно-телекомунікаційних системах на стадії модернізації – [1]; розроблені складові технології забезпечення функціональної безпеки інформаційних систем на стадії модернізації та сформована її структура – [2]; проведено аналіз підсистем відеоспостереження прикордонного відомства та враховані особливості їх функціонування – [4]; наведено ієрархічний класифікатор автоматизованих систем прикордонного відомства та сформульована і доказана теорема безпеки для взаємодіючих систем – [5]; розроблено спосіб визначення кількості інформації з урахуванням фактору її старіння – [6]; розроблено технологію забезпечення функціональної безпеки інформаційних систем на стадії модернізації – [8]; встановлена класифікація загроз інформаційному ресурсу ДПСУ на стадії модернізації – [15]; розроблений метод узгодження решіток рівнів конфіденційності систем мандатного розмежування доступу інформаційно-телекомунікаційних систем на стадії модернізації – [19]; здійснено аналіз загроз інформаційній безпеці прикордонного відомства – [20]; розроблений метод узгодження систем рольового розмежування доступу інформаційно-телекомунікаційних систем на стадії модернізації – [22]; проведено дослідження інформаційних потоків у системі висвітлення надводної обстановки – [24]; визначені перспективи впровадження нових інформаційних джерел у структуру інформаційних систем прикордонної служби – [25]; проведено аналіз сучасних методів оцінювання ефективності – [26]; визначено структуру та взаємозв’язок складових інтегрованої інформаційно-телекомунікаційної системи прикордонного відомства – [27]; визначені шляхи захисту інформації в інтегрованій інформаційній системі прикордонного відомства – [28]; сформовані конструктивні елементи моделі

системного захисту інформації в інтегрованій інформаційно-телекомунікаційній системі Державної прикордонної служби України – [29]; проведена декомпозиція технології захисту інформації в корпоративних системах – [30], сформовані елементи моделі системного захисту інформації – [31]; проведений аналіз впливу процесів інформатизації прикордонного відомства на складові національної безпеки – [32]; сформовані загрози функціональній безпеці під час проведення нечіткого пошуку інформації – [33]; проведений аналіз прихованих каналів витоку інформації в інформаційно-телекомунікаційних системах на стадії модернізації – [38].

Апробація результатів дисертації. Основні теоретичні положення та результати дослідження доповідались та обговорювались на: III Науково-практичній конференції "Пріоритетні напрямки розвитку телекомунікаційних систем спеціального призначення" (м. Київ, 2007), II Всеукраїнській науково-практичній конференції "Освітньо-наукове забезпечення діяльності правоохоронних органів і військових формувань України" (м. Хмельницький 2009), VII Міжнародній науково-технічній конференції "Проблеми телекомунікацій" (м. Київ, 2013), V Всеукраїнській науково-практичній конференції «Освітньо-наукове забезпечення діяльності правоохоронних органів і військових формувань України» (м. Хмельницький, 2012), VI Всеукраїнській науково-практичній конференції «Освітньо-наукове забезпечення діяльності правоохоронних органів і військових формувань України» (м. Хмельницький, 2013), VII Всеукраїнській науково-практичній конференції «Освітньо-наукове забезпечення діяльності правоохоронних органів і військових формувань України» (м. Хмельницький, 2014), Міжнародній науково-практичній конференції "Історія, сучасність та перспективи розвитку ДПСУ та охорони державного кордону" (м. Київ, 2015), XI Міжнародній науково-практичній конференції "Військова освіта і наука: сьогодення та майбутнє" (м. Київ, 2015), VIII Всеукраїнській науково-практичній конференції «Освітньо-наукове забезпечення діяльності правоохоронних органів і військових формувань України» (м. Хмельницький, 2015), VII Науково-практичній конференції “Наукове

забезпечення службово-бойової діяльності Національної гвардії України” (м. Харків, 2015), Міжнародній науково-технічній конференції "Перспективи розвитку озброєння та військової техніки сухопутних військ" (м. Львів, 2016), Всеукраїнській науково-практичній конференції "Кібербезпека в Україні: правові та організаційні питання" (м. Одеса, 2016), Международной заочной научно-практической конференции Государственного учреждения образования "Институт пограничной службы Республики Беларусь" (г. Минск, 2017), X Всеукраїнській науково-практичній конференції «Освітньо-наукове забезпечення діяльності правоохоронних органів і військових формувань України" (м. Хмельницький, 2017).

Публікації. За темою дисертації опубліковано 41 наукову працю, у тому числі: 2 монографії, 24 статті у фахових виданнях переліку МОН України (з них 13 одноосібних); 14 матеріалів і тез доповідей на науково-практичних конференціях, 6 статей опубліковано у виданнях, що входять до міжнародних наукометричних баз.

Структура і обсяг дисертації. Дисертація складається із вступу, шести розділів, висновків та додатків. Повний обсяг дисертації складає 453 сторінки. Обсяг анотації складає 17 сторінок. Дисертація містить 71 ілюстрацію (із них тих, що займають повну сторінку – 8), 41 таблицю (із них тих, що займають повну сторінку – 4). Список використаних джерел із 347 найменувань займає 44 сторінки. Додатки містять 102 сторінки. Обсяг основної частини дисертації становить 283 сторінки.

РОЗДІЛ 1
ПРОБЛЕМА ЗАБЕЗПЕЧЕННЯ ФУНКЦІОНАЛЬНОЇ БЕЗПЕКИ ІНТЕГРОВАНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ ДЕРЖАВНОЇ ПРИКОРДОННОЇ СЛУЖБИ УКРАЇНИ НА СТАДІЇ МОДЕРНІЗАЦІЇ

1.1 Аналіз потреб у забезпеченні функціональної безпеки на сучасному етапі еволюції відомчої інформаційної системи Державної прикордонної служби України

Неминучий процес глобалізації вимагає пошуку шляхів забезпечення національної безпеки в інформаційній сфері. Як відомо, інформація стала однією з головних стратегічних національних ресурсів держави – основою її економічної та оборонної могутності [1–4]. Від інформації у сучасному світі залежить ефективність життєдіяльності суспільства.

Державна прикордонна служба України як суб’єкт забезпечення національної безпеки [5–8] у своїй діяльності використовує інформаційний ресурс, який є складовою інформаційного ресурсу держави. Персонал прикордонного відомства оперує цим ресурсом для прийняття критичних рішень, які безпосередньо впливають на стан національної безпеки держави. При такому розумінні інформаційного ресурсу виникає потреба у дотриманні складових його функціональних критеріїв: цілісності, доступності, конфіденційності та спостереженості для забезпечення функціональної безпеки інтегрованої інформаційної системи прикордонного відомства.

У свою чергу, оперативне реагування ДПСУ на загрози національній безпеці передбачає якісні та кількісні зміни інформаційних систем. Процес інтеграції нових та старих програмно-апаратних засобів створює необхідність адаптації відпрацьованих функціональних задач, алгоритмів їх вирішення та механізмів забезпечення функціональної безпеки в нове програмно-апаратне середовище. У результаті утворюється загальне поле даних, яке використовується як старими, так і новими компонентами інформаційних систем. На цій стадії життєвого циклу інформаційних систем

виникає потреба у забезпеченні переходу на нову програмно-апаратну платформу без порушення життєвого циклу, при одночасному забезпеченні функціональної безпеки інтегрованої інформаційної системи в цілому.

Функціонування інформаційних систем ДПСУ як суб'єкта забезпечення національної безпеки України (НБУ) безпосередньо пов'язано із запобіганням основних загроз національним інтересам і національній безпеці України в інформаційній сфері [5–8]. Доцільно зазначити, що Концепцією інтегрованого управління кордонами [9] передбачена взаємодія суб'єктів інтегрованого управління кордонами у єдиному інформаційному просторі, що визначає структуру та характер інформаційних потоків між ними [10], суть яких полягає у забезпеченні основних принципів інформаційних відносин: достовірність і повнота інформації; правомірність одержання, використання, поширення, зберігання та захисту інформації, тощо [11].

Вищенаведене обумовлює складність створення системи забезпечення функціональної безпеки відомчої інтегрованої інформаційної системи, зокрема на стадії модернізації.

1.1.1 Аналіз особливостей функціонування інтегрованої інформаційної системи Державної прикордонної служби України. Функціонування єдиного інформаційного простору суб'єктів інтегрованого управління кордонами [12] забезпечується прикордонним відомством шляхом упровадження та експлуатації інформаційних систем різного призначення. Державна прикордонна служба як правоохоронний орган спеціального призначення виконує своє завдання щодо забезпечення недоторканності державного кордону та охорони суверенних прав України в її виключній (морській) економічній зоні через органи охорони державного кордону та прикордонні підрозділи, які безпосередньо виконують це завдання [13]. Значна віддаленість органів і підрозділів ДПСУ, їх маневреність, комплексне застосування різнорідних сил і засобів, глибока

побудова охорони державного кордону, широке залучення до неї місцевого населення, різка зміна обстановки ставлять високі вимоги до оперативності управління. З метою забезпечення ефективного управління виникає потреба у розвиненій, гнучкій та високоефективній інформаційній системі [14], яка повинна збирати різнопланову і значну за обсягом інформацію, швидко її обробляти, формувати рішення і в найкоротші строки доводити їх до підпорядкованих органів (підрозділів).

Вказане стало підґрунтям для створення в Адміністрації ДПСУ центрального сховища даних, розгортання в органах та підрозділах кордону інформаційних систем та комплексів різного призначення, забезпечення обміну інформацією між ними та центральним сховищем даних, забезпечення віддаленого доступу до нього посадових осіб органів, підрозділів охорони кордону та персоналу прикордонних нарядів, запровадження сучасних засобів перевірки осіб, їх документів, аналіз міграційних потоків, дієвої взаємодії між різнорідними силами та засобами охорони кордону, іншими правоохоронними органами та забезпечення функціонування єдиного інформаційного простору [15].

Виходячи з цього, розвиток комунікаційних мереж та інформаційних систем у ДПСУ сьогодні є об’єктивною потребою і здійснюється з урахуванням загальних тенденцій побудови та інтеграції мереж, засобів та послуг зв’язку [16]. Це вимагає запровадження обладнання і технологій, що відповідають сучасним міжнародним стандартам та рекомендаціям (наприклад ISO/IEC).

Органи та підрозділи Державної прикордонної служби України дислокуються у районах, де комунікаційні мережі загального користування далеко не в повному обсязі забезпечують потребу в послугах зв’язку, що відповідали б сучасним стандартам, чим і зумовлено необхідність створення в цих районах власних комунікаційних мереж на основі сучасних технологій і протоколів та їх узгодження з комунікаційними мережами загального використання [17].

Використання інформаційного ресурсу ДПСУ передбачало створення інтегрованої інформаційної системи "Гарт", завдання якої полягало [17]:

– у підвищенні повноти та достовірності інформації, що використовується у процесі діяльності персоналу ДПСУ;

– оперативності доступу до інформації суб’єктів інтегрованого управління кордонами та обробки даних;

– розширенні можливості аналізу та узагальненні інформації, яка використовується в процесі керування органами ДПСУ;

– скороченні часу для прийняття рішень з керування органами ДПСУ;

– підвищенні якості рішень, що приймаються;

– забезпеченні оперативності та своєчасності контролю за виконанням директивних розпоряджень.

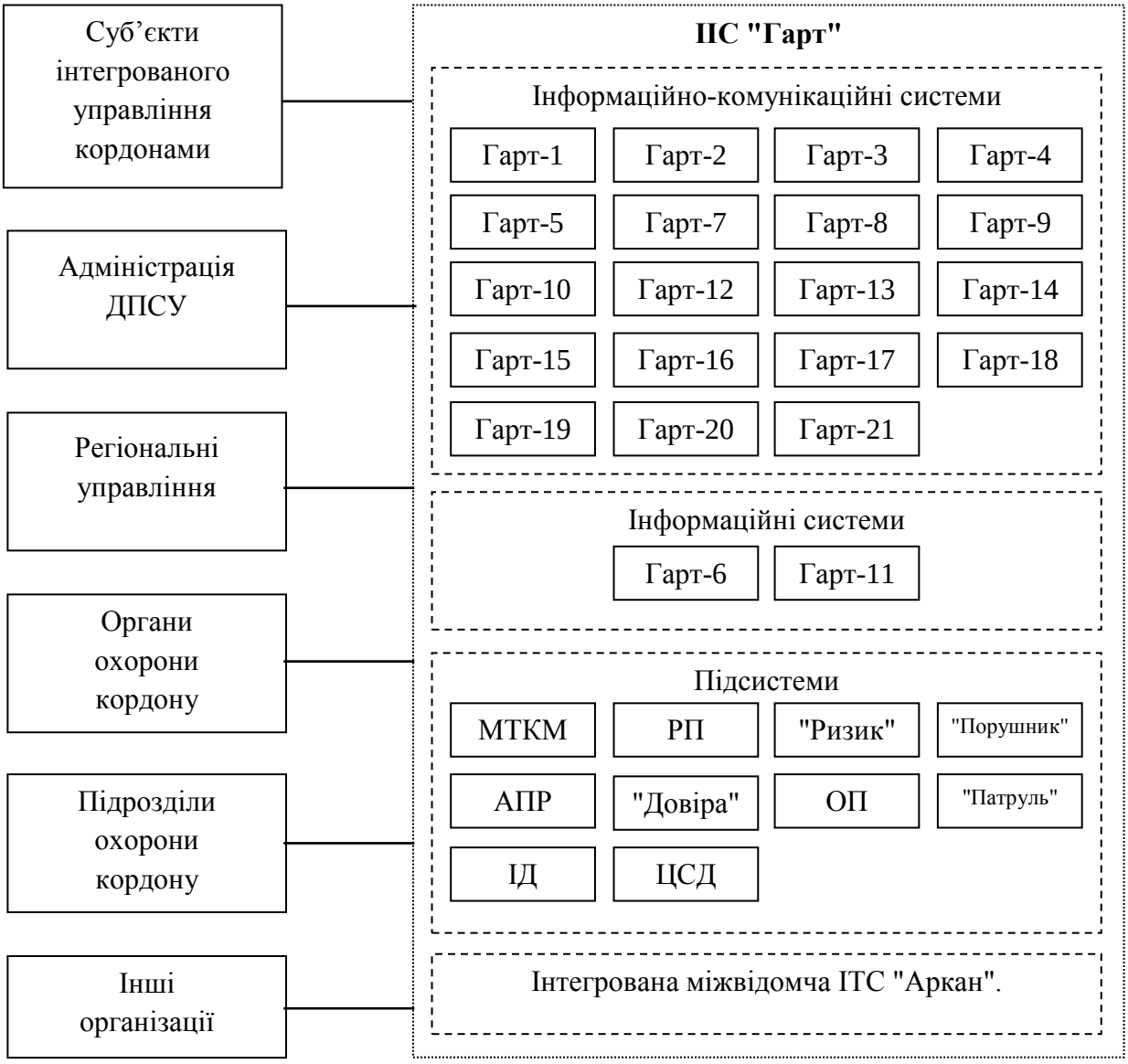
Інтегрована інформаційна система ДПСУ "Гарт" призначена для створення єдиного інформаційного простору суб’єктів інтегрованого управління кордонами та електронної системи управління ДПСУ, виконання завдань з підвищення ефективності керування органами ДПСУ під час охорони державного кордону (ДК) за рахунок:

– забезпечення високого ступеня оперативності, повноти і достовірності обліку, обробки і передачі інформації про обстановку на ДК та стану оперативно-службової діяльності (ОСД) ДПС;

– підвищення оперативності та якості аналізу, оцінки і прогнозу розвитку обстановки на кордоні та в органах ДПСУ;

– забезпечення своєчасною, цілісною і достовірною інформацією відповідних департаментів Адміністрації Держприкордонслужби для формування рішень з управління органами ДПСУ.

Структурно ІІС складається з (рисунок 1.1): інформаційно-комунікаційних систем; інформаційних систем (ІС); підсистем (ПС); інтегрованої міжвідомчої ІТС "Аркан" [18, 19].



де: "Гарт-1" – ІС прикордонного контролю; "Гарт-2" – ІС оперативно-чергової служби; "Гарт –3" – ІС прикордонної служби; "Гарт-4" – ІС тилового забезпечення; "Гарт-5" – ІС інформаційно-аналітичної служби; "Гарт-6" – ІС фінансового забезпечення; "Гарт-7" – ІС кадрового забезпечення; "Гарт-8" – ІС професійної підготовки; "Гарт-9" – ІС медичного забезпечення; "Гарт-10" – ІС оперативно-розшукової діяльності; "Гарт-11" – ІС виховної роботи; "Гарт-12" – ІС морської охорони; "Гарт-13" – ІС правового забезпечення; "Гарт-14" – ІС контролю та висвітлення обстановки; "Гарт-15" – ІС радіаційного, хімічного, біологічного захисту та екологічної безпеки; "Гарт-16" – ІС авіаційної служби; "Гарт-17" – ІС геоінформаційної системи; "Гарт-18" – ІС документального забезпечення; "Гарт-19" – ІС електронної пошти; "Гарт-20" – ІС факсимільних повідомлень; "Гарт-21" – ІС підрозділів внутрішньої безпеки; МТКМ – моніторинг комунікаційної мережі; РП – реєстрація подій; АПР – аналіз та профілювання ризиків; ОП – оперативні повідомлення; ІД – інтерактивна довідка; ЦСД – центральне сховище даних.

Рисунок 1.1 – Структура ІІС "Гарт" ДПСУ

Інтегрована інформаційна система ДПСУ "Гарт" за своєю архітектурою є структурно-ієрархічною системою [20–22] і складається з множини взаємодіючих і зв’язаних по горизонталі та ієрархічно викладених по вертикалі функціональних складових. Структура ІІС ДПСУ "Гарт" відображає існуючу організаційну структуру ДПСУ і включає чотири взаємозв’язані рівні автоматизації:

– Адміністрація Держприкордонслужби (рівень – "АДПС");

– регіональне управління Державної прикордонної служби України (рівень – "РУ");

– органи Державної прикордонної служби України (рівень – "ООДК");

– підрозділи органів Державної прикордонної служби України (рівень – "підрозділ ООДК") та інтеграцію суб’єктів інтегрованого управління кордонами (інших організацій) у єдиний інформаційний простір.

Інтегрована інформаційна система ДПСУ "Гарт" формується шляхом об’єднання інформаційних ресурсів інформаційних підсистем органів ДПСУ [23, 24], які забезпечують надання інформації згідно з Переліком інформаційних ресурсів ІІС ДПСУ "Гарт".

Особливістю ІІС є [24]: створення потужного обчислювального центру колективного користування – центрального сховища даних (ЦСД); наявність та сумісне функціонування багатьох складових (ІС, ПС), об’єднання їх мережею передачі даних; масове поширення автоматизованих робочих місць (АРМ) у всі рівні управління; об’єднання АРМ у локальні інформаційно-обчислювальні мережі; поєднання відомчої інтранет мережі із суб’єктами інтегрованого управління кордонами. Усе це передбачає використання ІІС не тільки фахівцями для вирішення окремих трудомістких завдань, а всім персоналом ДПСУ та співробітниками інших організації, які реалізують свої повноваження з питань інтегрованого управління кордонами у своїй повсякденній діяльності.

1.1.2 Аналіз інформаційних дестабілізаційних факторів викликаних стадією модернізації. Економічна ситуація в країні, упровадження в експлуатацію нових програмно-апаратних платформ, тривалий і трудомісткий процес вдосконалення функціональних завдань ІІС обумовлює те, що у сформованих умовах від старого парку засобів обчислювальної техніки (ЗОТ) та існуючого спеціального програмного забезпечення відмовлятися недоцільно [25, 26].

Як свідчить досвід експлуатації ІС АПК "Гарт-1", перехід на нову програмно-апаратну платформу здійснюється поетапно. На теперішньому етапі має місце ситуація, коли у прикордонних підрозділах функціонують АРМ на базі старого парку обчислювальної техніки та сучасні (модернізовані) АРМи. Така ситуація є логічною та прогнозованою. Це пов’язано з тим, що старий парк АРМ зарекомендував себе надійно з точки зору експлуатаційних характеристик, питань функціональної безпеки та живучості ІС і дотримання властивостей інформаційного ресурсу [27]. Разом з тим, упровадження новітніх засобів автоматизації в процес прикордонного контролю пов’язане з викликами сучасності, наприклад із застосуванням паспортних документів нової формації – паспортів з біометричними даними.

На цій стадії життєвого циклу ІІС інтеграція різнорідних компонентів в гетерогенну систему призводить до утворення спільного поля даних, що використовуються у функціональних завданнях як старих, так і нових компонентів ІІС. Як наслідок, в такій ситуації виникають інтегровані інформаційні дестабілізаційні фактори (ІІДФ), які сприяють порушенню властивостей ІС (рисунок 1.2).

Під інформаційним дестабілізаційним фактором (ІДФ) розуміється подія або дія, яка може викликати порушення функціонування ІІС, включаючи спотворення, знищення або несанкціоноване використання (розмноження) оброблюваного і збереженого в ній інформаційного ресурсу (ІнР). Згідно із запропонованою класифікацією умовно можливі ІДФ можна

поділити на три групи відповідно до трьох видів джерел (аналогічно в роботах [28–34]).

Інформаційні дестабілізаційні фактори першої групи, пов’язані з надійністю програмно-технічних засобів ІІС. Вони пов’язані з раптовим тимчасовим припиненням або порушенням роботи ІС і призводять до втрат інформації та управління об’єктами в ІС управління.

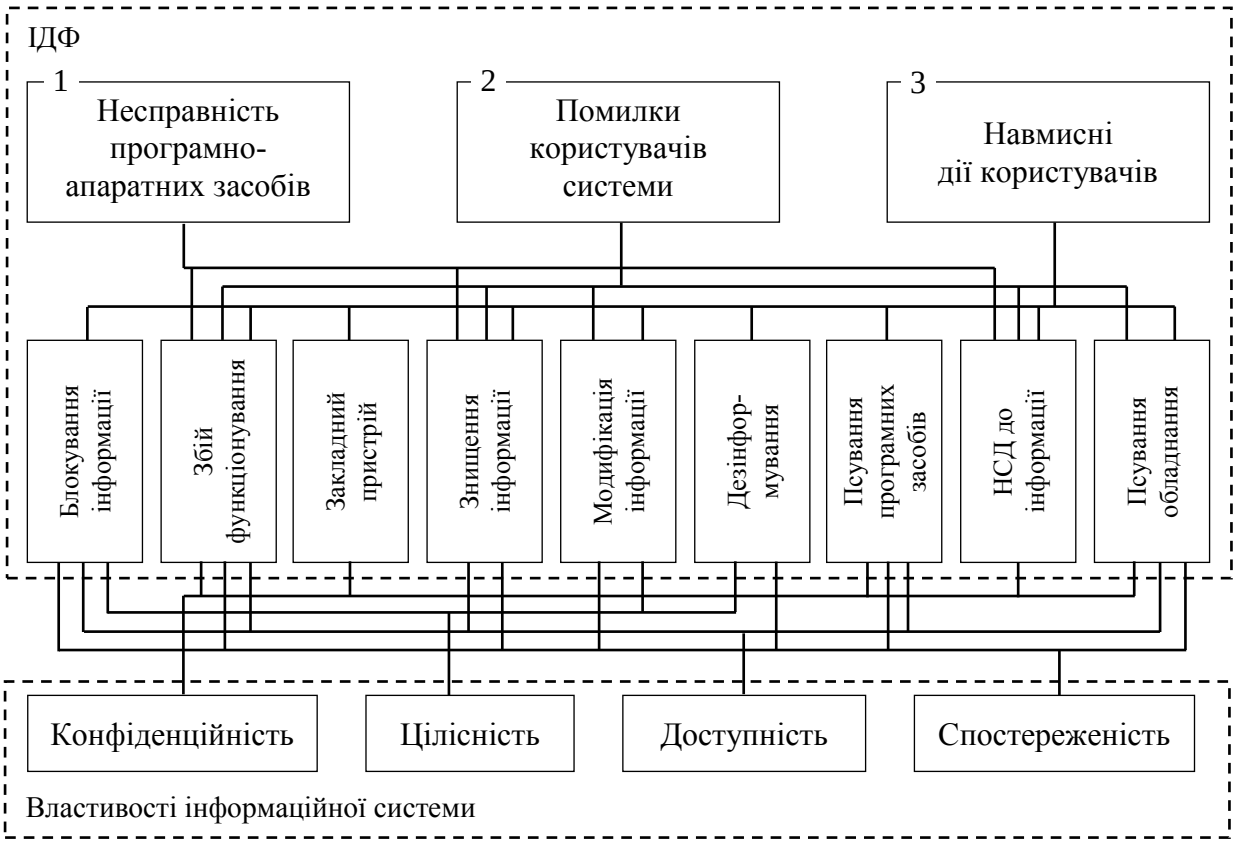


Рисунок 1.2 – Вплив інформаційних дестабілізаційних факторів на властивості інформаційної системи

Інформаційно-дестабілізаційні фактори другої групи пов’язані з випадковими ненавмисними діями користувачів, помилками адміністраторів, управлінського персоналу та інших і ведуть до модифікації (спотворення) чи знищення інформації, порушення виконання ІІС своїх функцій, помилок в роботі програм і засобах управління безпекою ІС.

Інформаційні дестабілізаційні фактори третьої групи пов’язані з навмисними діями людей для отримання особистих привілеїв і доходів, які спрямовані на нанесення шкоди ІС, на спричинення шкоди іншим особам, організаціям або державі.

Аналіз наведеного переліку загроз інформаційному ресурсу в ІІС властивих стадії модернізації показав, що в цей період мають місце певні особливості, які дозволяють безконтрольно маніпулювати інформацією як персоналу ІІС, так і стороннім особам, а також приховано отримувати доступ до інформації, яка зберігається на значній відстані від АРМ [35].

1.1.3 Аналіз і систематизація причин виникнення збитків від реалізації дестабілізаційних чинників процесу модернізації. У рамках запропонованої в [36] інтерпретації надійності інформації в ІІС систему забезпечення функціональної безпеки можна розглядати як "посередника", який забезпечує якість інформаційного ресурсу з точки зору дотримання його властивостей. Аналіз робіт [37–39] з визначення найбільш небезпечних дій у відношені до інформаційного ресурсу дозволив встановити причинно-наслідкові зв’язки, які описують процес нанесення шкоди суб’єктами ІІС.

На основі накопиченого досвіду прояву різних ІДФ можна побудувати структурну схему механізму їх виникнення і проявів [31, 40, 41] (загальний вміст проілюстровано на рисунку 1.3.)

Пропонована класифікація характеризує, як певний фактор впливає на конкретні властивості інформаційної системи. У рамках цієї класифікації можуть характеризуватися апаратні засоби, програмні засоби, фізичні носії інформації і безпосередньо люди-носії інформації [42, 43].

Вплив ІДФ на апаратні засоби ІІС призводить до погіршення якості її функціонування, яке може проявлятися як погіршення їх тактико-технічних характеристик [31, 44].

Враховуючи, що апаратні засоби є матеріальною основою процесу обробки інформації в ІІС, погіршення їх тактико-технічних характеристик (ТТХ) автоматично веде до зниження ефективності процесу обробки

інформації та, далі, через зниження ефективності часткових завдань, що розв'язуються ІІС – до зниження ефективності функціонування системи в цілому, зокрема живучості системи управління критичного застосування.

У свою чергу, це призводить до втрат (витрат) ресурсів (людських, моральних, матеріальних) суб'єктів інтегрованого управління кордонами.

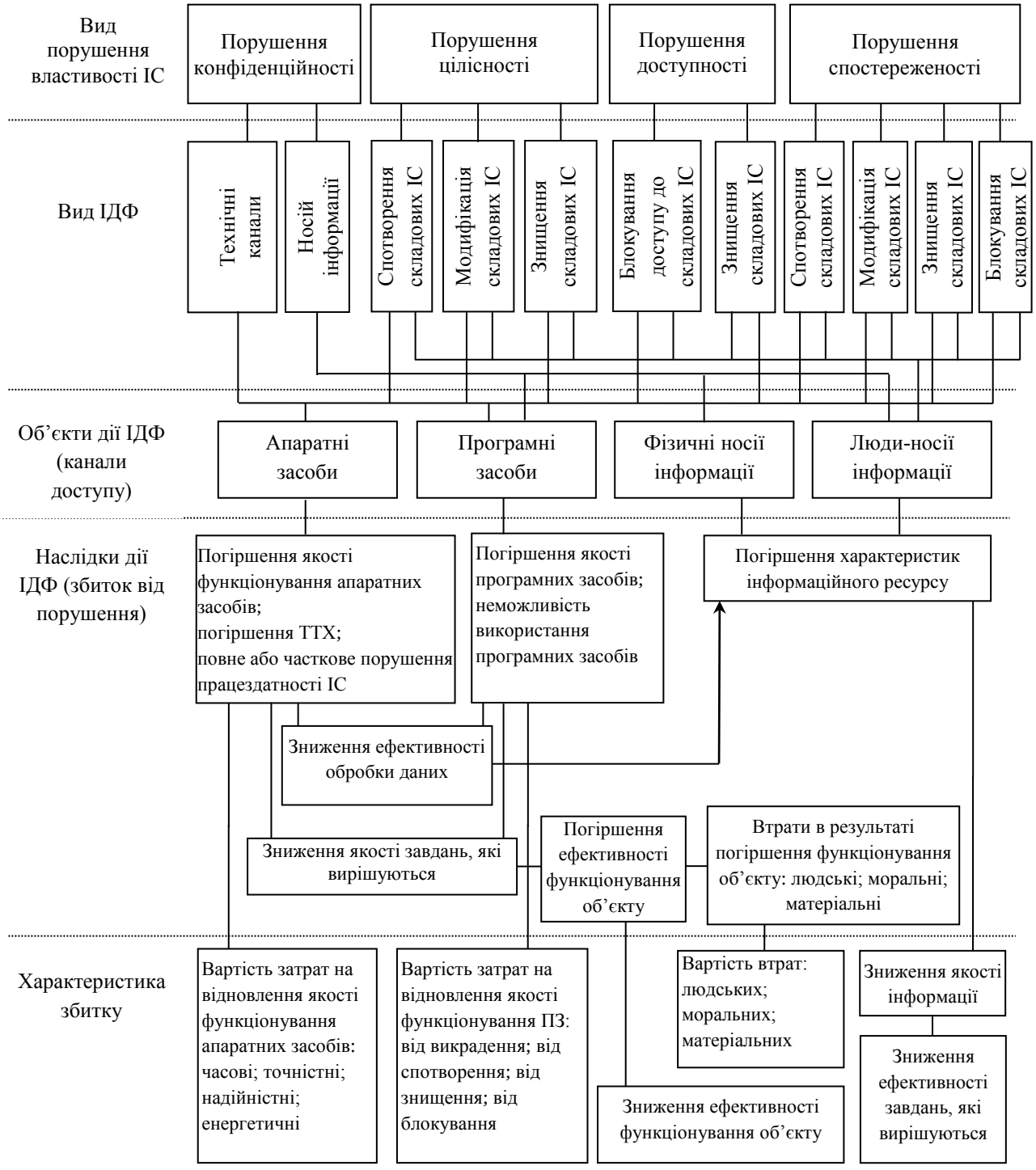


Рисунок 1.3 – Структурна схема механізму виникнення і проявів ІДФ

Вид і масштаб цих втрат (витрат) визначається такими факторами [38, 45]:

– змістом інформації, що обробляється в ІІС;

– сферою застосування (використання) результатів обробки інформації (вихідної інформації);

– ступенем і видом порушення функціональної безпеки;

– видом джерела ІДФ і метою його діяльності.

Аналогічні наслідки виникають при впливі ІДФ на програмні засоби, які використовуються в процесі обробки інформації, а також при впливі на фізичне поле – носії інформації та (або) на людей – носіїв інформації, які беруть участь у процесі обробки інформації (персонал, користувачі ІС, джерела інформації тощо).

При модернізації спеціалізованих організаційних систем, пов’язаної з інтеграцією різнорідних програмно-апаратних засобів, актуальним є завдання формування комплексу заходів щодо усунення протиріч між вигодами від впровадження передових технологій обробки інформації і можливого збитку від порушення властивостей інформаційних систем, викликаних систематизованими вище причинами. Відсутність в даний час адекватних підходів раціонального сполучення різнорідних програмно-апаратних компонентів стримує вирішення цих питань [46–48].

1.2 Аналіз підходів до забезпечення функціональної безпеки в інтегрованих інформаційних системах на стадії модернізації

Аналіз сучасних досягнень в галузі інформаційних технологій показав, що головним стратегічним національним ресурсом стає інформація [49] та інформаційні технології, ключовою з яких є технологія забезпечення функціональної безпеки інформаційних систем. Згідно з [50] під функціональною безпекою мається на увазі коректне функціонування як системи управління, так і керованого нею обладнання. Отже, забезпечення

властивостей інформаційного ресурсу як керуючого носія інформаційної системи є актуальною проблемою.

Однією із складових властивостей є конфіденційність інформації, теоретичну базу якої забезпечує така галузь знань, як теорія захисту інформації, яка визначає загальні принципи та методи побудови захищених інформаційних систем [51–55], основним методологічним інструментом якої є методи системного аналізу та теорії прийняття рішення. Використання цих підходів до вирішення завдань із захисту інформації дозволяє вирішувати два класи завдань: завдання аналізу існуючих систем захисту інформації та завдання синтезу системи захисту інформації за визначеними критеріями [56].

Відомо, що на систему захисту інформації (СЗІ) впливає випадковий потік дестабілізаційних факторів [57], який передбачає використання методів теорії ймовірностей. Вирішення обох класів завдань в теорії захисту інформації здійснюється в умовах, як правило, значної невизначеності та здійснюється двома шляхами: формальним описом СЗІ та неформальним (описовим).

Формальний підхід передбачає опис встановлених правил та обмежень (політика безпеки) та на їх основі формулювання та доказ теорем безпеки. Наявність формального доказу безпеки дозволяє стверджувати про "гарантованість" захисту інформації. Разом із тим, однією із проблем теорії захисту інформації є саме побудова "гарантовано захищеної системи" як протиріччя між вимогами гарантованості та неможливістю її побудувати у класі відкритих систем [51, 58].

За допомогою неформального підходу описується структура СЗІ, її методи та способи. Зазначений підхід використовується при неможливості застосування формальних методів.

Відповідно до визначення теорія захисту інформації оперує такими поняттями як безпека інформації та інформаційна безпеки. Ці поняття досліджували в своїх роботах В. Богуш, В. Герасименк, В. Дудикевич,

М. Згуровський, О. Корченко, Г. Конахович, В. Хорошко, що свідчить про багатовекторність опису та відсутність єдиного підходу. У роботах [59–61] запропоновано визначення цих понять як стан захищеності об'єкта від інформаційних дестабілізаційних факторів. Разом із тим у роботі [62] інформаційну безпеку системи пропонується розглядати у двох аспектах: з точки зору здатності системи протидіяти впливу дестабілізаційних внутрішніх і зовнішніх факторів та функціональної безпеки, створення загроз для самої системи та зовнішнього середовища, яке викликане функціонуванням системи. Такий підхід, на наш погляд, є більш повним та враховує тенденції розвитку нових інформаційних технологій, тобто саме функціонування системи може змінювати рівень загроз. Це дозволяє розглядати безпеку як базис технології, її властивість.

Отже, забезпечення інформаційної безпеки вимагає вирішення двох груп завдань:

перша група – захист інформації та елементів ІС від дестабілізаційного впливу загроз зовнішнього та внутрішнього характеру;

друга група – захист зовнішнього середовища від інформаційних загроз інформаційної системи.

Дослідження [63–68] найбільш повно зосереджені на першій групі завдань. Друга група, зокрема, на сьогодні досліджена не достатньо. Разом із тим, існують певні труднощі, які не сприяють повному вирішенню завдань першої групи, це випадковий характер факторів, які впливають на процеси захисту інформації, недостатньо чітким описом інструментальних засобів для вирішення завдань аналізу та синтезу СЗІ, необхідність отримання значної кількості вихідних даних, у тому числі статистичних. Причому окремі вихідні дані можуть бути отримані тільки при експлуатації системи, що є недопустимим.

1.3 Вплив процесів інформатизації прикордонного відомства на складові національної безпеки України

Аналіз основних напрямів державної політики з питань національної безпеки [5–8] свідчить, що практично кожний із них залежить від рівня інформатизації суспільства. Держава законодавчо закріпила власні пріоритети в інформаційній сфері [5–8, 9, 69–72], котрі полягають у підвищенні рівня координації діяльності правоохоронних органів, забезпеченні інформаційного суверенітету України; упровадженні новітніх технологій в інформаційній сфері; вжитті комплексних заходів щодо захисту національного інформаційного простору та протидії монополізації інформаційної сфери України тощо.

Стратегією національної безпеки України [73] передбачені завдання політики національної безпеки у забезпеченні інформаційної безпеки, а саме упровадження сучасних засобів і систем захисту інформаційних ресурсів та забезпечення безпеки інформаційних систем, що функціонують в інтересах управління державою тощо.

Державна прикордонна служба, як суб’єкт забезпечення національної безпеки [5–8] зобов’язана дотримуватись загальних принципів, пріоритетних цілей, завдань і механізмів захисту життєво важливих інтересів особи, суспільства і держави від зовнішніх і внутрішніх загроз.

Це вимагає від ДПСУ розробки та впровадження нових засобів автоматизації управлінської діяльності прикордонного відомства та вдосконалення існуючих інформаційних систем відповідно до викликів сучасності в інформаційній сфері. Із розвитком інформатизації ДПСУ зростає актуальність і важливість проблеми забезпечення безпеки інформаційного ресурсу Держприкордонслужби як суб’єкта забезпечення національної безпеки України.

Виконання завдань щодо забезпечення недоторканності державного кордону та охорони суверенних прав України в її виключній (морській) економічній зоні пов’язано з боротьбою різновекторних інтересів інших

держав. Сучасні інформаційні технології дають змогу державам реалізувати власні інтереси без застосування воєнної сили, послабити або завдати значної шкоди безпеці конкурентної держави, яка не має дієвої системи захисту від негативних інформаційних впливів [74–78].

За сучасних умов інформаційна складова набуває дедалі більшої ваги і стає одним із найважливіших елементів забезпечення національної безпеки [79, 80]. Інформаційний простір, інформаційні ресурси, інформаційна інфраструктура та інформаційні технології значною мірою впливають на рівень і темпи соціально-економічного, науково-технічного розвитку тощо. Від обсягу, швидкості та якості обробки інформації значною мірою залежить ефективність управлінських рішень правоохоронних органів, зростає значення методів управління з використанням інформаційних технологій, що впливає на якість виконання завдань ДПСУ та ефективність управління підрозділами прикордонного відомства. Спроможність своєчасно ідентифікувати загрози національної безпеки ДПСУ, здійснення їх моніторингу, прогнозування наслідків безпосередньо залежать від ефективності використання інформаційної інфраструктури [81, 82].

Виконання завдань, які покладені на ДПСУ в контексті інтегрованого управління кордонами, вимагає чіткої і злагодженої системи управління силами та засобами прикордонного відомства, розвиненої системи інформаційного забезпечення. На відміну від інших відомств, підрозділи прикордонної служби розосереджені по всьому державного кордону. Здійснення ними оперативно-службової діяльності передбачає використання інформаційного ресурсу прикордонного відомства, яким забезпечує здійснення в установленому порядку прикордонного контролю і пропуску через державний кордон України осіб, транспортних засобів, вантажів, а також виявлення і припинення випадків незаконного їх переміщення; ведення розвідувальної, інформаційно-аналітичної та оперативно-розшукової діяльності в інтересах забезпечення захисту державного кордону; координацію діяльності військових формувань та відповідних

правоохоронних органів, пов’язаних із захистом державного кордону України, а також діяльність державних органів, що здійснюють різні види контролю при перетинанні державного кордону України або беруть участь у забезпеченні режиму державного кордону, прикордонного режиму і режиму в пунктах пропуску через державний кордон України [13].

Обробка специфічної "прикордонної" інформації здійснюється в інтегрованій інформаційній системі "Гарт". Залежно від типу інформації, її важливості, вимогам щодо оперативності її обробки в ДПСУ розробляються та впроваджуються інформаційні системи (ІС), які забезпечують автоматизацію виконання окремих завдань оперативно-службової діяльності прикордонного відомства. Враховуючи структуру ДПСУ, а саме чотирирівневу модель управління, кожна із ІС передбачає наявність функціоналу певного рівня.

Оперативно-службова діяльність Державної прикордонної служби України, зміст якої викладено в [13], передбачає використання та підтримання в актуальному стані інформаційного ресурсу прикордонного відомства. З метою визначення залежності між змістом оперативно-службової діяльності ДПСУ та складовими інформаційного ресурсу проведено порівняльний аналіз впроваджених інформаційних систем та підсистем і основними функціями ДПСУ, результати якого подано у додатку А таблиця А.1.

Вплив процесів інформатизації прикордонного відомства на складові національної безпеки України необхідно розглядати через призму поняття "прикордонної сфери національної безпеки" як частини сфери діяльності ДПСУ, через яку реалізуються загрози НБУ, і явно або неявно виявляється можливість або наміри у завданні шкоди життєво важливим інтересам особи, суспільства або держави [83]. Враховуючи масштабну інформатизацію ДПСУ як сукупність взаємопов’язаних організаційних, правових, політичних, соціально-економічних, науково-технічних, виробничих процесів, що спрямовані на створення умов для задоволення інформаційних

потреб прикордонного відомства на основі створення, розвитку і використання інформаційних систем, мереж, ресурсів та інформаційних технологій, які побудовані на основі застосування сучасної обчислювальної та комунікаційної техніки [84], визначимо взаємозалежність цих процесів через завдання ДПСУ (додаток А, таблиця А.1) із загрозами національної безпеки у прикордонній сфері (додаток А, таблиця А.2).

Аналіз взаємозалежності завдань ДПСУ із загрозами національної безпеки у прикордонній сфері показав [85], що велику роль у запобіганні реалізації загроз національній безпеці України ДПСУ відіграє у перших трьох сферах, а саме: зовнішньополітичній, державної безпеки і воєнній сфері та сфері державного кордону України. Причому, інформаційний ресурс прикордонного відомства, який є основою здійснення оперативно-службової діяльності, забезпечує виконання прикордонним відомством власних основних функцій.

Логічним є припущення, що у такому підході інформаційний ресурс прикордонного відомства як одного із суб’єктів забезпечення НБУ набуває визначення як "важливий інтерес". Тобто інформаційний ресурс може впливати на стійкий розвиток суспільства. Доцільно нагадати, що поняття "національна безпека" трактується в [5–8] як стан захищеності життєво важливих інтересів особи, громадянина, суспільства і держави, при якому забезпечується стійкий розвиток суспільства, запобігання та нейтралізація реальних і потенційних, внутрішніх та зовнішніх загроз національним інтересам, що є необхідною умовою збереження і примноження духовних та матеріальних цінностей. Тобто збереження інформаційного ресурсу прикордонного відомства як одного із суб’єктів забезпечення НБУ є питанням національної безпеки держави.

Своєчасне виявлення загрози НБУ можливе за умови наявності оперативної та достовірної інформації. Наявні інформаційні системи та підсистеми, які направлені на автоматизацію конкретних завдань ДПСУ, дозволяють значно підвищити оперативність прийняття управлінських

рішень з питань нейтралізації загроз національної безпеки. Окремо в цьому аспекті необхідно виділити проблему забезпечення достовірності, доступності, конфіденційності та спостереженості інформаційних систем прикордонного відомства. Знайдені взаємозв'язки процесів інформатизації Державної прикордонної служби України та складових національної безпеки України дозволяють стверджувати про наявність істотного впливу забезпечення безпеки інформаційного ресурсу прикордонного відомства на національну безпеку у прикордонній сфері, а відтак і на національну безпеку в цілому.

1.4 Сучасні підходи до проблеми забезпечення функціональної безпеки в інформаційних системах

Інформаційний ресурс є одним із визначальних факторів економічного розвитку в сучасному світі [86]. Саме тому проблема забезпечення безпеки інформаційних ресурсів держави є актуальною. Водночас, забезпечення необхідного рівня функціональної безпеки потребує розробки, впровадження та підтримання у працездатному стані достатньо складної комплексної системи, до якої входять різні методи та засоби вирішення цього завдання.

Однією із складових функціональної безпеки відомчої ІІС є інформаційна безпека [87] з причини використання персоналом інформаційного ресурсу системи для прийняття рішень, які впливають на рівень національної безпеки. Моделювання процесів інформаційної безпеки є основним науковим способом дослідити ефективність запропонованих заходів, сформувати найбільш ефективні підходи до вирішення завдання забезпечення функціональної безпеки в інформаційних системах та розподілу засобів її забезпечення.

Всі моделі інформаційної безпеки будуються за антагоністичним принципом "атака-захист" [88–90] та оперують двома ключовими поняттями: витратами на захист і збитками від порушення захисту інформації. Для

визначення величини збитку від порушення захисту використовуються різні підходи: статистичні, аналітичні, ігрові тощо [91–95].

Однією з моделей інформаційної безпеки є модель Гордона-Лоеба [96–99], яка використовує інвестиційний підхід та базується на дослідженні економічних моделей. Ця модель досить узагальнено описує взаємозв'язок між збільшенням інвестицій в інформаційну безпеку та зменшенням уразливості системи. Досягненням авторів моделі є визначення форми функції уразливості, що має визначальний характер при дослідженні процесу захисту інформації.

У роботі [100] визначені недоліки моделі Гордона-Лоеба, а саме:

1. Проста процедура визначення імовірності уразливості і нападу відсутня.

2. Визначення ймовірних втрат від порушення безпеки є проблемним.

3. Реалізація результатів дослідження щодо певного об'єкта є складною.

4. Зміна стратегії зловмисником при внесенні додаткових інвестицій для захисту, тобто відсутній аналіз протистояння в динамічному режимі.

Разом із тим, дослідження цієї моделі [101] показали наявність формально-аксіоматичного підходу до опису ризикової ситуації та практично виключення можливості конкретизації індивідуальних властивостей об'єкта інформаційної діяльності та профілю загроз.

Варто зазначити особливості застосування інвестиційних моделей або моделей економічного типу при моделюванні інформаційної безпеки правоохоронних відомств держави. Оцінка ефективності функціонування відомства і, зокрема, комплексної системи захисту інформації за економічним підходом є не зовсім доречною, через відсутність прибутку державних органів, таких як Держприкордонслужба України. Звісно, можливо представити "прибуток" як нереалізовані втрати у грошовому еквіваленті, але їх розрахунок є дуже проблемним.

Ще одна математична модель, яка наведена в [102, 103], враховує витрати на захист інформації і дозволяє розрахувати рівень збитків при реалізації загроз з урахуванням відомих законів розподілу ймовірностей. Автори цієї моделі оперують поняттям надійності комплексу технічного захисту інформації, що потребує наявність статистичних даних ймовірностей реалізації зловмисником загроз. Проблемність використання статистичних моделей полягає у складності збору статистичних даних про результати порушення властивостей інформаційного ресурсу. Крім того, необхідно при зборі статистики чітко знати, що факт порушення властивостей ІнР відбувся. Недоліком зазначеної моделі є необхідність отримання реальної ефективності засобів захисту, що може бути отримана тільки в результаті реальних порушень властивостей ІнР. У випадку інформаційних ресурсів правоохоронних органів як складових забезпечення національної безпеки така умова є недопустимою.

У роботі [104] цільова функція моделі представлена як сума втрат від витоку інформації та витрат на її захист. Аналогічно попереднім моделям, оцінка вартості втрат інформаційного ресурсу держави вимагає додаткового дослідження.

Окремі моделі [105–107] розглядають процес захисту інформації з точки зору ігрових моделей, що у свою чергу дозволяє врахувати різні стратегії поведінки порушника. У моделях, які базуються тільки на економічному характері інформації, всі засоби впливу та втрат приводяться до одного типу – грошового еквіваленту, а в ігрових моделях сторони можуть використовувати одночасно як декілька стратегій, так і декілька різнотипних засобів. Дані моделі розглядають систему захисту інформації як гру двох гравців із повною інформацією. Ходи в цій грі можуть бути детермінованими (дотримуватись певної стратегії або сукупності стратегій) або випадковими. Формалізація відносин між сторонами здійснюється шляхом запровадження функції ризику, яку одна із сторін старається максимізувати, а інша

мінімізувати. Особливістю таких моделей є динамічний характер протистояння між "зловмисником" та "захисником".

Процес захисту інформації можна описати моделлю протистояння двох сторін – моделлю Гроса [108–110], яка була розроблена наприкінці Другої світової війни та призначена для імітації тактичних військових операцій. Особливістю цієї моделі є дискретний характер цільової функції, однотипність об’єктів, що у свою чергу спрощує вирішення завдання з одного боку, а з іншого обмежує можливість застосування до реальних процесів функціонування систем захисту.

Аналіз наведених моделей показав, що їх ключовим фактором є визначений обсяг інвестицій у захист. Питанням раціонального розподілу засобів захисту присвячені тільки окремі роботи, а саме в [111] розкрито поетапний процес побудови моделі розподілу ресурсів.

На підставі аналізу авторами методики вибору засобів захисту інформації визначено, що методика: не розглядає питання протидії системи захисту інформації розподіленим атакам; не враховує той факт, що втрати, пов’язані зі зниженням продуктивності, викликані використанням засобів захисту інформації, залежать від їх розподілу; не дає можливість вибору між різними варіантами побудови комплексної системи захисту інформації; не забезпечує єдиний підхід до захисту інформації, яка має певний ступінь обмеження доступу.

Подані моделі є основою для побудови цільової функції завдання оптимізації, які вирішуються відомими методами. Разом з тим, моделювання процесів інформаційної безпеки та пошук раціонального розподілу засобів захисту повинен враховувати характеристики кожного засобу окремо та їх вплив на рівень загального захисту інформації ІТС.

Відомо, що системи захисту відомчих інформаційних систем є ієрархічними багаторівневими системмами великої складності [112]. Типова структура таких систем розподіляється за рівнями управління, утворюючи ієрархічну складову і включає в себе відмінності по горизонтальній

декомпозиції, враховуючи особливості кожного об’єкту інформаційної діяльності.

Такого типу системи розвиваються як державні територіально-розподілені гетерогенні системи, які об’єднують об’єкти інформатизації органів охорони кордону, регіональних управлінь, об’єктів інформаційної діяльності інших організацій, з якими взаємодіє прикордонне відомство з метою забезпечення прикордонної безпеки. У загальному вигляді ця система є сукупністю об’єктів інформатизації, які складаються з локальних обчислювальних мереж (програмно-технічних комплексів) автоматизованих робочих місць, що об’єднані мережами передачі даних (засобами комунікації). Кожна мережа об’єднує певний перелік взаємопов’язаних автоматизованих систем, які забезпечують вирішення окремих завдань. Окремі об’єкти інформатизації здійснюють взаємодію із зовнішніми державними та міжнародними організаціями через комутовані або виділені канали зв’язку з використанням засобів передачі інформації.

Програмно-технічні комплекси на об’єктах інформатизації включають технічні засоби обробки даних, засоби обміну даними з можливістю виходу в мережі передачі даних, а також засоби зберігання. У технологічному плані об’єкти інформатизації містять:

– технологічне обладнання (програмно-технічні комплекси, мережеве та кабельне обладнання;

– програмні засоби (операційні системи, системи керування базами даних та інше загальносистемне, спеціальне і прикладне програмне забезпечення, геоінформаційні системи та інше);

– інформаційні ресурси, які містять загальнодоступні відомості, відомості конфіденційного характеру і відомості, які містять інформацію з обмеженим доступом;

– засоби зв’язку і передачі даних;

– канали зв’язку;

– відповідні службові приміщення;

– технічні засоби та системи, які не обробляють інформацію, але розташовані в приміщеннях, де циркулює критична для прийняття рішень, інформація;

– засоби захисту інформації від несанкціонованого доступу тощо.

Опис такого типу складних систем за наведеними моделями інформаційної безпеки є або занадто складним, або таким, який не зможе адекватно описати всі процеси системи захисту інформації. В основному всі підходи та рекомендації, які описані в керівних документах, розглядають створення комплексної системи захисту інформації тільки на об’єкті інформаційної діяльності. Такий підхід до проблеми захисту інформації працює достатньо ефективно, про що свідчить існуючий стан захисту, але основне зусилля таких принципів зосереджено на такій властивості інформації, як конфіденційність. При здійсненні модернізації програмно-технічних комплексів, які функціонують на загальному полі даних гетерогенної системи, можлива ситуація порушення інших властивостей: цілісності, доступності та спостереженості. Не можна виключити і порушення самої конфіденційності. Отже, існуючі підходи не дозволяють повно описати процес зміни рівня забезпечення функціональної безпеки на стадії модернізації гетерогенної інформаційної системи.

1.5 Аналіз моделей розмежування доступу в інформаційних системах

Моделі розмежування доступу є найбільш розробленими до теперішнього часу. Історично вони виникли з робіт з теорії захисту операційних систем. Перша спроба використання моделі захисту була здійснена при розробці захищеної операційної системи ADEPT-50 [113] на замовлення Міністерства Оборони США. Ця модель складається з множини об’єктів захисту: користувачі, будівлі, термінали і файли, яким задаються такі характеристики, як рівень конфіденційності, категорія прикладної

області (з дискретного набору рубрик, що описують прикладну область), повноваження і режим (вид) доступу [114]. Поведінка моделі описується такими простими правилами [115]:

– користувачеві дозволений доступ в систему, якщо він входить в множину відомих системі користувачів;

– користувачеві дозволяється доступ до терміналу, якщо він входить в підмножину користувачів, закріплених за даними терміналом;

– користувачеві дозволено доступ до файлу, якщо:

1) рівень конфіденційності користувача не нижче рівня конфіденційності файлу;

2) прикладна область файлу включається в прикладну область завдання користувача;

3) режим доступу завдання користувача включає режим доступу до файлу;

4) користувач входить в підмножину допущених до файлу користувачів.

Характеристики безпеки об’єкта отримуються на основі прав завдання, а не прав користувача і використовуються в моделі для управління доступом, що забезпечує однорідний контроль права на доступ над неоднорідною множиною програм і даних, файлів, користувачів і терміналів.

У моделі Хартсона як одна з основних характеристик використовується множина так званого п’ятивимірного "простору" безпеки [116–118] встановлених повноважень; користувачів; операцій; ресурсів; станів.

Область безпечних станів подається у вигляді декартового добутку перерахованих множин [119]. Кожен запит на доступ представляється підпростором чотиривимірної проекції простору безпеки. Запити отримують право на доступ в тому випадку, коли вони повністю знаходяться у відповідних підпросторах [120].

У моделі безпеки з повним перекриттям [121] передбачається принаймні один засіб захисту для забезпечення безпеки на кожному

можливому шляху проникнення в систему або порушення захисту об’єктів, що охороняються. Модель має більш простий вигляд за рахунок видалення з розгляду "області користувача" та "зовнішніх обмежень". У моделі точно визначається кожна область, яка вимагає захисту, оцінюються засоби забезпечення з точки зору їхньої ефективності та їх внесок у забезпечення безпеки у всій автоматизованій системі.

Одна з перших фундаментальних моделей була розроблена Лемпсоном [122], а потім удосконалена Грехемом і Деннінгом [116].

Основу їх моделі становить правило доступу, яке визначає вид доступу суб’єкта доступу стосовно об’єкта доступу. У контексті операційних систем об’єктами доступу можуть бути сторінки оперативної пам’яті, програми, пристрої зовнішньої пам’яті ЕОМ і файли. Суб’єктами зазвичай є пари виду процес – домен. Процес являє собою активну програму, яка виконується, а домен – оточення, в якому виконується процес. Прикладами доменів в системі IBM System/370 є стани процесора [123]: супервізора та прикладної програми. Видами доступу можуть бути: виконання, виділення (пам’яті), читання, запис. Множину всіх можливих правил доступу можна подати у вигляді матриці (таблиці) доступу, в якій стовпці $O_1, O_2, ... O_n$ представляють суб’єкти доступу. Елемент таблиці $A\{S_i, O_j\}$ містить список видів доступу $T_1, T_2, ... T_r$, який визначає привілеї суб’єкта S_i стосовно об’єкта O_j.

Ця модель передбачає, що всі спроби доступу до об’єктів перехоплюються і перевіряються спеціальним керуючим процесом, який, як правило, називають монітором. Отже, коли суб’єкт S_i ініціює доступ виду T_k до об’єкта O_j, монітор перевіряє наявність T_k в елементі матриці $A\{S_i, O_j\}$. Оскільки під час виконання програми можлива передача управління від одного процесу до іншого, то правила доступу повинні динамічно змінюватися так, щоб права доступу одного суб’єкта могли передаватися іншому. Права доступу в матриці позначаються, якщо дозволена їх передача (копіювання). Суб’єкту можна заборонити довільно передавати свої права.

Цінність такого підходу полягає в обмеженні впливу помилок. Помилки в цьому випадку не можуть безконтрольно поширюватися по всій системі. Тому збільшується надійність (оскільки інші частини системи в більшості випадків можуть продовжувати свою роботу безпомилково) і спрощується налагодження.

У такій моделі безпека всіх об’єктів системи розглядається однаково. Проте при розгляді питань безпеки баз даних (БД) така модель становить тільки одну з підмножин безпеки операційних систем. Безпека баз даних припускає включення в матрицю доступу не тільки сторінок пам’яті, зовнішніх пристроїв і файлів, але також і об’єктів, притаманних самим системам управління базами даних, таких як записи і поля записів. Тому модель може бути розширена для дослідження всіх аспектів безпеки в автоматизованій системі. Існує кілька принципових відмінностей між безпекою операційної системи та безпекою даних. Вони полягають в наступному:

– у базах даних більша кількість захищених об’єктів:

– безпека БД пов’язана з великою кількістю рівнів агрегованих даних, таких, як файли, записи, поля записів і значення полів записів;

– операційні системи пов’язані із захистом фізичних ресурсів, а в БД об’єкти можуть являти собою складні логічні структури, певна множина яких може відображатися на одні і ті ж фізичні об’єкти даних;

– можливе існування різних вимог з безпеки для різних рівнів: внутрішнього, концептуального і зовнішнього для БД і операційних систем:

– безпека БД пов’язана із семантикою даних, а не з фізичними характеристиками.

Єдина модель захисту операційної системи і БД значно ускладнює розгляд питань безпеки. Тому розроблені спеціальні моделі захисту БД. Одним із прикладів моделей захисту баз даних є модель Фернандеза, Саммерса і Колмана [124].

Розглянуті моделі захисту належать до класу матричних і набули найбільшого поширення внаслідок того, що вони служать не тільки для цілей аналізу логічного функціонування системи, а й успішно піддаються реалізації в конкретних програмних системах. Оскільки програми виступають в правилах доступу як суб'єкти, то вони можуть при необхідності розширювати права конкретних користувачів. Наприклад, програма може мати права на сортування файлу, читання якого користувачеві заборонено. У моделі Хартсона і Сяо [37, 118, 125] кожне правило може мати розширення, яке визначає права програм. В інших випадках може знадобитися звуження прав користувачів правами програм, що використовуються. Водночас, програми можуть виступати в як об'єкти доступу, типовими операціями для яких є виконання і використання.

Іншим видом моделей є багаторівневі моделі [126]. Вони відрізняються від матричних моделей за кількома аспектами.

По перше, вони розглядають управління доступом не в межах, що задаються певним адміністратором прав користувачам, а в межах представлення всієї системи таким чином, щоб дані однієї категорії або області не були доступні користувачам іншої категорії [127]. Перший вид керування отримав назву дискреційний контроль доступу, а другий недискреційний, хоча можливі і поєднання видів керування доступом. Наприклад, адміністратор може встановити дискреційні правила доступу для персоналу всередині підрозділу і недискреційні правила доступу для виключення доступу до даних підрозділу з боку співробітників з іншого підрозділу. Цінність недискреційної моделей управління доступом полягає в можливості проведення формального висновку щодо їх безпеки, у той час як для дискреційних моделей в загальному випадку теоретично неможливо встановити, чи є вони безпечними (основна теорема Харрісона) [128, 129].

По-друге, багаторівневі моделі розглядають не тільки сам факт доступу до інформації всередині системи. Подібно дискреційним (матричним)

моделям, багаторівневі моделі також були розроблені для розгляду аспектів безпеки операційних систем і надалі були поширені на безпеку баз даних.

Найбільшого поширення набула багаторівнева модель захисту, розроблена Беллом і Ла Падулом у фірмі MITRE Corp. [128, 130]. У цій моделі вводяться поняття рівня і категорії. Кожному суб'єкту приписується рівень допуску (форма допуску), а кожному об'єкту – рівень конфіденційності (гриф обмеження доступу). Суб'єкт зазвичай – процес, що виконується за запитом користувача і має той же рівень допуску, що і користувач. Об'єктами можуть бути області пам'яті, змінні програм, файли, пристрої введення-виведення, користувачі та інші елементи системи, що містять інформацію. Кожному суб'єкту і об'єкту приписується також множина категорій у вигляді прикладних областей. Тоді рівень безпеки надається у вигляді сполучення: рівень конфіденційності, множина категорій.

Один рівень безпеки домінує над іншим тоді і тільки тоді, коли його рівень конфіденційності або рівень допуску більше або дорівнює іншому і його множина категорій включає відповідну множину іншого. Рівні допуску та конфіденційності є впорядкованими, у той час як рівні безпеки впорядковані частково, так що деякі суб'єкти і об'єкти можуть бути порівняні.

Доступ до об'єкта може розглядатися або як читання (одержання з нього інформації), або як зміна (запис в нього інформації). Тоді види доступу визначаються будь-якими можливими поєднаннями таких операцій, тобто: ні читання, ні зміна, тільки читання, тільки зміна; читання і зміна.

Модель розглядає стани системи безпеки, які визначаються поточною множиною доступів, які представляються у вигляді тріад <суб'єкт, об'єкт, доступ>; матрицею доступу; рівнем безпеки кожного об'єкта; максимальним і поточним рівнями безпеки кожного суб'єкта [130, 131].

Будь-який запит викликає зміну стану системи. Запити можуть бути: на доступ до об'єктів, на зміну рівня безпеки або матриці доступу, на створення або видалення об'єктів. Реакція системи на запити називається рішенням.

При цьому запиті і поточному стані рішення та новий стан визначаються правилами. Ці правила поведінки системи вказують, як буде оброблятися кожен вид запиту. Доказ безпеки системи включає доказ того, що будь-який новий запит викликає перехід системи в новий безпечний стан.

Безпечний стан визначається простою умовою безпеки ($L_i \in L_j$), яку називають також обмежувальною. Проста умова безпеки полягає в тому, що для кожного поточного доступу (суб'єкт, об'єкт, доступ), пов'язаного з читанням об'єкта, рівень безпеки суб'єкта повинен домінувати над рівнем безпеки об'єкта. Інакше таку умову можна сформулювати як "заборона читання з більш високих рівнів". Проста умова не виключає розгляд безпеки при поєднанні безпечних доступів.

Для випадку, коли суб'єкт-порушник може прочитати інформацію з "секретного" об'єкта і записати його в "конфіденційний" об'єкт, передбачається умова $L_i \in L_j$. Вона запобігає потоку інформації з об'єктів більш високого рівня в об'єкти низького рівня. Ця умова визначається так: якщо запит на читання, то рівень суб'єкта повинен домінувати над рівнем об'єкта; якщо запит на зміну, то рівень об'єкта повинен домінувати над поточним рівнем суб'єкта; якщо запит на читання-запис, то рівень об'єкта повинен бути рівний поточного рівня суб'єкта.

Проста умова безпеки є недискреційною моделлю безпеки, в якій доступ розглядається стосовно рівнів суб'єкта та об'єкта. У дискреційній ж моделі безпека забезпечується, якщо кожний поточний доступ дозволений в рамках поточної матриці доступу.

Деннінг розглянув потоки інформації в багаторівневій моделі у більш загальному вигляді [132]. Поняття рівнів конфіденційності та категорій він поєднав в одне поняття класів безпеки і ввів змінну "оператор з'єднання класів" замість раніше постійної. Модель потоків інформації, що описує конкретну систему, визначається п'ятьма компонентами: множиною об'єктів, множиною процесів, множиною класів безпеки, оператором з'єднання класів

і потоковим відношенням. Оператор з’єднання класів визначає клас результату будь-якої операції. Наприклад, якщо з’єднати два об’єкти a і b, класів A і B відповідно, то клас результату представляється як A + B. Потокове відношення між двома класами, наприклад у напрямку від A до B означає, що інформація класу A може бути записана (передана) в клас B. Потокова модель є безпечною, якщо потокове відношення не порушено.

Підбиваючи підсумки розгляду двох класів моделей розмежування доступу, можна зазначити, що перевага матричних моделей полягає в легкості подання широкого спектру правил безпеки інформації. Наприклад, правила доступу, що залежать від виду доступу (операції) і об’єкта доступу (файл), досить просто представляються в рамках матричних моделей. Основний недолік матричних моделей полягає у відсутності контролю за потоками інформації. Основним недоліком моделей управління потоками інформації є неможливість управління доступом до конкретних об’єктів на індивідуальній основі суб’єктів. Отже, обидва підходи включають різні компроміси між ефективністю, гнучкістю і безпекою. Очевидно, що оптимальні рішення питань безпеки можуть здійснюватись при застосуванні обох видів моделей захисту.

Отже, математичний апарат формування систем розмежування доступу для окремих інформаційних систем на сьогодні досить добре розроблений. Разом із тим, як показав аналіз, існуючі моделі не передбачають їх спільного функціонування на загальному полі даних гетерогенної інформаційної системи.

1.6 Обґрунтування напряму дослідження

Виконання основних функцій Державної прикордонної служби України [13] з питань здійснення в установленому порядку прикордонного контролю і пропуску через державний кордон України осіб, транспортних засобів, вантажів, а також виявлення і припинення випадків незаконного їх переміщення, ведення інформаційно-аналітичної діяльності, координація

діяльності військових формувань та відповідних правоохоронних органів, пов’язаної із захистом державного кордону України, а також діяльності державних органів, що здійснюють різні види контролю при перетинанні державного кордону України пов’язане із зберіганням та обміном інформації службового характеру між суб’єктами інтегрованого управління кордонами.

Відповідно до Порядку функціонування, застосування та використання інтранет–мережі Державної прикордонної служби України інформаційними складовими частинами інтранет–мережі Державної прикордонної служби України є [15]: компоненти ІІС Державної прикордонної служби України; інтранет веб-сайти та FTP-сервери структурних підрозділів Державної прикордонної служби України; інтранет пошта Державної прикордонної служби України тощо.

Відомчу інтранет–мережу Державної прикордонної служби України необхідно розглядати у трьох аспектах.

Перший. Функціонування інформаційних систем ДПСУ як суб’єкта забезпечення національної безпеки України безпосередньо пов’язано із запобіганням основних загроз національним інтересам і національній безпеці України в інформаційній сфері [5–8].

Другий. Відповідно до Концепції інтегрованого управління кордонами виконання завдань, які покладаються на ДПСУ, вимагає створення єдиного інформаційного простору, в межах якого реалізують свої повноваження суб’єкти інтегрованого управління кордонами: Адміністрація Держприкордонслужби, Держмитслужба, МВС, МЗС та інші органи державної влади відповідно до компетенції [9].

Третій. Доктриною інформаційної безпеки України визначені життєво важливі інтереси України в інформаційній сфері, які лежать у площині виконання завдань ДПСУ [32].

Отже, одним із напрямів діяльності органів виконавчої влади у сфері забезпечення інформаційної безпеки України є функціональна безпека ІІС, у тому числі захист від кібернетичних атак [81].

Особливістю інтранет мережі Державної прикордонної служби України є те, що вона:

– виключно відомча та не має виходу до всесвітньої глобальної мережі Інтернет;

– функціонування інформаційних складових в інтранет–мережі здійснюється з використанням орендованих каналів зв'язку;

– забезпечує обмін даними між суб'єктами інтегрованого управління кордонами.

Функціональна структура відомчої інтранет–мережі, її інформаційні потоки та взаємодія із суб'єктами інтегрованого управління кордонами та іншими організаціями представлена в додатку В.

Інформаційне наповнення інтранет–мережі здійснюється на засадах уніфікації технічного, технологічного, інформаційного та організаційного забезпечення підрозділів Державної прикордонної служби України з урахуванням рівня розвитку інформаційної інфраструктури і технологічних можливостей кожного з них та забезпечується шляхом: організації та забезпечення інформаційного обміну між складовими частинами ІІС "Гарт"; безпосереднього цілодобового супроводження та моніторингу працездатності компонентів інтранет–мережі.

Виконання Державною прикордонною службою завдань з охорони державного кордону вимагає оперативного реагування на загрози НБУ, що приводить до постійної модернізації інформаційних систем. Такі умови функціонування відомчої інформаційної системи передбачають інтеграцію нових програмно-апаратних засобів з існуючими, у результаті чого утворюється загальне поле даних, яке використовується як старими, так і новими компонентами інформаційних систем. На цій стадії життєвого циклу виникає завдання забезпечення функціональної безпеки в умовах модернізації відомчої інформаційної системи.

Актуальність формування теоретичних основ функціональної безпеки обумовлюється відсутністю науково-обґрунтованих методів комплексного

узгодження різних версій інформаційних систем відомчої інтегрованої інформаційної системи на стадії модернізації та в умовах взаємодії із суб'єктами інтегрованого управління кордонами, які надають можливість вирішити виявлену проблему адекватно загрозам НБУ в інформаційній сфері.

1.7 Висновки до розділу 1

1. Аналіз потреб у забезпеченні функціональної безпеки на сучасному етапі еволюції відомчої інформаційної системи Державної прикордонної служби України показав, що функціонування відомчих інформаційних систем безпосередньо пов'язано із запобіганням основних загроз національним інтересам і національній безпеці України в інформаційній сфері. Упровадження новітніх засобів автоматизації призводить до утворення спільного поля даних, що використовуються у функціональних завданнях як старих, так і нових компонентів ІІС. Як наслідок, у такій ситуації виникають інтегровані інформаційні дестабілізаційні фактори, які сприяють порушенню властивостей ІС. Модернізація інформаційних систем вимагає вирішення завдання усунення протиріч між вигодами від впровадження передових технологій обробки інформації і можливого збитку від порушення властивостей інформаційних систем, викликаного систематизованими вище причинами. Відсутність на даний час адекватних підходів раціонального сполучення різнорідних програмно-апаратних компонентів стримує вирішення цих питань.

2. Аналіз підходів до забезпечення функціональної безпеки в інтегрованих інформаційних системах показав достатньо глибоке опрацювання питань щодо захисту інформаційного ресурсу та елементів ІС від дестабілізаційного впливу загроз зовнішнього та внутрішнього характеру окремо для кожної інформаційної системи. Разом із тим, питання захисту зовнішнього середовища від інформаційних загроз інформаційної системи та питання забезпечення функціональної безпеки при спільному

функціонуванні різних версій інформаційних систем на загальному полі даних досліджені не достатньо.

3. Аналіз взаємозалежності завдань ДПСУ із загрозами національної безпеки у прикордонній сфері показав, що велику роль у запобіганні реалізації загроз національній безпеці України ДПСУ відіграє у зовнішньополітичній сфері, державній безпеці і воєнній сфері та сфері державного кордону України. Знайдені взаємозв'язки процесів інформатизації Державної прикордонної служби України та складових національної безпеки України дозволяють стверджувати про наявність істотного впливу забезпечення безпеки інформаційного ресурсу прикордонного відомства на національну безпеку у прикордонній сфері, а відтак і на національну безпеку в цілому.

4. Аналіз сучасних підходів до проблеми забезпечення функціональної безпеки в інформаційних системах показав глибоке опрацювання з питань забезпечення окремих властивостей інформаційних систем окремо, зокрема конфіденційності. При здійсненні модернізації програмно-технічних комплексів, які функціонують на загальному полі даних гетерогенної системи, можлива ситуація порушення інших властивостей: цілісності, доступності та спостереженості. Не можна виключити і порушення самої конфіденційності. Отже, наявні підходи не дозволяють повно описати процес зміни рівня забезпечення функціональної безпеки на стадії модернізації гетерогенної інформаційної системи.

5. Аналіз моделей розмежування доступу в інформаційних системах показав їх ґрунтовне опрацювання та формальний доказ безпеки в більшості з них. Водночас, наявні моделі не передбачають їх спільного функціонування на загальному полі даних гетерогенної інформаційної системи, що можливе на стадії модернізації.

Список використаних джерел у першому розділі

1. Степко О. М. Аналіз головних складових інформаційної безпеки держави. / О. М. Степко // Науковий вісник Інституту міжнародних відносин НАУ. Серія: економіка, право, політологія, туризм № 3, 2011.

2. Концептуальні засади розвитку системи забезпечення національної безпеки України : аналіт. доп. / О. О. Резнікова, В. Ю. Цюкало, В. О. Паливода, С. В. Дрьомов, С. В. Сьомін. – К. : НІСД, 2015. – 58 с

3. Про затвердження Концепції формування системи національних електронних інформаційних ресурсів : Розпорядження КМУ від 5.05.2003 [Електронний ресурс] // Законодавство України. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/259-2003-%D1%80

4. Про Національну стратегію розвитку освіти в Україні на період до 2021 року // Указ Президента України; Стратегія від 25.06.2013 № 344/2013 [Електронний ресурс] // Законодавство України. – Режим доступу : http://zakon5.rada.gov.ua/laws/show/344/2013

5. Про основи національної безпеки України : Закон України // Офіційний вісник України. – 2003. – № 29. – ст. 1433.

6. Зайцев М. М. Суб’єкти забезпечення інформаційної безпеки України // М. М. Зайцев // Форум права. – 2013. - № 4. – С. 231-238 – Режим доступу: http://nbuv.gov.ua/j-pdf/FP_index.htm_2013_3_40.pdf

7. Ліпкан В. А. Національна безпека України. К. : КНТ (2009).

8. Ліпкан В. А., Максименко Ю. Є., Желіховський В. М. "Інформаційна безпека України в умовах євроінтеграції." К.: КНТ (2006).

9. Розпорядження Кабінету Міністрів України від 27 жовтня 2010 р. № 2031-р Про схвалення Концепції інтегрованого управління кордонами // Урядовий кур’єр – [офіційне видання] від 11.11.2015. – № 210.

10. Стрельбіцький М. А., Кириленко В. А. Системний захист інформації як складова забезпечення національної безпеки в інформаційній сфері / М. А. Стрельбіцький, В. А. Кириленко // Матеріали VI Всеукраїнської науково-практичної конференції "Освітньо-наукове забезпечення діяльності

правоохоронних органів і військових формувань України" (м. Хмельницький, 2013).

11. Ухлинов Л. М. Защита данных в информационно-вычислительных сетях: обзор технологий / Л. М. Ухлинов // Вестник ВОИВТ. - 1992, №1-2, С. 39-47.

12. Кушнір І. П. Сучасний вимір прикордонної безпеки в аспекті інтегрованого управління кордонами. / І. П. Кушнір // Митна безпека 1-2 (2012).

13. Закон України Про Державну прикордонну службу України // Відомості Верховної Ради України (ВВР), 2003, N 27, ст. 208

14. Катеринчук І. С. Розвиток інформаційного та математичного забезпечення функціонування системи управління у складі технічного оснащення Державної прикордонної служби України. / І. С. Катеринчук // Хмельницький: Вид-во НАДПСУ (2006).

15. Порядок функціонування, застосування та використання Інтранет-мережі Державної прикордонної служби України : наказ Адміністрації Державної прикордонної служби від 09.08.2004 № 663.

16. Програма розвитку телекомунікаційної мережі та інформатизації Державної прикордонної служби України на період до 2015 року. Наказ Адмін. ДПСУ України від 05 трав. 2006 р. № 326. – [Електронний ресурс]. – Режим доступу до матеріалу : http://www.pvu.gov.ua/control/uk

17. Шинкарук О. М. Аналіз досвіду створення та використання інтегрованих телекомунікаційних систем Гарт в Державній прикордонній службі України. / О. М. Шинкарук, А. В. Федорченко // Збірник наукових праць Національної академії Державної прикордонної служби України. Сер.: Військові та технічні науки № 2 (2015): С.221-233.

18. Barannik V. Method of Ciphergrams Coding for Increasing the Effectiveness of Selective Cyber-Protection Technologies / Barannik V., Barannik D., Hahanova A., Medvedev D., Strelbtskiy M. // Radioelectronics & Informatics № 4 (75) –2016 –P. 34–40

19. Юдін О.К. Ієрархічний класифікатор автоматизованих систем прикордонного відомства / О. К. Юдін, М. А. Стрельбіцький // Харьківський національний університет радіоелектроніки. Радіоелектроніка і інформатика. Науково-технічний журнал № 1(76), 2017. С. 57-60

20. Савенко І. М. Принципи та функції державної прикордонної служби України / І. М. Савенко // Демократичне врядування 15 (2015).

21. Стрельбіцький М. А. Конструктивні елементи моделі системного захисту інформації в інтегрованій інформаційно-телекомунікаційній системі Державної прикордонної служби України / М. А. Стрельбіцький, Д. А. Мул // II Всеукраїнська науково-практична конференція "Освітньо-наукове забезпечення діяльності правоохоронних органів і військових формувань України" (м. Хмельницький, 2009).

22. Стрельбіцький М. А. Конструктивні елементи моделі системного захисту інформації в рамках сучасних концепцій / М. А. Стрельбіцький, О. А. Ваврічен // Матеріали V всеукраїнської науково-практичної конференції "Освітньо-наукове забезпечення діяльності правоохоронних органів і військових формувань України" (м. Хмельницький, 2012).

23. Боровик О. В. Особливості визначення функцій густини розподілу висот місцевості. / О. В. Боровик, Р. В. Рачок // Збірник наукових праць [Військового інституту телекомунікацій та інформатизації] №1. – 2017: –С. 28-35.

24. Боровик О. В. Дослідження характеристик ефективності функціонування інформаційно-телекомунікаційної системи Гарт-1 на основі застосування методів імітаційного моделювання / О. В. Боровик, Л. В. Боровик, Л. М. Трасковецька // Збірник наукових праць Національної академії Державної прикордонної служби України. Сер.: Військові та технічні науки 1 (2015): –С. 167-182.

25. Стрельбіцький М.А. Перспективні напрямки розвитку системи висвітлення надводної обстановки в Азово-Чорноморському басейні на сучасному етапі/ М. А. Стрельбіцький, В. І. Кривий // Збірник наукових

праць Військового інституту Київського національного університету імені Тараса Шевченка – Вип. № 4. – К.: ВІКНУ, 2006. – С 130-133

26. Шевченко В.Л. Перспективи застосування волоконно-оптичних системи у системі інформаційного забезпечення Державної прикордонної служби України / В. Л. Шевченко, М. А. Стрельбіцький, М. І. Лисий // Збірник наукових праць Національної академії Державної прикордонної служби України. Сер. : Військові та технічні науки. – 2008. – № 42. – С. 70-72

27. Стрельбіцький М.А. Шляхи захисту інформації в корпоративній мережі Державної прикордонної служби України на стадії модернізації / М. А. Стрельбіцький, Д. А. Купрієнко // III Науково-практична конференція "Пріоритетні напрямки розвитку телекомунікаційних систем спеціального призначення" (м. Київ 2007)

28. Моисеенков И.Э. Основы безопасности компьютерных систем. / И. Э. Моисеенков // Компьютер-Пресс, 1991, № 10, – С. 19-24

29. Тимофеев Ю.А. Комплексный подход к защите информации: почему и как надо защищать компьютерные системы / Ю. А. Тимофеев // Защита информации. 1992. Вып. 1 с. 62-80.

30. Кент С. Обеспечение безопасности в. вычислительных сетях: Протоколы и методы управления в сетях передачи данных / Пер.с англ.; Под ред. Ф.Ф.Куо. М.: Радио и связь. 1985. с. 358-424.

31. Хоффман Л.Дж. Современные методы защиты информации - М.: Сов. Радио, 1980. - 264с.

32. Расторгуев С.П., Дмитриевский Н.Н. Искусство защиты и "раздевания программ". М.: Центр Совмаркет. 1991.

33. International Carnahan Conference on Security Technology, October 10-12, 1990.

34. Стрельбіцький М.А. Аналіз загроз інформаційної безпеки при використанні у Державній прикордонній службі України геоінформаційних систем / М. А. Стрельбіцький, Р. В. Рачок, Д. А. Мул, Є. В. Прокопенко // Збірник наукових праць Національної академії Державної прикордонної

служби імені Б. Хмельницького. Серія військові та технічні науки №1(71) 2017 С-394-403

35. Юдін О.К. Класифікація загроз інформаційному ресурсу ДПСУ на стадії модернізації/ О. К. Юдін, М. А. Стрельбіцький. // Вісник інженерної академії України, вип 4, 2016 С.166-170

36. Герасименко В. А. Защита информации в АСОД (в 2-х томах). – М.: Энергоатомиздат, 1994. – 400 с.

37. Шураков В.В. Обеспечение сохранности информации в системах обработки данных. Финансы и Статистика, 1985. -224 с.

38. Уолкер Б Дж , Блейк Я.Ф. Безопасность ЭВМ и организация их защиты / Пер. с англ. М.: Связь. 1980. -112 с.

39. Державний стандарт України. Захист інформації. Технічний захист інформації. Терміни та визначення. ДСТУ 3396.2-97

40. Стрельбіцький М.А. Аналіз і систематизація причин виникнення збитків від реалізації загроз в інтегрованій інформаційно-телекомунікаційній системі державної прикордонної служби України / М. А. Стрельбіцький // Збірник наукових праць № 58 Частина ІІ. – Хмельницький: НАДПСУ, 2012 – С. 53-54.

41. Стрельбіцький М. А. Аналіз і систематизація причин виникнення збитків від реалізації загроз у відомчих інформаційно-телекомунікаційних системах / М. А. Стрельбіцький // Матеріали Міжнародної науково-технічної конференції "Перспективи розвитку озброєння та військової техніки Сухопутних військ" 18-20 травня 2016 м. Львів.

42. Стрельбіцький М.А. Класифікація загроз інформації в інтегрованій інформаційно-телекомунікаційній системі прикордонного відомства на етапі модернізації / М. А. Стрельбіцький // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка –К.: ВІКНУ, 2015. – Вип. № 50. – 386с С. 248-252

43. Стрельбіцький М. А. Класифікація загроз інформації в інтегрованій інформаційно-телекомунікаційній системі прикордонного відомства на етапі

модернізації / М. А. Стрельбіцький // Матеріали XI міжнародної науково-практичної конференції "Військова освіта і наука: сьогодення та майбутнє" (м. Київ, 2015);

44. Зарубежная радиоэлектроника. Специальный выпуск: "Защита информации", декабрь 1989, - М.: Радио и связь.

45. Горбатов В. С., Кондратьева Т. А. Информационная безопасность. Основы правовой защиты: Учебное пособие. М.: МИФИ, 1995. - 52 с.

46. Мафтик С. Механизмы защиты в сетях ЭВМ: Пер. с англ. - М.: Мир, 1993.

47. Курило А.П. Основы организации системы защиты информации / А. П. Курило // Защита информации. 1992. Вып.1. с.35-49.

48. Терминология в области защиты информации. Справочник. М.: ВНИИ стандарт, 1993.

49. Соснін О.В. Національні інтереси в інформаційній сфері. / О. В. Соснін // Віче 9 (2011): – С. 32-36.

50. IEC 61508-1 Edition 2.0 2010-04 International Standard // Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements [Електронний ресурс]. – Режим доступу: https://webstore.iec.ch/preview/info_iec61508-1%7Bed2.0%7Db.pdf

51. Пфо, О. М. Основні проблеми теорії захисту інформації / О. М. Пфо // Актуальні задачі та досягнення у галузі кібербезпеки : матеріали Всеукр. наук.-практ. конф., м. Кропивницький, 23–25 листоп. 2016 р. – Кропивницький : КНТУ, 2016. – С. 151–152.

52. Малюк А.А. Теория защиты информации. – М.: Горячая линия - Телеком, 2012. – 184 с.

53 Куприянов А.О. Основы защиты информации. / А. О. Куприянов, А. В. Сахаров, В. А. Шевцов // Академия, 2007.

54. Загинайлов Ю.Н. Теория информационной безопасности и методология защиты информации. / Ю.Н. Загинайлов // Directmedia, 2015.

55. Котенко В.В., Румянцев К.Е. Теория информации и защита телекоммуникаций : монография / В.В. Котенко, К.Е. Румянцев // – Ростов-на-Дону: Изд. ЮФУ. 2009. – 369 с.

56. Ермакова А. Н. Анализ и синтез современных подходов к защите офисной информации / А. Н. Ермакова, Д. А. Бондарь, А. С. Печникова. // Моделирование производственных процессов и развитие информационных систем. 2012.

57. Меньших В.В. Теоретическое обоснование и синтез математической модели защищенной информационной системы ОВД как сети автоматов / В. В. Меньших, Е. В. Петрова // Вестник Воронежского института МВД России 3 (2010).

58. Порядок з організації та забезпечення режиму секретності в державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях : Постанова КМУ № 1561-12 від 2.10.03

59. Архипов О.Є. Особливості розуміння понять "інформаційна безпека" та "безпека інформації" / О.Є. Архипов, Є.О. Архипова // Информационные технологии и безопасность: основы обеспечения информационной безопасности (ИТБ-2014): Материалы XIV международной научно- практической конференции. – К.: ИПРИ НАН Украины, 2014. – С.18-30

60. Архипова Є. О. Забезпечення інформаційної безпеки та захисту інформації: методичні аспекти / Є. О. Архипова // Публічне управління та адміністрування 1 (2016): С. 16-22.

61. Волошина Н. М. Поняття "безпека інформації" та "інформаційна безпека" в сучасному науковому просторі / Н. М. Волошина // Сучасні інформаційні технології у сфері безпеки та оборони. - 2010. - № 2. - С. 53-56. - Режим доступу: http://nbuv.gov.ua/UJRN/sitsbo_2010_2_14

62. Малюк А. А. На пути к созданию теории защиты информации / А. А. Малюк, Н. Г. Милославская // Вестник РГГУ № 11 (133) Научный

журнал Серия "Информатика. Защита информации. Математика" Москва 2014

63. Конахович, Г. Ф., Климчук, В. П., Паук, С. М., Потапов, В. Г. (2005). Защита информации в телекоммуникационных системах. К.: "МК-Пресс.

64. Меньших В. В. Моделирование действий дестабилизирующих факторов на распределенные информационные системы с помощью аппарата сетей Петри / В. В. Меньших, Ю. С. Лунев. // Системы управления и информационные технологии 31.1 (2008): 71-75.

65. Крылова В. А. Разработка методов оценки эффективности систем защиты информации в распределенных компьютерных системах. / В. А. Крылова, А. Н. Мирошник // Інформаційно-керуючі системи на залізничному транспорті 2 (2015): 43-51.

66. Костин Н. А. Общая математическая модель защиты информации / Н. А. Костин // Актуальные проблемы гуманитарных и естественных наук 11 (2011): 58-63.

67. Баранник В. В. Анализ действия кибератак на видеоинформационный ресурс в информационно-телекоммуникационных сетях / В. В. Баранник, С.А. Подлесный // Автоматизированные системы управления и приборы автоматики 169 (2014).

68. Баранник, В. В. Обоснование значимых угроз безопасности видеоинформационного ресурса систем видеоконференцсвязи профильных систем управления. / В. В. Баранник // Інформаційно-керуючі системи на залізничному транспорті3 (2014): 69-77.

69. Конах В. К. Національний інформаційний простір України: проблеми формування та регулювання / В. К. Конах // Стратегічні пріоритети 2 (2013): 97-103.

70. Присяжнюк М. М. Інформаційна безпека України в сучасних умовах / М. М. Присяжнюк, Я. С. Бєлошевич // Вісник Київського

національного університету імені Тараса Шевченка. Військово-спеціальні науки 30 (2013): 42-46.

71. Марущак А. І. Інформаційні ресурси держави: зміст та проблема захисту. / А. І. Марущак // Правова інформатика 1 (2009): 64-70.

72. Стоєцький О. В. Характеристика інформаційної безпеки як складової інформаційної сфери України. / О. В. Стоєцький // Підприємництво, господарство і право 12 (2009): 72-75.

73. Про Стратегію національної безпеки України : Указ Президента України від 26.05.2015 № 287 Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року // Урядовий кур'єр від 29.05.2015 – № 95.

74. Радковець Ю. І. Ознаки технологій гібридної війни в агресивних діях Росії проти України / Ю. І. Радковець // Наука і оборона 3 (2014): 36-42.

75. Буров О. Ю. Технології й інновації в діяльності людини ери інформації: інформація і технології. / О. Ю. Буров // Інформаційні технології і засоби навчання 49, вип. 5 (2015): 16-25.

76. Кириченко І. О. Визначення поняття інформаційно-бойовий простір, змісту та ролі його складових елементів для досягнення перемоги у воєнних конфліктах XXI століття. / І. О. Кириченко, С. П. Ярош. // Системи озброєння і військова техніка 3 (2011): 102-108.

77. Дубов Д.В. Стратегічні аспекти кібербезпеки України. / Д. В. Дубов // Стратегічні пріоритети 4 (2013): 119-127.

78. Пєвцов Г. В. Реалізація підходів інформаційної війни Російською Федерацією в сучасному інформаційному просторі України. / Г. В. Пєвцов // Наука і техніка Повітряних Сил Збройних Сил України 2 (2014): 10-13.

79. Клочко В. О. Інформаційна безпека як складова національної безпеки України / В. О. Клочко // Вісник Харківського національного університету імені ВН Каразіна. Серія: Право 14 (2013): 274-276.

80. Григор’єв В. І. Інформаційна безпека у державному управлінні. / В. І. Григор’єв // Бібліотекознавство. Документознавство. Інформологія 4 (2013): 53-55.

81. Доктрина "Інформаційної безпеки України" // Урядовий кур’єр від 28.02.2017 – № 38.

82. Інформаційні державно-управлінські ресурси України: визначення і розуміння / Олександр Соснін, Олександр Твердохліб, Віче №22, 2011

83. Теоретичні основи інформаційно-аналітичного забезпечення процесів охорони державного кордону (в контексті завдань національної безпеки України в прикордонній сфері): моногр. / М.М. Литвин, В.П. Городнов, Д.В. Іщенко, В.А. Кириленко. – Хм.: Вид-во НАДПСУ. 2009. – 471 с

84. Стрельбіцький М.А. Окремі питання синтезу системного захисту інформації в інтегрованій інформаційно-телекомунікаційній системі прикордонного відомства на стадії модернізації / М. А. Стрельбіцький // Збірник наукових праць № 3 (65) Частина ІІ. – Хмельницький: НАДПСУ, 2014. С. 353-364

85. Стрельбіцький М.А. Вплив процесів інформатизації прикордонного відомства на складові національної безпеки України / М. А. Стрельбіцький // Матеріали науково-практичної конференції "Наукове забезпечення службово-бойової діяльності Національної гвардії України" 31 березня 2015, м. Харків.

86. Марутян Р.В. Інформаційні ресурси: нові підходи до визначення поняття / Р. В. Марутян // Сучасна українська політика. Політики і політологи про неї (2009).

87. Стецiв І. С. Економічна безпека ВНЗ: сутність та особливості планування / І.С. Стецiв // Менеджмент та підприємництво в Україні: етапи становлення і проблеми розвитку: [збірник наукових праць] – Львів: видавництво Львівської політехніки, 2010, – 416 с.

88. Грищук Р. В., О. Г. Корченко. Методологія синтезу та аналізу диференціально-ігрових моделей та методів моделювання процесів кібернападу. / Р. В. Грищук, О. Г. Корченко. // Захист інформації 14.3 (56) (2012): 115-122.

89. Грищук Р. В. Верифікація і дослідження спектральних Р-та гібридних PL-моделей процесу нападу на інформацію. / Р. В. Грищук // Вісник Житомирського державного технологічного університету. Серія: Технічні науки 2 (49) (2009): 69-76.

90. Гладиш С. В. Модель мультиагентної системи інформаційної безпеки в телекомунікаційній мережі / С. В. Гладиш // Научные труды ОНАС им. АС Попова 1 (2007).

91. Конахович Г. Ф. Оцінка ефективності систем захисту інформації в телекомунікаційних системах / Г. Ф. Конахович, О. Г. Голубничий, О. Ю. Пузиренко. // Проблеми інформатизації та управління 3.21 (2007): 75-83.

92. Бойченко О. В. Модель корпоративного інформаційного захисту об’єкту інформатизації / О. В. Бойченко, Я. І. Торошанко. // Наукові записки Українського науково-дослідного інституту зв’язку 4 (2011): 15-19.

93. Берко А. Ю. Методи та засоби оцінювання ризиків безпеки інформації в системах електронної комерції / А. Ю. Берко, В. А. Висоцька, І. В. Рішняк // Вісник Національного університету "Львівська політехніка". – 2007. № 591

94. Юдин О. К., Загальна модель формування системи захисту державних інформаційних ресурсів. / О. К. Юдін, С. С. Бучик, О. В. Фролов // Наукоємні технології 28.4 (2015): 332-337.

95. Корченко А. О. Метод оцінки рівня критичності для систем управління кризовими ситуаціями. / А. О. Корченко, В. А. Козачок, А. І. Гізун. // Захист інформації 17.1 (2015): 86-98.

96. Gordon L. The Economics of Information Security Investment / L. Gordon, M. Loeb // ACM Transactions on Information and System Security. – Nov. 2002. – Vol. 5. – №4. – pp. 438-457.

97. Архипов А.В. Применение экономико-стоимостных моделей информационных рисков для оценивания предельных объемов инвестиций в безопасность информации / А. В. Архипов // Захист інформації 17, № 3 (2015): – С. 211-218.

98. Информационная безопасность компании на основе метода анализа причинно-следственных взаимосвязей / А. В. Скиба // Wschodnioeuropejskie Czasopismo Naukowe 4.2 (2015): 81-86.

99. Левченко Є. Г. Математичні моделі економічного менеджменту інформаційної безпеки / Є. Г. Левченко, М. В. Демчишин, А.О. Рабчун / Систем. дослідж. та інформ. технології. 2011. – № 4. – С. 88–96.

100. Прус Р. Б. Методи та моделі динамічного управління ресурсами захисту інформації / Р. Б. Прус // Дисертація на здобуття наукового ступеня кандидата технічних наук, Національний авіаційний університет, м. Київ – 2014 р

101. Скиба А. В. Информационные риски: модели рисков, исследование и использование / А. В. Скиба, О. Є. Архипов // Інвестиції: практика та досвід № 1/2016. С 51-60

102. Журиленко Б. Е. Математическая модель вероятностной надежности комплекса технической защиты информации / Б. Е. Журиленко // Безпека інформації. – 2012. – №2(18). – С.61-65.

103. Журиленко Б. Е. Определение вероятностной надежности единичной технической защиты информации из реальных попыток взлома / Б. Е. Журиленко // Безопасность информации. – 2013. – №1(19). – С.34-39.

104. Задірака В. К. Фінансування витрат на захист інформації в економічній діяльності / В. К.Задірака, О. С. Олексюк, Р. П. Смоленюк, П. І. Штабалюк // Університетські наукові записки. – 2006. – №3-4 (19-20). – С. 479-490.

105. Глушак В. В. Синтез структури системи захисту інформації з використанням позиційної гри захисника та зловмисника / В. В. Глушак, О. М. Новіков // Системні дослідження та інформаційні технології. – 2013. – №2. – С. 89-100.

106. Морозов В. В. Игровая модель распределения ресурсов при защите объекта / В. В. Морозов, К. Д. Шалбузов. // Математическая теория игр и ее приложения, т. 5, вып. 4 Петрозаводск: КарНЦ РАН, 2013. 121 с.

107. Грищук Р. В. Ігрові методи аналізу кібератак на інформаційну сферу / Р. В. Грищук, С. Ж. Піскун, В. О. Хорошко, Ю. Є. Хохлачова // Захист інформації. – 2012. – №1.

108. Молодцов Д. В. Модель Гросса / Д. В. Молодцов // ЖВММФ. – 1972. – т.2. – №12. – С.309-320.

109. Применение теории игр в военном деле / под ред. В.О. Ашкеназы. – М.: Сов. Радио. – 1964. – 360 с.

110. Карлин С. Математические методы в теории игр, программировании и экономике. М.: Мир, 1964

111. Цымбалова А. А. Анализ и совершенствование модели распределения и использования ресурсов с точки зрения информационной безоппасности / А. А Цымбалова, Н. Е. Губенко // Четверта міжнародна науково-технічна конференція 5-8 жовтня 2011 р. "Моделювання та комп’ютерна графіка", Донецкий национальный технический университет.

112. Вунш Г. Теория системи / Вунш Г. – М.: Сов. радио, 1978. –288 с.

113. Weissman, Clark. "Security controls in the ADEPT-50 time-sharing system." Proceedings of the November 18-20, 1969, fall joint computer conference. ACM, 1969.

114. Linde, Richard R., Clark Weissman, and Clay E. Fox. "The ADEPT-50 time-sharing system." Proceedings of the November 18-20, 1969, fall joint computer conference. ACM, 1969.

115. Долгин А. Потанин М., Железные изюминки защиты. // КомпьютерПресс, №8, 1992, стр. 15-20.

116. Тимофеев Ю. А. Анализ работ в области международной стандартизации методов и средств криптографической защиты данных для вычислительных систем и сетей. / Ю. А. Тимофеев // Вопросы специальной радиоэлектроники: серия ЭВТ. 1990, вып.3.

117. Чипига А. Ф. Объектная модель дискреционного (избирательного) доступа на основе четырехмерного пространства / А. Ф. Чипига, А. А. Ерещенко, В. А. Галкина. // Информационное противодействие угрозам терроризма 5 (2005): 34-37.

118. Hartson H. Rex. A semantic model for data base protection languages / Hartson H. Rex, David K. Hsiao // Proceedings of the second international conference on Systems for Large Data Bases. VLDB Endowment, 1976.

119. Тхінь Ву Дик. Методи та засоби адміністрування компонентами захисту інформації в розподілених комп'ютерних системах : дис. канд. техн. наук // Київський національний технічний університет України ім. Ігоря Сікорського, 2015.

120. Volokita A. N. Hierarchical Security Agents in Distributed Computing Systems / A. N. Volokita, Vu Dyk Tkhin // Visnyk NTUU "KPI": Informatics, operation and computer science 2012.55 (2012).

121. Томас К. Нельсон. Диагностика вирусов / К. Нельсон Томас // Мир ПК. 1990. №1. с. 60-62

122. Lampson, B. W. 1973. A note of the confinement problem. Commun. ACM 16(10):613–615.

123. Gum, Peter H. "System/370 extended architecture: facilities for virtual machines." IBM Journal of Research and Development27.6 (1983): 530-544.

124. Варфоломеев А.А., Фомичёв В.М Информационная безопасность. Математические основы криптологии: Учебное пособие. М.: МИФИ, I994.

125. Секреты коммерческой безопасности. Агентство коммерческой безопасности. М.: ИНФОАРТ, 1993.

126. Лепешкин О. М. Анализ моделей разграничения доступа, реализованных в современных социотехнических системах /

О. М. Лепешкин, П. В. Харечкин. // Инфокоммуникационные технологии № 6 2008. – С. 91-93.

127. Горковенко Е. В. Формализованное представление механизмов защиты при мандатном разграничении доступа. Формирование множеств субъектов и объектов защиты для многоуровневой модели разграничения доступа / Е. В Горковенко. // Вест. Казах. нац. ун-та им. аль-Фараби. Алматы: КазНУ 3 (2006): 50.

128. Молотков С. В. Информационная безопасность. Защита информации от компьютерных вирусов в сетях ЭВМ / С. В. Молотков, Д. П. Зегежда, Ю. И. Мазничка, В. А. Петров // Учебн. пособие. - М.: 1993, 68с.

129. Мельников В.В. Защита информации в компьютерных системах / В.В. Мельников. – М.: Финансы и статистика; Электроинформ, 1997. – 368 с.

130. Bell D.E., La Padula L.J. Secure Computer Systems: Mathematical foundations and model. //Report ESD-TR-73-278, Mitre Corp., Bedford, Mass, Nov 1973 - June 1974, V.l-fll.

131. Mark Smith. Towards a Policy-Free Protocol Supporting a Secure X Window System, In Proceedings of the 15th Annual National Computer Security Conference, Baltimore MD, October, 1992.

132. Петров В.А., Пискарёв А.С., Шеин А.В. Информационная безопасность. Защита от несанкционированного доступа в автоматизированных системах: Учебное пособие.М.: МИФИ, 1993.

РОЗДІЛ 2
КОНЦЕПТУАЛЬНІ ОСНОВИ ТЕХНОЛОГІЇ ЗАБЕЗПЕЧЕННЯ ФУНКЦІОНАЛЬНОЇ БЕЗПЕКИ В ІНТЕГРОВАНІЙ ІНФОРМАЦІЙНІЙ СИСТЕМІ НА СТАДІЇ МОДЕРНІЗАЦІЇ

2.1 Основні теоретичні аспекти технології забезпечення функціональної безпеки в інтегрованих інформаційних системах на стадії модернізації

Виконання основних функцій Державної прикордонної служби України [1–4] з питань здійснення в установленому порядку прикордонного контролю і пропуску через державний кордон України осіб, транспортних засобів, вантажів, а також виявлення і припинення випадків незаконного їх переміщення, ведення інформаційно-аналітичної діяльності, координація діяльності військових формувань та відповідних правоохоронних органів, пов’язаної із захистом державного кордону України, а також діяльності державних органів, що здійснюють різні види контролю при перетинанні державного кордону України, пов’язане із зберіганням, обробкою та передаванням інформаційних повідомлень службового характеру між суб’єктами інтегрованого управління кордонами. Оперування інтегрованою інформаційною системою прикордонного відомства критичним для прийняття рішення інформаційним ресурсом вимагає від системи функціональної безпеки забезпечення дотримання всіх властивостей інформаційних систем.

Проведений у першому розділі аналіз підходів до забезпечення функціональної безпеки в інтегрованих інформаційних системах показав, що більшість досліджень зосереджені на проблемах захисту інформації. Уперше уніфіковану концепцію захисту інформації запропонував В. А. Герасименко [5], структура якої наведена на рисунку 2.1.

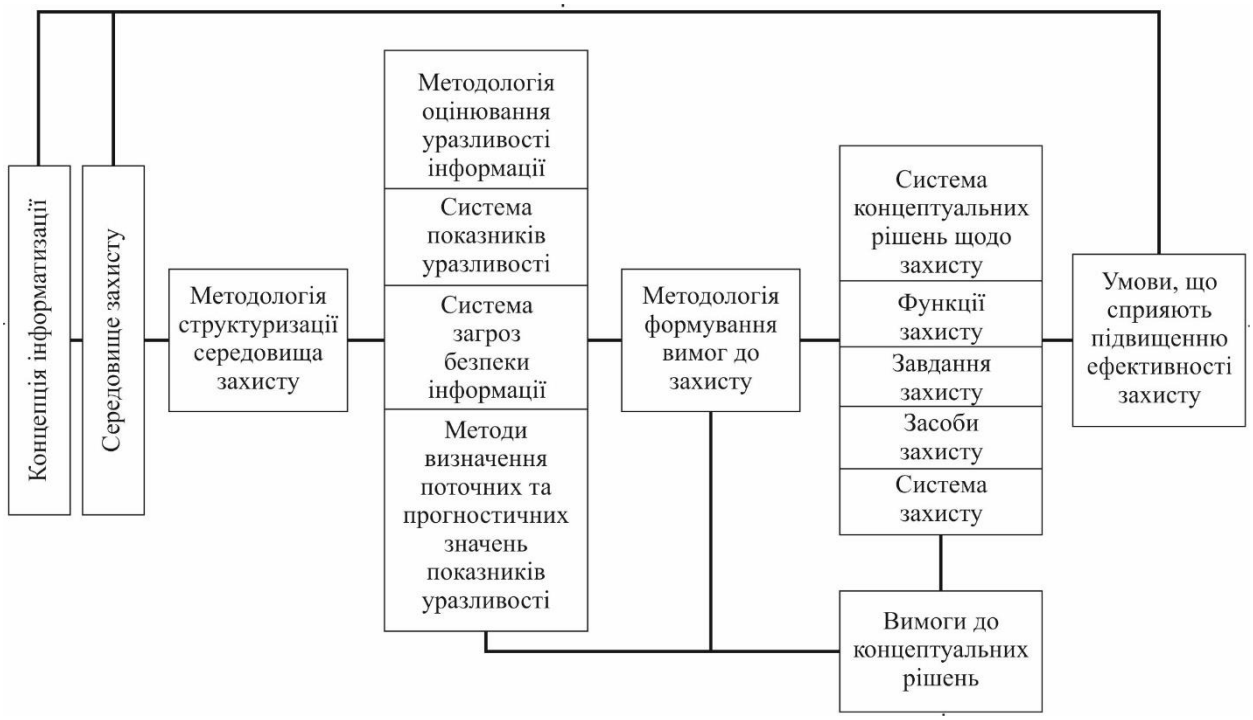


Рисунок 2.1 – Уніфікована концепція захисту інформації

Застосування зазначеної концепції створює передумови для впровадження всіх досліджень в галузі захисту інформації, а саме: структурованого середовища захисту, всебічної оцінки уразливості інформації залежно від дії дестабілізаційних факторів зовнішніх та внутрішніх загроз, формування вимог до захисту, побудова СЗІ в залежності від умов функціонування, формування рекомендацій з підвищення ефективності захисту.

Концепція загалом передбачає циклічний процес вдосконалення системи захисту інформації. Разом із тим, сам процес модернізації, його методологічні засади в уніфікованій концепції не розглянуті. Для наявних систем захисту, які реалізовані в сучасних ІС, загалом не передбачається спільного функціонування різних версій програмно-апаратного забезпечення, систем захисту тощо. Вищенаведене вимагає структурованого аналізу та декомпозиції факторів, що впливають на надійність інформації на стадії модернізації.

Сам процес модернізації ІС здійснюється за окремими складовими системи або комплексно та загалом вимагає їх узгодження в процесі спільного функціонування (рисунок 2.2).

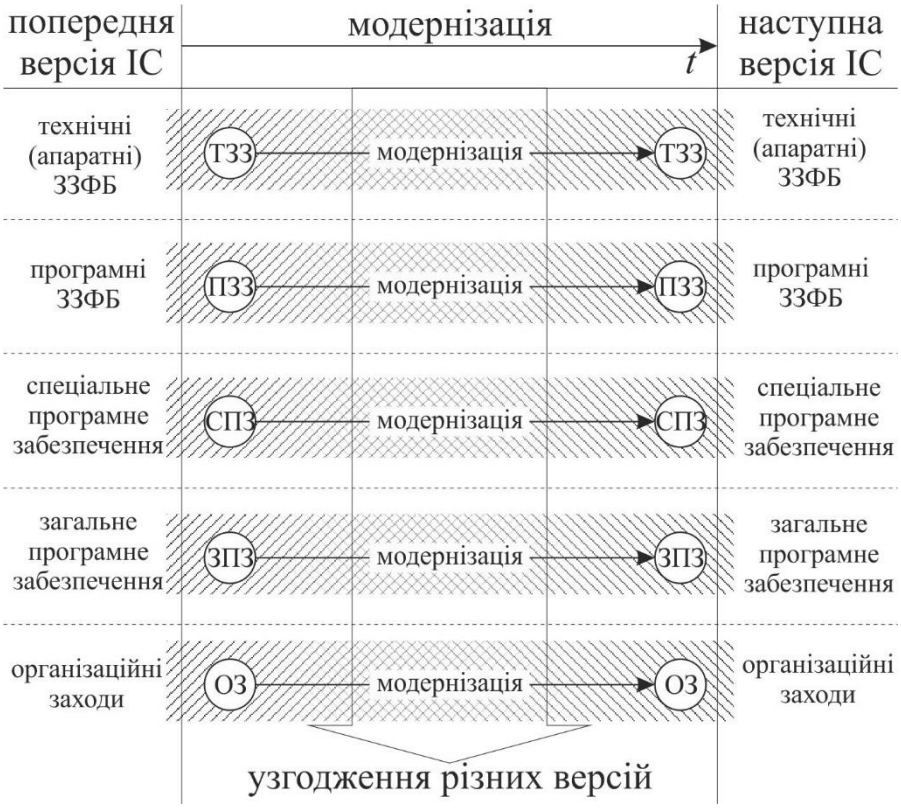


Рисунок 2.2 – Структура процесу модернізації ІС

Отже, з точки зору функціональної безпеки модернізація вимагає формулювання стратегії як головної мети зазначеного процесу. Стратегія функціональної безпеки на стадії модернізації як модель узагальнених дій, спрямованих на досягнення зазначеної мети, полягає у такій сукупності заходів по заміні складових інформаційної системи, за якої рівень функціональної безпеки відповідає нормативному.

Водночас, умови функціонування різних ІС, їх структура та вимоги до функціональної безпеки можуть суттєво відрізнятись. Через це загальне формулювання стратегії функціональної безпеки на стадії модернізації може дещо відрізнятись один від одного. Загалом, організація процесу модернізації в рамках розглянутої стратегії полягає в пошуку раціонального співвідношення між вимогами до нової версії ІС та рівнем інформаційних

дестабілізаційних факторів, викликаних невідповідністю версій. Таке формулювання проблеми належить до галузі оптимізаційних завдань. Разом із тим, значна кількість випадкових факторів не дозволяє сформувати функціональні залежності для їх вирішення відомими оптимізаційними методами.

Обґрунтування стратегій модернізації будемо здійснювати за групами критеріїв: рівня функціональної безпеки, особливостей функціонування ІС.

Формуванню першої групи критеріїв присвячена велика кількість робіт [6–10], в яких дослідники обґрунтовують його фізичний сенс. У більшості досліджень як показник рівня функціональної безпеки пропонується використовувати ймовірність попередження шкоди, враховуючи стохастичну природу дестабілізаційних впливів. Варто зазначити, що значення ймовірності виникнення шкоди протягом всього терміну модернізації буде різною, тобто $P(t)$. Так обирати стратегію модернізації за значенням ймовірності в довільний момент часу є не коректним. Необхідно враховувати загальну тенденцію функції зміни зазначеної ймовірності.

На наш погляд, найбільш доцільними є розподіл цієї групи критеріїв на три складових критерії рівня забезпечення функціональної безпеки:

– нормативний – критерій, за якого поточне значення ймовірності порушення функціональної безпеки не перевищуватиме заданого;

– середній – критерій, за якого середнє значення ймовірності порушення функціональної безпеки не перевищуватиме заданого;

– зважений – критерій, за якого середнє зважене значення ймовірності порушення функціональної безпеки не перевищуватиме заданого.

Друга група критеріїв, яка визначає особливості функціонування ІС [11–13] на стадії модернізації, характеризує можливості щодо втручання в процес роботи системи. За цією групою критерії поділяються на три види:

– системи реального часу характеризуються практичною відсутністю будь-яких можливостей щодо втручання в процес їх функціонування. Прикладом такої системи є ІС "Гарт-1", система автоматизації пропуску осіб,

транспортних засобів через державний кордон України. Зупинка такої системи навіть на невеликий термін є недопустимою, оскільки може призвести до збитків національного масштабу;

– системи з можливістю часткової зупинки характеризуються більшими можливостями для процесу модернізації. Прикладом такої ІС може бути "Гарт-5", система автоматизації інформаційно-аналітичної діяльності. Ці системи функціонують, як правило, під час робочого дня, тобто третину доби.

– системи з можливістю повної зупинки характеризуються максимальними можливостями для процесу модернізації. Такого типу системи мають обмеження тільки терміном експлуатації.

Вищенаведене дозволяє сформувати узагальнену таблицю раціональних стратегій модернізації як декартового добутку обох критеріїв (таблиця 2.1)

Таблиця 2.1 – Раціональні стратегії модернізації

Критерій рівня забезпечення функціональної безпеки	**Особливості функціонування ІС**		
	реального часу	**часткова зупинка**	**повна зупинка**
Нормативний	+	–	–
Середній	–	+	–
Зважений	–	+	–

Отже, нормативний рівень варто застосовувати до систем реального часу з причини забезпечення неперевищення значення ймовірності порушення функціональної безпеки протягом всього терміну модернізації.

Середній та зважений критерії захисту доцільно використовувати при модернізації систем з можливістю часткової зупинки функціонування. Вибір критерію залежить від величин часу та періодичності часткової зупини системи.

Такі дослідження дозволяють сформувати загальну концепцію забезпечення функціональної безпеки ІС на стадії модернізації як

інструментально-методологічну базу що забезпечує виконання розглянутих стратегій (рисунок 2.3).

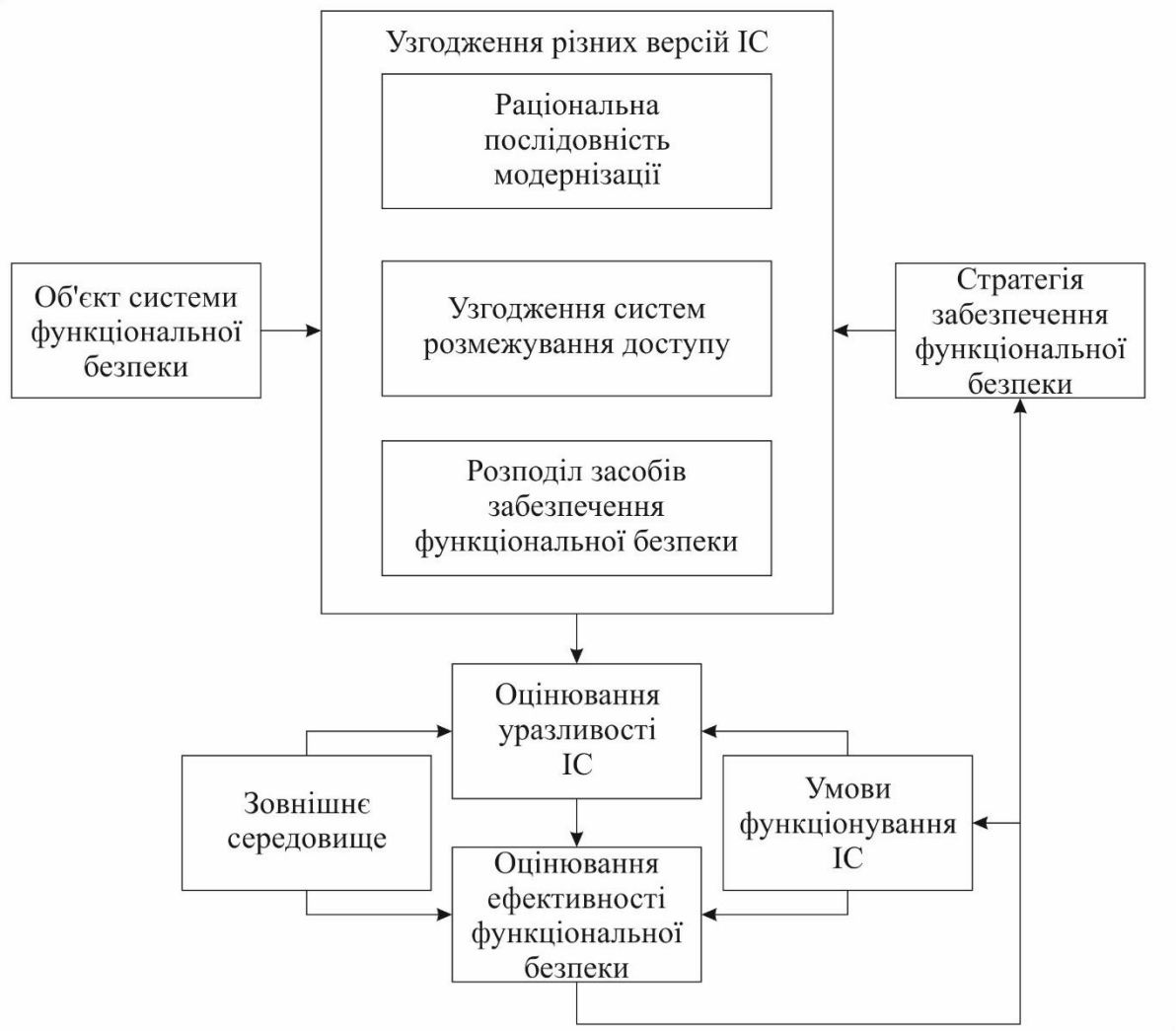


Рисунок 2.3 – Загальна концепція забезпечення функціональної безпеки на стадії модернізації

Першочерговим етапом є обґрунтування самого об’єкту СФБ. Саме від визначення цього поняття та його властивостей залежить формування всієї концепції функціональної безпеки на стадії модернізації. Разом із тим, ключовим питанням є визначення стратегії модернізації як напрямку зосередження основних зусиль всієї системи. Базуючись на визначених обох складових, здійснюється узгодження різних версій ІС.

У більшості випадків модернізація загального програмного забезпечення не здійснює впливу на уразливість ІС з причини завчасної перевірки можливості функціонування різних версій [14, 15]. Загальне ПЗ не

є частиною ІС, а використовується як платформа для функціонування СПЗ на конкретному АРМ або серверному обладнанні. Організаційні заходи, що спрямовані на забезпечення функціональної безпеки, теж не є складовою ІС, хоча здійснюють вплив на процес функціональної безпеки. Ці два елементи виходять за межі дослідження та не включені в загальну концепцію забезпечення функціональної безпеки на стадії модернізації.

Здійснювати завдання узгодження різних версій ІС необхідно тільки в умовах їх спільного функціонування через врахування основного припущенням дослідження, що в різних версіях ІС окремо функціональна безпека дотримується відповідно до встановлених вимог. Отже, в системах з можливістю повної зупинки функціонування на період модернізації не виникають дестабілізаційні фактори, викликані спільним функціонуванням різних версій ІС.

Концепцією передбачено три завдання узгодження. Перше завдання – це узгодження спільного функціонування спеціального програмного забезпечення АРМ інформаційних систем. Модернізація СПЗ здійснюється фахівцями відділів зв’язку, автоматизації та захисту інформації почергово кожного АРМ. Так виникає ситуація спільного функціонування в системі АРМ з різними версіями СПЗ. Вирішення цього завдання можливе шляхом визначення раціональної послідовності модернізації АРМ в інформаційній системі відповідно до обраної стратегії забезпечення функціональної безпеки.

Другим завданням є узгодження програмних засобів захисту, а саме розробка сукупності методів узгодження систем розмежування доступу до інформаційних ресурсів ІС та на їх основі формування методологічного базису. Вирішення цього завдання дозволить науково обґрунтувати принципову можливість функціонування різних версій систем розмежування доступу на спільному полі даних.

Третім завданням є вдосконалення технічних (апаратних) засобів забезпечення функціональної безпеки. Під час модернізації ІІС можлива зміна структури технічних засобів забезпечення функціональної безпеки. Це

вимагає вирішення завдання раціонального їх розподілу на стадії модернізації з урахуванням взаємодії наявних та доданих засобів, а також вимог до загального рівня безпеки інформаційної системи.

Наступними етапами концепції є визначення величини уразливості даних при проведенні заходів з модернізації та оцінювання ефективності функціональної безпеки в ІС на стадії модернізації. На даних етапах враховуються умови функціонування системи та вплив зовнішнього середовища на процес функціональної безпеки. Результатом є отримання оцінки ефективності проведених заходів, яка використовується власником системи для прийняття рішення щодо проведення модернізації та визначення організаційних заходів з особливості проведення самого процесу оновлення складових ІС.

2.2 Обґрунтування об’єкта системи функціональної безпеки в інтегрованій інформаційній системі Держприкордонслужби

Відповідно до нормативно-правових актів України [16, 17] та досліджень в цій галузі [18–21] належність інформації до конфіденційної категорії встановлюють фізичні та юридичні особи з метою захисту власних інтересів, а належність інформації до таємної – держава в публічних інтересах. Для визнання інформації конфіденційною необхідно мати певне право на таку інформацію. Держава, у свою чергу, визнаючи інформацію таємною, керується своїми повноваженнями щодо захисту публічних інтересів [22], а не правом на інформацію.

Процес формування інформаційного суспільства змінив розуміння поняття інформації, яка стала однією з головних стратегічних національних ресурсів загалом держави та окремо кожного суб’єкта забезпечення національної безпеки – Державної прикордонної служби України у тому числі. Поняття "інформаційний ресурс" (ІР) широко вживається у науковій літературі та розкривається у роботах І. В. Арістової [23], А. І Марущака [24, 25], О. В. Сирового [26–28] та інших авторів. Незважаючи на велику

кількість публікацій щодо цієї тематики, на сьогодні відсутній єдиний підхід щодо визначення терміну "інформаційний ресурс", а ті визначення, що існують не повною мірою відповідають специфічному поняттю інформаційного ресурсу, який використовується в прикордонному відомстві держави. Це викликає необхідність у розширенні дефініції терміну "інформаційний ресурс".

Функціонування Державної прикордонної служби як суб'єкта забезпечення національної безпеки передбачає участь прикордонного відомства у формуванні національного інформаційного ресурсу держави у вигляді "прикордонного інформаційного ресурсу". Отже, поняття "прикордонний інформаційний ресурс" потребує уточнення

Держава на законодавчому рівні закріпила поняття "інформація", причому, кожний закон трактує це поняття по-своєму. Так, у [29] поняття інформації трактується як "… будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді". У [30] під інформацією розуміють "… відомості в будь-якій формі й вигляді та збережені на будь-яких носіях інформації…". У [31] поняття трактується так: "інформація – відомості, подані у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб". Відомчі керівні документи визначають поняття інформації більш загально: "… сукупність відомостей, знань і повідомлень про об'єкти, явища та процеси" [32]. У наведених законодавчих актах та відомчих документах відсутнє розмежування понять "дані" та "інформація", що в свою чергу призводить до некоректного використання цих термінів в нормативних документах. Так, у Законі України "Про телекомунікації" визначення поняття "дані" здійснюється через поняття "інформація", а саме "дані – інформація у формі, придатній для автоматизованої обробки її засобами обчислювальної техніки" [31].

Як на наш погляд, то найбільш точно наведено визначення поняття інформації у Державному Стандарті України (ДСТУ) 2396-94 "Теорія

інформації. Терміни та визначення", – як "повідомлення, які знімають невизначеність, що існувала до їх надходження, і є об’єктом зберігання, пересилання та перетворення". Змістовно, дані перетворюються в інформацію тільки в тому випадку, якщо людина усвідомила їх значення і вони спричинили вплив на поведінку людини.

Вищенаведене дозволяє сформувати поняття прикордонної інформації як повідомлення прикордонної сфери діяльності, які знімають невизначеність, що існувала до їх надходження, і є об’єктом зберігання, пересилання та перетворення. Іншими словами, прикордонна інформація – це повідомлення, яке впливає на прийняття рішення персоналом Державної прикордонної служби України щодо питань оперативно-службової діяльності.

Аналогічно поняттю "інформація", існує багато визначень поняття "інформаційний ресурс". Так, у [33] наведено визначення поняття інформаційний ресурс як сукупність документів у інформаційних системах (бібліотеках, архівах, банках даних тощо). Окремими авторами визначення інформаційного ресурсу наводиться як окремий документ та/або масив документів, створений в результаті людської діяльності, який є джерелом інформації або засобом для отримання фізичними та/або юридичними особами знань, які формуються в результаті такої діяльності [34].

За сучасних умов інформаційна складова прикордонного відомства набуває дедалі більшої ваги і стає одним із найважливіших елементів забезпечення національної безпеки. Інформаційні ресурси значною мірою впливають на рівень і темпи соціально-економічного, науково-технічного і культурного розвитку [35].

У такому підході аналізу дефініції інформаційний ресурс держави (інформаційний ресурс прикордонного відомства як одного із суб’єктів забезпечення НБУ), набуває визначення як "важливий інтерес". Так інформаційний ресурс може впливати на стійкий розвиток суспільства.

Доцільно нагадати, що поняття "національна безпека" у [36] трактується як стан захищеності життєво важливих інтересів особи, громадянина, суспільства і держави, за якого забезпечується стійкий розвиток суспільства, запобігання та нейтралізація реальних і потенційних, внутрішніх та зовнішніх загроз національним інтересам, що є необхідною умовою збереження і примноження духовних та матеріальних цінностей. Тобто збереження інформаційного ресурсу прикордонного відомства як одного із суб'єктів забезпечення НБУ, є питанням національної безпеки держави.

При визначенні поняття "прикордонний інформаційний ресурс" необхідно врахувати призначення цього специфічного ресурсу. Загалом, прикордонний ресурс це: джерело, запаси, засоби, можливості ДПСУ. Так, прикордонний інформаційний ресурс (ПІР) повинен забезпечувати оперативно-службову діяльність прикордонного відомства певною (необхідною) інформацією, властивості якої відповідають вимогам достовірності, своєчасності (доступності) та конфіденційності.

Доцільно зазначити, що органи та підрозділи Державної прикордонної служби України дислокуються у районах, де є труднощі у використанні ПІР. Це вимагає створення в цих районах власних комунікаційних мереж на основі сучасних технологій і протоколів та їх узгодження з комунікаційними мережами загального використання.

Отже, прикордонний інформаційний ресурс – це систематизована прикордонна інформація, що міститься на матеріальних носіях та призначена для забезпечення інформаційних потреб прикордонного відомства [37–39]. Електронний прикордонний інформаційний ресурс як складова ПІР зосереджений в інтегрованій інформаційній системі прикордонного відомства.

Аналіз поняття ПІР дозволив визначити його основні особливості:

– він не підлягає фізичному зношенню, можливе тільки старіння інформації та зниження рівня її потреби і як результат зниження потреби в забезпеченні його властивостей;

– він не підлягає фізичному знищенню, оскільки за своєю суттю не є матеріальним. Знищений може бути тільки носій;

– використання інформаційного ресурсу дозволить значно підвищити рівень національної безпеки, оскільки ДПСУ є її складовою;

– величина інформаційного ресурсу тільки зростає з причини неможливості його знищення. Зменшення можливе тільки штучно, завдяки вилученню із системи певної інформації.

З огляду на це існує необхідність у застосуванні системного підходу до загроз властивостям інформації та заходів протидії цим загрозам з метою зменшення втрат (витрат) від реалізації цих загроз.

Так, з точки зору організації забезпечення функціональної безпеки ІІС ДПСУ один із найбільш істотних параметрів є місцезнаходження критичного інформаційного ресурсу, що впливає на властивості інформаційної системи. За цим параметром характерними є три різновиди умов [40]:

– інформаційний ресурс, що знаходиться в організації розробника;

– інформаційний ресурс, що знаходиться в створюваній (функціонуючій) інформаційній системі;

– інформаційний ресурс, що знаходиться в зовнішніх організаціях (суб’єктів інтегрованого управління кордонами).

Забезпечення дотримання властивостей інформаційного ресурсу в організаціях розробки зводиться до попередження НСД, модифікації або розкрадання методів і моделей вирішення тих чи інших задач, алгоритмів і програм їх реалізації, що розробляються, а також масивів даних, які створюються [41].

В інтегрованій інформаційній системі дотримання властивостей інформаційного ресурсу полягає в попередженні НСД, знищенні, модифікації і розкраданні документів, програм, масивів даних, що зберігаються в складових ІІС.

У зовнішніх організаціях дотримання властивостей інформаційного ресурсу аналогічне попереднім заходам.

У загальному випадку даними, що потребують забезпечення дотримання властивостей, можуть бути [42]:

– отримані ІІС для зберігання (аналізу, статистичної обробки, тощо) від користувачів або інших взаємодіючих систем;

– результати обробки (аналітичні звіти, результати статистичного аналізу тощо), отримані в процесі функціонування ІІС;

– нормативні, службові, довідкові та інші дані, у тому числі щодо різних систем забезпечення функціонування ІІС;

– СПЗ, програмні засоби забезпечення функціональної безпеки;

– алгоритми функціонування СПЗ та програмних засобів забезпечення функціональної безпеки;

– методи, методики, принципи, підходи та моделі, на базі яких функціонують складові СПЗ;

– інша документація, яка міститься на елементах ІІС, тощо.

Зазначені види інформації є об’єктами системи забезпечення функціональної безпеки ІІС при переході на нову програмно-апаратну платформу. З метою забезпечення дотримання властивостей інформаційного ресурсу на загальному полі гетерогенного середовища вказані об’єкти вимагають доопрацювання функціональних завдань СФБ. За окремими видами інформаційного ресурсу забезпечення дотримання властивостей може здійснюватися тільки організаційними способами. Вищенаведене вимагає аналізу структури та інформаційних потоків в інтегрованій інформаційній системі прикордонного відомства.

2.3 Декомпозиція структури та інформаційних потоків інтегрованої інформаційної системи прикордонного відомства

Інтегрована інформаційна система Державної прикордонної служби України (шифр "Гарт") являє собою комплекс взаємопов’язаних інформаційних систем, підсистем, засобів комунікації, які функціонують у єдиному інформаційному просторі прикордонного відомства, регламентуються відповідними організаційними та розпорядчими керівними документами та призначені для інформаційного супроводу посадових осіб ДПСУ. Метою створення ІІС "Гарт" є автоматизація функціональних завдань та процесів суб’єктів системи щодо виконання ними завдань із оперативно-розшукової, оперативно-службової та інформаційно-аналітичної діяльності органів та підрозділів ДПСУ. Основою ІІС є комунікаційна мережа ДПСУ, на якій розгорнуті інформаційно-комунікаційні системи, інформаційні системи, автоматизовані робочі місця, програмно-технічні комплекси різного призначення тощо (рисунок 2.4)

Особливістю комунікаційної мережі ДПСУ є те, що вона суто відомча та не має виходу до всесвітньої глобальної мережі Інтернет, функціонування інформаційних складових здійснюється з використанням орендованих каналів зв’язку, забезпечує обмін критичною інформацією щодо прийняття рішень між суб’єктами інтегрованого управління кордонами.

Основною концепцією ІІС є створення єдиного інформаційного простору Державної прикордонної служби України, що сприятиме підвищенню оперативності, повноти та достовірності інформації, яка використовується персоналом органів та підрозділів ДПСУ, розширенню можливостей аналізу та узагальненню інформації, підвищенню якості та скороченню часу на прийняття рішень управлінською ланкою, контроль за виконанням розпорядчих актів Адміністрації та регіональних управлінь прикордонної служби.

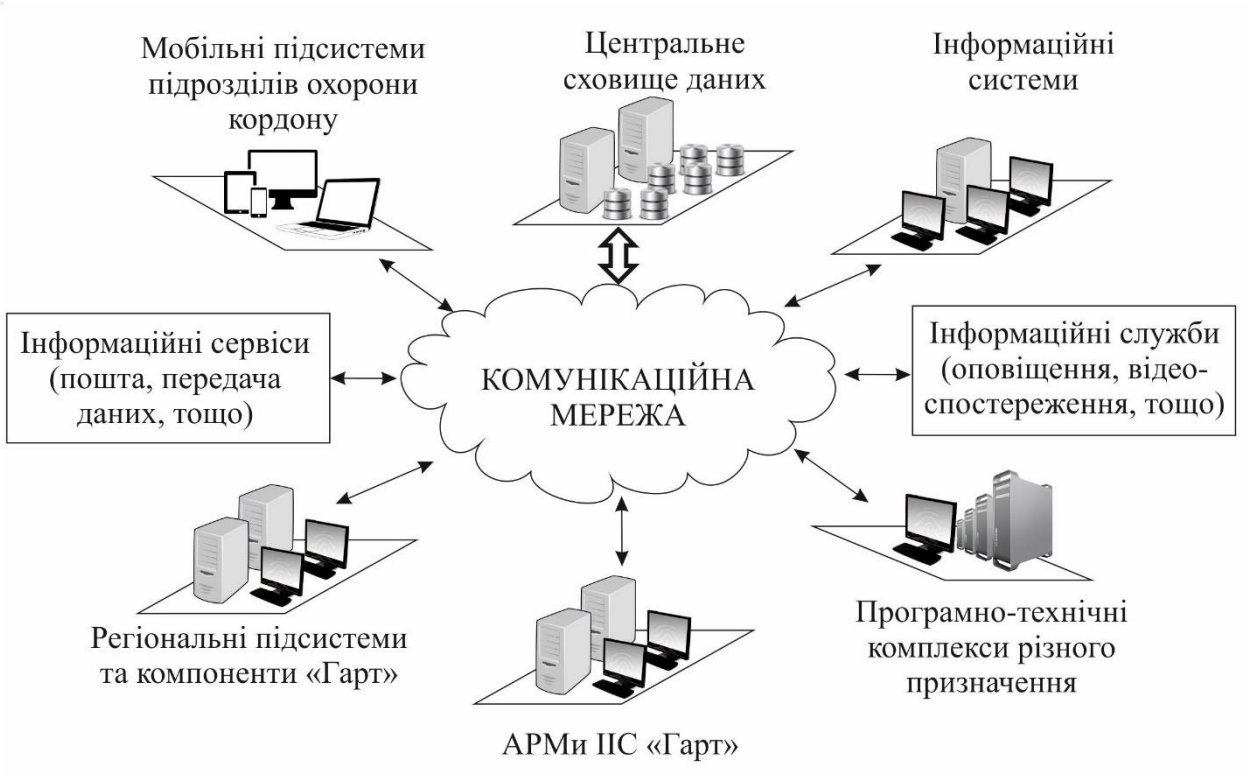


Рисунок 2.4 – Загальна структура ІІС "Гарт" прикордонного відомства

Інтегрована інформаційна система ДПСУ "Гарт" за своєю архітектурою є структурно-ієрархічною системою, яка складається з множини взаємодіючих функціональних складових, що виділені за ознаками територіального розташування, напрямів діяльності та функціональної деталізації та відображає існуючу організаційну структуру прикордонного відомства (рисунок 2.5). Основою функціонування складових ІІС "Гарт" є комунікаційна мережа, яка складається із власних та орендованих каналів, які утворюють цифрові потоки.

Цифрова комунікаційна мережа Державної прикордонної служби [43] України призначена для забезпечення обміну інформацією між автоматизованими інформаційними системами різних рівнів, збільшення обсягів та швидкості обробки інформації в центральному сховищі даних, віддаленого доступу до нього посадових осіб органів та підрозділів охорони кордону, особового складу прикордонних нарядів, істотного підвищення якості та захищеності телефонії, створення системи відеозв’язку.

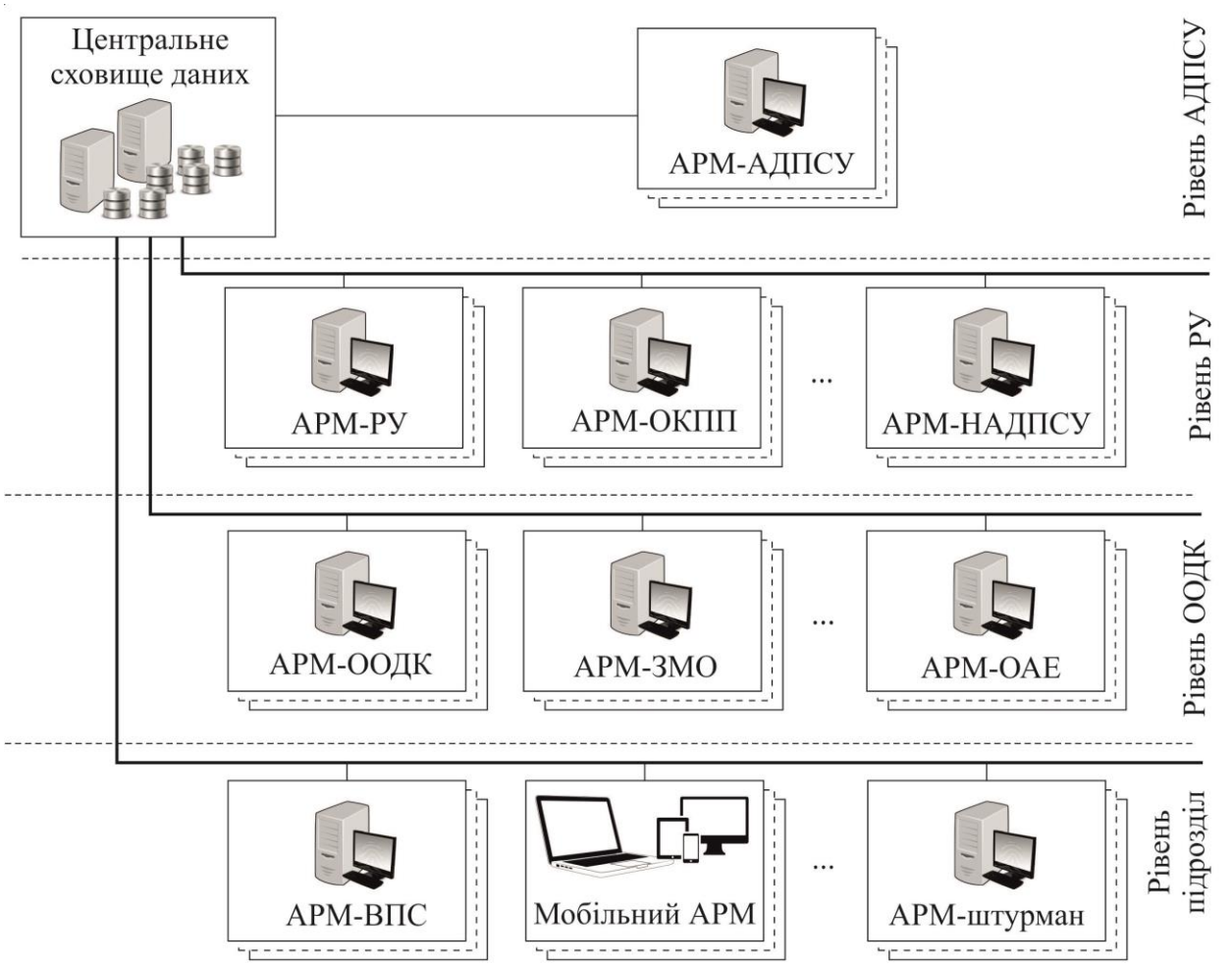


Рисунок 2.5 – Розподіл складових ІІС "Гарт" за рівнями автоматизації

Розгортання цифрової комунікаційної мережі Державної прикордонної служби здійснюється на основі запровадження сучасних засобів зв’язку, маршрутизаторів, комутаторів, передових технологій та IP- протоколів.

Основною і найважливішою складовою цифрової комунікаційної мережі Державної прикордонної служби України є центри та пункти комутації цифрових потоків. Центри комутації цифрових потоків розгортаються, як правило, у місцях найбільшого зосередження та розподілу цифрових потоків (тобто, на площах операторів зв’язку) що дозволяє:

– підвищити живучість системи зв’язку, зменшити імовірність відключення обладнання від мережі електроживлення в разі аварії або несплати за електроенергію;

– залишити існуючі лінії прив’язки до органів та підрозділів охорони кордону.

Пункти комутації цифрових потоків розгортаються в органах та підрозділах Державної прикордонної служби.

Структурою ІІС передбачено чотири рівні автоматизації: підрозділів, органів охорони кордону, регіональних управлінь, адміністрації Держприкордонслужби. Всі елементи ІІС на кожному рівні автоматизації взаємодіють з центральним елементом системи – ЦСД. Разом із тим, наявність великого числа ІС у складі відомчої системи передбачає автоматизацію практично всіх сфер діяльності ДПСУ. Враховуючи це, елементи ІІС використовує практично весь персонал прикордонного відомства, а інтеграція із суб’єктами інтегрованого управління кордонами розширює цей перелік до міжвідомчого масштабу.

Взаємодія ІІС "Гарт" з органами виконавчої влади здійснюється через ІТС "Аркан" [44], яка призначена для обміну даними при перетині державного кордону особами, транспортними засобами, вантажами. Адміністрація Держприкордонслужби є розпорядником зазначеної ІТС, суб’єктами якої є Державна фіскальна служба, Міністерство праці та соціальної політики України, Міністерство закордонної справ, силові відомства та інші зацікавлені органи виконавчої влади. Головною метою створення ІТС для взаємодії суб’єктів інтегрованого управління кордонами є достовірне та повне їх інформаційне забезпечення з питань недопущення в’їзду (виїзду) особам, яким згідно із законодавством не дозволяється в’їзд (виїзд) в (з) Україну [44]. Крім того, в інформаційному середовищі ІТС "Аркан" міститься інформація щодо втрачених (загублених, недійсних) документів, відомості про осіб, які перебувають у розшуку, відомості про викрадені транспортні засоби, тощо [45]. Використання цих даних сприяє виконанню завдань у сфері національної безпеки. Схема взаємодії із суб’єктами інтегрованого управління кордонами показана на рисунку 2.6.

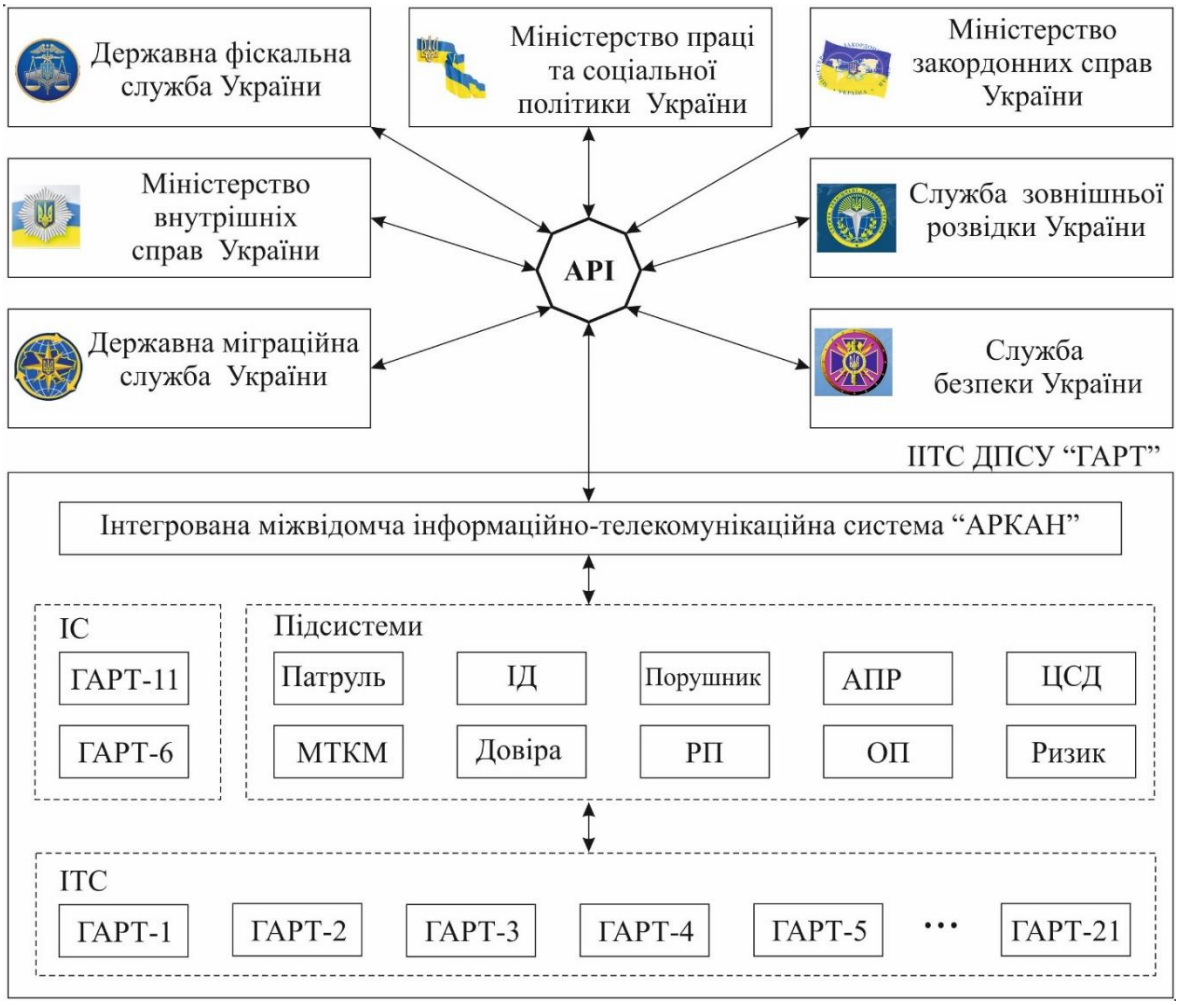


Рисунок 2.6 – Взаємодія із суб’єктами інтегрованого управління кордонами

Так, використання ІІС передбачено не тільки персоналом прикордонної служби для вирішення функціональних завдань відповідно до посад, а й співробітниками інших організації, які реалізують свої повноваження з питань інтегрованого управління кордонами у своїй повсякденній діяльності.

Інтегрована інформаційна система ДПСУ "Гарт" формується шляхом об’єднання інформаційних ресурсів інформаційних підсистем органів ДПСУ, які забезпечують надання інформації згідно з Переліком інформаційних ресурсів ІІС ДПСУ "Гарт".

Залежно від покладених на орган (підрозділ) охорони кордону функціональних завдань на автоматизованих робочих місцях ІС розгорнуто різне спеціальне програмне забезпечення. Як приклад розглянемо структуру інформаційної системи прикордонної служби "Гарт-3" (рисунок 2.7).

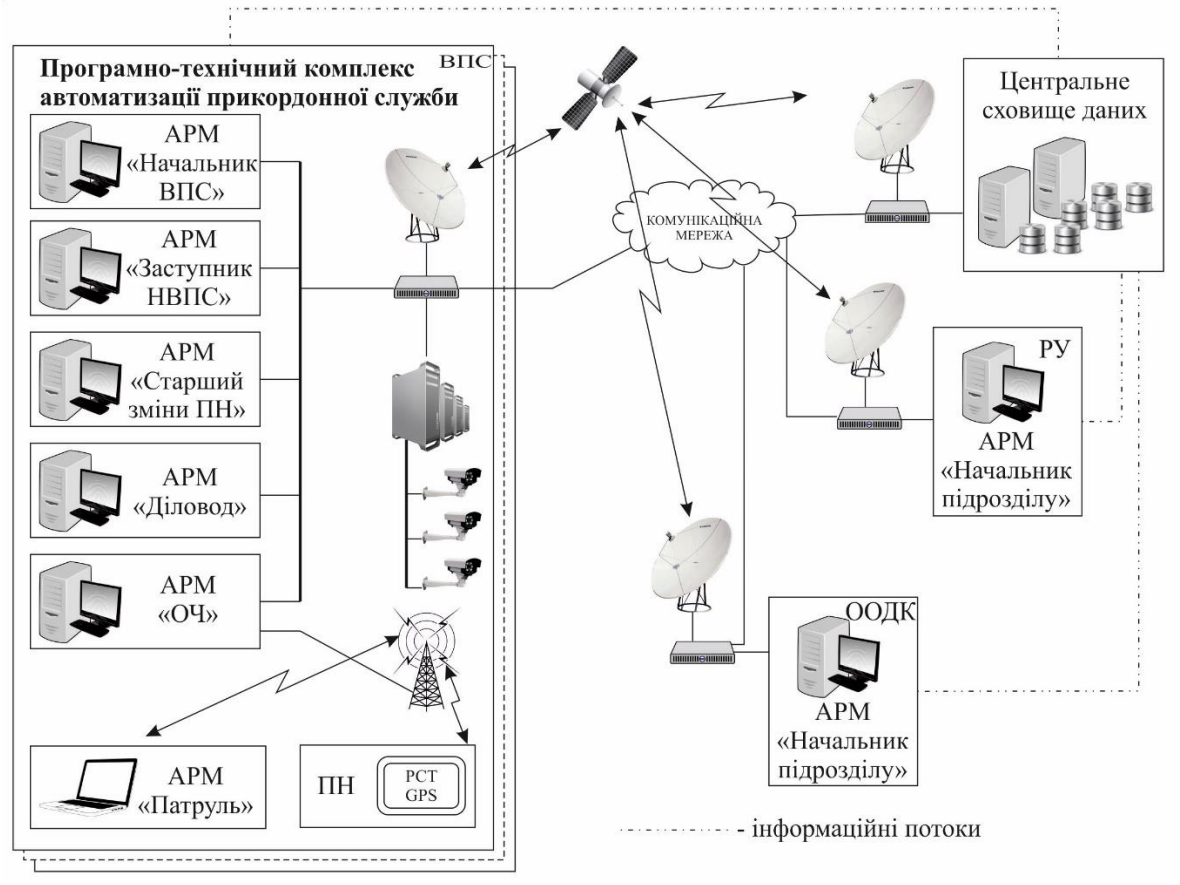


Рисунок 2.7 – Структура інформаційної системи "Гарт-3"

Аналіз структури ІС "Гарт 3" показав наявність інформаційних потоків з відділів прикордонної служби (ВПС) до всіх рівнів управління: АДПСУ, регіональних управлінь, органів охорони кордону [46, 47].

Розглянемо процес модернізації ІС "Гарт-3" як цілеспрямовану діяльність персоналу ДПСУ на заміну загального або спеціального програмного забезпечення, апаратного забезпечення або комплексного програмно-апаратного забезпечення протягом визначеного розпорядчими документами певного часу [48]. У роботі прийнято припущення про забезпечення функціональної безпеки окремо в старій та новій версіях програмно-апаратного забезпечення ІС. З огляду на це припущення розглянемо тільки період модернізації.

Під час модернізації ІС "Гарт-3" фахівцями відділу зв’язку, автоматизації та захисту інформації провадяться роботи із заміни програмних та (або) апаратних складових системи прикордонної служби. Процес

модернізації здійснюється в масштабах ДПСУ у кожному відділі прикордонної служби окремо та носить випадковий характер щодо конкретного часу модернізації конкретного АРМ. Виникає ситуація спільного функціонування старих і модернізованих АРМ та, відповідно, наявність інформаційних потоків старої та нової версій. На рисунку 2.8 показано варіант виникнення інформаційних потоків різних версій ІС.

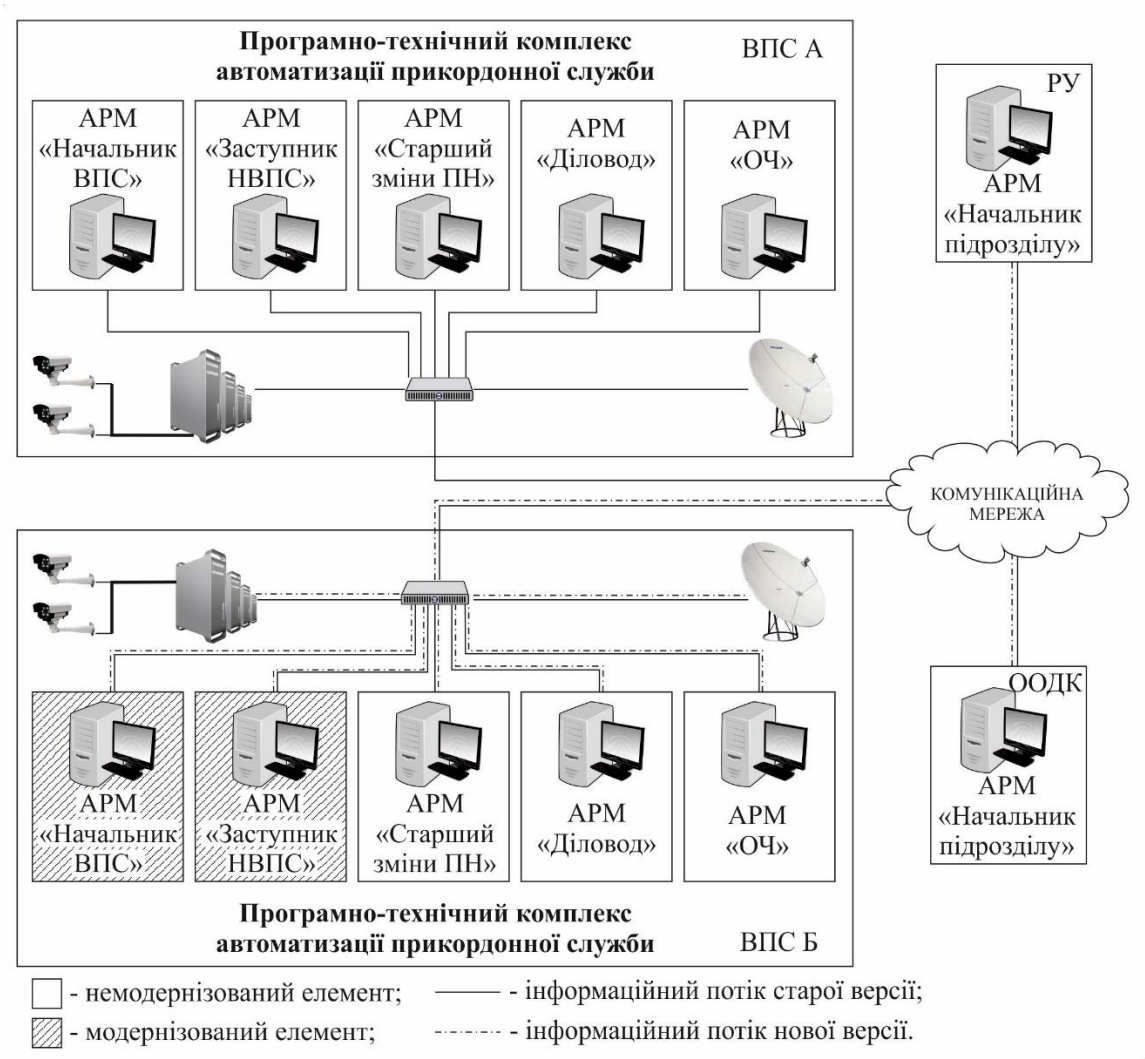


Рисунок 2.8 – Наявність інформаційних потоків різних версій в ІС (варіант)

Зазначені інформаційні потоки виникають як всередині програмно-технічних комплексів автоматизації прикордонної служби, так і між рівнями автоматизації.

Отже, при модернізації хоча б одного АРМ в ІС виникають змішані інформаційні потоки старих та нових версій. Причому, якщо при модернізації

нова версія СПЗ може враховувати формати та протоколи обміну старої версії, то в старій версії це принципово не можливо.

Основою ІС "Гарт-3" є програмно-технічні комплекси автоматизації прикордонної служби (ПТК АПС) "Гарт-3/П-В", що призначені для автоматизації процесів планування і контролю за оперативно-службовою діяльністю у відділах прикордонної служби Державної прикордонної служби України. АРМ вищих рівнів автоматизації виконують контролюючу функцію.

Структура та інформаційні потоки ІС "Гарт-3" не передбачають обмін даними між відділами прикордонної служби (ПТК АПС). Інформаційний потік здійснюється в основному в середині самого ПТК АПС та на верхні рівні автоматизації.

Однією із основних інформаційних систем прикордонного відомства є ІС прикордонного контролю "Гарт-1" (рисунок 2.9).

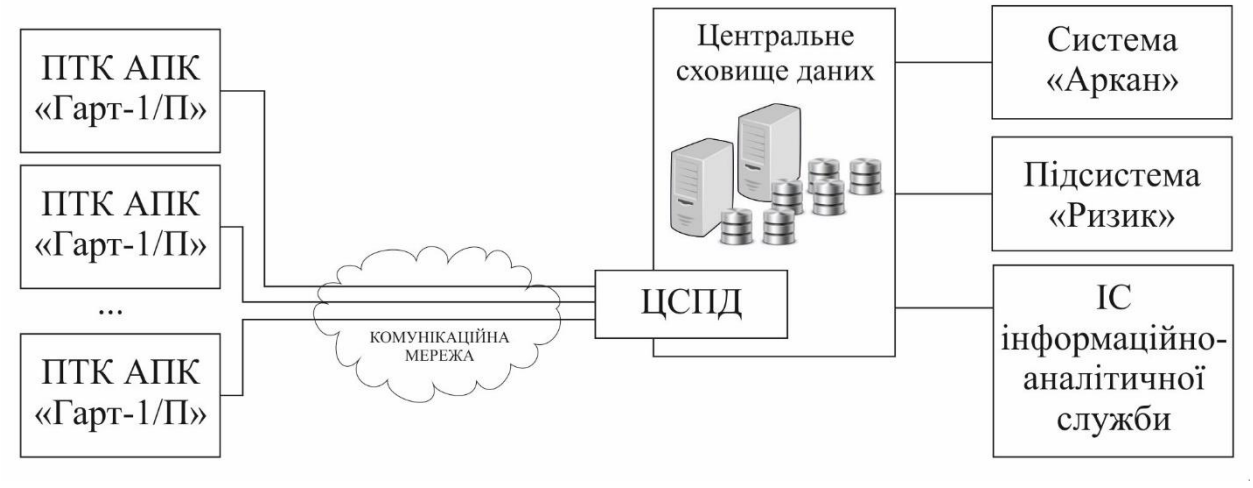


Рисунок 2.9 – Узагальнена структура ІС прикордонного контролю "Гарт-1"

Інформаційна прикордонного контролю "Гарт-1" призначена для скорочення часу на перевірку осіб та їх паспортних документів безпосередньо у пункті пропуску, а також підвищення якості прикордонного контролю [49–53]. Системою охоплено всі пункти пропуску та забезпечено обробку інформації щодо контролю осіб і транспортних засобів, які перетинають державний кордон України.

З цією метою на пунктах пропуску встановлено програмно-технічні комплекси автоматизації прикордонного контролю "Гарт-1/П", які додатково містять підсистеми відеоспостереження та електронного зчитування державних номерних знаків транспортних засобів (рисунок 2.10).

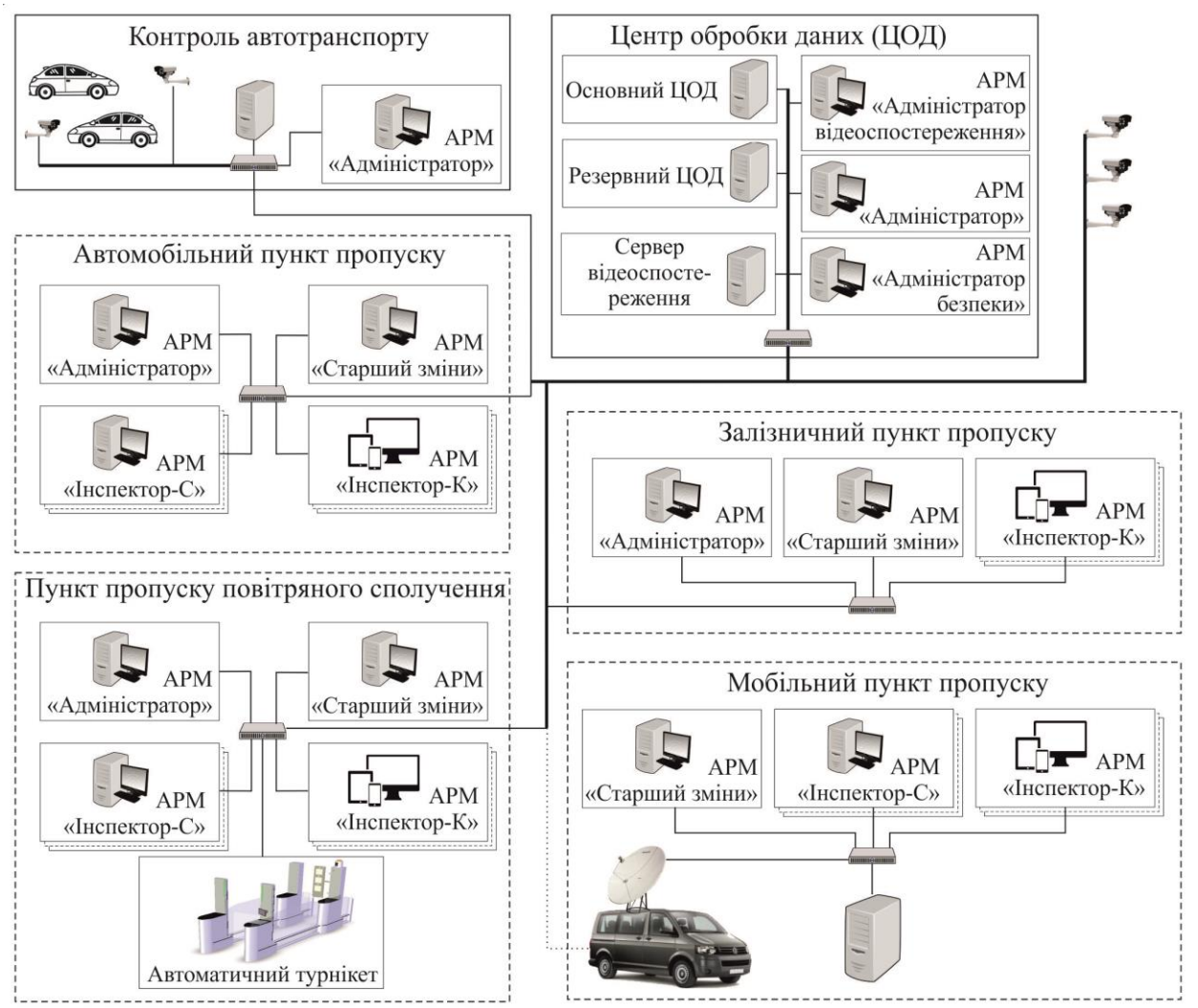


Рисунок 2.10 – Структура програмно-технічного комплексу автоматизації прикордонного контролю "Гарт-1"

Система може застосовуватись у міжнародних пунктах пропуску через державний кордон таких типів: пункти пропуску автомобільного сполучення; пункти пропуску повітряного сполучення; пункти пропуску морського (річкового) сполучення; пункти пропуску залізничного сполучення; пішохідні пункти пропуску.

З точки зору загальної структури програмно-технічні комплекси ІС "Гарт-1" інформаційно пов’язані через центральне сховище даних, на якому розгорнуто центральний сервер передачі даних (ЦСПД).

Обмін інформацією між центральним сховищем даних і ПТК АПК "Гарт-1/П" здійснюється за двома напрямами – "вгору" і "вниз". За напрямом "вниз" від ЦСПД до ПТК "Гарт-1/П" в пунктах пропуску передається інформація про доручення, нові класифікатори тощо. За напрямом "вгору" від ПТК "Гарт-1/П" до ЦСПД надходить інформація про оформлених осіб, транспортні засоби та ін.

З іншого боку, ЦСПД взаємодіє з центральним сховищем даних, в яке надходить інформація щодо постановки на облік, зняття з обліку та ін. Така побудова системи дає можливість автоматично здійснювати обмін інформацією між ЦСД, ЦСПД і ПТК "Гарт-1/П".

Інтегрована інформаційна система "Гарт" містить тільки дві ІС, які базуються на програмно-технічних комплексах, що суттєво відрізняються за основними інформаційними потоками. У програмно-технічних комплексах автоматизації прикордонної служби основні інформаційні потоки зосереджені в середині комплексу, інформація на верхні рівні автоматизації надходить періодично при збереженні даних в центральному сховищі. Разом із тим, в ПТК АПК основні інформаційні потоки зосереджені між АРМ, серверним обладнанням та центральним сховищем. Обмін інформації між АРМ всередині комплексу є не суттєвим.

Отже, ІІС "Гарт" містить ІС, які за структурою інформаційних потоків є односторонніми "знизу-вверх", двосторонніми. Крім того, окремі ІС взаємодіють між собою через центральне сховище даних.

На відміну від ІС прикордонного контрою та прикордонної служби, які у своєму складі містять програмно-технічні комплекси, ІС Морської охорони "Гарт-12" [54, 55] структурно складається тільки з АРМ підключених до комунікаційної системи ДПСУ та серверної частини, яка розгорнута в

центральному сховищі даних. Загальна структура ІС "Гарт-12" та її інформаційні потоки зображені на рисунку 2.11.

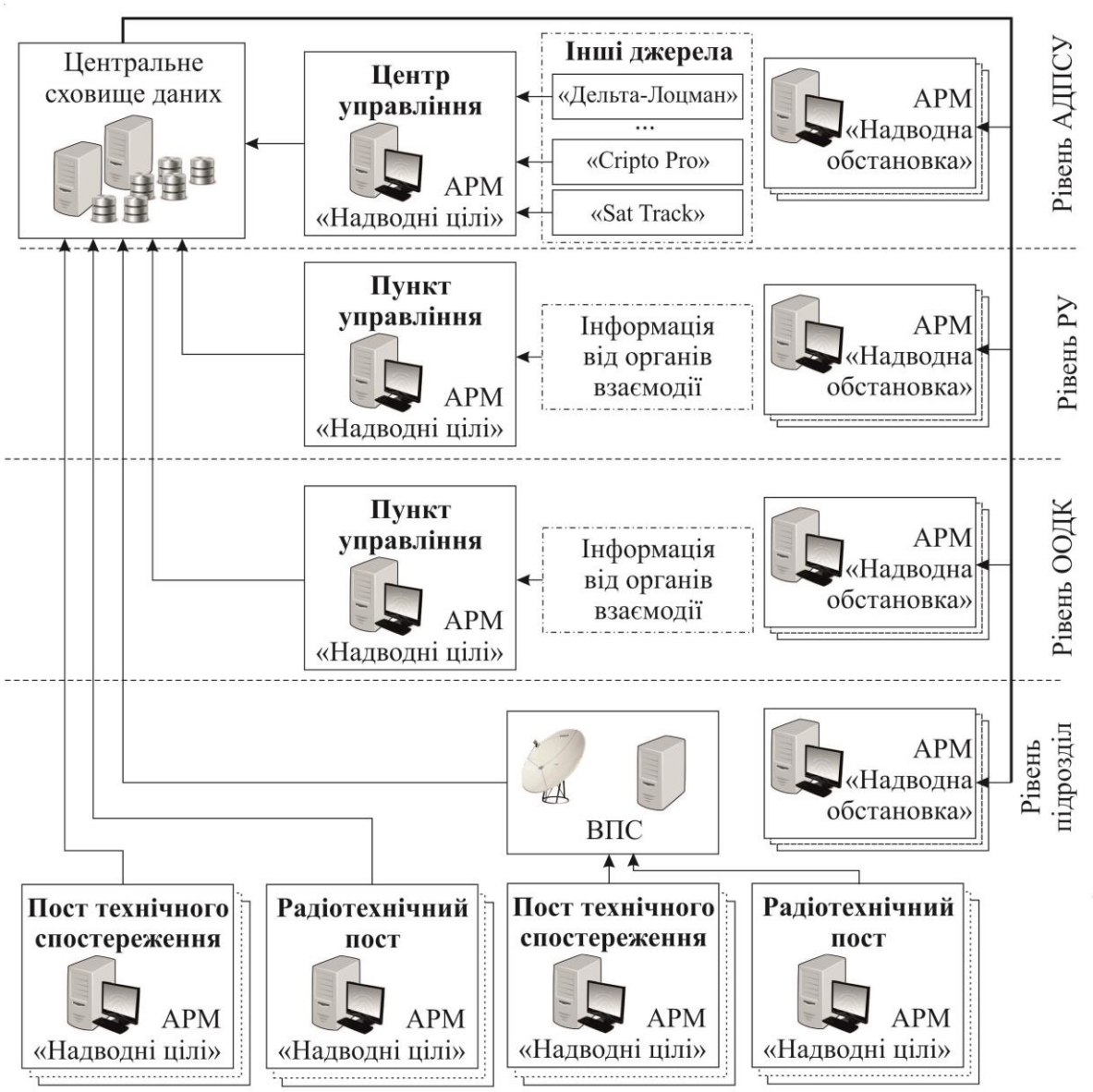


Рисунок 2.11 – Інформаційні потоки ІС "Гарт-12"

Головним завданням ІС "Гарт-12" є автоматизований збір облікових даних надводної обстановки з постів технічного спостереження за результатами візуального і радіолокаційного спостереження, а також роботи сучасних засобів автоматизованої ідентифікації. Разом із тим, система передбачає автоматизований та операторський збір облікових даних за результатами взаємодії з органами та організаціями на відповідних рівнях і формування на центральному рівні узагальнених достовірних та

несуперечливих даних про надводну обстановку. Користувачі ІС мають можливість отримати на базі електронної карти узагальнену інформацію про надводну обстановку на визначені рівні управління служби для прийняття відповідних управлінських рішень.

Інформаційна система Морської охорони обробляє та відображає інформацію про надводну обстановку, яка надходить з програмно-технічних та радіолокаційних засобів постів технічного спостереження Державної прикордонної служби, що розгорнуті уздовж узбережжя Чорного та Азовського морів, засобів, що встановлені на корабельно-катерному складі Морської охорони, інформаційних систем державних органів, які забезпечують контроль руху і безпеку судноплавства на водних шляхах. Це перша в Україні система висвітлення надводної обстановки, яка інтегрує дані про надводну обстановку від всіх доступних джерел і дозволяє контролювати пересування всіх суден у територіальному морі.

Окремі ІС прикордонного відомства використовують інші ІС як транспортну підсистему (рисунок 2.12).

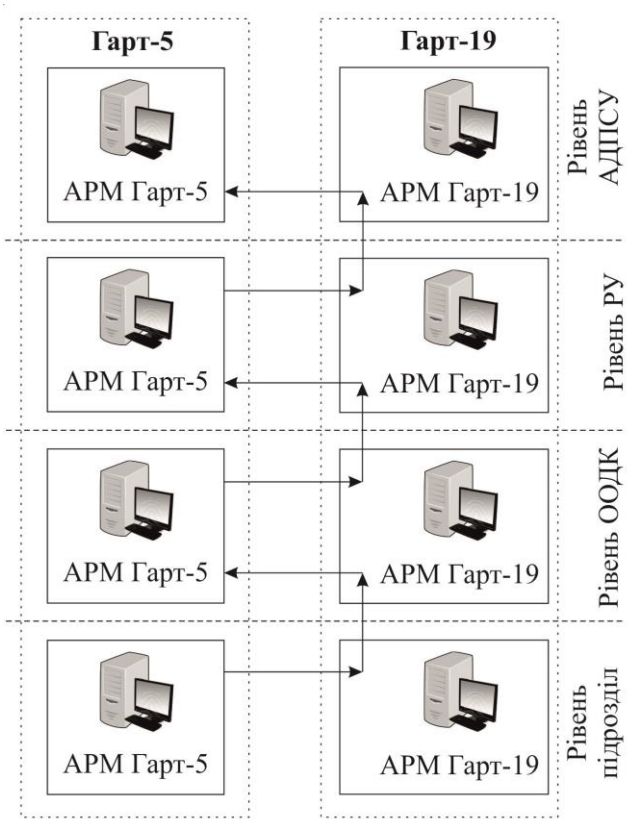


Рисунок 2.12 – Взаємодія ІС "Гарт-5" та ІС "Гарт-19"

Прикладом взаємодії обох систем є ІС "Гарт-5" інформаційно-аналітичної діяльності та ІС "Гарт-19" електронної пошти. Автоматизовані робочі місця персоналу інформаційно-аналітичного відділів пов’язані з АРМ "Гарт-19", що дозволяє здійснювати обмін інформацією між рівнями автоматизації.

Отже, наявні інформаційні потоки інформаційних систем та їх програмно-технічних комплексів здійснюються між рівнями автоматизації та всередині ПТК.

2.4 Метод визначення раціональної послідовності модернізації елементів інформаційної системи

Процес обміну інформації в інтегрованій інформаційній системі має сталий характер. При модернізації складових інтегрованої системи інформаційні потоки мають змішану структуру як нової, так і старої версії програмно-апаратного забезпечення. Модернізація апаратного забезпечення пов’язана із типом системного програмного забезпечення та із спеціальним програмним забезпеченням.

При модернізації апаратного забезпечення, яке сумісне за фізичними принципами та протоколами взаємодії із попередньою версією, характеристики інформаційних потоків не змінюються. Це пов’язано із тим, що джерелом інформаційних потоків є спеціальне програмне забезпечення ІС. Невідповідність версій СПЗ на елементах ІС може призвести до їх некоректного функціонування, що є порушенням функціональної безпеки ІС в цілому.

При розробці методу визначення раціональної послідовності модернізації елементів ІС під порушенням властивостей елементу ІС розуміється його некоректне функціонування, що викликане невідповідністю версій СПЗ. З метою деталізації характеристик визначеного поняття можна використати наведену в роботі [55] класифікацію властивостей інформаційних систем, а саме конфіденційність, доступність та цілісність

інформаційних ресурсів інформаційної системи. Під час застосування методу ймовірність порушення властивостей елементу ІС може визначатись окремо за кожною властивістю ІС або комплексно, залежно від особливостей функціонування інформаційної системи.

2.4.1 Модель інформаційних потоків інформаційної системи на стадії модернізації. На стадії модернізації програмного забезпечення здійснюється зміна структури та (або) кількості даних, що надходить до інших елементів ІІС. Так, під час заміни СПЗ можливий негативний вплив такого дестабілізаційного фактору, як невідповідність версій інформаційних потоків.

В попередньому підрозділі наведені структури типових інформаційних систем та їх інформаційні потоки. На окремих інформаційних системах (Гарт-1, Гарт-3) на четвертому рівні автоматизації з метою підвищення надійності даних, зокрема доступності інформації, розгорнуті програмно-технічні комплекси, які є за своєю суттю локальними представленнями (реплікацією з точки зору даних) інформації, яка міститься в центральному сховищі даних.

Автоматизовані робочі місця програмно-технічних комплексів взаємодіють тільки із локальними серверами (основними та резервними), а система передачі даних забезпечує синхронізацію даних із центральним сховищем даних. Таке рішення забезпечує певну автономність функціонування програмно-технічних комплексів, що в умовах, як правило, нестабільного зв’язку з підрозділами охорони кордону (відділами прикордонної служби, пунктами пропуску, контрольними постами в’їзду-виїзду) які дислокуються переважно у віддалених районах, є раціональним рішенням.

Аналіз інформаційних систем прикордонного відомства дозволив сформувати їх узагальнену структуру (рисунок 2.13).

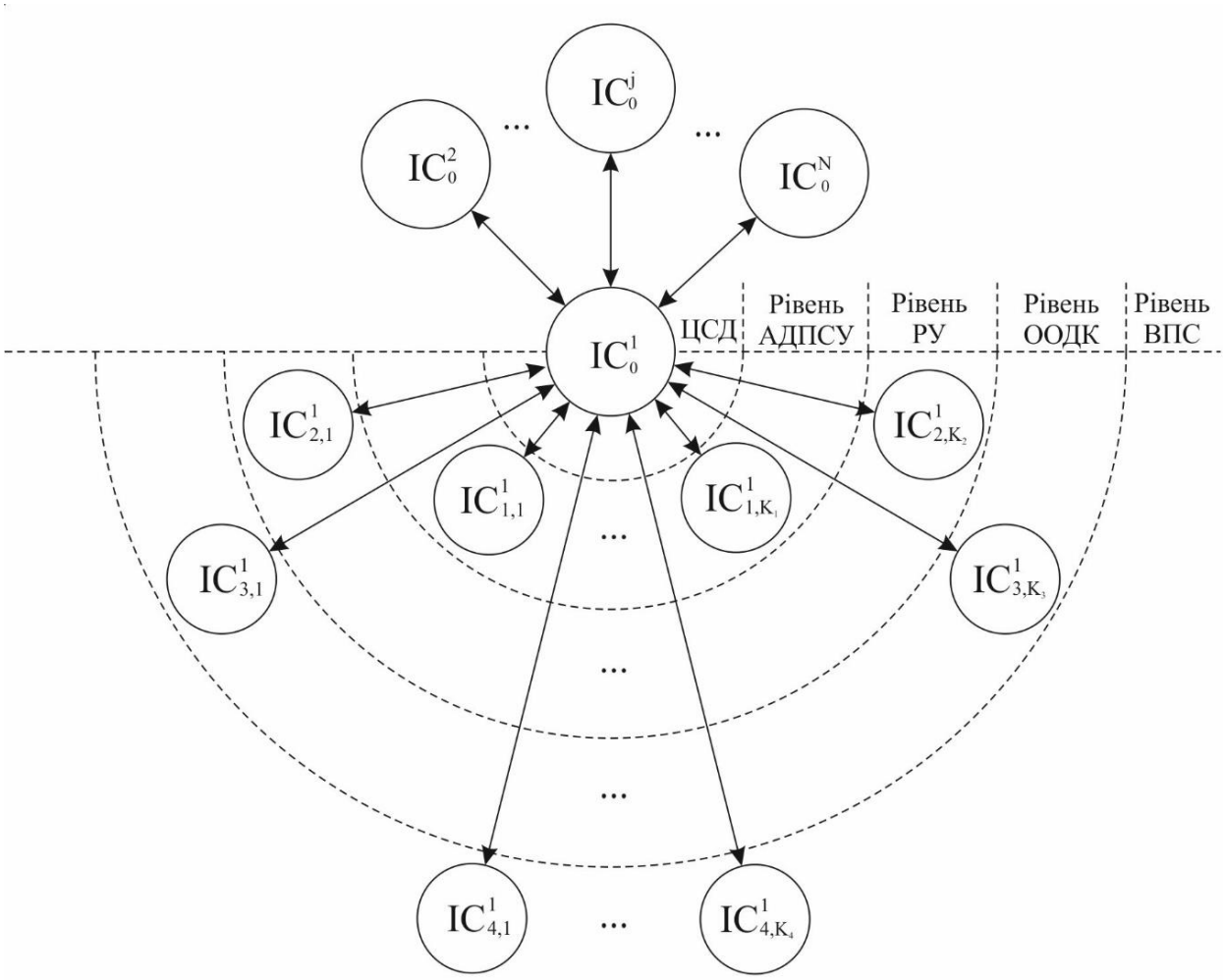


Рисунок 2.13 – Узагальнена структура інформаційних систем в ІІС

На рисунку 2.13 представлена взаємодія першої ІС з рештою N інформаційних систем прикордонного відомства. Порядок ІС та призначення порядкових номерів є довільним та може застосовуватись до кожної із систем залежно від потреби. На кожному рівні автоматизації знаходиться K_i автоматизованих робочих місць, де i–індекс рівня автоматизації (1 – рівень АДПСУ, 4 – рівень підрозділу).

Аналіз узагальненої структури інформаційних потоків в ІІС дозволяє в кожному конкретному випадку щодо певної ІС, подати інші інформаційні системи (підсистеми) як агреговані автоматизовані місця системи, що розглядається. Такий підхід ґрунтується на терміні "чорної скриньки" [56, 57] як об’єкта про принцип роботи якого нічого не відомо, крім відповідності

вхідного сигналу вихідному. Це дозволить абстрагуватись від конкретної реалізації інших ІС та спростити аналітичний опис моделі.

Разом із тим, наявність різних рівнів автоматизації не змінює топологічну структуру інформаційних потоків, що дозволяє розглядати всі АРМ як рівноправні, тобто такі, які не впливають один на одного безпосередньо, але з власними значеннями величин інформаційних потоків. Обмін даними між АРМ здійснюється через складову ІС, яка розгорнута в центральному сховищі даних.

Так, до моделі інформаційних потоків ІС на стадії модернізації входять дві групи елементів: центральний елемент (E_0) та периферійні елементи ($E_i, i = \overline{1, K}$), що представлені автоматизованими робочими місцями, взаємодіючими ІС та підсистемами. Елементи з'єднані один з одним за топологією "зірка" (рисунок 2.14). Між елементами моделі (центральним та периферійними елементами) здійснюється інформаційний потік величиною $\lambda_{i,j}$, де $i, j = \overline{0, K}$. Ймовірність порушення властивостей j елементу ІС при отриманні даних від i-го елементу при невідповідності версій спеціального програмного забезпечення визначається через $P_{i,j}$, де $i, j = \overline{0, K}$.

У моделі передбачається взаємодія елементу ІС із центральним вузлом та інформаційний обмін між елементами системи через центральний вузол. Наведена модель відповідає структурі інформаційних потоків ІС прикордонного відомства та процесу взаємодії автоматизованих робочих місць через підсистему, яка розгорнута в центральному сховищі даних.

Враховуючи, що всі ІС прикордонного відомства побудовані за клієнт-серверною технологією, розмірність величини інформаційного потоку $\lambda_{i,j}$ між елементами моделі приймемо як кількість запитів за одиницю часу.

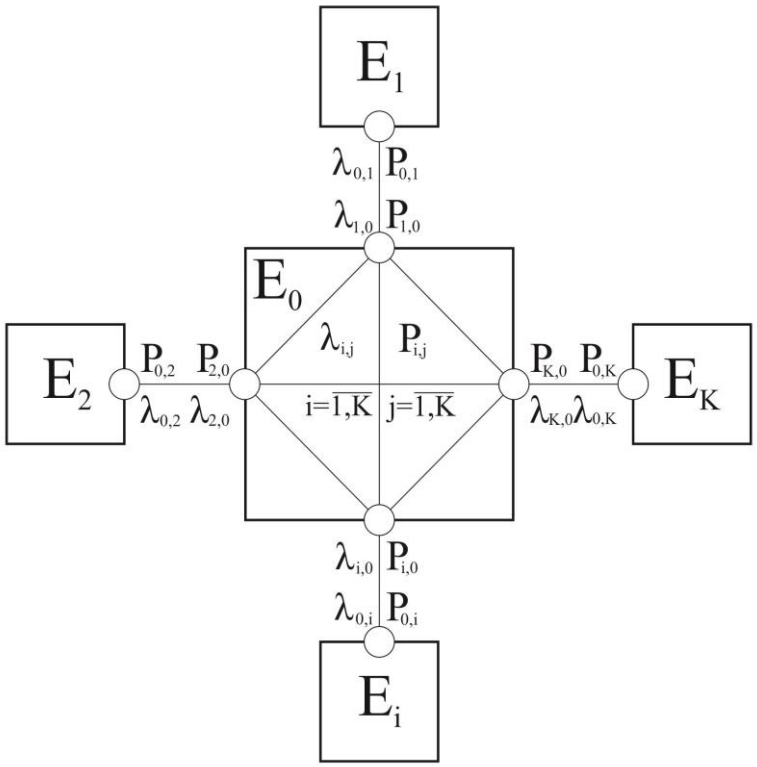


Рисунок 2.14 – Модель інформаційних потоків ІС на стадії модернізації

Ймовірність порушення властивостей елементу ІС при здійсненні однієї операції запит-відповідь від іншого елементу системи (рисунок 2.15) залежить від ймовірностей модернізації взаємодіючих елементів $P_i^m(t)$, $P_j^m(t)$ та ймовірності порушення властивостей елементу ІС при невідповідності версій спеціального програмного забезпечення $P_{i,j}$.

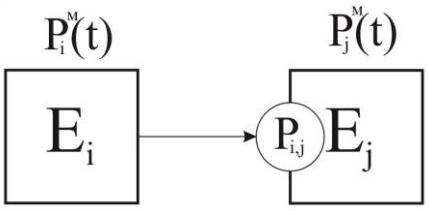


Рисунок 2.15 – До визначення ймовірності порушення властивостей елементу інформаційної системи

Отже, ймовірність порушення властивостей елементу ІС при отриманні даних з іншого елементу становить

$$P_{i,j}^{*}(t) = P_i^m(t) \cdot \left(1 - P_j^m(t)\right) \cdot P_{i,j}\,. \qquad (2.1)$$

У функціональній залежності (2.1) прийнято припущення, що порушення властивостей елементу ІС здійснюється тільки за умови наявності інформаційного потоку від нової версії СПЗ до старої.

В іншому випадку порушення властивостей елементу ІС не здійснюється з причини узгодженості нової версії СПЗ. За потреби зміни форматів даних чи інших причин невідповідності різних версій СПЗ модернізацію можна здійснити за допомогою проміжної версії з дотриманням припущення в (2.1).

Ймовірність порушення властивостей елементу ІС при отриманні хоча б одного блоку даних протягом терміну t при взаємодії з j-м елементом визначається функціональною залежністю

$$P_{i,j}^{E}(t) = 1 - \left(1 - P_{i,j}^{*}(t)\right)^{k_{i,j}(t)}, \qquad (2.2)$$

де $k_{i,j}(t)$ – кількість запитів від i-го до j-го елементу за час t модернізації ІС.

Кількість запитів (блоків даних) від i-го елементу до j-го за час t модернізації ІС визначається як

$$k_{i,j}(t) = \lambda_{i,j} t\,. \qquad (2.3)$$

Тоді ймовірність порушення властивостей елементу ІС протягом терміну t при модернізації ІС на її окремому елементі $P_i^E(t)$ при взаємодії із рештою складових визначається функціональною залежністю

$$P_i^E(t) = 1 - \prod_{j=0}^{K} \left[1 - P_{j,i}^{E}(t)\right]. \qquad (2.4)$$

Ймовірність модернізації елементу ІС змінюється за експоненційним законом (додаток В), функція розподілу якого має вигляд

$$P_i^m(t) = 1 - e^{-\mu_i t}, \tag{2.5}$$

де μ_i – параметр швидкості здійснення модернізації *i*-го елементу ІС.

Аналіз динаміки зміни ймовірності порушення властивостей одного елементу ІС (рисунок 2.16) показав наявність двох фаз: фази зростання та спадання. Причому, швидкість зростання ймовірності порушення властивостей більша за швидкість спадання.

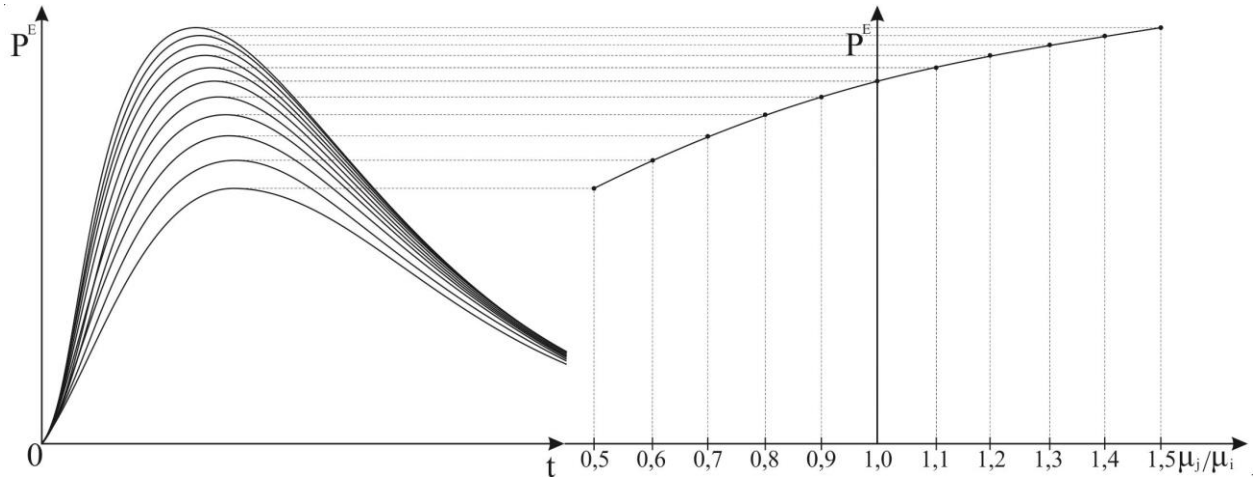


Рисунок 2.16 – Динаміка зміни ймовірності порушення надійності даних на одному елементі ІС

Динаміка зміни екстремумів функції (2.2) при різних співвідношеннях параметрів швидкостей здійснення модернізації взаємодіючих елементів ІС μ_j / μ_i має логарифмічну складову. З метою визначення екстремуму (2.2) визначимо часткову похідну за параметром часу [58], а саме:

$$\frac{\partial P_{i,j}^{E}(t)}{\partial t} = -\left(1 - P_{i,j} e^{-\mu_i t}\left(1 - e^{-\mu_j}\right)\right)^{\lambda_{i,j} t} \times$$
$$\times \left(\begin{array}{l} \lambda_{i,j} \ln\left(1 - P_{i,j} e^{-\mu_i t}\left(1 - e^{-\mu_j}\right)\right) + \\ + \dfrac{\lambda_{i,j} t\left(\mu_i P_{i,j} e^{-\mu_i t}\left(1 - e^{-\mu_j}\right) - \mu_j P_{i,j} e^{-t(\mu_i + \mu_j)}\right)}{1 - P_{i,j} e^{-\mu_i t}\left(1 - e^{-\mu_j}\right)} \end{array} \right). \qquad (2.6)$$

Зазначимо, що всі складові функціональної залежності (2.6) більші нуля, тому перша частина не може бути рівною нулю. Так, для виконання умови рівності (2.6) нулю достатньо:

$$-\lambda_{i,j} \ln\left(1 - P_{i,j} e^{-\mu_i t}\left(1 - e^{-\mu_j}\right)\right) = \frac{\lambda_{i,j} t\left(\mu_i P_{i,j} e^{-\mu_i t}\left(1 - e^{-\mu_j}\right) - \mu_j P_{i,j} e^{-t(\mu_i + \mu_j)}\right)}{1 - P_{i,j} e^{-\mu_i t}\left(1 - e^{-\mu_j}\right)}. \qquad (2.7)$$

За співвідношенням (2.7) визначається час, коли буде досягнуто максимальне значення ймовірності порушення властивостей елементу ІС, що дозволить організаційними засобами раціоналізувати процес модернізації.

Враховуючи (2.4), визначимо ймовірність порушення властивостей ІС в цілому

$$P^{IC}(t) = 1 - \prod_{i=0}^{K}\left[1 - P_i^{E}(t)\right], \qquad (2.8)$$

Динаміка зміни ймовірності порушення властивостей ІС на одному елементі ІС показала тенденцію до її зниження при збільшенні швидкості оновлення елементу, на який надходять дані відносно іншого елементу. Таким чином, організаційними заходами щодо порядку модернізації можливо знизити порушення властивостей ІС.

Для врахування поетапного процесу модернізації модифікуємо (2.5) наступним чином:

$$P_i^m(t,t_i^b)=\begin{cases}0, t<t_i^b\\ 1-e^{-\mu_i\left(t-t_i^b\right)}, t\geq t_i^b\end{cases}, \quad (2.9)$$

де μ_i – параметр швидкості здійснення модернізації *i*-го елементу ІС;

t_i^b – час початку проведення модернізації.

Враховуючи (2.9), функціональна залежність (2.1) прийме вигляд:

$$P_{i,j}^*(t)=\left(1-P_i^m\left(t,t_i^b\right)\right)\cdot P_j^m\left(t,t_i^b\right)\cdot P_{i,j}. \quad (2.10)$$

Цей принцип модернізації зменшує ймовірність порушення властивостей елементу ІС, викликаних невідповідностями версій СПЗ (рисунок 2.17).

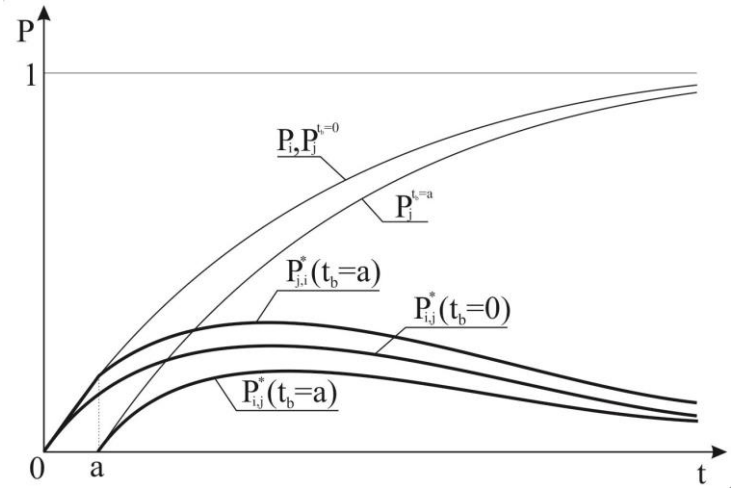


Рисунок 2.17 – Зміна ймовірності порушення властивостей елементу ІС залежно від послідовності модернізації елементів

Зміна послідовності модернізації призводить до збільшення ймовірності порушення властивостей ІС. Основним принципом послідовності модернізації елементів ІС, який знижує ймовірність порушення властивостей ІС, є модернізація за величиною вихідного потоку та ймовірності порушення властивостей елементу ІС при невідповідності версій СПЗ. При однаковій ймовірності порушення властивостей елементу ІС з

причини невідповідності версій СПЗ серед двох елементів модернізується перший той, в кого вхідний потік менший.

2.4.2 Обґрунтування показників ефективності процесу модернізації. Процес модернізації будь-якої ІС можливо здійснювати декількома шляхами. Перший. Повна зупинка функціонування ІС та здійснення заміни визначених програмних елементів з подальшим введенням в експлуатацію зазначеної системи. Цей спосіб з точки зору функціональної безпеки є найбільш раціональним. В даному випадку взагалі виключена можливість реалізації загроз, викликаних процесом модернізації. Водночас застосування першого підходу можливе тільки на невеликих системах та й на таких, які не мають вимоги функціонування в режимі реального часу. Як правило, вимогою до переважної більшості інформаційних систем та підсистем ІІС прикордонного відомства є цілодобове функціонування. Навіть невеликий збій може призвести до непоправних збитків національного масштабу. Територіальна розподіленість елементів окремих ІС та достатньо велика їх кількість при застосуванні першого підходу вимагатиме досить значного часу на проведення модернізації. Використання такого підходу в ДПСУ є неприпустимим.

Другий підхід передбачає модернізацію ІС в процесі її функціонування. У цьому випадку можливе порушення властивостей ІС і, в свою чергу, функціональної безпеки, оскільки з’являються додаткові дестабілізаційні фактори, викликані невідповідністю версій СПЗ. Отже, головним чинником, який визначатиме ефективність процесу модернізації, є максимально можливе зменшення ймовірності порушення властивостей ІС. Разом із тим, варто зазначити, що модернізація ІС це процес, який має певну тривалість та не може бути описаний окремими точковими показниками поза межами часу.

Визначимо основні показники, які характеризують ефективність процесу модернізації: $P_M(t)$ – ймовірність порушення властивостей ІС; t_M – загальний час модернізації.

Різні варіанти модернізації можна порівняти за загальним часом модернізації, але в більшості випадків він задається директивно та не відображає величину порушення властивостей ІС. Отже, цей показник може бути тільки як допоміжний у випадку рівності інших показників. З іншого боку порівнювати різні варіанти послідовності модернізації елементів ІС за миттєвим значенням ймовірності порушення властивостей ІС є неможливим з причини її зміни протягом всього терміну модернізації.

Вищенаведене вимагає використання інтегрованих показників, що характеризують весь процес модернізації. Одним із показників такого типу є максимально можливе значення ймовірності порушення властивостей ІС в процесі модернізації

$$P_M^{\max} = \max_{0 \le t \le t_M} \left(P_M(t) \right). \tag{2.11}$$

Перевагою цього показника є можливість визначення допустимого значення ймовірності порушення ІС на стадії модернізації.

Наступним показником, який характеризує ефективність процесу модернізації, є середнє значення ймовірності порушення властивостей ІС в процесі модернізації.

В інтегральній формі

$$P_M^{mid} = \frac{1}{t_M} \int_0^{t_M} P_M(t) dt \tag{2.12}$$

У дискретній формі

$$P_M^{mid} = \frac{1}{N} \sum_{i=1}^{N} P_M(t_i) \tag{2.13}$$

де N – кількість інтервалів вимірювання значення ймовірності.

Такий показник доцільно застосовувати при забезпеченні якомога меншого значення ймовірності порушення властивостей ІС під час

модернізації. Вибір показника ефективності залежить від способу застосування ІС та процесу її модернізації.

Наступним показником ефективності процесу модернізації може бути середньозважене значення ймовірності порушення властивостей ІС.

В інтегральній формі

$$P_M^w = \frac{1}{t_M} \int_0^{t_M} f^w(t) P_M(t) dt, \tag{2.14}$$

де $f^w(t)$ – функція ваги.

За умови, що

$$\int_0^{t_M} f^w(t) dt = 1. \tag{2.15}$$

У дискретній формі

$$P_M^w = \frac{1}{N} \sum_{i=1}^{N} f^w(t_i) P_M(t_i). \tag{2.16}$$

За умови, що

$$\sum_{i=1}^{N} f^w(t_i) = 1. \tag{2.17}$$

Пріоритетним показником ефективності процесу модернізації є максимальне значення ймовірності порушення властивостей ІС в процесі модернізації. Чим менше цей показник, тим ефективніше провадиться заміна СПЗ на елементах ІС. При рівності значень цього показника в різних варіантах модернізації доцільно застосувати другий або третій показники.

2.4.3 Структура методу визначення раціональної послідовності модернізації елементів інформаційної системи. Для прийняття рішення на основі інформації, яка обробляється в системах реального часу, ключовим аспектом є своєчасність і достовірність виконання запиту користувача. На стадії модернізації ІС можливе виникнення порушення її властивостей викликане невідповідністю версій СПЗ. У попередньому розділі на підставі

побудованих моделей з'ясовані основні принципи послідовності модернізації, які сприяють зменшенню значення ймовірності порушення властивостей ІС, а також визначені показники ефективності процесу модернізації. Забезпечення виконання наведених підходів вимагає розробки методу визначення послідовності модернізації елементів ІС.

Структура наявних локальних мереж, на базі яких розгортаються програмно-технічні комплекси ІС ДПСУ, як правило, визначена та представляє собою топологію "зірка". Таке обмеження не є обов'язковим, структура інших ІС може бути довільною.

Отже, метою розробки методу є раціоналізація процесу модернізації елементів ІС довільної структури за обраною стратегією модернізації.

Вихідними даними методу визначення послідовності модернізації елементів ІС є:

$E = \{E_i\}$ – множина елементів ІС, де $i = \overline{0, K}$;

$\Lambda = \lfloor \lambda_{i,j} \rfloor$ – матриця величин інформаційних потоків між елементами ІС;

$P^v = \{P_{i,j}\}$ – матриця ймовірностей порушення властивостей елементів ІС під час обміну між ними при невідповідності версій спеціального програмного забезпечення.

Загалом, визначення раціональної послідовності можливе шляхом повного перебору варіантів перестановок множини елементів ІС, кількість яких становить $N = |E|!$. Зазначимо, що окремі ІС прикордонного відомства містять тисячі елементів, тому вирішення цієї проблеми таким підходом при існуючих обчислювальних потужностях є неможливим. Визначення раціональної послідовності будемо здійснювати за допомогою загального алгоритмічного підходу – методу гілок та меж.

Першим етапом методу є визначення часу початку проведення модернізації i-го елементу. Разом із тим, структура та особливості інформаційних потоків окремих ІС можуть передбачати ізоляцію окремих

елементів один від одного з причини відсутності впливу дестабілізаційних факторів модернізації. Тобто обмін між елементами здійснюється, але ймовірність порушення властивостей ІС, викликаних стадією модернізації відсутня. Це дозволить здійснювати модернізацію таких елементів у будь-який момент протягом терміну модернізації.

З метою зменшення часу модернізації такі елементи об'єднаємо в групи із загальним часом початку проведення модернізації. Так, послідовність модернізації задається параметром t_k^b часу початку проведення модернізації елементів k-ї групи. Значення даного параметру визначається через величину ймовірності того, що елемент буде модернізовано за даний час та параметру швидкості модернізації. Час початку модернізації початкової елементу (групи) становить $t_0^b = 0$. Час початку модернізації для елементів будь-якої групи становитиме максимальний час з елементів попередньої групи модернізації. Визначимо час, при якому елемент ІС e_i буде модернізовано з ймовірністю P^b

$$t_i^b = -\frac{\ln\left(1 - P^b\right)}{\mu_i}. \tag{2.18}$$

Таким чином, час початку модернізації для будь-якої групи становитиме

$$t_k^b = t_{k-1}^b + \max\left(t_i^b\right), t_i^b \in M_{k-1}, k > 0. \tag{2.19}$$

Другим етапом методу є побудова матриці величин ймовірностей порушення властивостей складових ІС $\Xi = \left\lfloor \xi_{i,j} \right\rfloor$ при заданому інформаційному потоці $\lambda_{i,j}$ за одиницю часу, де $j = \overline{0, K}$.

Елемент $\xi_{i,j}$ розраховується так:

$$\xi_{i,j} = 1 - \left(1 - P_{i,j}\right)^{\lambda_{i,j}}. \quad (2.20)$$

Фізичним сенсом функціональної залежності (2.20) є ймовірність порушення властивостей j елементу ІС при здійсненні інформаційного обміну з i елементом ІС із заданою інтенсивністю за одиницю часу.

Третім етапом методу є побудова матриці суміжностей навантаженого графу функцією (2.20) $A = \lfloor a_{i,j} \rfloor$, де елемент $a_{i,j}$ формується наступним чином:

$$a_{i,j} = \begin{cases} 1, \xi_{i,j} > 0 \\ 0, \xi_{i,j} = 0 \end{cases}, \quad (2.21)$$

Четвертим етапом методу є формування списку послідовності модернізації вузлів ІС, які не здійснюють дестабілізаційного впливу на інші елементи. Принцип побудови такого списку полягає у почерговому видаленні вузлів графу, представленого матрицею $A = \lfloor a_{i,j} \rfloor$, у яких напівстепінь виходу

$$dev^{+}\left(e_i\right) = 0, \quad (2.22)$$

де e_i – вершина графу.

Умова (2.22) означає відсутність дуг, що виходять із вузла, тобто на елементі ІС в переважній більшості буде здійснено порушення властивостей чим на іншому пов’язаному елементі. При наявності у графі декількох вузлів, для яких виконується умова (2.22), обирається вузол, сумарне значення ймовірностей для якого максимальне, а саме:

$$e_i = \arg\max_{j} \left(\sum_{\forall j} a_{j,i} \xi_{j,i} \right). \quad (2.23)$$

Причому, зазначені вузли об’єднується в групу $M_0 = \{e_i^0\}$, де 0 – індекс ітерації (групи). Це дозволить надалі раціоналізувати процедуру модернізації за критерієм мінімізації часу шляхом паралельного оновлення СПЗ в усіх органах та підрозділах охорони кордону елементів, які належать одній групі.

П’ятим етапом методу є формування уточненої матриці величин ймовірностей порушення надійності ІС між елементами ІС, в яких видалені вузли, які об’єднані в групу $M_0 = \{e_i^0\}$, а саме $E' = E \setminus M_0$. Ця операція дозволить зменшити обсяг розрахунків, які будуть проводитись в наступних етапах.

В загальному випадку, наявність вершин у графі, в яких виконується умова (2.22), не є обов’язковою. Це можливо при наявності циклів у графі, тобто взаємного впливу різних версій СПЗ один на одного. Для пошуку оптимальної за визначеним критерієм послідовності модернізації на шостому етапі використовується метод гілок та меж [59–62], де поточне значення ймовірності порушення даних в ІС обраної послідовності модернізації являє собою нижню межу для відхилення від розгляду решти "гілок дерева" перестановки. Загальна структурна модель методу визначення послідовності модернізації елементів ІС зображена на рисунку 2.18.

Основними складовими методу гілок та меж є формування двох процедур [63]: знаходження нижньої оцінки (нижню межу значення ймовірності порушення властивостей ІС) та розгалуження (формування дерева перестановок). Формування процедури знаходження нижньої оцінки здійснюється відповідно до функціональної залежності (2.8).

Разом із тим, необхідно здійснити доказ відсутності значень ймовірності нижчої, чим задана, а саме довести, що додавання у послідовність модернізації наступних елементів не призводить до зниження ймовірності порушення властивостей ІС, тобто що виконується нерівність

$$1-\prod_{i=0}^{K_1}\left[1-P_i^E(t)\right] \le 1-\prod_{i=0}^{K_2}\left[1-P_i^E(t)\right], \text{при } K_1 < K_2 . \qquad (2.24)$$

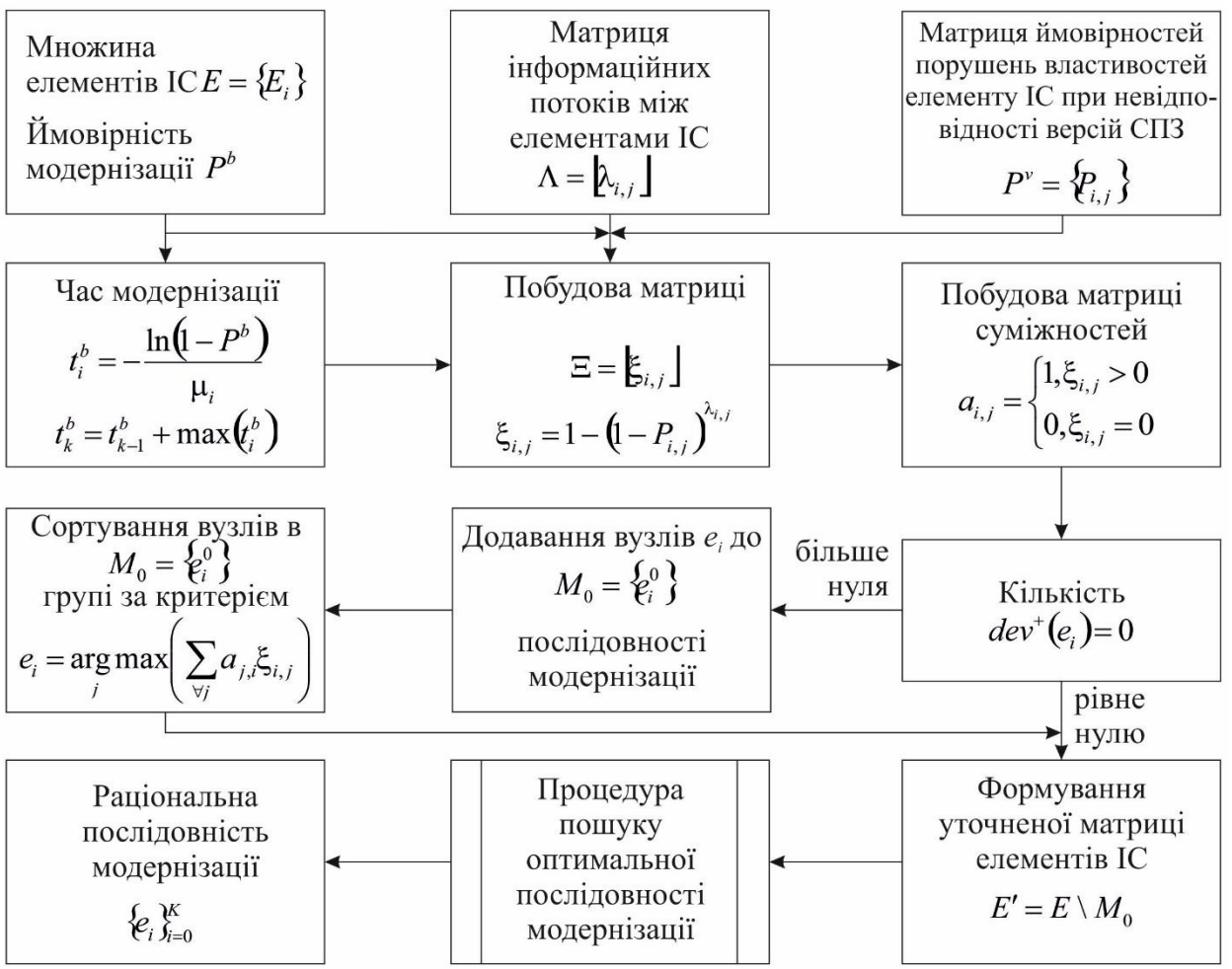


Рисунок 2.18 – Структурна схема методу визначення послідовності модернізації елементів ІС

Після декількох перетворень (2.19) отримаємо

$$\prod_{i=0}^{K_1}\left[1-P_i^E(t)\right] \geq \prod_{i=0}^{K_1}\left[1-P_i^E(t)\right]\prod_{i=K_1+1}^{K_2}\left[1-P_i^E(t)\right], \qquad (2.25)$$

у свою чергу призводить до нерівності

$$\prod_{i=K_1+1}^{K_2}\left[1-P_i^E(t)\right] \leq 1. \qquad (2.26)$$

Враховуючи, що фізичний сенс величини $P_i^E(t)$ ймовірнісний, а її значення лежить в межах $[0..1]$, то ліва частина нерівності (2.26) не може

бути більшою одиниці. Таким чином, функціональна залежність (2.8) може бути нижньою оцінкою для визначення порушення властивостей ІС при певній послідовності модернізації.

Іншою процедурою методу є формування дерева перестановок, суть якої полягає у послідовному формуванні "гілок дерева" з відсутніх в послідовності елементів. Одна ітерація процедури додає тільки один елемент, який відсутній в "батьківських" вузлах та в "листках" вузла, який розглядається. Отже, алгоритм пошуку послідовності модернізації (рисунок 2.22.), в якій найменша ймовірність порушення властивостей ІС даних протягом всього процесу модернізації, описується наступними кроками.

Крок 1. Формування початкового рівня дерева перестановок, що входять до переліку елементів ІС сформованих на п’ятому етапі методу (рисунок 2.19). Для зручності оперування обрані елементи проіндексовані заново.

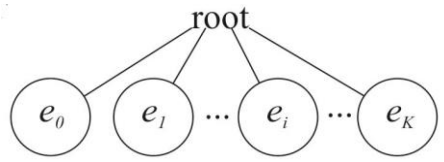


Рисунок 2.19 – Початковий рівень дерева перестановок

Крок 2. Формування наступного рівня дерева за процедурою формування дерева перестановок (рисунок 2.20).

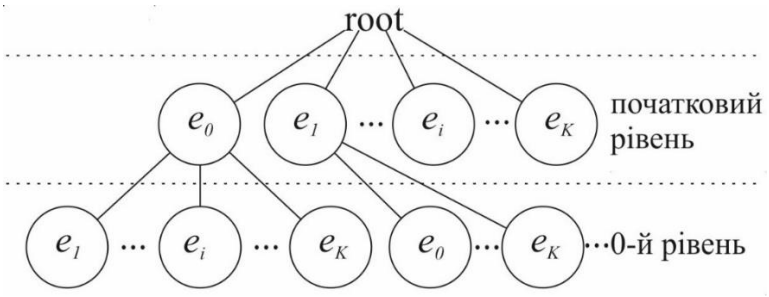


Рисунок 2.20 – Формування рівня дерева перестановок

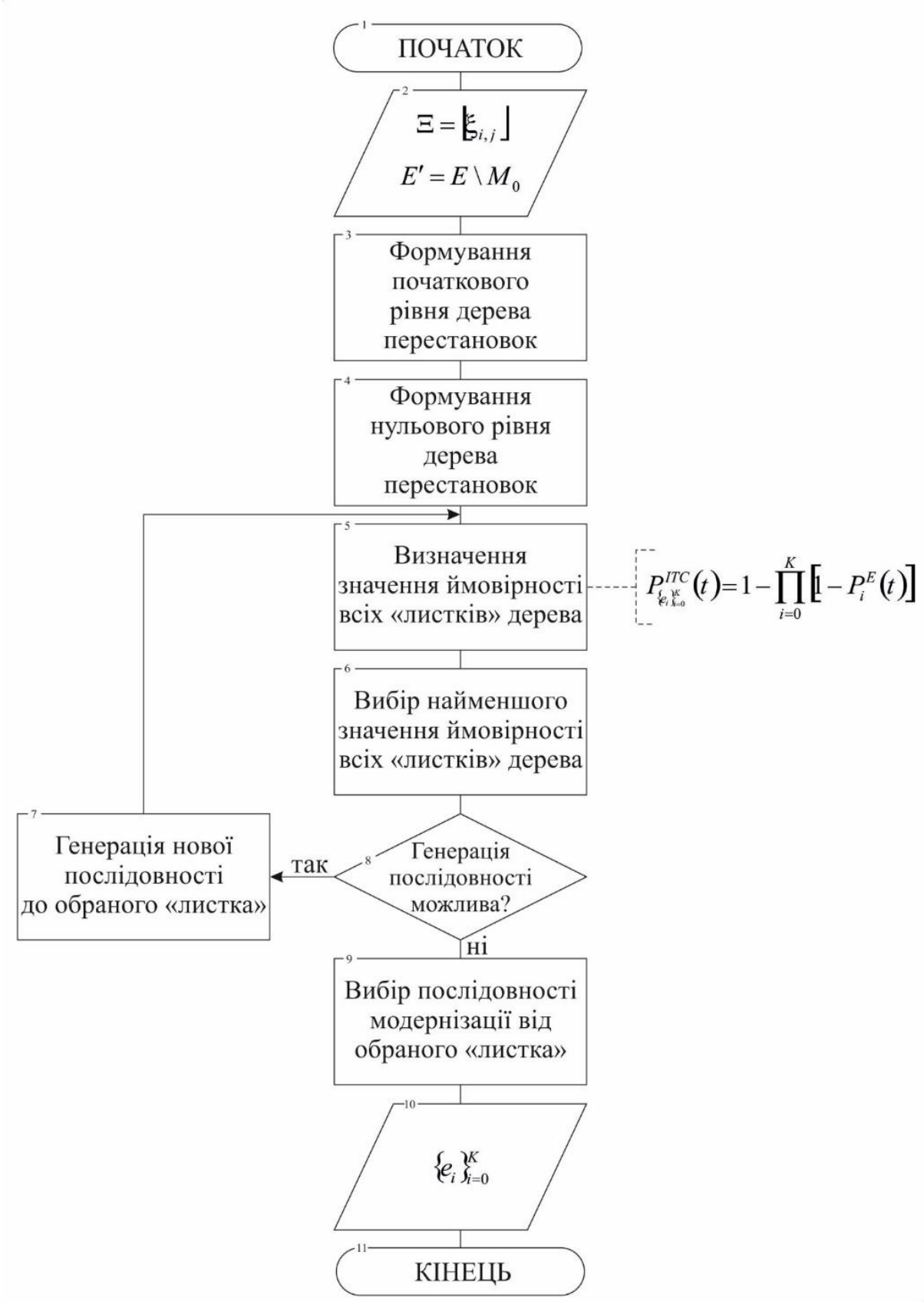


Рисунок 2.22 – Алгоритм процедури пошуку оптимальної послідовності модернізації

Крок 3. Визначення значення ймовірності кожного "листка" для послідовності модернізації відповідно до "гілок" дерева перестановок за формулою (2.8), в якій значення індексу часу початку модернізації i-ї групи відповідає рівню дерева перестановок.

Крок 4. Визначення найменшого значення ймовірності порушення властивостей ІС серед всіх "листків" дерева. Генерація наступної послідовності здійснюється до визначеного "листка". Якщо генерація нової послідовності неможлива, робота алгоритму завершується з послідовністю, яка визначається "листком" дерева з мінімальним значенням ймовірності. В іншому випадку здійснюється перехід до кроку 3.

Результатом роботи наведеного на рисунку 2.22 алгоритму буде визначена послідовність $\{e_i\}_{i=0}^{K}$, при дотриманні якої ймовірність порушення властивостей ІС протягом всього періоду модернізації буде відповідати обраній стратегії.

Таким чином, раціональна послідовність процесу модернізації визначається обраним показником ефективності та ґрунтується на визначених замовником особливостях функціонування ІС та самого процесу оновлення СПЗ.

2.5 Висновки до розділу 2

1. Аналіз існуючих підходів до проблеми забезпечення функціональної безпеки показав наявність циклічного процесу вдосконалення такого типу систем. Водночас, сам процес модернізації, його методологічні засади у цих підходах не розглянуті. Для наявних систем забезпечення функціональної безпеки, які реалізовані в сучасних ІС, загалом не передбачається спільного функціонування різних версій програмно-апаратного забезпечення, систем забезпечення функціональної безпеки, тощо. Це вимагає структурованого аналізу та декомпозиції факторів, що впливають на дотримання властивостей інформаційної системи на стадії модернізації.

2. Опис процесу модернізації ІС дозволив сформулювати стратегію функціональної безпеки, яка полягає у такій сукупності заходів по заміні складових інформаційної системи, за якої рівень функціональної безпеки відповідав нормативному. Разом із тим, умови функціонування різних ІС, їх структура та вимоги до функціональної безпеки можуть суттєво відрізнятись. Через це загальне формулювання стратегії функціональної безпеки на стадії модернізації може дещо відрізнятись один від одного. Аналіз критеріїв та особливостей функціонування дозволив сформувати раціональні стратегії модернізації.

3. Вищенаведені дослідження дозволили сформувати загальну концепцію функціональної безпеки на стадії модернізації як інструментально-методологічну базу, що забезпечує виконання розглянутих стратегій. Концепцією передбачено три завдання узгодження спільного функціонування: спеціального програмного забезпечення, програмних та технічних (апаратних) засобів забезпечення функціональної безпеки, а також визначення величини уразливості інформаційної системи при проведенні заходів з модернізації та оцінювання ефективності функціональної безпеки в ІС на стадії модернізації. Результатом є отримання оцінки ефективності проведених заходів, яка використовується власником системи для прийняття рішення щодо проведення модернізації та визначення організаційних заходів щодо особливості проведення самого процесу оновлення складових ІС.

4. Аналіз наявних підходів до визначення поняття "інформаційний ресурс" та особливості функціонування прикордонного відомства дозволили сформулювати поняття прикордонного інформаційного ресурсу та його похідної – електронного прикордонного інформаційного ресурсу, який зосереджений в інтегрованій інформаційній системі прикордонного відомства. Обґрунтування об’єкту функціональної безпеки є першочерговим завданням загальної концепції функціональної безпеки на стадії модернізації.

5. Аналіз структури та наявних інформаційних потоків ІІС "Гарт" прикордонного відомства показав, що особливістю комунікаційної мережі

ДПСУ є те, що вона виключно відомча та не має виходу до всесвітньої глобальної мережі Інтернет, функціонування інформаційних складових здійснюється з використанням орендованих каналів зв'язку, забезпечує обмін даними між суб'єктами інтегрованого управління кордонами. Інтегрована інформаційна система "Гарт" за своєю архітектурою є структурно-ієрархічною системою, яка складається із множини взаємодіючих функціональних складових, що виділені за ознаками територіального розташування, напрямів діяльності та функціональної деталізації та відображає існуючу організаційну структуру прикордонного відомства. Інтегрована інформаційна система формується шляхом об'єднання інформаційних ресурсів інформаційних підсистем органів ДПСУ, які забезпечують надання інформації згідно з Переліком інформаційних ресурсів ІІС ДПСУ "Гарт".

6. Модернізація складових інтегрованої системи обумовлює наявність інформаційних потоків, які мають змішану структуру як нової, так і старої версії програмно-апаратного забезпечення. Аналіз інформаційних потоків ІС прикордонного відомства дозволив сформувати їх узагальнену структуру та побудувати модель інформаційних потоків ІІС на стадії модернізації. Дослідження розробленої моделі показало, що основним принципом послідовності модернізації елементів ІС, який знижує ймовірність порушення властивостей ІС, є модернізація за величиною вихідного потоку та ймовірності порушення властивостей елементу ІС при невідповідності версій СПЗ. При однаковій ймовірності порушення властивостей елементів ІС з причини невідповідності версій СПЗ модернізується перший той, в кого вхідний потік менший.

7. Визначення раціональної стратегії модернізації вимагає обґрунтування показників ефективності здійснення процесу модернізації. Аналіз особливостей функціонування різних ІС дозволив сформувати три види показників: за максимально можливим значенням ймовірності порушення властивостей ІС під час модернізації, за середнім значенням

ймовірності порушення властивостей ІС у процесі модернізації та середньозваженим значення ймовірності. З'ясовано, що пріоритетним показником ефективності процесу модернізації є максимальне значення ймовірності порушення властивостей ІС у процесі модернізації. Чим менше цей показник, тим ефективніше провадиться заміна СПЗ на елементах інформаційної системи.

8. Розроблений метод визначення раціональної послідовності модернізації елементів ІС ґрунтується на визначеній розпорядником системи стратегії модернізації. Вихідними даними методу є множина елементів ІС, матриця величин інформаційних потоків між елементами ІС та ймовірностей порушення властивостей елементів ІС при здійсненні обміну між ними за невідповідності версій спеціального програмного забезпечення. Результатом методу є раціональна послідовність модернізації елементів ІС, при якій дотримується визначена стратегія модернізації.

Список використаних джерел у другому розділі

1. Закон України Про Державну прикордонну службу України // Відомості Верховної Ради України (ВВР), 2003, № 27, ст.208

2. Марченко Б. М. Адміністративна діяльність Державної прикордонної служби України. дис. ... к-та юр. наук. / Марченко Борис Миколайович.– Дніпропетровськ, 2009.–220 с, 2009.

3. Савенко І. М. Принципи та функції державної прикордонної служби України. / І. М. Савенко // Демократичне врядування № 15 (2015).

4. Мельников О. В. Регіональні аспекти забезпечення прикордонної безпеки в Україні / О. В. Мельников, С. М. Морозов // Актуальні проблеми державного управління. – вип. 4 (2011): – С. 97-100.

5. Герасименко В. А. Защита информации в АСОД (в 2-х томах). – М.: Энергоатомиздат, 1994. – 400 с.

6. Харибін О. В. Інформаційна технологія забезпечення функціональної безпеки бортових інформаційно-керуючих систем авіації на етапі

експлуатації / О. В. Харибін // Системи озброєння і військова техніка № 2. – 2010. – С. 173-177.

7. Муляр, І. В. Аналіз проблем забезпечення функціональної безпеки інформаційних систем обробки даних / І. В. Муляр, А. В. Джулій, М. В. Костюк // Вимірювальна та обчислювальна техніка в технологічних процесах. – 2013. – № 1. – С. 133-138.

8. Манжос Ю. С. Використання аналізу розмірностей для підвищення рівня функціональної безпеки I&C систем. / Ю. С. Манжос // Радіоелектронні і комп'ютерні системи – № 7. – 2012. – С. 313-318.

9. Семенов С. Г. GERT-модель прогнозування параметрів функціональної безпеки технічних систем / С. Г. Семенов, С. Ю. Гавриленко, Кассем Халіфе // Системи обробки інформації. – № 2. – 2016. – С. 50-52.

10. Борзов Ю. Інформаційні технології підвищення функціональної безпеки систем обробки інформації критичного застосування. Автореферат дисертації на здобуття наукового ступеня кандидата технічних наук / Львівський державний університет безпеки життєдіяльності. м. Львів (2015).

11. Юдкова К. В. Класифікація інформаційних систем. / К. В. Юдкова, Г. Г. Чернишина // Інформація і право – № 3. – 2015. – С. 92-98.

12. Гужва В. М. Інформаційні системи і технології на підприємствах. К.: КНЕУ (2001): 133-170.

13. Маслянко П. П. Інформаційно-комунікаційні системи та технології обробки інформаційних ресурсів / П. П. Маслянко, П. М. Ліссов // Вісн. КУЕІТУ "Нові технології – № 1-2. – 2007. – С. 15-16.

14. Стрельбіцький М. А.Декомпозиція технології захисту інформації в корпоративних системах / М. А. Стрельбіцький // Збірник наукових праць Національної академії Державної прикордонної служби України. № 59: Військові та технічні науки. – 2013. – № 1. –С. 296-301.

15. Стрельбіцький М. А. Декомпозиція технології захисту сенсорної інформації в корпоративних системах. / М. А. Стрельбіцький, Т.О. Прищепа

// 7-ма Міжнародна науково-технічна конференція "Проблеми телекомунікацій" (м. Київ, 2013).

16. України, Закон. "Про доступ до публічної інформації." // Відомості Верховної Ради України офіційне видання від 12.08.2011 – 2011 р., № 32, стор. 1491, стаття 314

17. Про інформацію : Закон України // Відомості Верховної Ради України 48 (1992): 650.

18. Олійник О. В. Організаційно-правові засади захисту інформаційних ресурсів України. – К. : Інститут законодавства Верховної Ради України – 2006.

19. Ліпкан В. А. Захист інформації з обмеженим доступом в умовах боротьби з організованою злочинністю / В. А. Ліпкан, В. Ю. Баскаков. // Боротьба з організованою злочинністю і корупцією (теорія і практика) – № 24. – 2011. – С. 263-269.

20. Нашинець-Наумова А. Ю. Проблеми правового регулювання доступу до конфіденційної інформації на підприємстві / А. Ю. Нашинець-Наумова // Наукові праці Національного авіаційного університету. Серія: Юридичний вісник "Повітряне і космічне право" 4.25 (2012): 118-122.

21. Марущак А. І. Теоретико-правові основи забезпечення доступу до державної інформації / А. І. Марущак // Боротьба з організованою злочинністю і корупцією (теорія і практика) – № 18. – 2008. – С. 270-278.

22. Савченко С. В. Співвідношення приватних і публічних інтересів: досвід України / С. В. Савченко // Форум права – № 3. – 2013. – С. 520-528.

23. Арістова І. В. Управління інформаційними ресурсами органів внутрішніх справ України: організаційно-правовий аспект : Навчальний посібник / І. В. Арістова, О. В. Сировой.– Харків: Вид-во Нац. ун-ту внутр. справ, 2005. – 106 с

24. Марущак А. І. До питання про забезпечення безпеки інформаційного простору та інформаційних ресурсів / А. І. Марущак // Юридичний радник – № 4. – 2009. – С. 64-67.

25. Марущак А. І. Щодо поняття "інформаційні ресурси держави". / А. І. Марущак // Інформаційна безпека людини, суспільства, держави – № 1. – 2009.

26. Сировой О.В. Організаційно-правові засади управління інформаційними ресурсами ор- ганів внутрішніх справ України : автореф. дис. ... канд. юрид. наук : 12.00.07 / О.В. Сировой / Харк. нац. ун-т внутр. справ. – Х., 2006. – 20 с.

27. Сировой О. В. Управління інформаційними ресурсами: теоретичний аспект. Актуальні проблеми державотворення в умовах адміністративної реформи / О. В. Сировой // Матеріали Всеукраїнської науково-практичної конференції (2003): 11-12.

28. Сировой, О. В. Поняття та види інформаційних ресурсів у законодавстві України / О. В. Сировой // Вісник Запорізького юридичного інституту 4 (2002): 79-84.

29. Герасименко В.А., Малюк А.А. Основы защиты информации // Москва: МИФИ, 1997. – 537 с.

30. Про захист економічної конкуренції : Закон України // Відомості Верховної Ради України (ВВР), 2001 р., № 12, стаття 64

31. Про телекомунікації : Закон України // Відомості Верховної Ради України (ВВР),від 19.03.2004 № 12, стаття 155

32. Порядок функціонування, застосування та використання Інтранет-мережі Державної прикордонної служби України : Наказ Адміністрації Державної прикордонної служби від 09.08.2004 № 663

33. Про Національну програму інформатизації : Закон України // Відомості Верховної Ради України (ВВР), 1998, N 27-28

34. Науковий вісник Національного університету біоресурсів і природокористування України 2012 – Вип. 173 частина 1 Серія "Право"

35. Доктрина "Інформаційної безпеки України" [Електронний ресурс] // Офіційна веб-сторінка Верховної Ради України: Законодавство.

36. Про основи національної безпеки України: Закон України // Офіційний Вісник України. – 2003. – № 29. – Ст. 1433.

37. Стрельбіцький М. А. Прикордонний інформаційний ресурс: визначення поняття / М. А. Стрельбіцький // Сучасні інформаційні технології у сфері безпеки та оборони. Національний університет оборони України імені Івана Черняховського №1(25) 2016. С. 205-208.

38. Стрельбіцький М. А. Прикордонний інформаційний ресурс: визначення поняття / М. А. Стрельбіцький // Матеріали міжнародної науково-практичної конференції "Історія, сучасність та перспективи розвитку ДПСУ та охорони державного кордону" (м. Київ, 2015).

39. Стрельбицкий М. А. Информационный ресурс пограничной службы– составляющая национальной безопасности Украины / М. А. Стрельбіцький // Материалы международной заочной научно-практической конференции Государственного учреждения образования "Институт пограничной службы Республики Беларусь" (Минск, 2017).

40. Вирковский В. Правовые основы защиты информации / В. Вирковский, С. Вихорев // Банковские технологии. - М.: №7, 1995.С. 16-20.

41. Ведев Д. Л. Защита данных в компьютерных сетях / Д. Л. Ведев // Открытые системы. - М.:№3, 1995, с.12-16.

42. Ловцов Д. А. Планирование и прогнозирование обмена привилегированной информацией в АСУ / Д. А. Ловцов // Зарубежная радиоэлектроника, 1996. №1. с.57-62

43. Ананьїн О. В. Відомча телекомунікаційна мережа державної прикордонної служби України / О. В. Ананьїн // Науково-технічна інформація. – 2012. – С. 38-41.

44. Про затвердження Положення про інтегровану міжвідомчу інформаційно-телекомунікаційну систему щодо контролю осіб, транспортних засобів та вантажів, які перетинають державний кордон : Наказ Адміністрації Державної прикордонної служби України, Державної митної служби

України, Державної податкової адміністрації України, Міністерства внутрішніх справ України, Міністерства закордонних справ України, Міністерства праці та соціальної політики України, Служби безпеки України, Служби зовнішньої розвідки України від 3 квітня 2008 року N 284/287/214/150/64/175/266/75 // Офіційний вісник України офіційне видання від 02.06.2008 – 2008 р., № 37, стор. 54, стаття 1249, код акта 43118/2008

45. Бєляков К. І. Інформаційно-телекомунікаційні системи правоохоронних органів України: організаційні та правові проблеми створення і функціонування / К. І. Бєляков // Боротьба з організованою злочинністю і корупцією (теорія і практика) №16 (2007): 231-238.

46. Юдін О. К. Зміст та ієрархія реєстру інформаційних ресурсів Держприкордонслужби України / О. К. Юдін, М. А. Стрельбіцький // Проблеми інформатизації на управління, – №4 (56) – 2016. – С. 85-91

47. Юдін О.К. Ієрархічний класифікатор автоматизованих систем прикордонного відомства / О. К. Юдін, М. А. Стрельбіцький // Радиоэлектроника и информатика. Научно-технический журнал № 1(76), январь – май 2017

48. Організація керівництво оперативно-службовою діяльністю та управління службою в повсякденних умовах у разі ускладнення обстановки та виникненні надзвичайних ситуацій на державному кордоні // навчальний посібник за заг. ред. В.В.Заложа Хмельницький Видавництво Національної академії Державної прикордонної служби України ім Б. Хмельницького 2009. – 240 с.

49. Стрельбіцький М. А. Нечіткий пошук інформації у базі даних програмно-технічного комплексу "Гарт-1/П" / М. А. Стрельбіцький, Р. В. Рачок, Д. А. Мул // Матеріали VII Всеукраїнської науково-практичної конференції "Освітньо-наукове забезпечення діяльності правоохоронних органів і військових формувань України" (м. Хмельницький 2014 р).

50. Тіщенко В. М. Інформаційне забезпечення фільтраційно-перевірочної діяльності державної прикордонної служби України /

В. М. Тіщенко // Актуальні проблеми управління інформаційною безпекою держави // VIII науково-практична конференція Збірник матеріалів (Київ, 2017).

51. Мота А. Ф. Недодержання іноземцями та особами без громадянства встановленого порядку реєстрації або порушення встановленого терміну перебування в Україні, виявлені в пунктах пропуску через державний кордон України: особливості юридичного складу / А. Ф. Мота // Вісник Національної академії Державної прикордонної служби України. Серія: Юридичні науки – №1. – 2017.

52. Купрієнко Д. А. Обґрунтування графічних моделей та формальних залежностей транспарентності державного кордону (на прикладі вантажотранспортних потоків) / Д. А. Купрієнко // Збірник наукових праць Національної академії Державної прикордонної служби України. Сер.: Військові та технічні науки №1 (2015): 54-68.

53. Barannik V. Method of Ciphergrams Coding for Increasing the Effectiveness of Selective Cyber-Protection Technologies / Barannik V., Barannik D., Hahanova A., Medvedev D., Strelbtskiy M. // Radioelectronics & Informatics. – Kharkiv: 2016. – № 4 (75) – P. 34–40.

54. Шинкарук О. М. Аналіз досвіду створення та використання інтегрованих телекомунікаційних систем Гарт" в Державній прикордонній службі України / О. М. Шинкарук, А. В. Федорченко. // Збірник наукових праць Національної академії Державної прикордонної служби України. Сер.: Військові та технічні науки – №2. – 2015. – С. 221-233.

55. Юдін О.К. Інформаційна безпека. Нормативно-правове забезпечення. – К., 2010 – 640 с.

56. "Енциклопедія кібернетики", відповідальний ред. В. Глушков, 2 тт., 1973, рос. вид. 1974;

57. Кушнірецька І. "Методика "чорної скриньки" та агентно-орієнтованого підходу для забезпечення Mash-Up інтеграції інформаційних

ресурсів." / І. Кушнірецька, А. Берко // Інформація, комунікація, суспільство 2014 : матеріали 3-ої Міжнар. наук. конф. ІКС-2014.

58. Захарченко М.В., Горохов С.М., Балан М.М., Гаджієв М.М., Корчинський В.В., Ложковський А.Г. Математичні основи оптимізації телекомунікаційних систем: Підручник. – Одеса: ОНАЗ ім. О.С. Попова, 2010. – 240 с.

59. Морозов А. В. Метод гілок та меж у гамільтоновій задачі про сільського листоношу / А. В. Морозов, А. В. Панішев // Системні дослідження та інформаційні технології : науково-технічний журнал. – 2012. – № 2. – С. 57–66

60. Парфьонова Т.О. Евклідова комбінаторна транспортна задача на переставленнях, її розв’язування методом гілок та меж / Т.О. Парфьонова // Матеріали Другої ювілейної міжнародної науково-технічної конференції "Комп’ютерна математика в інженерії, науці та освіті" (CMSEE-2008), м. Полтава, 29-31.10.2008р. - Київ: Вид-во НАН України, 2008. - С.24.

61. Леонова М. В. Алгоритм розв’язування задачі про оптимальні призначення методом гілок та меж / М. В. Леонова // Штучний інтелект – № 2. – 2013. – С. 14-20.

62. Олексійчук Ю. Ф. Метод гілок та меж для комбінаторної задачі знаходження потоку мінімальної вартості / Ю. Ф. Олексійчук // Інформатика та системні науки (ІСН-2015): матеріали VI Всеукраїнської науково-практичної конференції за міжнародною участю, (м. Полтава, 19–21 берез. 2015 р.). – Полтава: ПУЕТ, 2015.

63. Шаповалов Ю. О. Оптимізація розміщення прямокутних об’єктів на опуклій області методом гілок та меж / Ю. О. Шаповалов, С. І. Яремчук. // Вісник Житомирського державного технологічного університету. Серія: Технічні науки 4 (31) Т. 2 (2004): 161-167.

РОЗДІЛ 3
РОЗПОДІЛ ЗАСОБІВ ЗАБЕЗПЕЧЕННЯ ФУНКЦІОНАЛЬНОЇ БЕЗПЕКИ ТА ОЦІНЮВАННЯ УРАЗЛИВОСТІ ІНФОРМАЦІЙНОЇ СИСТЕМИ НА СТАДІЇ МОДЕРНІЗАЦІЇ

Модернізація ІС прикордонного відомства здійснюється з метою запобігання ризикам та зменшення негативних впливів реалізації загроз національній безпеці в прикордонній сфері. Ступінь модернізації може змінюватись від незначного вдосконалення інтерфейсу автоматизованого робочого місця до суттєвих розробок з інтеграцією до міжнародних інформаційних систем. Прикладом такого є підключення ПТК АПК "Гарт-1" до міжнародної бази даних Інтерполу [1]. Разом із модернізацією як програмних, так і апаратних засобів автоматизованих систем змінюється і структура та кількість засобів забезпечення функціональної безпеки в ІС. На стадії модернізації та після її завершення рівень забезпечення функціональної безпеки об’єктів інформаційної діяльності не повинен зменшуватись.

На стадії модернізації ІІС ймовірна зміна її фізичної структури, потоків даних, програмно-апаратних складових. Це вимагає вдосконалення методу розподілу засобів забезпечення функціональної безпеки в інтегрованих інформаційних системах на стадії модернізації з урахуванням впливу наявних та доданих засобів захисту, а також вимог до загального рівня захищеності системи.

3.1 Метод розподілу засобів забезпечення функціональної безпеки в інформаційних системах на стадії модернізації

Забезпечення функціональної безпеки на об’єктах інформаційної діяльності в органах та підрозділах прикордонного відомства має визначальний вплив на складові національної безпеки [2]. Персонал прикордонного відомства оперує критичною інформацією щодо прийняття

рішень. Таким чином, дотримання властивостей прикордонного інформаційного ресурсу є головним чинником забезпечення функціональної безпеки ІС.

При формуванні системи функціональної безпеки враховується комплексна взаємодія її елементів як складових системи. Використання системного підходу передбачає створення відповідних механізмів забезпечення безпеки на кожній із стадій життєвого циклу ІС. Особливо гостро постає питання функціональної безпеки при модернізації інформаційних систем, так як розробниками, як правило, не досліджується дане питання у розрізі впливу на інші ІС, які взаємодіють з модернізованою системою через загальне поле даних, як це здійснюється в ІІС "Гарт".

Аналіз існуючих досліджень в галузі забезпечення складових функціональної безпеки [3–8] показав, що в них розглядається оцінювання системи в цілому, її аналіз та рівень забезпечення безпеки. Це в свою чергу призводить до необхідності здійснення повного процесу оцінювання при модернізації системи, а у випадку ІІС "Гарт" як інтегрованої системи такий підхід є проблематичним. Вищенаведене вимагає розробки таких підходів та вимог до процесу модернізації, щоб на цій стадії життєвого циклу загальної системи не було знижено рівень функціональної безпеки.

Рівень ефективності системи функціональної безпеки в основному залежить від ефективності застосування наявних апаратних засобів та якості програмних засобів. У випадку їх модернізації загальний рівень безпеки системи, як правило, буде змінюватись. Таким чином, розробка методів оцінювання уразливості інформаційної системи на стадії модернізації та розподілу засобів забезпечення функціональної безпеки дозволить вирішити проблему забезпечення функціональної безпеки на стадії модернізації.

Основою сучасних концепцій функціональної безпеки є системно-концептуальний підхід [9–11], суть якого полягає в тому, що при вивченні та описі проблеми враховуються у взаємному зв'язку всі значущі елементи, фактори і параметри (системність підходу), а для досягнення поставлених

цілей не просто знаходиться рішення (оптимальне, раціональне або наближене) для конкретних умов, а розробляється повна і несуперечлива сукупність методів, правил і прийомів, що дозволяє порівняно легко генерувати необхідні рішення в будь-яких потенційно можливих умовах (концептуальність підходу).

Обґрунтування структури СФБ і технології її функціонування в ІІС передбачає вибір та використання широкого спектру засобів забезпечення функціональної безпеки з метою забезпечення властивостей інформаційної системи.

3.1.1 Аналітична модель розподілу засобів забезпечення функціональної безпеки в інформаційних системах на стадії модернізації. Побудова загальної аналітичної моделі розподілу засобів забезпечення функціональної безпеки в інформаційних системах на стадії модернізації вимагає розробки часткових моделей, а саме: моделі каналу інформаційного дестабілізаційного впливу (КІДВ), моделі функціональної захищеності ІІС та методу розподілу засобів забезпечення функціональної безпеки відповідно до КІДВ.

3.1.1.1 Розробка моделі каналу інформаційного дестабілізаційного впливу. При виборі кількісних характеристик можливих каналів інформаційного дестабілізаційного впливу використаємо загальновідомий емпіричний факт, який полягає в тому, що всі КІДВ не рівноцінні [12]. Це дозволяє здійснити ранжування КІДВ. Кожному КІДВ при цьому ставиться у відповідність безрозмірна позитивна величина C_i, яку будемо називати ваговим коефіцієнтом КІДВ або вагою КІДВ. У випадку рівноцінності КІДВ всі їх вагові коефіцієнти мають однакове значення. В іншому випадку їх можливо упорядкувати за вагою.

Нехай виявлені можливі канали інформаційного дестабілізаційного впливу у кількості N одиниць та нехай КІДВ з номерами i мають значення вагового коефіцієнту C_i, де $i = \overline{1, N}$.

Очевидно, що

$$\sum_{i=1}^{N} C_i = 1, \tag{3.1}$$

$$0 \le C_i \le 1. \tag{3.2}$$

Фізичний сенс ваги КІДВ полягає в тому, що він характеризує можливу долю інформаційного дестабілізаційного впливу через заданий КІДВ відносно можливого інформаційного дестабілізаційного впливу через всі КІДВ та має аналогію в теорії ймовірностей для повної групи подій.

Визначення ваги КІДВ можливо двома шляхами. Перший підхід ґрунтується на здоровому глузді при наявності достовірних відомостей про КІДВ, а також практичного досвіду їх оцінювання і полягає у визначенні ваги експертним шляхом. По суті цей підхід використовується на практиці дуже давно, хоч і не спирається на кількісні оцінки. Кількісні оцінки величин, які не вимірюються фізично, почали застосовуватися в експертних процедурах порівняно недавно і вимагають, як правило, використання обчислювальної техніки (зокрема в експертних процедурах можна задаватися різними гіпотезами про закон розподілу вагових коефіцієнтів КІДВ і при мінімальному обсязі спостережень підбирати адекватні закони розподілу в межах прийнятної точності). З розвитком інтелектуальних систем і експертних систем цей підхід слід визнати досить перспективним.

Другий підхід полягає у використанні виміру або визначення кількості інформації, яка проходить через КІДВ, з урахуванням її рангу важливості, наприклад: ступеня її обмеження доступу, вартості, ступеня впливу на зовнішнє середовище тощо. Кількість інформації при цьому визначається за відомими та практично апробованими співвідношеннями теорії інформації [13–15].

Позначимо символом I_{ik} кількість інформації, яка потенційно проходить через незахищений КІДВ з номером i та рангом важливості k. Варто зазначити, що номер k встановлюється декларативно та в рамках

формального опису не повинен змінюватись. Позначимо g_k як коефіцієнт важливості однієї одиниці інформації, яка має ранг k. Під коефіцієнтом важливості будемо розуміти деяке дійсне число, яке характеризує цінність одиниці інформації з точки зору обраного критерію. Прикладом цього може бути вартість втрати інформації, можливий збиток від порушення конфіденційності тощо. Розроблені на теперішній час моделі оцінки цінності інформації [16–19] дозволяють розглянути зазначену властивість з точки зору: адитивної моделі як суми вартостей елементів інформації, як кінцевої множини елементів, де експерти здійснюють оцінку кожного елементу окремо; аналізу ризику, що базується на адитивній моделі, але оцінюється вартість втрат, з урахуванням прогнозу можливих загроз компонентам інформації; порядкової шкали цінностей – моделі, що оцінює інформацію як порівняння цінностей окремих інформаційних елементів між собою; моделі решітки цінностей як узагальненої моделі порядкової шкали цінностей.

З урахуванням прийнятих позначень та допущень визначимо ваговий коефіцієнт КІДВ

$$C_i = \frac{\sum_{k=1}^{R} I_{ik} \cdot g_k}{\sum_{i=1}^{N} \sum_{k=1}^{R} I_{ik} \cdot g_k}. \qquad (3.3)$$

Варто зазначити, що вага КІДВ може змінюватись з плином часу. Це проходить щоразу, коли змінюється значення N та величина I_{ik}.

Відомо, що КІДВ потребує захисту певними засобами забезпечення функціональної безпеки (ЗЗФБ). При виборі кількісних характеристик засобів ЗЗФБ необхідно врахувати, що дана характеристика, в часткових випадках, коли виконується закон великих чисел, повинна виражатись через ймовірність успішного захисту. З іншого боку, ця характеристика повинна залишатись прийнятною також у випадку, коли теоретико-ймовірнісні методи призводять до помилкових результатів.

Нехай маємо S різних типів ЗЗФБ. Розглянемо ЗЗФБ з номером $j, j=\overline{1,S}$, яким захищається КІДВ з номером $i, i=\overline{1,N}$. Даному ЗЗФБ поставимо у відповідність безрозмірну величину q_{ij}, яку назвемо коефіцієнтом забезпечення функціональної безпеки та безрозмірну величину u_{ij}, яку будемо називати коефіцієнтом проходження інформаційного дестабілізаційного впливу.

Величини q_{ij} та u_{ij} повинні дотримуватись таких вимог

$$0 \le q_{ij} \le 1, \tag{3.4}$$

$$0 \le u_{ij} \le 1, \tag{3.5}$$

при цьому $q_{ij}=0$, $u_{ij}=1$, якщо інформаційний дестабілізаційний вплив, який поступає на вхід ЗЗФБ, рівний впливу на його виході (ЗЗФБ повністю не виконує своїх функцій) та $q_{ij}=1$, $u_{ij}=0$, якщо інформаційний дестабілізаційний вплив на виході ЗЗФБ рівний нулю (проходження відсутнє). При цьому

$$q_{ij}=1-u_{ij}, \tag{3.6}$$

$$u_{ij}=1-q_{ij}. \tag{3.7}$$

Розглянемо тепер КІДВ з номером j, який захищений не одним, а декількома ЗЗФБ одночасно. При цьому припустимо, що якщо ЗЗФБ з номером j не використовується, то $q_{ij}=0$, $u_{ij}=1$. Позначимо через x_j та y_j безрозмірні величини, які будемо називати захищеністю та незахищеністю КІДВ з номером j відповідно. Фізичний сенс величин x_j та y_j аналогічний фізичному сенсу величин q_{ij} та u_{ij}, при цьому

$$x_j = 1 - y_j, \tag{3.8}$$

$$y_j = 1 - x_j, \tag{3.9}$$

$$0 \le x_j \le 1,\ j = \overline{1, N}, \tag{3.10}$$

$$0 \le y_j \le 1,\ j = \overline{1, N}. \tag{3.11}$$

Очевидно, що

$$y_j = \prod_{j=1}^{S} u_{ij}. \tag{3.12}$$

З урахуванням виразів (3.6) – (3.9) отримаємо

$$x_i = 1 - \prod_{j=1}^{S} \left(1 - q_{ij}\right). \tag{3.13}$$

Таким чином, захищеність x_j КІДВ з номером j вираховується через коефіцієнти ЗЗФБ з номерами $j, j = \overline{1, S}$ аналогічно тому, як вираховується надійність послідовного з'єднання елементів через надійність цих елементів [3, 4].

У випадку системної взаємодії ЗЗФБ та прояву ефекту емержентності їх спільного функціонування зазначена група ЗЗФБ може розглядатись як окремий засіб із власною (системною) характеристикою, яка відрізняється від характеристик її складових.

3.1.1.2 Модель функціональної захищеності ІІС. Інтегровану інформаційну систему з точки зору функціональної безпеки можна ототожнити з набором незалежних КІДВ, котрі мають номери $i, i = \overline{1, N}$. Позначимо через X безрозмірну величину, яку будемо називати функціональною захищеністю об'єкта. Величина X повинна відповідати умові

$$0 \le X \le 1, \tag{3.14}$$

причому $X = 0$, якщо функціональна захищеність відсутня та $X = 1$ у протилежному випадку.

Потенційний інформаційний дестабілізаційний вплив I незахищеного об'єкта і потенційний інформаційний дестабілізаційний вплив I_i через незахищений КІДВ з номером i має вигляд

$$I = \sum_{i=1}^{N} \sum_{k=1}^{R} I_{ik} q_k , \tag{3.15}$$

$$I_i = \sum_{k=1}^{R} I_{ik} q_k . \tag{3.16}$$

Після заходів із забезпечення функціональної безпеки I та I_i отримаємо відповідно величину захищеності H та H_i

$$H = IX , \tag{3.17}$$
$$H_i = I_i X_i .$$

Очевидно, що захищеність H об'єкта дорівнює сумі захищених інформаційних потоків H_i КІДВ, тобто

$$H = \sum_{i=1}^{N} H_i . \tag{3.19}$$

Ураховуючи вирази (3.3) та (3.15) – (3.19) в результаті отримаємо

$$X = \sum_{i=1}^{N} C_i x_i . \tag{3.20}$$

Аналіз виразу (3.20) показав, що захищеність X об’єкта визначається через ваговий коефіцієнт C_i і захищеність x_i можливих каналів інформаційного дестабілізаційного впливу. Таким чином, вираз (3.20) доцільно обрати як цільову функцію функціональної безпеки, в якій величини C_i і x_i відіграють роль макрохарактеристик [20].

Пряма задача оцінювання функціональної захищеності ІІС (задача аналізу функціональної безпеки)

Пряму задачу або задачу аналізу функціональної безпеки можна сформулювати так.

Дані величини C_i і x_i.

Потрібно знайти величину X.

На практиці це означає, що розробник у результаті обстеження, аналізу і моделювання об'єкта забезпечення функціональної безпеки отримав значення ваг КІДВ, у результаті прийнятих проектних рішень за вибором ЗЗФБ з урахуванням їх коефіцієнтів визначив захищеність КІДВ і його цікавить, яка захищеність об'єкта в цілому.

Вирішення цієї задачі неважко отримати за співвідношенням (3.20).

Зворотна задача оцінювання функціональної захищеності ІІС (задача синтезу функціональної безпеки)

Зворотну задачу чи задачу синтезу функціональної безпеки можна сформулювати так.

Дано величини X, C_i і x_i, $i=\overline{1,M}, M<N$.

Потрібно знайти величини x_i, $i=\overline{M+1,N}$.

На практиці це означає, що Державна прикордонна служба України у технічному завданні на модернізацію (розробку) інформаційних систем (підсистем) визначила вимоги до захищеності об'єкта (ІІС "Гарт") в цілому і вказала на вже реалізовані вимоги до захищеності окремих КІДВ. Розробник у результаті обстеження, аналізу або моделювання об'єкта отримав значення

ваг КІДВ і його цікавить, які проектні рішення щодо вибору ЗЗФБ для незахищених КІДВ слід прийняти, щоб задовольнити вимоги замовника.

Рішення такого завдання в загальному вигляді є невизначеним. Іншими словами, це завдання має нескінченно багато рішень, якщо не вводити додаткові умови [21].

Ціле коло таких умов, при цьому істотних, пов'язане з моделлю порушення функціональної безпеки, впливу хибного прийняття рішення персоналом прикордонного відомства на складові національної безпеки, проте в цілому щодо інтегрованої інформаційної системи "Гарт" така модель відсутня. Ця обставина суттєво ускладнює подальші дослідження та знижує їх ефективність. По суті в цьому випадку функціональна безпека будується від гіпотетичного порушення функціональної безпеки.

Щоб знайти одне з рішень оберненої задачі, приймемо найбільш несприятливу для нас гіпотезу про порушення функціональної безпеки, яка полягає в тому, що інформаційний дестабілізаційний вплив можливий з будь-якого КІДВ в будь-який момент часу.

При такій гіпотезі функціональна безпека повинна бути рівноміцною, тобто допустимий інформаційний дестабілізаційний вплив через всі КІДВ повинний бути однаковим, що математично означає

$$C_i y_i = C_j y_j = const, i, j = \overline{M+1, N}, \tag{3.21}$$

або, що те ж саме,

$$C_i(1 - x_i) = C, C = const. \tag{3.22}$$

З виразів (3.22), (3.10) маємо

$$x_i = 1 - \frac{C}{C_i}, 0 \le C \le C_i. \tag{3.23}$$

Іншими словами, якщо відома вага C_i і допустима величина C, то необхідна захищеність КІДВ знаходиться за виразом (3.23).

Виразимо C через вихідні дані задачі. Для цього уточнимо постановку задачі. Нехай замовником задані значення X та $x_i, i=\overline{1,M}, M<N$, а розробником визначено значення $C_i, i=\overline{1,N}$. Необхідно знайти значення $x_i, i=\overline{M+1,N}$, при яких забезпечується рівноміцність функціональної безпеки.

Зауважимо, що випадок $M=N$ не представляє інтересу, оскільки величини $x_i, i=\overline{1,N}$ та X повинні задовольняти співвідношення (3.20). Представимо це співвідношення таким чином

$$X=\sum_{i=1}^{M} C_i x_i + \sum_{i=M+1}^{N} C_i x_i \,. \tag{3.24}$$

Перенесемо задані величини в праву частину, а шукані величини в ліву частину рівняння (3.23)

$$\sum_{i=M+1}^{N} C_i x_i = X - \sum_{i=1}^{M} C_i x_i + \sum_{i=M+1}^{N} C_i x_i \,. \tag{3.25}$$

Визначимо тепер сумарний допустимий вплив через ті КІДВ, відносно яких замовник не обумовив вимоги щодо захищеності $x_i, i=\overline{1,M}, M<N$. Для цього просумуємо співвідношення (3.22) $N-M$ разів.

$$\sum_{i=M+1}^{N} C_i\left(1-x_i\right)=C\left(N-M\right). \tag{3.26}$$

Із цього виразу випливає, що

$$C = \frac{1}{N-M}\left(\sum_{i=M+1}^{N} C_i - \sum_{i=M+1}^{N} C_i x_i \right). \qquad (3.27)$$

Зазначимо, що оскільки

$$\sum_{i=1}^{N} C_i = 1,$$

то

$$\sum_{i=M+1}^{N} C_i = 1 - \sum_{i=1}^{M} C_i . \qquad (3.28)$$

Об'єднаймо вирази (3.23), (3.24), (3.26), (3.27), отримаємо остаточно

$$\left.\begin{aligned} x_i &= 1 - \frac{C}{C_i}, i = \overline{M+1, N} \\ C &= \frac{1}{N-M}\left[(1-X) - \sum_{i=1}^{M} (1-x_i) C_i \right] \end{aligned}\right\}. \qquad (3.29)$$

Таким чином, якщо замовником задані вимоги з функціональної захищеності X об'єкта і із захищеності $x_i, i = \overline{1, M}$ перших M КІДВ (це не обмежує спільності, так як КІДВ завжди можна пронумерувати), а розробником визначені ваги $C_i, i = \overline{1, N}$, всіх КІДВ, то необхідні для рівноміцної функціональної безпеки значення захищеності $x_i, i = \overline{M+1, N}$ решти КІДВ можна знайти за отриманими вище виразами (3.29). Іншими словами, отримано рішення оберненої задачі для випадку рівноміцної функціональної безпеки. Інші варіанти забезпечення СФБ, які відповідають різним моделям порушень, вимагають окремого розгляду.

Зазначимо, що рішення (3.29) задачі синтезу рівноміцної функціональної безпеки неважко реалізувати на ЕОМ, зокрема в діалоговому режимі, а також представити у вигляді таблиць і графіків,

зручних для математично непідготовленого користувача. Розробка цих питань також вимагає окремого розгляду.

3.1.1.3 Метод розподілу засобів забезпечення функціональної безпеки у відповідності до КІДВ. У процесі введення в експлуатацію ІІС розробляється система функціональної безпеки, в якій відповідно до застосованої на цьому етапі методу розподіляються ЗЗФБ. На стадії модернізації складової інтегрованої інформаційної системи виникає потреба раціонально розподілити як існуючі, так і додані ЗЗФБ. Це вимагає розробки методу розподілу засобів забезпечення функціональної безпеки на стадії модернізації відповідно до КІДВ, призначенням якої є раціональний розподіл ЗЗФБ певних типів з метою забезпечення заданого рівня функціональної безпеки об'єкта.

Вихідними даними методу є:

- нормативні значення захищеності x_i КІДВ;
- типи ЗЗФБ (S типів);
- коефіцієнти захисту i-го КІДВ ЗЗФБ кожного типу ($q_{i1}, q_{i2}, ..., q_{iS}$).

Основні етапи методу.

У результаті синтезу функціональної безпеки знайдено необхідне значення захищеності x_i КІДВ. Таким чином, ця задача зводиться до дослідження одного КІДВ, для якого вірно рівняння (3.13).

На першому етапі з метою раціоналізації розподілу ЗЗФБ сформуємо їх в групи за критеріями: обов'язковості, сучасності і т. п. Позначимо коефіцієнтами захисту кожну з груп $q_{ij}^1, q_{ij}^1, ..., q_{ij}^k$, провівши ранжування ЗЗФБ всередині кожної з цих груп.

На другому етапі методу визначається необхідна кількість ЗЗФБ (за типами) для забезпечення захисту зазначеного КІДВ. Іншими словами, для забезпечення нормативного значення захищеності КІДВ повинна виконуватись нерівність

$$x_i \le 1 - \prod_{j=1}^{S} \left(1 - q_{ij}\right). \qquad (3.30)$$

Це рівняння має одне рішення щодо невідомих тільки при застосуванні одного ЗЗФБ певного типу, тобто $j = 1$, і тоді

$$x_i = q_{ij},\ j = 1.$$

У цьому випадку визначається необхідний коефіцієнт q_{ij} захисту ЗЗФБ і далі серед S типів ЗЗФБ підбирається такий, що задовольняє (3.30).

Якщо $j > 1$, то рішення рівняння (3.13) є невизначеним і потребує проведення додаткових розрахунків. Таким чином, у загальному випадку (при $j > 1$) здійснюється аналіз комбінацій ЗЗФБ першої групи за нерівності

$$x_i \le 1 - \prod_{j=1}^{S_1} \left(1 - q_{ij}^{1}\right). \qquad (3.31)$$

Якщо ця нерівність задовольняється, то вибирається така комбінація ЗЗФБ, при якій досягається мінімальне значення захищеності. КІДВ в цьому випадку вважається захищеним, і йому присвоюється номер $m+1$.

$$\left(x_i\right)_{\min} = x_{m+1}, \qquad (3.32)$$

де m – кількість КІДВ, для яких раніше були знайдені комбінації ЗЗФБ, що задовольняють необхідним значенням захищеності x_i цих каналів.

На третьому етапі, для решти незахищених КІДВ проводиться перерахунок необхідних значень їх захищеності x_i за виразами (3.28) при

$M = m+1$ і здійснюється перехід до підбору ЗЗФБ наступного незахищеного КІДВ.

Якщо ж нерівність (3.31) не задовольняється, то склад комбінацій ЗЗФБ розширюється за рахунок наступної групи ЗЗФБ і потім аналіз комбінацій проводиться за нерівності

$$x_i \le 1 - \prod_{j=1}^{S_1}\left(1 - q_{ij}^{1}\right) \prod_{j=S_1+1}^{S_2}\left(1 - q_{ij}^{2}\right). \tag{3.33}$$

Якщо ця нерівність задовольняється, то вибирається така комбінація ЗЗФБ, при якій досягається мінімальне значення захищеності, КІДВ вважається захищеним і процедура перерахунку, викладена вище, повторюється.

Якщо ж нерівність (3.33) не задовольняється, то склад комбінацій ЗЗФБ розширюється за рахунок третьої групи ЗЗФБ і потім аналіз комбінацій проводиться за нерівності

$$x_i \le 1 - \prod_{j=1}^{S_1}\left(1 - q_{ij}^{1}\right) \prod_{j=S_1+1}^{S_2}\left(1 - q_{ij}^{2}\right) \prod_{j=S_2+1}^{S_3}\left(1 - q_{ij}^{3}\right), \tag{3.34}$$

де $S_1 < S_2 < S_3$.

Аналіз функціональних залежностей (3.31, 3.33, 3.34) дозволив формально описати кожну ітерацію при обробці k-ї групи ЗЗФБ.

$$x_i \le 1 - \prod_{k=1}^{K}\left(\prod_{j=1+S_{k-1}}^{S_k}\left(1 - q_{ij}^{k}\right)\right), \tag{3.35}$$

де K – кількість груп ЗЗФБ розподілених за певними критеріями;

S_k – кількість ЗЗФБ в k-й групі (при чому S_0=0).

У результаті наведених функціональних залежностей, науково обґрунтованих вихідних параметрів метод розподілу засобів забезпечення функціональної безпеки відповідно до КІДВ прийме вид, зображений на рисунку 3.2.

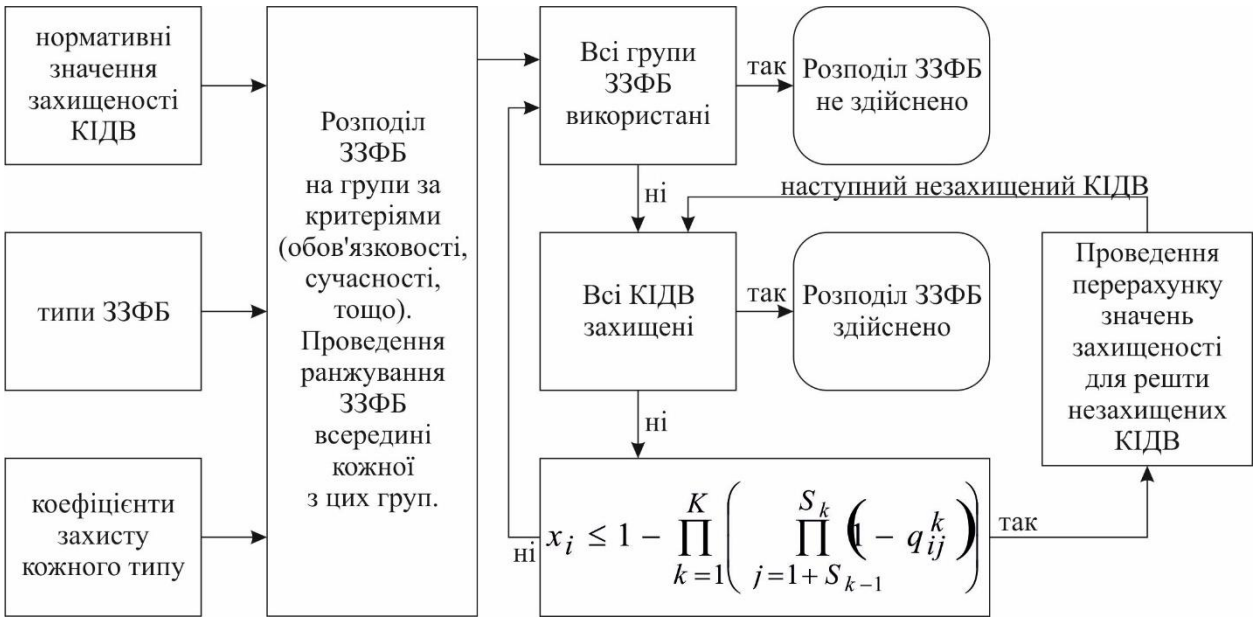


Рисунок 3.2 – Структурна схема методу розподілу засобів забезпечення інформаційної безпеки відповідно до КІДВ

Відповідно до структурної схеми принцип розподілу ЗЗФБ полягає у послідовному підборі засобів забезпечення функціональної безпеки до тих пір, поки не буде забезпечено захист кожного КІДВ. Зазначимо, що перелік ЗЗФБ ранжований експертами за критеріями обов’язковості, сучасності, ефективності тощо. Метод є інваріантним до процесу ранжування, яке виконують експерти, тому для кожного об’єкта інформаційної діяльності (ІС, підсистеми) перелік засобів може бути індивідуальним. Результатом методу є два варіанти: розподіл здійснено або не здійснено.

На стадії модернізації, коли окремі ЗЗФБ вже є встановленими, можливе створення окремої категорії таких засобів, яка є обов’язковою до використання.

Таким чином, розроблений метод розподілу засобів забезпечення функціонального захисту відповідно до можливих каналів інформаційного дестабілізаційного впливу дозволить раціонально розподілити ЗЗФБ за умови дотримання нормативного рівня функціональної безпеки системи в цілому.

3.1.2. Структурна схема методу розподілу засобів забезпечення функціональної безпеки в інтегрованих інформаційних системах на стадії модернізації. До формулювання структури методу розподілу ЗЗФБ системно-концептуальний підхід висуває такі вимоги:

1. Загальнотеоретичні:

а) повнота, тобто достатність для вирішення задачі аналізу та синтезу СФБ і керування їх функціонуванням;

б) відсутність протиріч, тобто взаємопов'язаність та логічний зв’язок всіх компонентів;

2. Прикладні:

а) уніфікованість, тобто здатність забезпечити потребу вирішення завдання комплексного забезпечення функціональної безпеки;

б) урахування основних положень сучасних та перспективних концепцій побудови і використання автоматизованих систем обробки даних;

в) можливість реалізації при сучасному розвитку науки, техніки, виробництва;

г) перспективність, тобто адекватність не тільки для теперішніх, а і для перспективних потреб та умов функціональної безпеки в ІІС.

У результаті аналізу вихідних даних та мети забезпечення функціональної безпеки визначаються об’єкти та елементи захисту, обґрунтовується система показників захищеності ІІС і, з урахуванням цього, система інформаційних дестабілізаційних факторів, потенційно можливих в процесі створення і функціонування ІІС.

Метод розподілу засобів забезпечення функціональної безпеки в інтегрованих інформаційних системах на стадії модернізації (рисунок 3.3) умовно поділимо на три етапи.

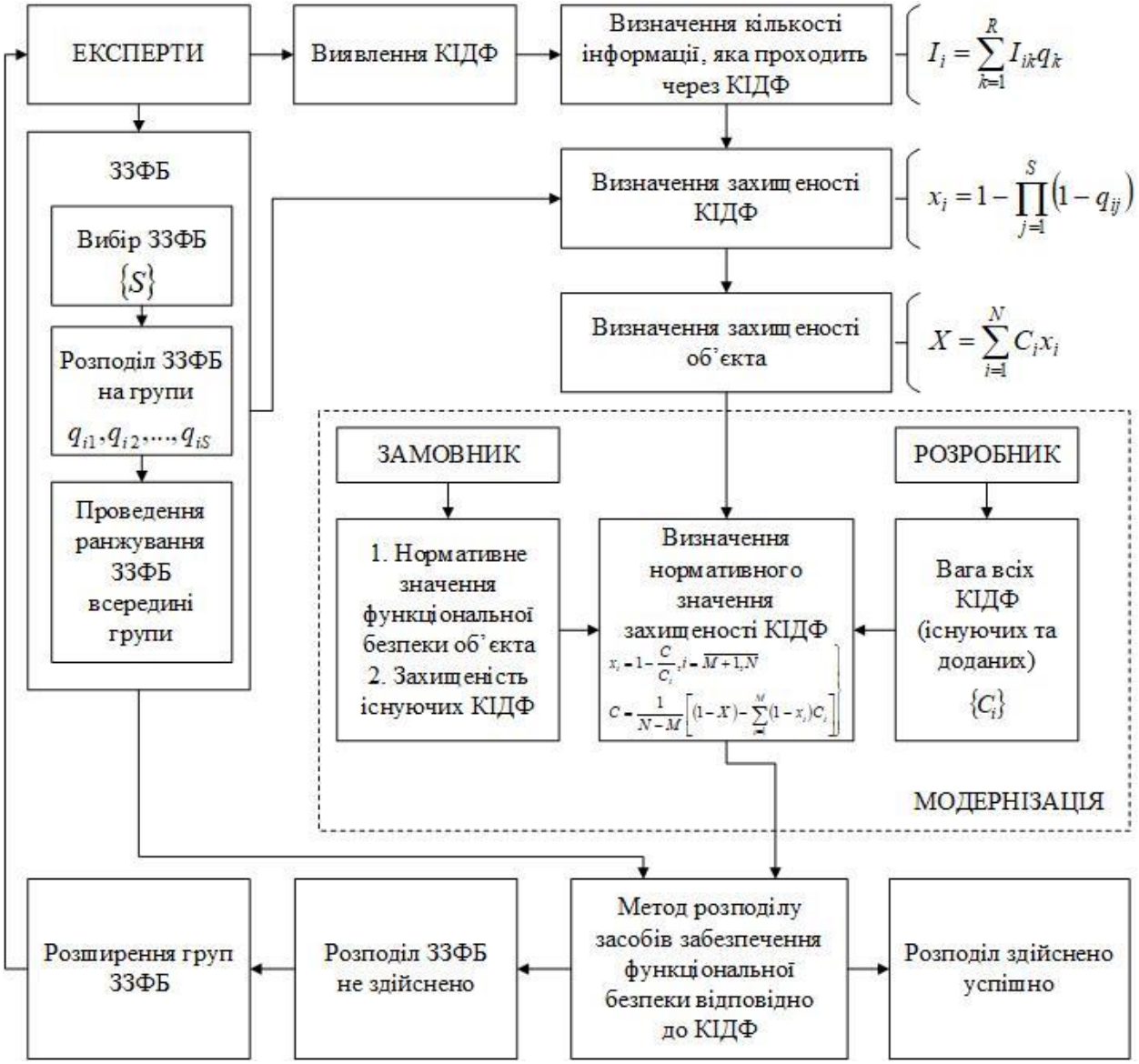


Рисунок 3.3 – Структурна схема методу розподілу засобів забезпечення функціональної безпеки в інтегрованій інформаційній системі на стадії модернізації

Перший етап – премодернізація, котрий передує безпосередньо модернізації. На цьому етапі експертами здійснюється виявлення КІДВ та вибір ЗЗФБ, які можуть бути потенційно використані в інтегрованій інформаційній системі. Ґрунтуючись на цих даних, аналітичними методами визначається кількість інформації, яка проходить через кожний КІДВ та відповідно до вимог керівних документів прикордонного відомства визначається нормативний ступінь функціональної безпеки та вибираються

відповідні ЗЗФБ для кожного каналу і, відповідно, визначається захищеність КІДВ. На підставі рівня захищеності кожного КІДВ визначається функціональна безпека об’єкта в цілому.

Другий етап – модернізація. На цьому етапі замовник визначає нормативне значення функціональної безпеки об’єкта. Загалом це значення може бути залишене з попереднього етапу або змінене замовником. Також надаються значення захищеності існуючих КІДВ. З іншого боку, розробником визначаються ваги всіх КІДВ, які були визначені на попередньому етапі. Це пов’язано з тим, що в процесі модернізації може бути змінена кількість інформації, котра проходить через КІДВ і, відповідно, змінений їх ваговий коефіцієнт. На підставі цих даних здійснюється визначення нормативного значення захищеності модернізованих та доданих КІДВ з урахуванням несприятливої для нас гіпотези про порушення, яке полягає в можливості здійснення дестабілізаційного впливу через будь-який КІДВ у будь-який момент часу.

На третьому етапі – постмодернізації здійснюється розподіл ЗЗФБ з визначеного експертами переліку та рангу. Результатом методу є раціональний розподіл ЗЗФБ між КІДВ. У випадку неможливості забезпечити нормативне значення функціональної безпеки експертам визначається завдання щодо розширення переліку ЗЗФБ і здійснюється повторне застосування методу розподілу ЗЗФБ.

Отже, застосування методу розподілу засобів забезпечення функціональної безпеки в інтегрованих інформаційних системах на стадії модернізації дозволить підтримувати нормативне її значення в ІІС у процесі модернізації як складових складної системи, так і при впровадженні нових елементів функціональної безпеки – засобів забезпечення функціональної безпеки. Водночас, комплексність проблеми функціональної безпеки вимагає розробки методу оцінювання уразливості інформаційної системи на стадії модернізації.

3.2 Метод оцінювання уразливості інформаційної системи на стадії модернізації

Для оцінювання уразливості ІС в інтегрованій інформаційній системі прикордонного відомства необхідна система показників, яка відображала б всі вимоги до забезпечення властивостей системи, а також структуру, технологію й умови автоматизованої обробки інформації [22]. Уразливість ІС необхідно оцінювати на всіх етапах її життєвого циклу: розробки, упровадження, функціонування. Кожний компонент системи робить свій внесок до загального стану уразливості ІС. Це призводить до того, що існуючий рівень складності програмних та апаратних складових ІС, організаційної структури функціонування системи, застосованих технологічних рішень вносить стохастичний характер до уразливості ІС. Разом із тим, вплив на елементи системи різних дестабілізаційних факторів в основному є випадковим. Отже, як кількісну міру уразливості ІС найдоцільніше прийняти ймовірність порушення її властивостей. У роботі [23] наведена класифікація властивостей інформаційної системи, порушення яких призводить до порушення функціональної безпеки інформаційних систем прикордонного відомства.

3.2.1 Введення показників уразливості інформаційної системи. Як згадувалося вище, показник уразливості ІС є однією зі складових інтегральної оцінки якості структури і технології функціонування СФБ. Модернізація складових ІІС "Гарт" зумовлює зростання інтенсивності потоку дестабілізаційний факторів (ДФ). Потік ДФ, що призводить до зниження властивостей ІІС, є стохастичним. Тому доцільно скористатися апаратом імовірнісного моделювання для адекватного представлення аналізованого аспекту якості СФБ у відомчій системі.

Дослідивши на моделі залежності, що призводять до підвищення інтенсивності потоку ДФ, можна ввести до моделі функції компенсації дестабілізаційних впливів [24]. Обґрунтувавши фізичний зміст компенсації,

можна отримати практично значущі результати щодо забезпечення надійного функціонування СФБ у модернізованій ІІС.

Закони розподілу ймовірностей загроз і ймовірностей успішної реалізації функції щодо конкретних ДФ, як зазначалося вище, не отримані. Однак, накопичений певний досвід у забезпеченні функціональної безпеки і формування чисельних значень можна проводити неформально-евристичними методами. У рамках моделі можливо врахувати також фрагментарне (спільне) використання видів функцій СФБ, що також характеризує надійність даних.

Для визначення аналітичних залежностей уразливості ІС необхідно врахувати активний вплив захисних функцій СФБ [25]. Приймемо ряд припущень:

1) внутрішні функції СФБ даних в окремо взятих старій і новій версіях ІС забезпечують захист від ІДФ, сформульованих в ТЗ, а також виявлених в процесі випробувань ІІС окремо;

2) різні ДФ діють на інформацію незалежно один від одного;

3) процес порушення надійності в компоненті ІІС не залежить від порушення властивостей ІС, що надходить в загальне поле гетерогенної системи (тобто програмно-апаратне середовище не робить збоїв і помилок, що впливає на загальний рівень функціональної безпеки).

Уразливість ІС на стадії модернізації – подія, яка виникає в результаті такого збігу обставин, в якій нова або стара версії спеціального програмного забезпечення не в стані протидіяти ДФ та негативному впливу останніх на ІС. В [9] наведені загальні моделі впливу на інформацію. Водночас в дослідженні не розглянута можливість спільного функціонуванні різних версій спеціального програмного забезпечення.

Введемо два види показників: базовий і узагальнений. Під базовим будемо розуміти показник уразливості ІС для одного елемента системи щодо одного дестабілізаційного фактору. Узагальнений – розраховується щодо сукупності будь-чого (складової ІІС, загроз, категорій даних) [9].

Далі, в рамках прийнятих припущень і позначень визначимо аналітичні залежності для оцінки уразливості ІС при різних варіантах реалізації захисних функцій СФБ.

3.2.2 Модель оцінювання уразливості інформаційної системи на стадії модернізації. Відповідно до структури критеріїв захищеності інформації [26] та властивостей ІС [23], а саме цілісності, конфіденційності, доступності, спостереженості, визначимо показник уразливості ІС (RI), фізичний сенс якого полягатиме у ймовірності порушення хоча б однієї властивості ІС.

Загальний вираз зазначеного показника буде виглядати так

$$RI = 1 - (1 - P_i) \cdot (1 - P_c) \cdot (1 - P_a) \cdot (1 - P_u), \tag{3.36}$$

де P_i – ймовірність порушення цілісності;

P_c – ймовірність порушення конфіденційності;

P_a – ймовірність порушення доступності.

P_u – ймовірність порушення спостереженості.

Визначимо імовірнісні залежності для оцінювання ключових аспектів властивостей інформаційної системи.

3.2.2.1 Порушення цілісності ІС. Для цілісності ІС, яка функціонує на загальному полі гетерогенної ІІС, щодо програмно реалізованих загроз представляють зовнішні та внутрішні фактори [27–30]. До зовнішніх загроз головними можна віднести два класи ДФ: віруси і помилки людей, що беруть участь в автоматизованій обробці інформації. До внутрішніх – наявність різних версій спеціального програмного забезпечення (СПЗ).

Відповідно до вищезазначеного та з урахуванням припущення, що програмно-апаратне середовище не робить збоїв і помилок, що знижують надійність даних, загальна модель процесу порушення цілісності ІС на

елементі ІС (АРМ, серверна частина, ЦСД) може бути представлена так, як це показано на рисунку 3.4.

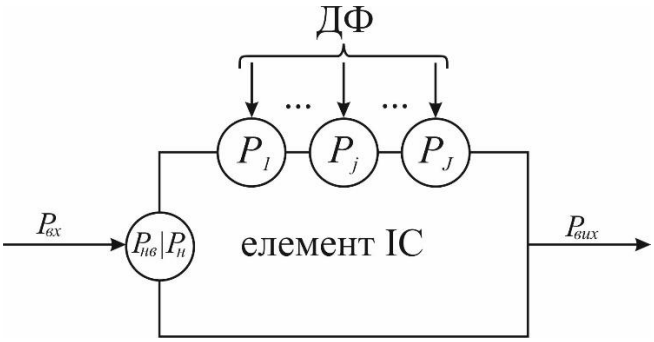


Рисунок 3.4 – Модель процесу порушення цілісності елемента ІС

Введемо такі позначення: $P_{вх}$ – ймовірність того, що дані певної категорії надходять у загальне поле елемента ІС зі старої або нової версій СПЗ з порушеною цілісністю; $P_н$ – ймовірність того, що дані надходять в елемент ІС іншої версії СПЗ; $P_{нв}$ – ймовірність того, що цілісність даних буде порушено в результаті неузгодженості версій СПЗ; P_j^i – ймовірність того, що цілісність даних буде порушена під впливом *j*-го ДФ (у разі злочинних дій щодо категорій порушників множина ДФ може бути розширена).

На загальному полі гетерогенної системи над даними, які надійшли, можуть відбуватися різні операції: криптографічне перетворення; постановка в чергу на збереження, передавання; запис даних у системні керуючі таблиці тощо. Усі вони мають різну тривалість і в кожній з них оператори беруть різну ступінь участі. Тому ймовірності реалізації конкретних загроз щодо різних категорій даних будуть відрізнятися.

Відповідно до теореми множення ймовірностей випадкових подій величина P_i може бути виражена такою залежністю

$$P_i = P_{вх} + (1 - P_{вх}) P_н P_{нв} \left(1 - \prod_{j=1}^{J} \left(1 - P_j^i \right) \right). \qquad (3.37)$$

Визначення значень $P_н$ можливе як співвідношення потоку даних на вхід елемента ІС. На рисунку 3.5 представлено фрагмент ІС ПТК АПК "Гарт-1" із одночасним функціонуванням різних версій СПЗ (варіант).

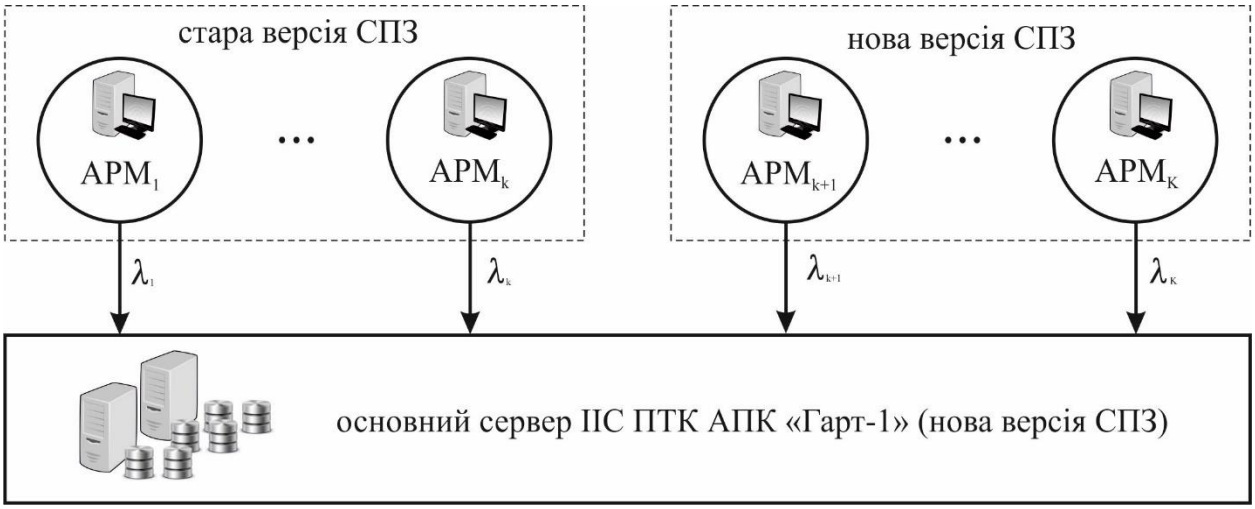


Рисунок 3.5 – Фрагмент ІС ПТК АПК "Гарт-1" із одночасним функціонуванням різних версій СПЗ (варіант)

Отже, ймовірність того, що дані надходять в елемент ІТС іншої версії СПЗ, є відношенням потоку даних старої версії СПЗ до загального потоку даних в наступний елемент ІТС, а саме

$$P_н = \frac{\sum_{i=1}^{k} \lambda_i}{\sum_{i=1}^{K} \lambda_i}. \qquad (3.38)$$

Визначення значень $P_{нв}$ в загальному випадку є проблемним з причини неможливості врахування всієї множини вихідних параметрів старої версії СПЗ. Водночас при визначенні ймовірності того, що цілісність даних буде порушено в результаті неузгодженості версій СПЗ, можна застосувати метод експертних оцінок або співвідношення кількості неузгоджених параметрів до загальної кількості з урахуванням ймовірності їх застосування.

3.2.2.2 Порушення конфіденційності. З точки зору порушення конфіденційності ІС головну небезпеку становлять злочинні дії [31–33]. У

роботах із захисту інформації проведена детальна систематизація цих дій для предметної області. Зазначимо, що дослідження питання порушення конфіденційності ІС здійснюється тільки у випадку сумісного використання даних різних версій СПЗ.

Введемо такі позначення:

$P_д$ – ймовірність доступу порушника до елемента ІС;

$P_{кідф}$ – ймовірність наявності каналу інформаційного дестабілізаційного впливу в елементі ІС до даних певної категорії;

$P_{дост}$ – ймовірність доступу порушника до КІДФ в елементі ІС;

$P_{нд}$ – ймовірність наявності даних певної категорії на елементі ІС;

P_j^c – ймовірність того що конфіденційність даних буде порушена під впливом *j*-го ДФ.

Тоді ймовірність порушення конфіденційності даних певної категорії порушником при умові надходження даних іншої версії СПЗ визначиться такою залежністю

$$P_c = P_д \cdot P_{кідф} \cdot P_{дост} \cdot P_{нд} \cdot P_{нв} \cdot P_н \left(1 - \prod_{j=1}^{J} \left(1 - P_j^c \right) \right). \qquad (3.39)$$

Відповідно до вищенаведеного визначення даний показник є базовим.

Ймовірність порушення конфіденційності ІС з урахуванням базового показника має вигляд:

$$P_c^{IC} = 1 - \prod_{i=1}^{m} \left(1 - P_c^i \right), \qquad (3.40)$$

де P_c^{IC} – ймовірність порушення конфіденційності інформаційної системи;

m – кількість складових, в яких може бути присутнім певна категорія даних;

P_c^i – базовий показник порушення конфіденційності в *i*-му елементі інформаційної системи.

Значення ймовірностей $P_н$ та $P_{нв}$ розраховуються аналогічно наведеними вище аналітичними залежностями.

3.2.2.3 Порушення доступності. Порушення можливості використання інформації, яка обробляється, або комп'ютерних систем становлять загрози доступності [26]. Окремі ІС прикордонного відомства надчутливі до даної загрози, наприклад, програмно-технічні комплекси автоматизації прикордонного контролю. У випадку недоступності певних даних можуть виникнути загрози національній безпеці при пропуску окремих осіб через державний кордон.

Для того, щоб ІС могла забезпечити доступність інформації, засоби забезпечення функціональної безпеки повинні надавати послуги щодо забезпечення можливості використання системи в цілому та окремих функцій або інформації, яка обробляється на певному проміжку часу і гарантувати спроможність ІС функціонувати у випадку відмови її компонентів [26].

Зазначимо, що в роботі прийнято припущення, що в окремих версіях ІС забезпечена послуга доступності інформації, апаратна складова не вносить дестабілізаційного фактору в роботу системи, а дослідження питання порушення доступності провадиться в умовах спільного використання даних різними версіями СПЗ.

Тоді ймовірність порушення доступності даних на елементі ІС при умові надходження даних іншої версії СПЗ визначиться такою залежністю

$$P_a = P_д \cdot P_{кідф} \cdot P_{дост} \cdot P_{нд} \cdot P_{нв} \cdot P_н \left(1 - \prod_{j=1}^{J} \left(1 - P_j^a \right) \right), \qquad (3.41)$$

де P_j^a – ймовірність того, що доступність даних буде порушена під впливом j-го ДФ.

Відповідно до вищенаведеного визначення даний показник є базовим.

Таким чином, порушення доступності ІС з урахуванням базового показника отримаємо

$$P_a^{IC} = 1 - \prod_{i=1}^{m} \left(1 - P_a^i\right), \tag{3.42}$$

де P_a^{IC} – ймовірність порушення доступності певної категорії даних у ІС;

P_a^i – базовий показник порушення доступності даних в i-му елементі ІС.

Зазначимо, що така властивість, як "доступність", залежить від наявності прав користувача на дану інформацію. Іншими словами, за відсутності таких прав порушення доступності не здійснюється. Питання доступності розглядається далі в межах систем розмежування доступу.

3.2.2.4 Порушення спостереженості. Ідентифікація і контроль за діями користувачів, керованість комп'ютерною системою становлять предмет спостереженості [26] та визначають події, які впливають на нього, а саме: реєстрація, ідентифікація і автентифікація, достовірний канал, розподіл обов'язків, цілісність комплексу засобів захисту, самотестування, автентифікація при обміні, автентифікація відправника (невідмова від авторства), автентифікація одержувача (невідмова від одержання). Зазначимо, що розподіл обов’язків визначається керівними документами та не буде розглядатись в цій моделі.

Спостереженість даних частково можна виразити через показники доступності, конфіденційності та цілісності. З метою визначення ймовірності порушення спостереженості даних введемо такі позначення: P_p – ймовірність порушення реєстрації події щодо певної категорії даних; P_{ia} – ймовірність

порушення ідентифікації і автентифікації порушника у складовій ІС; $P_{дк}$ – ймовірність порушення достовірності каналу доступу порушником при умові доступу порушника до складової ІІС; $P_{цкзз}$ – ймовірність порушення цілісності комплексу засобів забезпечення функціональної безпеки складової інформаційної системи.

Тоді ймовірність порушення спостереженості даних в елементі ІС визначиться такою залежністю

$$P_{и} = P_{н} \cdot P_{нв} \cdot P_{р} \cdot P_{іа} \cdot P_{дк} \cdot P_{цкзз}. \tag{3.43}$$

Ймовірність порушення реєстрації подій залежить від цілісності журналу обліку подій та його доступності. Зауважимо, що доступність журналу в рамках системи програмного адміністрування повинна бути постійною, тобто будь-яка подія повинна мати доступ та бути занесена до журналу ($P_p = P_i$). Ймовірність порушення ідентифікації і автентифікації порушником залежить від ймовірностей порушення цілісності та доступності

$$P_{ia} = \left(1 - \left(1 - P_i\right) \cdot \left(1 - P_c\right)\right) \cdot \prod_{m=1}^{M} P_m^{ia}, \tag{3.44}$$

де P_m^{ia} – ймовірність порушення ідентифікації і автентифікації m-м типом ідентифікації і автентифікації.

Ймовірність порушення цілісності комплексу засобів захисту виражається як змога протистояти множині дестабілізаційних факторів, а саме

$$P_{цкзз} = 1 - \prod_{j=1}^{J} \left(1 - P_j^{цкзз}\right). \tag{3.45}$$

Загалом структура моделі уразливості ІС на стадії модернізації відрізняється від існуючих (рисунок 3.6) доданими складовими, які враховують неузгодженість версій ІС та вимогами керівних документів.

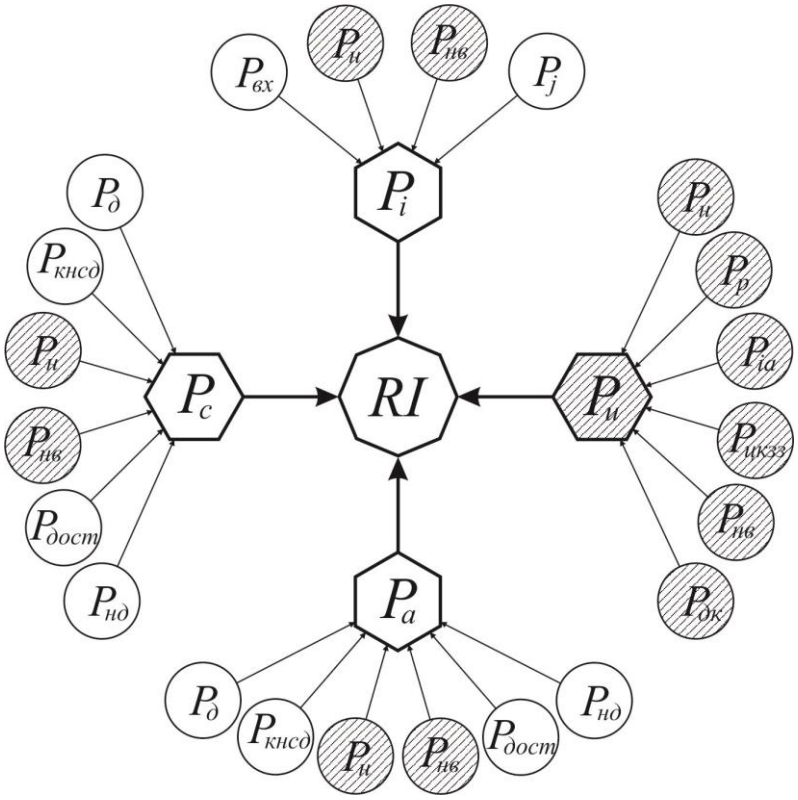


Рисунок 3.6 – Відмінність показника уразливості від існуючих моделей (додані елементи заштриховані)

Наведені вище функціональні залежності цілком можуть бути використані для визначення вірогідності порушення властивостей ІС. Однак для цього необхідні значення вищезазначених ймовірностей для всіх можливих дестабілізаційних факторів.

На сьогодні нам невідомі чітко визначені значення цих величин. Слід зробити ще одне зауваження. Основними елементами моделі, що розробляється, є випадкові величини. Для них необхідно знати закони розподілу, що характеризують випадкові події – прояв ДФ і числові характеристики цих розподілів, а також дані про дієвість застосування різних захисних функцій СЗІ в різних умовах.

Наскільки відомо, переважна кількість зазначених даних до цього часу також не сформовано. Проте, ґрунтуючись на евристичних даних (досвід, натурні експерименти, експертне оцінювання), можна використовувати дану модель для аналізу уразливості даних в потенційно можливих умовах, наприклад для прогнозу. Далі розширимо модель за рахунок введення, доданих функцій з метою компенсації потоку ДФ, обумовлених модернізацією ІІС.

3.2.3 Вплив доданих функцій узгодження на оцінку уразливості інформаційної системи. На стадії модернізації, з метою узгодження різних версій програмно-апаратного забезпечення ІС розробниками вводяться додані функції, які використовуються тільки на етапі спільного використання різних версій. Наочний вплив наявності цих функцій на загальний ступінь уразливості ІС і на ефективність функціонування СФБ.

Визначимо вимогу повноти множини функцій СФБ так: множина функцій повинна бути такою, щоб здійсненням їх в різних комбінаціях в будь-якій ситуації при функціонуванні ІС могли бути створені всі умови, необхідні для забезпечення дотримання властивостей інформаційної системи.

Вимога повноти функцій є абсолютною, проте регулярних методів вирішення подібних проблем не існує [34]. Отже, формування функцій СФБ доводиться здійснювати в такій ситуації, коли вимоги є абсолютними, а методи, що можуть бути при цьому використані, – відносні. При цьому доводиться використовувати неформальні методи – структурно-логічний аналіз, експертні оцінки і просто здоровий глузд компетентних фахівців.

В термінах структурно-логічного аналізу характеристика потенційно-можливих у процесі забезпечення функціональної безпеки ситуацій може бути подана в такому вигляді. Для того, щоб властивість інформаційної системи могла бути порушена, повинні мати місце такі умови, при яких можуть проявлятися ДФ. Якщо таких умов не буде, то не буде необхідності в дотриманні властивостей ІС. Якщо ж потенційні можливості для прояву ДФ матимуть місце, то треба оцінювати реальну можливість їх прояву, виявляти

факти прояву, вживати заходів до запобігання впливу їх на інформаційний ресурс ІС, виявлення, локалізації та ліквідації наслідків впливів на нього.

У окремих роботах [34–36] визначені три варіанти подій за результатами впливу ДФ щодо дотримання властивостей інформації. Разом із тим проведено аналіз необхідних базових функцій захисту. У роботі [34] доведено, що множина визначених функцій є повною в тому сенсі, що належним здійсненням кожної з перерахованих функцій можна забезпечити дотримання властивостей інформаційного ресурсу будь-якої ІС і в будь-яких умов їх функціонування. Ураховуючи те, що інформаційний ресурс ІІС є визначальним для прийняття управлінських рішень персоналом прикордонного відомства та безпосередньо впливає на ступінь функціональної безпеки, запропоновані варіанти можна перенести на ІС в цілому, тобто: властивість ІС забезпечена, властивість ІС порушена.

В умовах, коли функціональна безпека окремо забезпечена в різних версіях ІС, реалізація подій, пов'язаних з порушенням властивостей ІС, здійснюється за класичною схемою. При спільному функціонуванні на загальному полі даних різних версій технічних засобів забезпечення функціональної безпеки, програмних засобів забезпечення функціональної безпеки та спеціального програмного забезпечення виникають передумови до виникнення дестабілізаційних факторів, які викликані стадією модернізації. У даному випадку класична схема порушення властивостей ІС вимагає розширення, а саме визначення передумов прояву дестабілізаційних факторів, викликаних невідповідністю версій складових ІС, блок схема якої наведена на рисунку 3.7.

При виникненні передумов до спільного застосування технічних засобів забезпечення функціональної безпеки, програмних засобів забезпечення функціональної безпеки та спеціального програмного забезпечення необхідно виконати завдання їх узгодження під час здійснення модернізації.

В умовах модернізації ІС, коли апріорно в старій і новій версіях реалізуються умови спільного функціонування, для усунення колізій, викликаних відмінностями в форматах, системних протоколах тощо, потрібно призначення доданих функцій, відповідальних за дотримання властивостей ІС на загальному полі гетерогенного середовища [37].

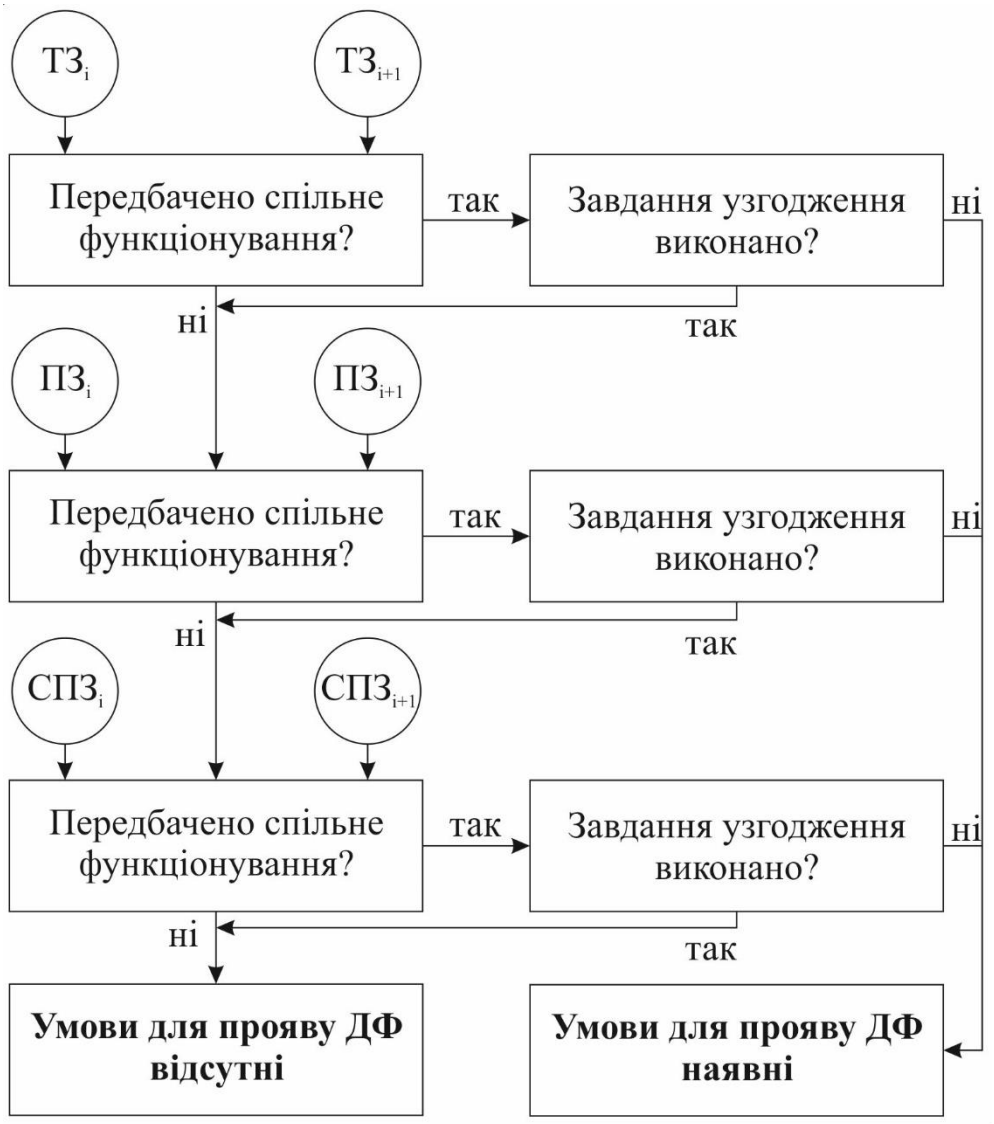


Рисунок 3.7 – Блок-схема визначення передумов прояву дестабілізаційних факторів викликаних невідповідністю версій складових ІС

Приймемо допущення – будемо визначати не безпосередні показники уразливості, а складові величини, що входять у вираз показників уразливості, такі як імовірності: 1) прояви ДФ; 2) наявність інформації в місці і під час

прояву ДФ; 3) порушення властивості ІС під впливом ДФ, незважаючи на застосування засобів забезпечення функціональної безпеки.

3.2.3.1 Імовірність прояву ДФ. На стадії модернізації ІІС процес функціонування системи не є сталим, тому потік ДФ відповідає розподілу Вейбулла на ділянці періоду модернізації [34]. Якщо через λ_{ij} позначити інтенсивність потоку *j*-го фактору відносно *i*-ї категорії даних, то щільність розподілу ймовірності Вейбулла буде мати вигляд

$$f_{ij}(t) = \lambda_{ij}\alpha t^{\alpha-1}e^{-\lambda_{ij}t^{\alpha}}, \tag{3.46}$$

де α – коефіцієнт, що характеризує етап життєвого циклу.

Графічне подання даного виразу показано на рисунку 3.8. Таким чином, ймовірність прояву дестабілізаційного фактору буде

$$p_{ij}(t) = \lambda_{ij}\alpha\int_{o}^{t} t^{\alpha-1}e^{-\lambda_{ij}x^{\alpha}}\,dx. \tag{3.47}$$

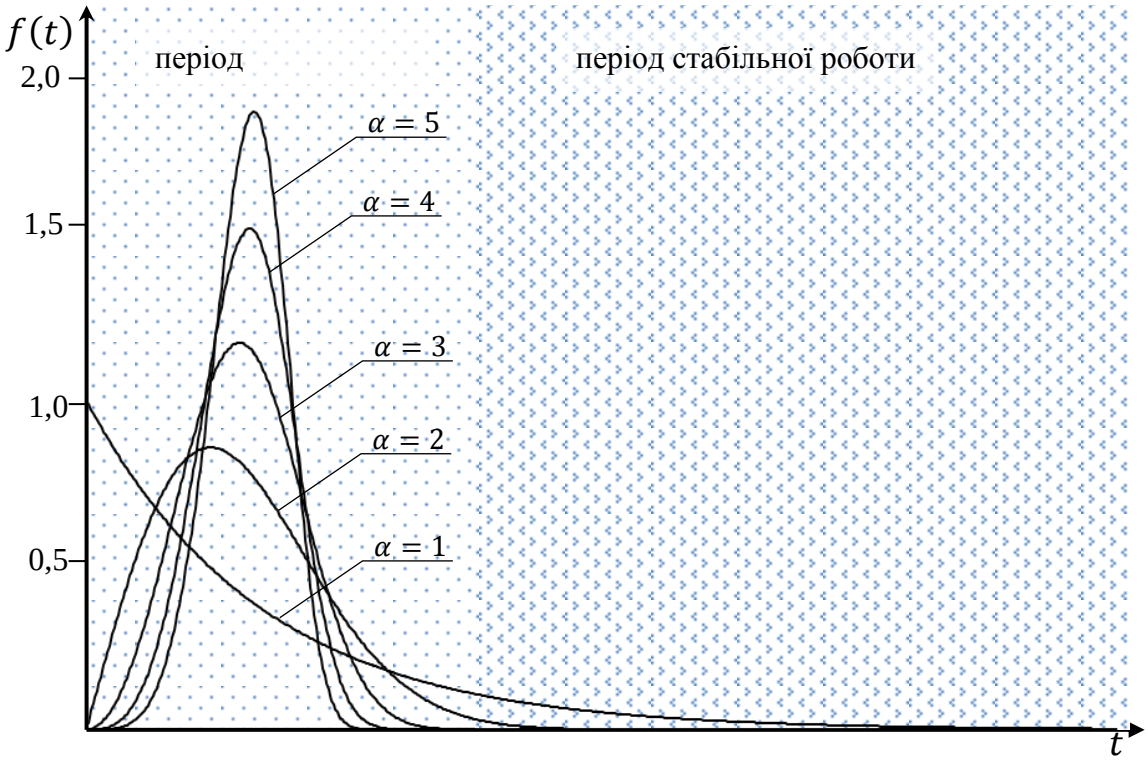


Рисунок 3.8 – Щільність розподілу ймовірності потоку ДФ на різних стадіях життєвого циклу інформаційної системи (при різних коефіцієнтах)

Розподіл ймовірності прояву ДФ $f_{ij}(t)$ має дві характерні ділянки: період модернізації та період стабільної роботи. У загальному випадку при розгляді у достатньо тривалому часі експлуатації період інтенсивних відмов в силу зношення апаратних засобів буде збільшуватись, але це виходить за рамки дослідження та детально розглянуто в теорії надійності.

Якщо до складу СФБ ввести деякі функції, що компенсують потік відмов, який зростає, то можна реально знизити ймовірність прояву, і, можливо, реалізації ДФ.

3.2.3.2 Ймовірність потреби забезпечення властивостей інформаційного ресурсу. Потреба у забезпеченні дотримання властивостей інформаційного ресурсу виникає тільки у випадку знаходження його складових у загальному полі гетерогенної ІІС, тобто при сумісному використанні спільних ресурсів системи користувачами з різними правами на дані, що розглядаються. Тільки тоді виникає загроза порушення властивостей інформаційного ресурсу. З метою визначення ймовірності знаходження даних *i*-ї категорії у загальному полі ІІС скористаємось логічним припущенням, що потреба в інформації залежить від її ступеня старіння, чим більший ступінь старіння, тим менша ймовірність її використання. Так, у керівних документах [38] визначаються терміни, після спливу яких здійснюється перегляд потреби у забезпеченні дотримання властивостей інформаційного ресурсу. Таким чином, чим старіші дані, тим менша ймовірність їх знаходження в загальному полі ІІС [39].

У багатьох наукових працях розглядається питання старіння інформації [18, 40–43]. Аргументується, але не доказується можливість експоненціальної формалізації старіння інформації. Тривалість існування корисної інформації, або такої, яка буде використовуватись та, відповідно, знаходитись в загальному полі ІІС, є випадковою величиною і залежить від певних факторів та може буди описана розподілом Гомперца-Мейкгама [44], в якому

параметр інтенсивності експоненційного розподілу має часовий тренд, котрий може бути описаний рівнянням модифікованої експоненти

$$\lambda(t) = a + be^{\lambda_0 t}, \tag{3.48}$$

де λ, a, b – параметри життєвого циклу інформації.

Таким чином, функція розподілу ймовірності невикористання (старіння) інформації набуде вигляду:

$$F_c(t) = \int_0^t \lambda(x) \cdot e^{\lambda(x)x} dx. \tag{3.49}$$

Позначимо величину ймовірності невикористання інформації через коефіцієнт використання, а саме:

$$K_в(t) = 1 - F_c(t). \tag{3.50}$$

Водночас у процесі експлуатації ІІС в систему постійно поступає нова інформація з параметром потоку $\lambda_{\text{вх}}$ та функцією розподілу

$$F_{вх}(t) = 1 - e^{-\lambda_{вх} t}. \tag{3.51}$$

Під одиницею інформації, яка поступає в систему, будемо розуміти певний блок даних, що пов’язаний логікою функціонування системи (інформація про перетин кордону особою, транспортним засобом, доручення правоохоронних органів).

Величина коефіцієнту використання інформації є випадковою та залежить від моменту появи інформації (рисунок 3.9), ймовірність якої розподілена за формулою (3.51).

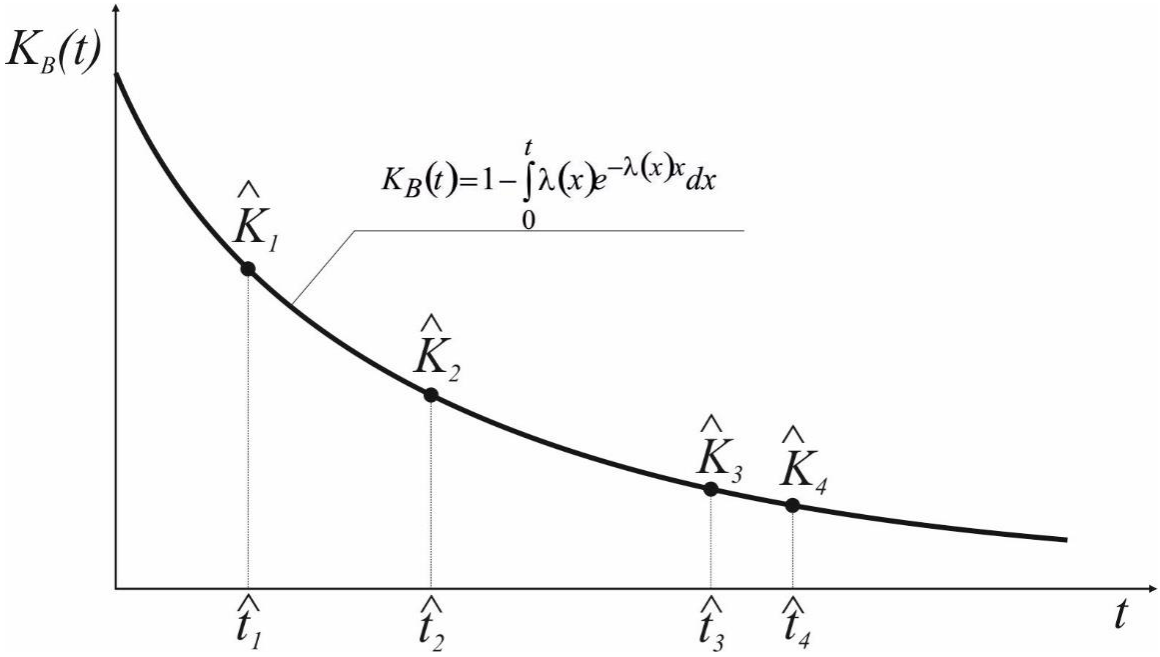


Рисунок 3.9 – Залежність коефіцієнту використання даних від часу їх перебування в ІІС

Функція розподілу випадкової величини коефіцієнту використання даних буде мати вигляд:

$$F(K) = P\left(K_в\left(\hat{t}\right) < K\right). \tag{3.52}$$

В результаті перетворень одновимірної випадкової величини, отримаємо:

$$F(K) = F_{вх}\left(K_в^{-1}(K)\right), \tag{3.53}$$

де $K_в^{-1}(K)$ – обернена функція до $K_в(t)$.

Фізичний сенс виразу (3.53) полягає у ймовірності появи інформації в загальному полі даних з величиною коефіцієнту використання не менше *K*.

Кількість інформації із рівнем коефіцієнту використання не менше *K*, яка поступила в систему в сталому режимі, становить

$$N = \lambda_{вх} K_в^{-1}(K). \tag{3.54}$$

Як видно із (3.54), кількість інформації із заданим рівнем коефіцієнту використання не залежить від часу експлуатації ІІС, а залежить тільки від величини інтенсивності вхідного потоку.

3.2.3.3 Імовірність порушення властивостей інформаційного ресурсу. Позначимо через $p_{ij}^{(\eta)}$ ймовірність того, що при використанні η-ї функції для захисту *i*-ї категорії даних при прояві *j*-го ДФ не буде порушення властивостей інформаційного ресурсу. Отже, ймовірність порушення властивостей *k*-го блоку *i*-ї категорії з величиною коефіцієнту використання не менше *K* даних становить

$$p_{ijk}(t) = 1 - F(K) \cdot \left(1 - p_{ij}(t)\right) \cdot \prod_{\forall \eta} \left(1 - p_{ij}^{\eta}\right). \tag{3.55}$$

Ймовірність порушення властивостей хоча б одного елемента даних *i*-ї категорії є

$$p_{ij}(t) = \prod_{k=1}^{N} \left(1 - p_{ijk}(t)\right). \tag{3.56}$$

При збільшенні числа η функцій, у тому числі і з перекриттям, значення показника уразливості знижується. Отже, для підвищення якості СФБ в гетерогенній ІІС доцільно ввести до її складу додані функції, що усувають колізії, що виникли в результаті сполучення. Водночас порушення властивостей ІнР залежить від інтенсивності потоку інформації в систему.

Таким чином, у запропонованій моделі оцінювання уразливості ІС досліджено зростаючий потік порушень уразливості інформаційного ресурсу, що має місце при сполученні різнорідних версій ІІС. Для зниження інтенсивності потоку в модель введені додані функції компенсації колізій, зумовлених невідповідностями структур ІС різних версій. Показано, що вони дозволяють зменшити уразливість ІнР. Реалізація фізичних аналогів цих функцій може бути проведена в складі СФБ, наприклад, як програмний

модуль, що підтримує захищений інтерфейс з СФБ обох версій і автономно контролює дотримання властивостей інформаційного ресурсу на загальному полі гетерогенної ІІС.

3.2.4 Структурна схема методу оцінювання уразливості інформаційної системи на стадії модернізації. Уразливість ІС – це випадкова подія, яка залежить від базових показників: цілісності, конфіденційності, доступності та спостереженості [26]. Загальний показник, у свою чергу, виражається через базові показники уразливості. У наведеному методі така складова, як доступність, розглядається тільки з урахуванням ДФ.

На стадії модернізації під впливом потоку дестабілізаційних факторів, спричинених дією як порушника, так і спільним використанням загального поля даних як нової, так і старої версій СПЗ, ступінь дотримання властивостей інформаційного ресурсу знижується. Узагальнений показник уразливості описується моделями процесів порушення властивостей ІС: цілісності, конфіденційності, доступності та спостереженості.

Вихідними даними для цих моделей, з одного боку, служать в основному висновки експертів, які визначають множину дестабілізаційних факторів та формують модель порушника. З іншого боку, організація-розробник спеціального програмного забезпечення визначає, які саме складові системи підлягають модернізації. На підставі вищезазначених вихідних даних визначається співвідношення параметрів різних версій СПЗ, що спільно функціонує. Разом з тим, у методі враховані й організаційні заходи, які провадить замовник при експлуатації ІІС, які можуть змінюватись залежно від вимог до модернізації системи.

На стадії модернізації окремі параметри системи зазнають змін, причому як структурні, так і функціональні. Ураховуючи масштабність існуючих ІІС, модернізація всієї системи здійснюється поступово протягом певного періоду часу, під час якого одночасно функціонують різні версії СПЗ, що вимагає врахування цього факту у зазначених моделях. У цей період

кількість ДФ зростає відповідно розподілу Вейбулла на ділянці періоду модернізації. Водночас ступінь уразливості визначає потребу забезпечення захисту інформаційного ресурсу на стадії модернізації тільки у випадку сумісного використання спільних ресурсів системи користувачами з різними правами на дані, що розглядаються, та різними версіями СПЗ (відповідно до прийнятого припущення, що окремі версії СПЗ забезпечують нормативний рівень функціональної безпеки). Це вимагає розробки та застосування в методі моделі визначення ймовірності використання інформаційного ресурсу різними версіями СПЗ. Зазначені моделі є вихідними для моделі порушення властивостей ІС на стадії модернізації [25].

Вищезазначене дозволяє сформувати структурну схему методу оцінювання уразливості ІС на стадії модернізації (рисунок 3.10).

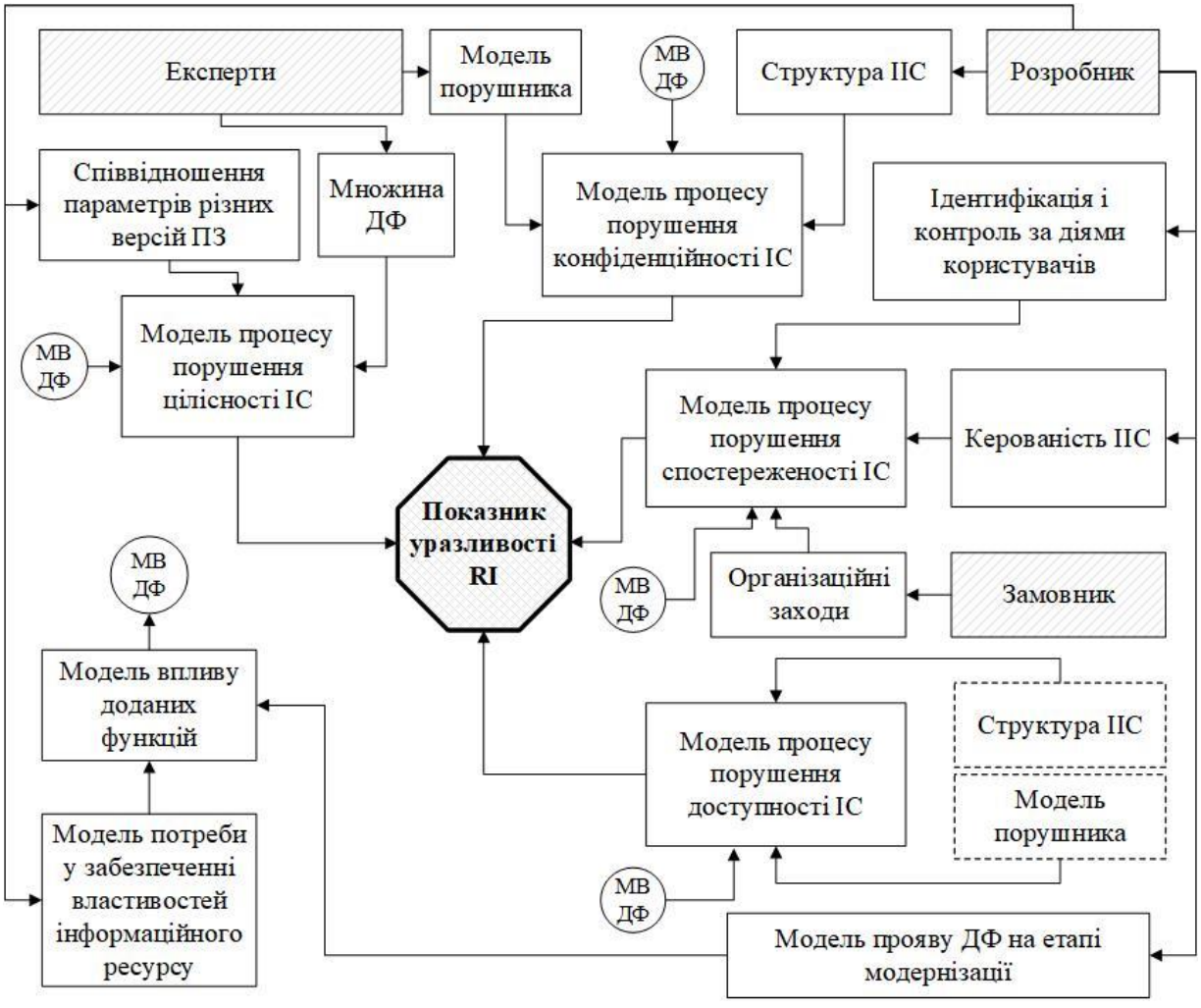


Рисунок 3.10 – Структурна схема методу оцінювання уразливості ІС на стадії модернізації.

Вихідні дані методу формують три категорії користувачів ІС: замовник, розробник та експерти. Експерти формують модель порушень та множину дестабілізаційних факторів, які впливають на властивості ІС.

Розробник відповідно до технічного завдання на модернізацію ІС формує нову структуру ІІС (за потреби), визначає співвідношення параметрів різних версій СПЗ. У залежності від призначення ІС визначаються величини інформаційного потоку в системах, які слугують вихідними даними для визначення потреби у забезпеченні властивостей інформаційного ресурсу.

Розробником регламентується технологія здійснення ідентифікації користувачів системи та функціонування системи контролю за їх діями. Зазначене разом із характеристиками керованості ІІС визначає величину порушення спостереженості ІС при її модернізації.

Замовник, у свою чергу, визначає, які організаційні заходи здійснюються для забезпечення функціональної безпеки на ОІД.

У результаті моделювання процесів порушення властивостей ІС визначається узагальнений показник уразливості ІС. Запровадження доданих функцій узгодження різних версій ІС впливає на загальний показник уразливості. Модель впливу доданих функцій враховує потребу у забезпечення властивостей інформаційного ресурсу та прояв дестабілізаційних факторів на стадії модернізації, тим самим корегуючи значення показника уразливості ІС.

3.3 Висновки до розділу 3

1. Розроблений метод розподілу засобів забезпечення функціональної безпеки містить: модель каналу інформаційного дестабілізаційного впливу, модель функціональної захищеності ІІС та метод розподілу засобів забезпечення функціональної безпеки відповідно до можливих каналів інформаційних дестабілізаційних впливів. Наведені дослідження дозволяють вирішити задачу аналізу та синтезу системи функціональної безпеки, при прийнятій гіпотезі, про найбільш несприятливу ситуацію про характер

дестабілізаційного впливу, яка полягає в можливості здійснення впливу з будь-якого КІДФ в будь-який момент часу.

2. Розроблений метод розподілу засобів забезпечення функціональної безпеки відповідно до можливих каналів інформаційного дестабілізаційного впливу дозволить раціонально розподілити ЗЗФБ за умови дотримання нормативного рівня захищеності системи в цілому. Отже, застосування методу розподілу засобів забезпечення функціональної безпеки в інтегрованих інформаційних системах на стадії модернізації дозволить підтримувати нормативне значення функціональної безпеки ІІС у процесі модернізації як складових складної системи, так і при впровадженні нових елементів СФБ – засобів захисту.

3. Модернізація складових ІІС "Гарт" зумовлює зростання інтенсивності потоку дестабілізаційних факторів, що призводить до порушень властивостей інформаційного ресурсу. У розділі відповідно до структури властивостей інформаційної системи визначено узагальнений показник уразливості ІС. З’ясовано ймовірність надходження даних в іншу версію спеціального програмного забезпечення. Обґрунтовано потребу забезпечення дотримання властивостей інформаційного ресурсу через рівень його старіння й аналітично визначена кількість інформації, яка має ступінь старіння не менше заданого. Показано, що кількість інформації із заданим рівнем коефіцієнта використання не залежить від часу експлуатації ІІС, а залежить тільки від величини інтенсивності вхідного потоку. Вищенаведене дозволить визначити ймовірність знаходження інформації на загальному полі даних обох версій СПЗ і, в свою чергу, ймовірність порушення функціональної безпеки.

4. З метою узгодження різних версій програмно-апаратного забезпечення ІС на стадії модернізації розробниками вводяться додані функції, які використовуються тільки на етапі спільного використання різних версій. Наявність цих функцій здійснює вплив на загальний ступінь уразливості ІС і на ефективність функціонування СФБ.

5. На стадії модернізації ІІС процес функціонування системи не є сталим, тому потік ДФ відповідає розподілу Вейбулла на ділянці періоду модернізації. Зазначене дозволить визначити величину потоку дестабілізаційних факторів, викликаних модернізацією.

6. У розробленій моделі оцінки уразливості ІС досліджено зростаючий потік ДФ, які спричиняють порушення властивостей інформаційного ресурсу за умови сполучення різнорідних версій ІІС. Для зниження інтенсивності потоку в модель введені додані функції компенсації колізій, зумовлених невідповідностями структур ІС різних версій. Показано, що вони дозволяють зменшити уразливість ІС.

7. У результаті моделювання процесів порушення властивостей ІС визначено узагальнений показник уразливості ІС. Запровадження доданих функцій узгодження різних версій ІС впливає на загальний показник уразливості. Модель впливу доданих функцій враховує потребу у забезпечення властивостей інформаційного ресурсу та прояв дестабілізаційних факторів на стадії модернізації, тим самим корегуючи значення показника уразливості ІС.

Список використаних джерел у третьому розділі

1. Стрельбіцький М. А. Окремі питання синтезу системного захисту інформації в інтегрованій інформаційно-телекомунікаційній системі прикордонного відомства на стадії модернізації / М. А. Стрельбіцький // Збірник наукових праць № 3 (65) Частина ІІ. – Хмельницький: НАДПСУ, 2014. С. 353-361

2. Стрельбіцький М. А. Системний захист інформації як складова забезпечення національної безпеки в інформаційній сфері / М. А. Стрельбіцький, В. А. Кириленко // Матеріали VI Всеукраїнської науково-практичної конференції "Освітньо-наукове забезпечення діяльності правоохоронних органів і військових формувань України" (м. Хмельницький, 2013).

3. Похил В. С. Удосконалений метод та інформаційна технологія забезпечення функціональної безпеки бортових інформаційно-керуючих систем авіації на етапі проектування / В. С. Похил // Наука і техніка Повітряних Сил Збройних Сил України – №2. –2010. – С. 65-70.

4. Похил В. С. Метод забезпечення функціональної безпеки бортових інформаційно-керуючих систем літальних апаратів на етапі їх експлуатації / В. С. Похил // Системи озброєння і військова техніка –№3. – 2010. – С. 68-74.

5. Харченко В. С. Гарантоздатність комп'ютерних систем: межа універсальності у контексті інформаційно-технічних станів / В. С. Харченко // Радіоелектронні і комп'ютерні системи – № 8. –2007. – С. 7-14.

6. Похил В. С. Удосконалений метод аналізу й оцінювання функціональної безпеки бортових інформаційно-керуючих систем повітряного судна / В. С. Похил // Системи озброєння і військова техніка – № 2. – 2010. – С. 136-142.

7. Харибін О. В. Інформаційна технологія забезпечення функціональної безпеки бортових інформаційно-керуючих систем авіації на етапі експлуатації / О. В. Харибін // Системи озброєння і військова техніка – № 2. – 2010. – С. 173-177.

8. Муляр І. В. Аналіз проблем забезпечення функціональної безпеки інформаційних систем обробки даних / І. В. Муляр, А. В. Джулій, М. В. Костюк // Вимірювальна та обчислювальна техніка в технологічних процесах. – 2013. – № 1. – С. 133-138.

9. Герасименко В.А., Малюк А.А. Основы защиты информации // Москва: МИФИ, 1997. — 537 с.

10. Дудатьев А. В. Метод оцінювання безпеки інформаційних ресурсів підприємства на основі аналізу вразливостей / А. В. Дудатьев, Ю. В. Баришев, О. П. Войтович // Вісник Хмельницького національного університету, - № 4, - 2008. - С.78-83.

11. Демідов Б. О. Системно-концептуальна модель управління життєвим циклом зразка озброєння і військової техніки. / Б. О. Демідов, О. О. Хмелевська // Системи озброєння і військова техніка №2 (2005): 47-53.

12. Стрельбіцький М. А. Окремі питання синтезу системного захисту інформації в інформаційно-телекомунікаційній системі прикордонного відомства на стадії модернізації / М. А. Стрельбіцький // Матеріали VIII всеукраїнської науково-практичної конференції "Освітньо-наукове забезпечення діяльності правоохоронних органів і військових формувань України" (м. Хмельницький, 2015).

13. Шеннон Клод. Работы по теории информации и кибернетике. Рипол Классик, 1963.

14. Колмогоров А. Н.. Теория информации и теория алгоритмов. – М.: Наука, 1987. – 304 с.

15. Стратонович, Руслан Леонтьевич. Теория информации. Сов. радио, 1975.

16. Грушо А. А. Ценность информации / А. А. Грушо, Е. Е. Тимонина // Теоретические основы защиты информации. – М.: Издательство Агентства "Яхтсмен", 1996.

17. Олійченко І. М. Побудова системи оцінки якості інформації в органах державного управління / І. М. Олійченко // Інвестиції: практика та досвід – № 3. –2010. – С. 71-72.

18. Архипов О. О. Про деякі аспекти визначення цінності конфіденційної інформації / О. О. Архипов // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні : науково-технічний збірник. – 2010. – Вип. 2(21). – С. 19-25.

19. Архипов А. О моделях прагматической ценности информации. / А. О. Архипов // Безпека інформації – № 1. – 2012. – С. 10-14.

20. Стрельбіцький М. А. Обґрунтування та вибір цільової функції системного захисту інформації в інтегрованій інформаційно-телекомунікаційній системі Державної прикордонної служби України /

М. А. Стрельбіцький // Збірник наукових праць Національної академії Державної прикордонної служби України. Сер. : Військові та технічні науки. – 2011. – № 56. – С. 63-64.

21. Стрельбіцький М.А. Окремі питання синтезу системного захисту інформації в інтегрованій інформаційно-телекомунікаційній системі прикордонного відомства на стадії модернізації / М. А. Стрельбіцький // Збірник наукових праць – № 3 (65) Частина ІІ. – Хмельницький: НАДПСУ, – 2014. С. 353-364

22. Аникин И. В. Теория информационной безопасности и методология защиты информации / И. В. Аникин, В. И. Глова, Л. И. Нейман// Учебное пособие. Казань: Изд-во Казан. гос. техн. ун-та, 2008 с. 358

23. Юдін О.К. Інформаційна безпека. Нормативно-правове забезпечення . – К., 2010 – 640 с.

24. Стрельбіцький М.А. Аналіз і систематизація причин виникнення збитків від реалізації загроз в інтегрованій інформаційно-телекомунікаційній системі державної прикордонної служби України / М. А. Стрельбіцький // Збірник наукових праць № 58 Частина ІІ. – Хмельницький: НАДПСУ, 2012 – С. 53-54.

25. Стрельбіцький М.А. Визначення показника уразливості даних в інформаційно-телекомунікаційних системах на стадії модернізації / М. А. Стрельбіцький // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка –К.: ВІКНУ, 2015. – Вип. № 51. – 241с С. 208-213

26. Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу НД ТЗІ 2.5-004-99. Затверджено наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від “28” квітня 1999 р. № 22 із змінами згідно наказу Адміністрації Держспецзв'язку від 28.12.2012 № 806

27. Юдін О. К. Концептуальний аналіз уразливості державних інформаційних ресурсів / О. К. Юдін, С. С. Бучик // Наукоємні технології – № 19.3 – 2013. – С. 299-304.

28. Інформаційна безпека. Навчальний посібник / С. В. Кавун, В. В. Носов, О. В. Манжай. – Харків: Вид. ХНЕУ, – 352 с.

29. Живко М. О. Основні чинники інформаційної безпеки підприємства / М. О. Живко, Х. З. Босак // Актуальні проблеми економіки №8 (2009).

30. Дзьобань О. П. Інформаційна безпека: нові виміри загроз, пов'язаних з інформаційно-комунікаційною сферою / О. П. Дзьобань, О. В. Соснін // Гуманітарний вісник Запорізької державної інженерної академії – № 61. – 2015. – С. 24-34.

31. Антонюк А. Загрози інформації і канали витоку / А.Антонюк, В. Жора // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні : науково-технічний збірник. – 2001. – Вип. 2. – С. 41-46.

32. Золотар О. О. Класифікація загроз інформаційній безпеці / О. О. Золотар, І. О. Трубін // Інформація і право – № 3. – 2013. – С. 105-112.

33. Цибуляк Б. Захист інформації з обмеженим доступом на засадах аутсорсингу / Б. Цибуляк // Вісн. НУ "Львівська політехніка". Серія "Автоматика, вимірювання та керування". – 2012. – № 741, ч. 2. – С. 246–250

34. Журиленко Б.Е. Математическая модель вероятностной надежности комплекса технической защиты информации / Б.Е. Журиленко // Безпека інформації. – 2012. – №2(18). – С.61-65.

35. Богуш В.М. Інформаційна безпека держави: навч. посіб. / В. М. Богуш, О. К. Юдін. – К.: "МК-Прес", 2005. – 432 с.

36. Канадские критерии безопасности компьютерных систем СТСРЕС [Електронний ресурс]. – Режим доступу: http://dehack.ru/mezhdunarodnye_standarty_po_otsenke_bezopasnosti_informatsio/kanadskie_kriterii_bezopasnosti_kompjuternyx_sistem_ctcpec/

37. Юдін О. К. Класифікація загроз інформаційному ресурсу ДПСУ на стадії модернізації / О. К. Юдін, М. А. Стрельбіцький // Вісник інженерної академії України, – вип 4, – 2016. – С.166-170.

38. Про затвердження Зводу відомостей, що становлять державну таємницю : Наказ Служби Безпеки України від 12.08.2005 № 440 / Зареєстровано в Міністерстві юстиції України 17 серпня 2005 р. за № 902/11182

39. Юдін О.К., Стрельбіцький М.А. Спосіб визначення кількості інформації з урахуванням фактору її старіння / О. К. Юдін, М. А. Стрельбіцький // Наукоємні Технології – Том 33, –№ 1 – 2017.

40. Ланде Д. В. Тренди відображення інформаційних операцій в інформаційному просторі / Д. В. Ланде // Інформація і право – № 1. – 2013. – С. 82-88.

41. Яковлєва Ю. В. Методика ранжування результатів пошуку в інформаційно-пошукових системах бібліотек / Ю. В. Яковлєва // Реєстрація, зберігання і оброб. даних. – 2004. – 6, № 3. – С. 66-73.

42. Мороз Б. І. Методи класифікації інформації для організації реплікацій у розподілених базах даних за ознаками цінності і старіння / Б. І. Мороз, Л. В. Кабак // Вісник Академії митної служби України. Сер.: Технічні науки – № 1. – 2010. – С. 86-92.

43. Гарасимчук О. І. Оцінка ефективності систем захисту інформації / О. І. Гарасимчук, Ю. М. Костів // Вісник КНУ ім. М. Остроградського – Кременчук: КНУ ім. М. Остроградського – № 1. – 2011.

44. Gompertz B., 1825. On the Nature of the Function Expressive of the Law of Human Mortality, and on a New Mode of Determining the Value of Life Contingencies. Philosophical Transactions of the Royal Society of London, Vol. 115 (1825) pp. 513—585.

РОЗДІЛ 4
ТЕОРЕТИЧНІ ОСНОВИ УЗГОДЖЕННЯ МОДЕЛЕЙ РОЗМЕЖУВАННЯ ДОСТУПУ ІНФОРМАЦІЙНИХ СИСТЕМ НА СТАДІЇ МОДЕРНІЗАЦІЇ

Проблеми забезпечення безпеки інформаційних систем держави є постійним та актуальним предметом обговорення в наукових колах. Дана проблема також є об'єктом уваги міжнародних організацій, зокрема ООН [1]. Сучасний стан розвитку суспільства характеризується великою роллю електронних ресурсів, які становлять інформаційну інфраструктуру держави та системи регулювання відносин, що виникають при цьому, зокрема політики безпеки.

Формування політики безпеки включає вирішення як технічних аспектів, так і організаційних проблем [2]. Це передбачає відповіді на певні запитання: яка інформаційна система потребує забезпечення відповідного рівня безпеки, безпеку якого інформаційного ресурсу здійснювати, які види інформаційних дестабілізаційних факторів враховувати, які дестабілізаційні впливи можуть бути здійснені, які сили та засоби використовувати для забезпечення дотримання властивостей інформаційного ресурсу. Як правило, основним завданням політики безпеки є присвоєння суб'єкту і об'єкту ідентифікаторів та фіксації набору правил, які дозволяють визначити, чи має даний суб'єкт вказаний тип доступу до даного об'єкта [3, 4].

Основним питанням формування політики безпеки є вирішення завдання забезпечення конфіденційності інформації. Разом із тим необхідно пам'ятати про решту властивостей інформації, а саме цілісність, доступність і спостереженість.

Політика безпеки є базовою категорією у галузі захисту інформації інформаційних систем. Під нею розуміють сукупність законів, правил, обмежень, рекомендацій, інструкцій тощо, які регламентують порядок обробки інформації [5].

Під час розробки інформаційних систем та визначення ступеня їх рівня захищеності суттєву роль відіграють моделі безпеки [6–8]. Їх застосування забезпечує системний та науково обґрунтований підхід до [9]:

– вибору й обґрунтування основних підходів до структури інформаційних систем, що визначає способи реалізації методик, методів та засобів забезпечення властивостей інформаційного ресурсу;

– формального підтвердження стану захищеності інформаційної системи шляхом доказу теорем безпеки використаних моделей політик безпеки;

– розробка формального опису політики безпеки.

Отже, моделі безпеки є базовою складовою, на основі яких замовники формулюють вимоги до захищеності інформаційних систем [9, 10]. Вибір моделі безпеки, яка буде застосована в конкретній ІС, залежить від особливостей її в інтегрованій ІС прикордонного відомства. Це також дозволить експертам розробити методики і специфікації оцінки захищеності зазначеної інформаційної системи, здійснити сертифікацію інформаційної системи за вимогами, що висуваються до складових властивостей інформаційного ресурсу.

Розробкою та дослідженням моделей інформаційної безпеки присвячена значна кількість робіт дослідників, серед яких Leonard J. LaPadula, D. Elliot Bell, M. Harrison, J. Hoffman , А.А. Грушо та інші. Методологічні основи до моделювання процесів захисту інформації розглянуті також в роботах В. А. Герасименко [11], одного з відомих дослідників теоретичних і практичних аспектів захисту інформації в автоматизованих системах, автора системно-концептуального підходу до інформаційної безпеки. Герасименко подав загальну модель процесів захисту інформації, структурувавши її на взаємопов'язані компоненти, і виділивши в окремий блок моделі систем розмежування доступу до ресурсів обчислювальної системи.

Водночас розроблена та впроваджена в дію велика сукупність міжнародних і вітчизняних стандартів та нормативних документів у галузі інформаційної безпеки [12–15].

Моделі інформаційної безпеки [16–18] не передбачають спільного функціонування з іншими аналогічними моделями на загальному полі даних, як це можливо під час модернізації інформаційних системи у складі ІІС. У всіх моделях передбачено функціонування єдиної системи (монітору безпеки, ядра безпеки тощо), яка забезпечує дотримання політики безпеки.

Серед програмно-технічних методів забезпечення властивостей інформаційного ресурсу ІС основним, у більшості випадків, є система розмежування доступу [19–22]. Зазначена система безпосередньо забезпечує конфіденційність інформаційного ресурсу, а також впливає на ймовірність порушення властивостей цілісності і доступності [23, 24].

4.1 Визначення критерію якості системи розмежування доступу інформаційної системи на стадії модернізації

Формування політики безпеки ІІС, під час дотримання якої забезпечується дотримання властивостей інформаційного ресурсу, неможливе без моделей інформаційної безпеки, як формалізованого опису її базових засад. Тільки за допомогою формальних моделей можна довести безпеку системи, спираючись при цьому на постулати математичної теорії. Моделі безпеки визначають базові принципи функціонування політики безпеки та використовуються під час її побудови, формування технологічних рішень та обґрунтовують здатність системи забезпечувати дотримання властивостей інформаційного ресурсу [20]. Аналіз структури зазначених моделей дозволяють визначити переваги та недоліки порівняно з іншими моделями, що зі свого боку сприяє опису виду критерію якості систем розмежування доступу, які побудовані на базі цих моделей [25–31].

На теперішній час запропоновано достатньо багато стратегій моделювання поведінки системи розмежування доступу [11, 32–35]. Частина з

них, не дозволяючи узагальнено описати деталі, змушені спрощувати або ігнорувати найчастіше важливі деталі системи [36]. У зв'язку з цим доцільно застосувати схему моделювання, що використовує абстрагування для спрощення аналізу захисту, і, разом з тим, ураховує всі деталі поведінки системи, необхідні для повного захисту.

Кожна із відомих моделей оперує трійкою: суб’єкт, об’єкт, операція, тобто яку операцію може здійснити суб’єкт над об’єктом (читання, запис, видалення тощо).

Для подання системи розмежування доступу (СРД) визначимо ряд множин:

– об'єктів $\{O\}$ – термінали, вузли мережі, канали зв'язку, зовнішні пристрої, програми, томи, каталоги, файли, записи, поля запису;

– суб'єктів $\{S\}$ – користувачі або процеси, що виконуються від їх імені (користувачі, адміністратори, програми, процеси, термінали);

– операцій $\{\Omega\}$ – послідовності дій суб'єкта по відношенню до об’єкта.

На основі введених вище понять СРД становить об'єкт теоретико-множинного обчислення – декартовий добуток виду: $S \times O \times \Omega$. Правила розмежування доступу тоді будуть описуватися моделлю інформаційної безпеки, результати якої характеризують дозвіл або заборону операції ω_i з боку s_j по відношенню до o_k.

Якщо СРД у складі старої версії подати у вигляді: $S_1 \times O_1 \times \Omega_1$, а нової версії як: $S_2 \times O_2 \times \Omega_2$, то для випадку, коли істинний, такий вираз,

$$\begin{array}{l}(S_1 \cap S_2 = \varnothing) \wedge (O_1 \cap O_2 = \varnothing) \wedge (\Omega_1 \cap \Omega_2 = \varnothing) \vee \\ \vee (S_1 \setminus S_2 = \varnothing) \wedge (O_1 \setminus O_2 = \varnothing) \wedge (\Omega_1 \setminus \Omega_2 = \varnothing)\end{array}, \qquad (4.1)$$

колізії між новою і старою версіями системи розмежування доступу в ІІС відсутні. Дана вироджена ситуація не входить в область дослідження.

Досліджувані суперечності існують, якщо результатом взяття декартової різниці між $S_1 \times O_1 \times \Omega_1$ та $S_2 \times O_2 \times \Omega_2$ буде відмінна від $\varnothing$ підмножина $S_R \times O_R \times \Omega_R$, яка, у загальному випадку, буде складатися з компонентів обох поколінь СРД гетерогенної системи. Фізично елементи цієї множини утворюють спільне поле, через яке здійснюється взаємодія різнорідних компонентів ІІС.

Проаналізуємо, якими властивостями повинна володіти і яким вимогам задовольняти структура СРД $S_R \times O_R \times \Omega_R$, з метою усунення невідповідностей, що призводять до можливості порушення політики безпеки.

Організація доступу до інформаційних ресурсів ІС користувачів або процесів від їх імені відповідно до їх повноважень є призначенням будь-якої СРД. Завдання такого розмежування полягає у дотриманні вимог політики безпеки яка запроваджена в ІС, а саме властивостей інформації. Порушення властивостей інформації трактується керівними документами та науковцями [37–39] як будь-які небажані дії, що призводять до порушення хоча б однієї із властивостей інформації. Отже, для порушення властивостей інформації необхідна дія (вплив) користувача на об’єкт системи, який містить дану інформацію.

Розглянемо кожну із властивостей інформації на предмет спільних ознак, які призводять до порушення заданої властивості. Відповідно до [5] конфіденційність – властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем і/або процесом. Тобто наявність недозволеного інформаційного потоку між об’єктом-носієм інформації та користувачем призводить до порушення конфіденційності. Наступна властивість інформації – цілісність, суть якої полягає в тому, що інформація не може бути модифікована неавторизованим користувачем і/або процесом [5].

Аналогічно попередній властивості, наявність недозволеного інформаційного потоку призводить до порушення цілісності. Ще одна

властивість інформації – доступність, як властивість ресурсу системи, яка полягає в тому, що користувач або процес від його імені, що має відповідні політикою безпеки повноваження, має право використовувати ресурс, не очікуючи довше заданого проміжку часу, тобто коли він знаходиться у вигляді, необхідному користувачеві, у місці, необхідному користувачеві, і в той час, коли він йому необхідний [5]. У даному випадку відсутність інформаційного потоку, який передбачено політикою безпеки як дозволений, призводить до порушення доступності.

Аналогічно іншим, спостереженість – властивість, що дозволяє фіксувати діяльність користувачів і процесів, використання пасивних об’єктів, а також однозначно установлювати ідентифікатори причетних до певних подій користувачів і процесів з метою запобігання порушення політики безпеки і/або забезпечення відповідальності за певні дії [5]. Дане визначення передбачає наявність дозволеного інформаційного потоку до журналів обліку діяльності користувачів та процесів, а також фіксації інших дій.

Загальною ознакою порушення кожної із властивостей інформації є наявність недозволеного або відсутність дозволеного інформаційного потоку. Як правило, такого виду потоки виникають в обхід політики безпеки та є прихованими. Під прихованим інформаційним потоком будемо розуміти механізм, за допомогою якого в ІІС може здійснюватися інформаційний потік (передача інформації) між сутностями в обхід політики (правил) розмежування доступу [40].

Водночас сам факт порушення правил виникнення інформаційних потоків (наявність прихованих інформаційних потоків) має імовірнісний характер. Отже, імовірність виникнення прихованих інформаційних потоків адекватно характеризує якість структури системи розмежування доступу.

4.2. Спільне функціонування моделей розмежування доступу на загальному полі даних під час модернізації інформаційних систем

Для дослідження спільного функціонування різних версій моделей безпеки комп'ютерних системи обрано такі види моделей: дискреційного, рольового, мандатного та тематичного розмежування доступу; безпеки інформаційних потоків; суб'єктно-орієнтовану модель ізольованого програмного середовища.

4.2.1 Спільне функціонування моделей дискреційного розмежування доступу. Моделі дискреційного розмежування (Харісона–Руззо–Ульмана, типізованих матриць доступу, Take–Grant, розширена модель Take–Grant та інші) оперують матрицею доступу $M[s,o]$, рядки якої відповідають суб'єктам, стовбці об'єктам системи, а комірки визначають право доступу суб'єкта s на об'єкт o [40–44].

У разі спільного функціонування різних версій цих моделей можлива реалізація двох ситуацій, за яких можливе порушення політики безпеки. Перша, значення прав доступу різних версій СРД для спільних суб'єктів та об'єктів різні, тобто $\exists s_i, \exists o_j$ за яких $M_1[s_i, o_j] \neq M_2[s_i, o_j]$, де $s_i \in S_1, s_i \in S_2, o_j \in O_1, o_j \in O_2$. У даному випадку існує порушення політики безпеки, тому що під час здійснення операції суб'єкта відносно до об'єкта, яку дозволяє СРД однієї версії є забороненою у іншій версії або навпаки. У другому випадку значення прав доступу різних версій СРД для спільних суб'єктів та об'єктів однакові, тобто $M_1[s_i, o_j] = M_2[s_i, o_j]$, для $\forall s_i \in S_1, \forall s_i \in S_2, \forall o_j \in O_1, \forall o_j \in O_2$. Водночас наявність суб'єктів та об'єктів, які не входять до СРД іншої версії, дозволяє здійснити інформаційний потік в обхід політики безпеки однієї із версій (рисунок 4.1).

На рисунку 4.1 показаний один елемент (суб'єкт S_1), який присутній у першій СРД та відсутній у другій і через який здійснюється інформаційний потік в обхід матриці доступу $M_2[s,o]$. Необхідно зазначити, що однією із

властивостей інформаційних потоків є їх транзитивність, тому під час визначення "обхідного" інформаційного потоку необхідно враховувати всі об’єкти та суб’єкти системи.

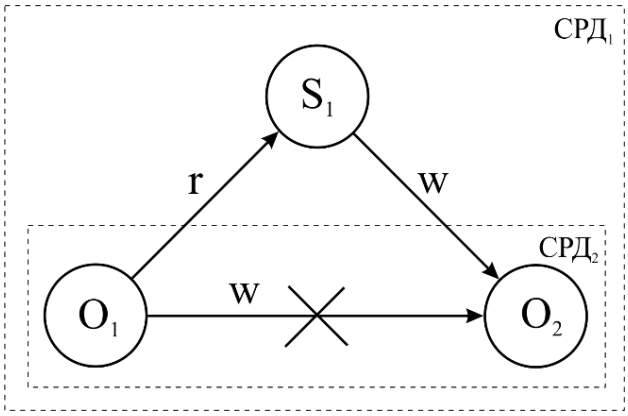


Рисунок 4.1 – Варіант реалізації інформаційного потоку в обхід політики безпеки однієї із версій системи розмежування доступу

4.2.2 Спільне функціонування моделей рольового розмежування доступу. Моделі рольового розмежування доступу є подальшим розвитком політики дискреційного розмежування доступу. Відмінністю є те, що права доступу суб’єктів системи об’єднуються, утворюючи групи з однаковими правами, які визначаються з урахуванням специфіки їх функціональних завдань у системі [30, 45]. Отже, у разі спільного функціонування двох СРД, які побудовані за принципом рольового розмежування доступу, можливе виникнення інформаційного потоку в обхід однієї із версій СРД аналогічно дискреційному розмежуванню доступу.

У загальному випадку не є обов’язковим рівність прав кожної ролі в умовах спільного функціонування різних версій СРД. У даному випадку, якщо існує роль r_i^1 – старої та r_j^2 – нової СРД за яких права на об’єкт o_k відрізняються, то існує порушення політики безпеки однієї із версій СРД, тому що під час здійснення операції користувача з роллю r_i^1 відносно об’єкта, яку дозволяє СРД однієї версії є забороненою операцією в ролі r_j^2 іншої версії або навпаки.

У результаті досліджень інформаційних потоків у разі спільного функціонування різних версій систем рольового розмежування доступу висунуто гіпотезу, що для дотримання політики безпеки при спільному функціонуванні обох версій рольового розмежування доступу необхідно та достатньо рівності множин прав доступу ролей різних версій СРД для спільних об’єктів.

4.2.3 Спільне функціонування моделей мандатного розмежування доступу. Моделі мандатного розмежування доступу (класична модель Белла–ЛаПадули, модель безпечного переходу, модель систем воєнних повідомлень, політика low–watermark, модель цілісності Біба й інші) передбачають аналіз умов, під час виконання яких неможливий інформаційний потік від об’єктів з більшим рівнем конфіденційності до об’єктів з меншим рівнем конфіденційності [32, 45–49].

Виникнення недозволеного інформаційного потоку в одній із версій СРД у разі спільного їх функціонування можливе у випадку:

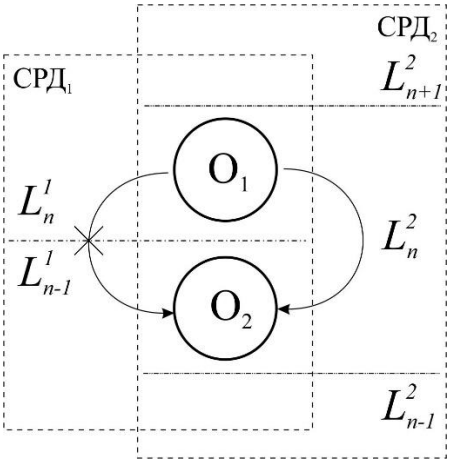
– невідповідності решіток рівнів конфіденційності об’єктів СРД, що може призвести до забороненого в одній із версій інформаційного потоку (рисунок 4.2);

– невідповідності матриць доступу $M[s,o]$;

Доцільно зазначити, що наявна нормативно-правова база чітко визначає решітку рівнів конфіденційності об’єктів, тому виникнення недозволеного інформаційного потоку у перший спосіб є малоймовірним. Водночас реалізація другого способу можлива аналогічно моделі дискреційного розмежування доступу.

4.2.4 Спільне функціонування моделей тематичного розмежування доступу. Моделі тематичного розмежування доступу оперують тематичним ієрархічним класифікатором (рубрикатором), що включає кінцеву множину тематичних рубрик, на яких встановлений частковий порядок, який визначається кореневим деревом [32, 40]. У моделях тематичного

розмежування доступу множина сутностей $X = S \cup O$ тематично класифікується на основі відображення на множину мультирубрик, які визначені на кореневому дереві ієрархічного рубрикатора.



де L^1, L^2 – решітки рівнів конфіденційності старої та нової версій системи МРД.

Рисунок 4.2 – Реалізація інформаційного потоку в обхід політики безпеки однієї із версій системи розмежування доступу у разі невідповідності решіток рівнів конфіденційності

Виникнення недозволеного інформаційного потоку в одній із версій тематичного розмежування доступу під час спільного їх функціонування можливе у разі невідповідності тематик сутностей системи (рисунок 4.3).

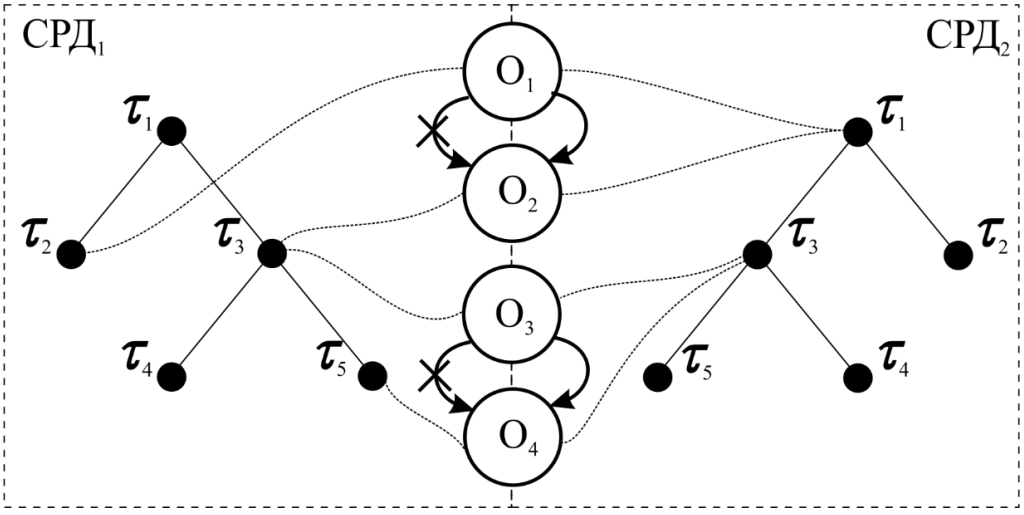


Рисунок 4.3 – Реалізація інформаційного потоку у разі невідповідності тематичних ієрархічних класифікаторів різних версій систем розмежування доступу

Як приклад наведемо два випадки суперечностей інформаційних потоків різних версій тематичного розмежування доступу для чотирьох спільних об’єктів, а саме:

– перший, СРД$_1$ об’єкти o_1 та o_2 знаходяться в непорівнюваних за тематикою сутностями і, як наслідок, такі потоки є забороненими. Водночас в СРД$_2$ зазначені об’єкти знаходяться в одній тематиці, тому інформаційний потік між ними дозволений;

– другий, СРД$_1$ об’єкт o_3 знаходиться в сутності з більш широкою тематикою, а o_4 з більш вузькою, тому такий потік є забороненим. Водночас у СРД$_2$ зазначені об’єкти знаходяться в одній тематиці, тому інформаційний потік між ними дозволений.

У результаті досліджень інформаційних потоків у разі спільного функціонування різних версій систем тематичного розмежування доступу висунуто гіпотезу, що для дотримання політики безпеки при спільному функціонуванні обох версій тематичного розмежування доступу необхідно та достатньо ієрархічної рівності тематичних класифікаторів різних версій СРД для спільних об’єктів.

4.2.5 Спільне функціонування моделей безпеки інформаційних потоків. Моделі безпеки інформаційних потоків (інформаційного не виведення та інформаційного невтручання) ґрунтуються на розподілі всіх можливих потоків між об’єктами інформаційної системи на дві множини, які не перетинаються, а саме на дозволені та недозволені потоки [32]. Отже, основне завдання системи захисту, яка побудована за моделлю безпеки інформаційних потоків, є недопущення виникнення недозволених інформаційних потоків.

Зазначена модель для сегрегації інформаційних потоків у більшості випадків базується на політиках безпеки інших видів, наприклад дискреційного або мандатного розмежування доступу. При спільному функціонуванні різних версій системи розмежування доступу, які побудовані

за моделлю безпеки інформаційних потоків, можливе порушення однієї з політик безпеки у разі невідповідності рівнів конфіденційності або, у випадку застосування політики безпеки інших видів, у випадку невідповідності матриць доступу.

4.2.6 Спільне функціонування суб'єктно-орієнтованих моделей ізольованого програмного середовища. Суб'єктно-орієнтована модель ізольованого програмного середовища аналогічно моделі безпеки інформаційних потоків оперує двома множинами, які не перетинаються, а саме на потоки, що характеризують несанкціонований доступ, і потоки, що характеризують легальний (санкціонований) доступ [32]. Варто зазначити, що у даній моделі не здійснюється уточнень відомих політик безпеки. Політика безпеки описує тільки критерій розподілу всіх інформаційних потоків на дві підмножини. Отже, суб'єктно-орієнтована модель ізольованого програмного середовища є інваріантною до прийнятої в системі політики безпеки та у разі спільного функціонування різних версій системи розмежування доступу має її недоліки.

Проведене дослідження спільного функціонування різних версій систем розмежування доступу, які побудовані на розглянутих моделях безпеки комп'ютерних систем показало можливі шляхи виникнення інформаційних потоків в обхід політики безпеки однієї із версій системи розмежування доступу.

Моделі дискреційного розмежування доступу оперують матрицею доступу, а мандатного – решіткою рівнів конфіденційності, які у разі спільного функціонування різних версій СРД потребують узгодження. Для моделей рольового та тематичного розмежування доступу сформульовані гіпотези дотримання політики безпеки у випадку спільного функціонування різних версій СРД.

4.3 Метод узгодження решіток рівнів конфіденційності систем мандатного розмежування доступу інформаційних систем на стадії модернізації

Функціонування інформаційних систем Державної прикордонної служби як суб'єкта забезпечення національної безпеки України [50] безпосередньо пов'язано із запобіганням основних загроз національним інтересам і національній безпеці України в інформаційній сфері. Широкомасштабна інтеграція програмно-технічних засобів автоматизації практично у всі сфери діяльності прикордонного відомства вимагає постійного вдосконалення та модернізації складових інтегрованої інформаційної системи. На теперішній час ІІС складається більш як з 20 інформаційних систем та 10 підсистем, що забезпечують виконання різних функціональних завдань, систем забезпечення та взаємодії з іншими відомствами з питань національної безпеки України в прикордонній сфері. Особливістю ІІС "Гарт" є функціонування її складових (ІС, підсистем) на загальному полі даних, що дозволяє максимально ефективно аналізувати прикордонну інформацію [51]. Ступінь безпеки інформації в інформаційних системах Державної прикордонної служби, як суб'єкта забезпечення національної безпеки, впливає на якість виконання завдань прикордонного відомства та, відповідно, на рівень національної безпеки України.

Водночас виклики та загрози національній безпеці держави у прикордонній сфері вимагають постійної адаптації засобів автоматизації до вимог сьогодення. Це вимагає узгодження засобів забезпечення функціональної безпеки під час модернізації складових ІІС (упровадження нових систем), які функціонують на загальному полі даних.

Моделі інформаційної безпеки є базисом формування політик безпеки різних інформаційних систем. Формальні моделі дозволяють довести безпеку системи відомими та апробованими методами наукових досліджень [48]. Отже, політика безпеки ІС, яка побудована за постулатами певної моделі

інформаційної безпеки, здатна гарантовано виконати функції щодо функціональної безпеки інформаційної системи в цілому.

Під час розробки складових ІІС формалізується та реалізовується певна політика безпеки, яка базується на відомих моделях інформаційної безпеки. Їх використання в окремих ІС та підсистемах забезпечує виконання функцій щодо забезпечення властивостей інформації. При модернізації наявних складових ІІС або інтеграції нових виникає ситуація спільного функціонування систем забезпечення функціональної безпеки на загальному полі даних.

Моделі мандатного розмежування (МРД) доступу (класична модель Белла–ЛаПадули, модель безпечного переходу, модель систем воєнних повідомлень, політика low–watermark, модель цілісності Біба та інші) аналізують умови, під час виконання яких неможливий інформаційний потік від об’єктів з більшим рівнем конфіденційності до об’єктів з меншим рівнем конфіденційності [32]. У даних моделях кожний суб’єкт і об’єкт системи асоціюється з відповідним рівнем безпеки (конфіденційності).

Під час спільного використання обох версій системи МРД об’єктів та суб’єктів загального поля даних можливе виникнення недозволеного інформаційного потоку в одній із версій з причини невідповідності решіток рівнів конфіденційності об’єктів.

Вищезазначене вимагає розробки методу узгодження решіток рівнів конфіденційності різних версій систем мандатного розмежування доступу.

Метод узгодження решіток рівнів конфіденційності різних версій систем мандатного розмежування доступу призначений для формування спільної для обох версій СРД решітки рівнів конфіденційності на стадії модернізації інформаційних систем.

Суть методу узгодження решіток рівнів конфіденційності різних версій систем мандатного розмежування доступу полягає у формуванні спільної для обох версій єдиної решітки рівнів конфіденційності, в якій неможливо

реалізувати недозволений інформаційний потік у кожній з версій СРД окремо (рисунок 4.2).

Структурна схема методу узгодження решіток рівнів конфіденційності різних версій систем розмежування доступу подана на рисунку 4.4.

Визначення спільної для обох версій СРД функції перетворення меж решітки конфіденційності здійснюється в кожному випадку окремо.

Прикладами такої функції може бути вартість втрати інформації, можливий збиток від порушення конфіденційності тощо.

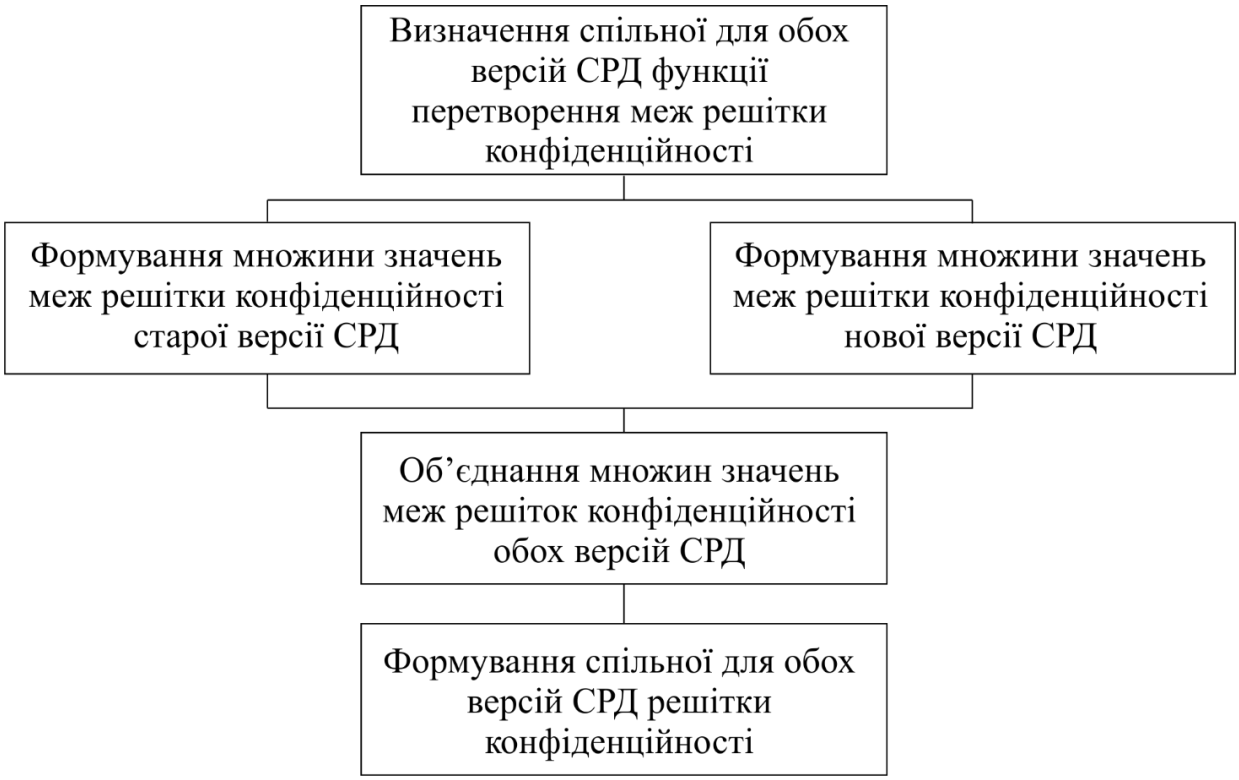


Рисунок 4.4 – Структурна схема методу узгодження решіток рівнів конфіденційності різних версій систем розмежування доступу

На теперішній час розроблено достатньо представницький арсенал моделей оцінки інформації. У роботі [52] наведено окремі з них, а саме:

– адитивна модель, в якій інформація подана як кінцева множина елементів, де експерти здійснюють оцінку кожного елемента окремо, а вартість інформації подається сумою вартостей її елементів;

– аналіз ризику – модель, яка базується на адитивній моделі, але оцінюється вартість втрат, виходячи із прогнозу можливих загроз компонентам інформації;

– порядкова шкала цінностей – модель, яка оцінює інформацію не за її грошовою оцінкою, а як порівняння цінностей окремих інформаційних елементів між собою;

– модель решітки цінностей – узагальнена модель порядкової шкали цінностей.

Призначення зазначеної функція полягає у перетворенні формально описаних меж решітки конфіденційності в числові значення.

Аналітично метод узгодження решіток рівнів конфіденційності різних версій систем розмежування доступу подається таким чином.

Нехай:

$\left(L^{old},\leq\right),\left(L^{new},\leq\right)$ та $\left(L^{join},\leq\right)$ – решітки рівнів конфіденційності старої, нової та спільної систем мандатного розмежування доступу;

$f:(L,\leq)\to Q, Q\in\mathbb{R}$ – відображення меж решітки конфіденційності в підмножину дійсних чисел.

Тоді спільна для обох версій СРД решітка конфіденційності визначається

$$f^{-1}:\left(\left(L^{old},\leq\right)\xrightarrow{f}Q^{old}\cup\left(L^{new},\leq\right)\xrightarrow{f}Q^{new}\right)\to\left(L^{join},\leq\right), \qquad (4.2)$$

де $f^{-1}:Q\to L$ – обернене відображення множини дійсних чисел у межі решітки конфіденційності.

Вищенаведений метод вимагає формулювання та доказу того, що у запропонованій спільній решітці конфіденційності неможливо реалізувати заборонений інформаційний потік в одній версії СРД та дозволений в іншій версії СРД (рисунок 4.1).

Теорема безпеки спільної решітки конфіденційності. У спільній решітці конфіденційності неможливо реалізувати заборонений інформаційний потік в одній версії СРД і дозволений в іншій версії СРД.

Доказ. У системах розмежування доступу під час використання решіток конфіденційності недозволеним інформаційним потоком є потік від об'єктів з вищим рівнем конфіденційності до об'єктів з нижчим рівнем конфіденційності. Припустимо, що у спільній решітці конфіденційності можливий такий потік, який в одній із версій СРД дозволений, а в другій – заборонений. Це означає, що об'єкти повинні знаходитись в одній множині решітки конфіденційності однієї версії (дозволений інформаційний потік) і в різних множинах решітки конфіденційності іншої версії (недозволений інформаційний потік). Водночас розбиття спільної решітки конфіденційності передбачає знаходження таких об'єктів у різних множинах спільної решітки конфіденційності (рисунок 4.5). Отже, зазначений інформаційний потік буде забороненим, що суперечить припущенню про його існування [53].

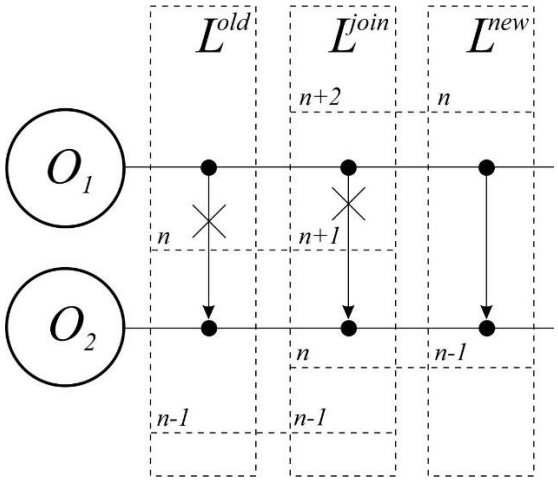


Рисунок 4.5 – До доказу теореми безпеки спільної решітки конфіденційності

Застосування методу узгодження решіток рівнів конфіденційності різних версій систем мандатного розмежування доступу здійснюється таким чином. Перед спільним функціонуванням наявної та модернізованої системи розмежування доступу здійснюється узгодження решіток рівнів конфіденційності та визначається спільна для обох версій решітка рівнів

конфіденційності. Наступним етапом є зміна параметрів кожної із версій СРД відповідно до сформованої спільної решітки рівнів конфіденційності. Заключним етапом є інтеграція модернізованої складової ІС до загальної системи, при чому параметри СРД яких уже узгоджені. Отже, під час спільного функціонування наявної та модернізованої ІС неможливе виникнення недозволених інформаційних потоків і, як наслідок, порушення безпеки інформації.

Розроблений метод узгодження решіток рівнів конфіденційності різних версій систем мандатного розмежування доступу дозволить формально описати процедуру спільного функціонування обох інформаційних систем з питань дотримання властивостей інформації та визначити умови, за яких неможливе виникнення недозволених інформаційних потоків [53].

4.4 Метод узгодження матриць доступу систем дискреційного розмежування доступу інформаційних систем на стадії модернізації

Виконання основних функцій Державної прикордонної служби України [50] з питань здійснення в установленому порядку прикордонного контролю і пропуску через державний кордон України осіб, транспортних засобів, вантажів, а також виявлення і припинення випадків незаконного їх переміщення, ведення інформаційно-аналітичної діяльності, координація діяльності військових формувань та відповідних правоохоронних органів, пов'язаної із захистом державного кордону України, а також діяльності державних органів, що здійснюють різні види контролю під час перетинання державного кордону України пов’язане зі зберіганням та обміном інформації службового характеру між суб’єктами інтегрованого управління кордонами.

У міру розвитку і розширення сфери застосування обчислювальної техніки все більша частина діяльності органів охорони державного кордону приходиться на автоматизовану обробку інформації. За допомогою програмно-апаратних засобів обчислювальної техніки виконуються операції над даними, від забезпечення безпеки яких залежить вирішення покладених на

ДПСУ функціональних завдань. Водночас постійна модернізація програмно-технічних комплексів автоматизації окремих завдань прикордонного відомства вимагає узгодження різних версій систем розмежування доступу, які функціонують на спільному полі даних.

Розробкою та дослідженням моделей дискреційного розмежування доступу присвячена значна кількість робіт дослідників. Перші роботи були опубліковані ще в 60-х роках минулого століття. Найбільш відомі з них: модель ADEPT-50 на замовлення МО США [54, 55], п'ятивимірний простір Хартсона [56], модель Харрісона–Руззо–Ульмана [57] та інші. Зазначені моделі оперують дискретним набором трійок "суб'єкт–потік (операція) – об'єкт".

Структура політик безпеки, які базуються на моделях дискреційного розмежування доступу не передбачає оперування спільними з іншими системами об'єктами та суб'єктами, як це можливо під час модернізації інформаційних систем у складі відомчих автоматизованих систем.

Безпека інформації, що циркулює в інтегрованій інформаційній системі прикордонного відомства забезпечується коректним формуванням політики безпеки, яка базується на відомих, формально доказаних моделях безпеки. Саме принципи, на яких базуються моделі безпеки, обґрунтовують здатність системи забезпечувати безпеку інформації.

На стадії модернізації ІІС, тобто в умовах спільного функціонування різних версій систем розмежування доступу, можливе виникнення недозволеного інформаційного потоку. Тому на цьому етапі життєвого циклу, коли апріорно різні версії програмного забезпечення оперують спільними даними, для усунення колізій, викликаних відмінностями моделей розмежування доступу, необхідно здійснити завдання їх узгодження.

Моделі дискреційного розмежування доступу (Харісона–Руззо–Ульмана, типізованих матриць доступу, Take–Grant, розширена модель Take–Grant та інші) оперують матрицею доступу $M\lfloor s_i, o_j \rfloor$, рядки якої відповідають

суб'єктам $S=\{s_i\}$, стовбці об'єктам $O=\{o_j\}$ системи, а комірки визначають право доступу суб'єкта s_i на об'єкт o_j [41].

Розглянемо дві ситуації, за яких можливе порушення політики безпеки в умовах функціонування на загальному полі даних різних версій СРД, які базуються на моделі дискреційного розмежування доступу.

Перша ситуація, значення прав доступу різних версій СРД для спільних суб'єктів та об'єктів різні, тобто $\exists s_i, \exists o_j$ за яких $M_1[s_i, o_j] \neq M_2[s_i, o_j]$, де $s_i \in S_1, s_i \in S_2, o_j \in O_1, o_j \in O_2$. У даному випадку існує порушення політики безпеки, тому що під час здійснення операції суб'єкта відносно до об'єкта, яку дозволяє СРД однієї версії є забороненою у іншій версії або навпаки.

У другому випадку значення прав доступу різних версій СРД для спільних суб'єктів та об'єктів однакові, тобто $M_1[s_i, o_j] = M_2[s_i, o_j]$, для $\forall s_i \in S_1, \forall s_i \in S_2, \forall o_j \in O_1, \forall o_j \in O_2$. Водночас наявність суб'єктів та об'єктів, які не входять до СРД іншої версії, дозволяють здійснити інформаційний потік в обхід політики безпеки однієї із версій.

На рисунку 4.1 показаний один елемент (суб'єкт S_1), який присутній у першій СРД та відсутній у другій і через який здійснюється інформаційний потік в обхід матриці доступу $M_2[s,o]$. Необхідно зазначити, що однією із властивостей інформаційних потоків є їх транзитивність, тому під час визначення "обхідного" інформаційного потоку необхідно враховувати всі об'єкти та суб'єкти системи.

Отже, дотримання безпеки інформації в умовах спільного функціонування різних версій СРД вимагає розробки методу їх узгодження.

Метод узгодження матриць доступу різних версій систем розмежування доступу призначений для формування спільної для обох версій СРД матриць доступу на етапі модернізації інформаційних систем.

Суть методу узгодження матриць доступу різних версій систем розмежування доступу полягає у формуванні спільної для обох версій єдиної

матриці доступу, в якій неможливо реалізувати недозволений інформаційний потік у кожній з версій СРД окремо (рисунок 4.1).

Для аналітичного опису методу опишемо вихідні дані.

$M^{old}_{|S_{old}|\times|O_{old}|} = M^{old}[s_{old}, o_{old}]$ – матриця доступу старої версії СРД;

$M^{new}_{|S_{new}|\times|O_{new}|} = M^{new}[s_{new}, o_{new}]$ – матриця доступу нової версії СРД;

$M^{join}_{|S_{join}|\times|O_{join}|} = M^{join}[s_{join}, o_{join}]$ – матриця доступу спільної версії СРД.

При чому, $S_{join} = S_{old} \cup S_{new}$ та $O_{join} = O_{old} \cup O_{new}$.

Визначимо множини суб'єктів та об'єктів, які є спільними для обох версій СДР, а саме $S_{sub} = S_{old} \cap S_{new}$ та $O_{sub} = O_{old} \cap O_{new}$.

За умови невідповідності елементів матриць доступу як старої, так і нової версій СРД узгодження матриць є неможливим, тому спільне функціонування обох версій системи розмежування доступу призведе до порушення властивостей інформації. Отже, необхідною, але не достатньою умовою узгодження різних версій систем розмежування доступу, а саме їх матриць доступу, є

$$M^{old}[s,o] = M^{new}[s,o], \forall s \in S_{sub}, \forall o \in O_{sub}. \quad (4.3)$$

Наступним етапом методу є визначення можливості створення інформаційного потоку, який є легальним в одній версії СРД і нелегальний в іншій.

Вихідними умовами узгодження різних версій СРД є те, що політика безпеки в кожній із них окремо сформована коректно та не допускає порушення властивостей інформації. Тому необхідно розглядати тільки спільну частину матриць доступу різних версій СРД, а саме $M^{sub}_{|S_{sub}|\times|O_{sub}|} = M^{sub}[s_{sub}, o_{sub}]$ у разі дотримання умови (4.3). Узгодженість різних версій СРД, а саме спільної матриці доступу $M^{join}[s_{join}, o_{join}]$ можлива

тільки у випадку рівності інформаційних потоків щодо об'єктів $M^{sub}_{|S_{sub}|\times|O_{sub}|}$ у різних матрицях доступу.

Нехай $F^{old}_{|O_{sub}|\times|O_{sub}|} = \Re\left(M^{old}_{|S_{old}|\times|O_{old}|}, O_{sub}\right)$, $F^{new}_{|O_{sub}|\times|O_{sub}|} = \Re\left(M^{new}_{|S_{new}|\times|O_{new}|}, O_{sub}\right)$ – бінарні матриці інформаційних потоків старої та нової версій СРД між спільними об'єктами відповідно, а $\Re$ – оператор формування бінарної матриці інформаційних потоків між спільними об'єктами обох версій СРД і певної матриці доступу.

Вихідними даними для оператора формування бінарної матриці інформаційних потоків є матриця доступу $M_{|S|\times|O|} = M[s,o]$ і підмножина об'єктів O', де $O' \in O$.

Наступним етапом є формування матриці суміжності. З цією метою розіб'ємо множину прав доступу R на підмножини: $\vec{R} \in R$ – підмножина прав доступу, яка формує інформаційний потік від суб'єкта до об'єкта (наприклад, право write), $\overleftarrow{R} \in R$ – підмножина прав доступу, яка формує інформаційний потік від об'єкта до суб'єкта (наприклад, право read), $\tilde{R} \in R$ – підмножина прав доступу, яка не формує інформаційний потік (наприклад, право delete). Елементи матриці суміжності $E_{|O|\times|O|} = \{e_{ij}\}$ формуються таким чином

$$e_{ij} = \begin{cases} 1, \exists k\, M[s_k, o_i] \in \overleftarrow{R}, M[s_k, o_j] \in \vec{R} \\ 0, else \end{cases}. \qquad (4.4)$$

Надалі, ураховуючи властивості графу [58] визначається матриця досяжності як сума диз'юнкцій матриць суміжності, а саме

$$E^* = E \vee E^2 \vee \ldots \vee E^{|O|}. \qquad (4.5)$$

З метою зменшення розрахунків пропонується використати алгоритм (рисунок 4.6).

Суть алгоритму полягає у припиненні розрахунків у випадку, якщо в наступній ітерації не з’являється новий шлях.

Завершальним етапом оператора формування бінарної матриці інформаційних потоків між спільними об’єктами обох версій СРД є формування підмножини інформаційних потоків між зазначеною підмножиною об’єктів

$$F = \left\{ e_{ij}^{*} \right\}, \forall o_i, o_j \in O'. \tag{4.6}$$

Отже, результатом наведеної методики розрахунків є визначення бінарної матриці інформаційних потоків між спільними об’єктами обох версій СРД.

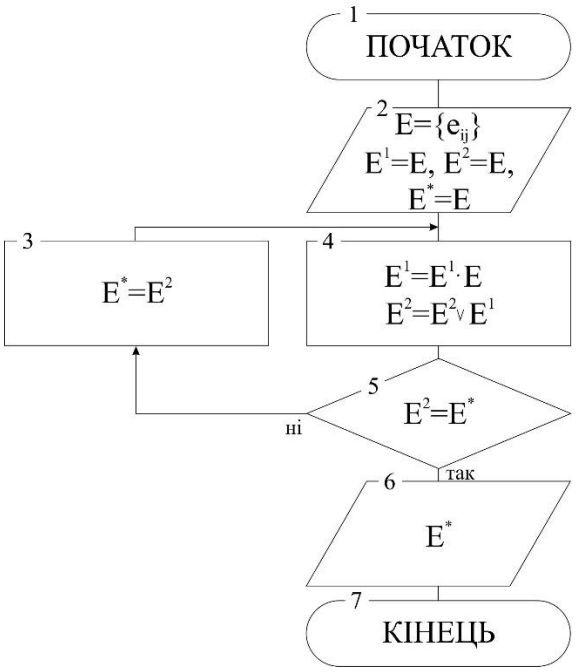


Рисунок 4.6 – Блок-схема алгоритму визначення матриці досяжності

Використання вищезазначеного оператора дозволить сформувати множину інформаційних потоків ураховуючи матриці доступу для кожної із версій СРД. Рівність бінарних матриць інформаційних потоків між спільними об’єктами в кожній версії свідчить про узгодженість обох версій СРД.

Структурна схема методу узгодження матриць доступу різних версій систем розмежування доступу подана на рисунку 4.7.

Вищенаведений метод вимагає формулювання та доказу того, що у разі рівності інформаційних потоків спільних об’єктів обох версій СРД неможливо реалізувати заборонений інформаційний потік в одній версії СРД та дозволений в іншій версії СРД (рисунок 4.1).

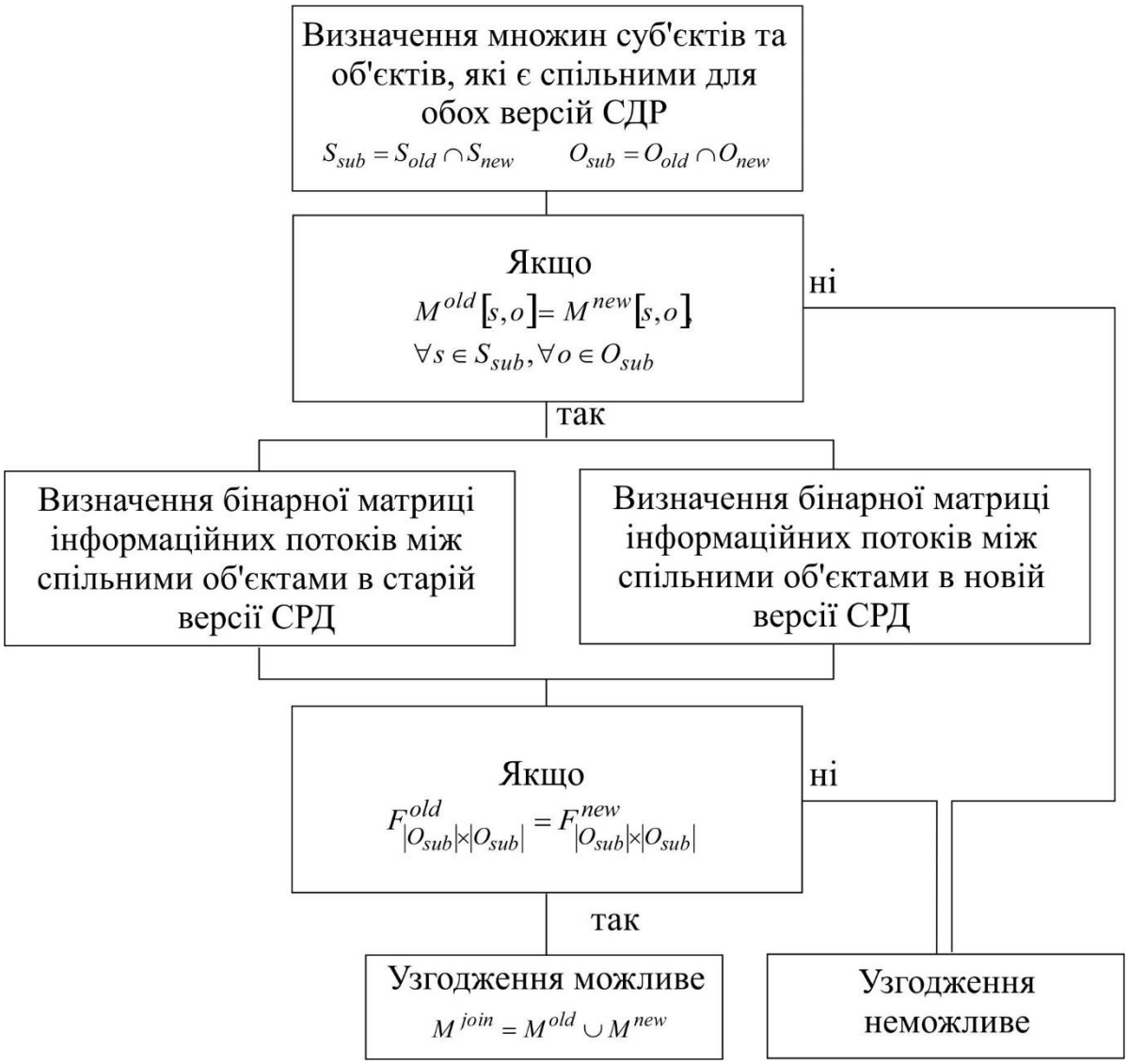


Рисунок 4.7 – Структурна схема методу узгодження матриць доступу різних версій систем розмежування доступу

Теорема. Для узгодження матриць доступу різних версій систем дискреційного розмежування доступу необхідно та достатньо забезпечити рівність інформаційних потоків між спільними об’єктами обох версій.

Доказ необхідності. У моделях дискреційного розмежування доступу недозволеним інформаційним потоком є потік, який не передбачений матрицею доступу. Зазначимо, що окремо в кожній версії СРД матриця доступу сформована коректно та не допускає порушення конфіденційності інформації, тобто виникнення недозволеного інформаційного потоку. Отже, у випадку рівності інформаційних потоків обох версій виникнення порушення безпеки інформації не можливе. Припустимо, що в одній із версій можливе виникнення недозволеного в іншій версії інформаційного потоку. Це означає, що в одній версії СРД такий потік можливий, а в другій – ні, іншими словами передбачається наявність різних інформаційних потоків між суб’єктами та об’єктами СРД, що суперечить умові теореми.

Доказ достатності. Будь-яке порушення конфіденційності інформації передбачає наявність інформаційного потоку тільки до суб’єкта системи всупереч матриці доступу. Інформаційний потік між об’єктами не призводить до порушення конфіденційності. Водночас передача інформації між суб’єктами можлива тільки через фізичний носій інформації (файл, база даних, тощо) – об’єкта системи. Отже, достатньо розглядати тільки спільні об’єкти системи, тому що коректність інформаційних потоків не спільних об’єктів забезпечуються окремою версією СРД.

Застосування методу узгодження матриць доступу різних версій систем дискреційного розмежування доступу здійснюється таким чином. Перед спільним функціонуванням наявної та модернізованої СРД здійснюється перевірка про можливість узгодження матриць доступу (виконання умови 4.3). У випадку неможливості їх узгодження провадиться зміна параметрів доступу в одній із версій СРД з метою підготовки до наступного етапу методу. Далі здійснюється перевірка узгодженості інформаційних потоків різних версій СРД. У випадку виявлення невідповідності можлива корекція однієї із версій

матриць доступу та повторна перевірка. У випадку рівності інформаційних потоків для спільних об’єктів різні версії СРД можуть спільно функціонувати на загальному полі даних. У разі виникнення потреби динамічної зміни параметрів матриць доступу можливо реалізувати механізм узгодження, який здійснюватиме перевірку змін на наявність недозволених інформаційних потоків. Отже, у випадку спільного функціонування наявної та модернізованої ІТС неможливе виникнення недозволених інформаційних потоків і, як наслідок, порушення безпеки інформації.

Розроблений метод узгодження матриць доступу різних версій систем дискреційного розмежування доступу дозволить формально описати процедуру спільного функціонування обох інформаційних систем з питань безпеки інформації та визначити умови, за яких неможливе виникнення недозволених інформаційних потоків [59].

4.5 Метод узгодження систем рольового розмежування доступу інформаційних систем на стадії модернізації

Аналіз структури та діяльності Державної прикордонної служби як правоохоронного органу спеціального призначення показав чітку ієрархію підпорядкування як органів і підрозділів прикордонного відомства, так і ІС, функціонал яких розподілений за рівнями управління. Посадові особи прикордонної служби виконують певні функціональні обов’язки в межах своєї посади, яка сприймається як певна роль, узагальнена сутність, що становить визначений перелік функцій та підпорядкованість працівника. Отже, реальні системи вимагають запровадження моделей розмежування доступу, побудованих на сутностях ролі, яка має певну множину прав та повноважень.

На початку 80-х років у дослідженнях процесів розмежування доступу вперше такий підхід був наведений корпорацією IBM та отримав назву рольового розмежування доступу. У цей час була розроблена модель Лендвера-Макліна [60], яка в літературі зустрічається під назвою MMS-моделі (Military Message System) [61]. Зазначена модель поєднує мандатний і

дискреційний підходи розмежування доступу з використанням базових понять і механізмів ролей. Пізніше були сформовані формальні визначення системи на базі рольових основ управління доступом (RBAC – Role-Based Access Control) [40, 62].

Системи, побудовані на моделі рольового розмежування доступу, передбачають розмежування процесу функціонування системи та роботи користувача на окремі сеанси, в кожному з яких виділяється два послідовних етапи: ідентифікація та автентифікація [63].

Рольові моделі поєднують дискреційний підхід, що забезпечує достатню адаптивність у налаштуванні системи розмежування доступу до конкретних функціональних та організаційних процесів автоматизації предметної області та мандатний підхід до здійснення доступу шляхом агрегації об'єктів та суб'єктів доступу, що також забезпечує дотримання правил розмежування доступу. Наведені можливості рольової політики дозволяють розробляти системи розмежування доступу з достатньою керованістю в інтегрованих інформаційних системах з великою кількістю об'єктів та користувачів, і тому знаходять широке застосування в наявних системах [64].

Системи розмежування доступу, які побудовані за рольовою моделлю, не передбачають оперування об’єктами, що є спільними з іншими системами. Виникнення такої ситуації можливо під час модернізації інформаційних систем у складі відомчих автоматизованих систем. На цій стадії апріорно різні версії програмного забезпечення оперують спільними даними для усунення колізій, викликаних відмінностями моделей розмежування доступу, необхідно здійснити завдання їх узгодження.

Метод узгодження систем рольового розмежування доступу призначений для визначення параметрів обох версій СРД при яких відсутнє порушення безпеки інформації під час їх функціонування на загальному полі даних.

Суть методу узгодження систем рольового розмежування доступу полягає у формуванні таких параметрів СРД, у якій неможливо реалізувати недозволений інформаційний потік у кожній з версій окремо.

Відповідно до формальної специфікації рольових моделей право доступу користувача визначається призначеною роллю, яка містить певний набір повноважень (рисунок 4.8).

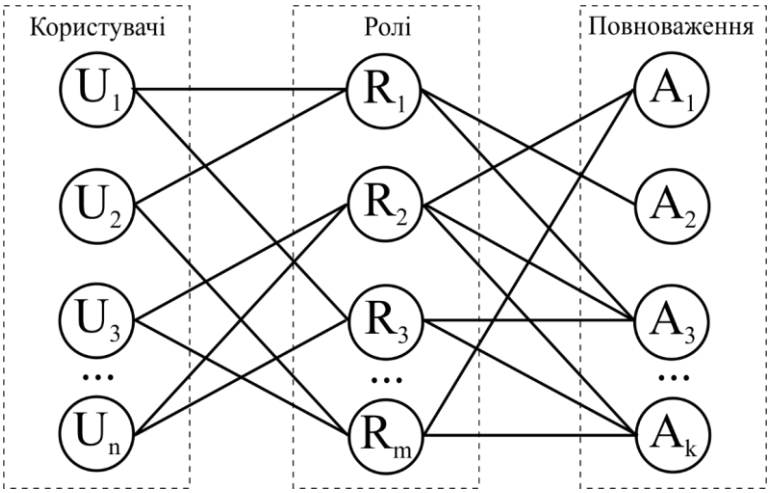


Рисунок 4.8 – Приклад надання користувачам ІС певних повноважень через їх ролі

Отже, через відображення множин сутностей рольової системи розмежування доступу можливо визначити відображення множини користувачів на множину повноважень.

У роботі [40] наведені різновиди рольових моделей, залежно від можливих відносин між ролями, у тому числі передавання (делегування) повноважень і прав від одних ролей іншим ролям:

– із ієрархічною організацією системи ролей;

– із взаємовиключними на будь-які сеанси ролями (модель статичного розподілу обов'язків);

– із взаємовиключними на один сеанс ролями (модель динамічного розподілу обов'язків);

– із кількісними обмеженнями за ролями;

– із групуванням ролей і повноважень.

Водночас наведені різновиди моделей тільки формують види відображень множини користувачів на множину ролей і множину повноважень на множину ролей, кінцевим результатом яких є відображення множини повноважень на множину користувачів у конкретний момент часу функціонування системи. Вищезазначене дозволить сформувати математичну модель методу узгодження рольових СРД.

Інформаційна система, в якій спільно функціонують дві різні версії рольових СРД (за необхідності узгодження більшої кількості метод може бути розширений за рахунок попарного узгодження), є сукупністю таких множин обох версій:

$U_1, U_2; U_1 \in U, U_2 \in U$ – множини користувачів;

$R_1, R_2; R_1 \in R, R_2 \in R$ – множини ролей;

$A_1, A_2; A_1 \in A, A_2 \in A$ – множини повноважень;

$F_1^{AR} : A_1 \to R_1, F_2^{AR} : A_2 \to R_2$ – відображення множини повноважень на множину ролей;

$F_1^{UR} : U_1 \to R_1, F_2^{UR} : U_2 \to R_2$ – відображення множини користувачів на множину ролей.

Зазначимо, що множини повноважень однозначно визначають операції над об’єктами та, відповідно, і самі об’єкти, над якими здійснюються визначені операції. Ця вимога накладає певні обмеження на множини повноважень, а саме повноваження різних версій СРД повинні бути атомарними на загальній множині повноважень A

$$a_i \cap a_j = \varnothing, \forall a_i \in A, \forall a_j \in A. \qquad (4.7)$$

Для випадку, коли $A_1 \cap A_2 = \varnothing$ спільні повноваження різних версій СРД відсутні, це також унеможливлює виникнення будь-яких інформаційних потоків між користувачами з причини відсутності спільних об’єктів. В іншому

випадку, коли $A_1 \cap A_2 \neq \varnothing$ – множини повноважень різних версій СРД перетинаються, що може призвести до недозволених інформаційних потоків. Визначимо множини повноважень користувачів кожної версії системи розмежування доступу через відображення користувачів на множину ролей і множину отриманих ролей на множину повноважень

$$\left(F_1^{AR}\right)^{-1} : \left(F_1^{UR} : U_1 \to R_1\right) \to U^{A_1}, \qquad (4.8)$$
$$\left(F_2^{AR}\right)^{-1} : \left(F_2^{UR} : U_2 \to R_2\right) \to U^{A_2},$$

де U^{A_1}, U^{A_2} – множини повноважень множин користувачів різних версій СРД;

$\left(F_1^{AR}\right)^{-1}, \left(F_2^{AR}\right)^{-1}$ – зворотні відображення множини повноважень на множини ролей.

Дані множини є підґрунтям визначення можливості узгодження обох версій СРД, а саме у випадку виконання умови

$$\left(U^{A_1} \cap U^{A_2} = \varnothing\right) \vee \left(U^{A_1} \setminus U^{A_2} = \varnothing\right), \qquad (4.9)$$

повноваження користувачів не суперечать один одному.

Отже, різні версії СРД можуть бути узгоджені. В іншому випадку, необхідно забезпечити дотримання основного правила безпеки для рольових СРД, а саме: система функціонує безпечно, якщо і тільки якщо будь-який користувач $u \in U$, який працює в сеансі $c \in C$, може здійснювати дії у межах повноваження $a \in A$, за умови де $A \in f_{permission}(c)$ [65]. Це вимагає рівності повноважень для спільних для обох версій СРД користувачів, тобто:

$$U_i^{A_1} = U_i^{A_2}, \forall U_i^{A_1} \in U_R, \forall U_i^{A_2} \in U_R. \qquad (4.10)$$

Вищезазначене дозволяє сформувати структурну схему методу узгодження різних версій рольових систем розмежування доступу (рисунок 4.9).

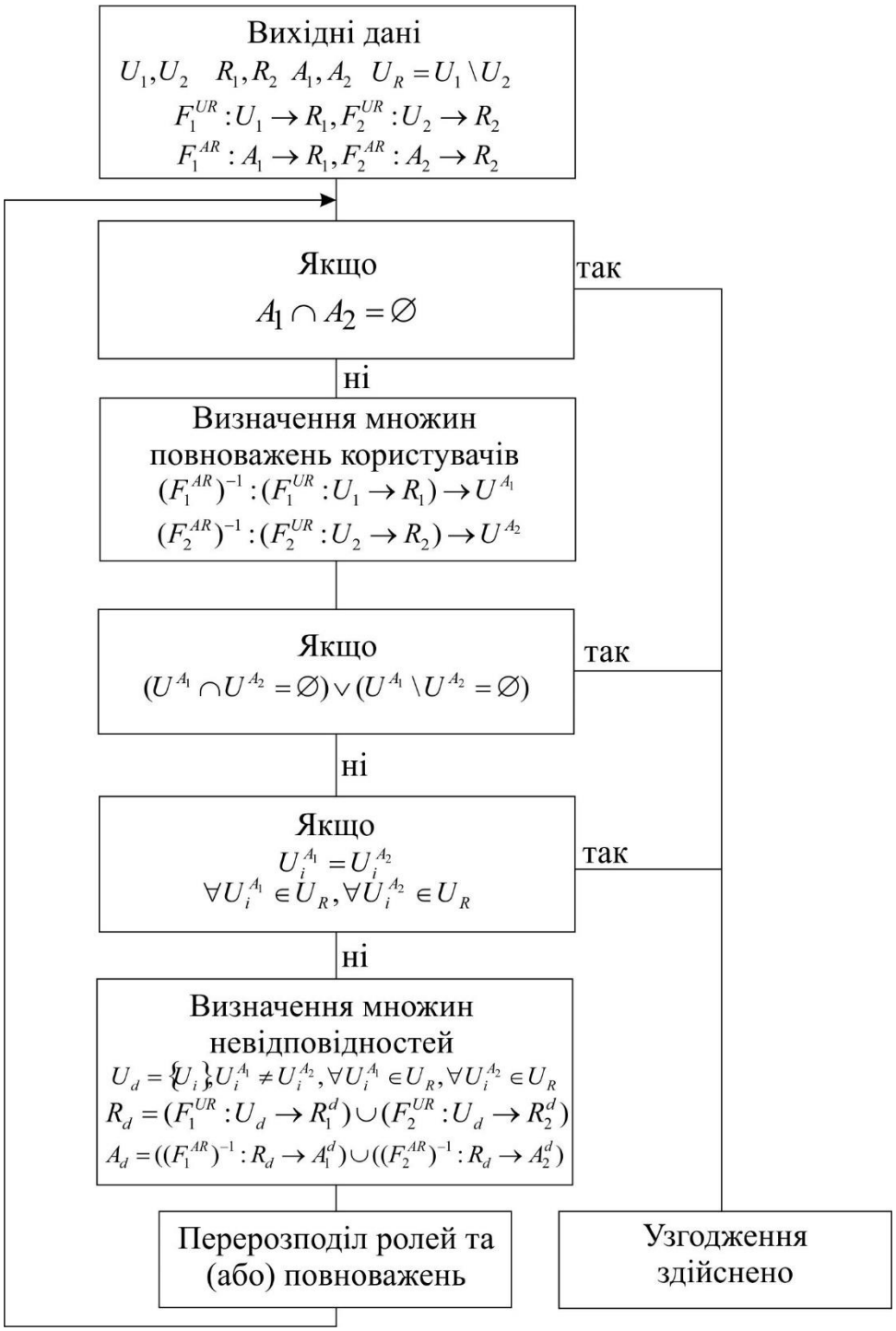


Рисунок 4.9 – Структурна схема методу узгодження різних версій рольових систем розмежування доступу

У випадку невиконання умови (4.10) отримуємо множини користувачів U_d, ролей R_d і повноважень A_d, які спричиняють порушення правила безпеки під час спільного функціонування обох версій СРД і потребують зміни:

$$U_d = \{U_i\}, U_i^{A_1} \neq U_i^{A_2}, \forall U_i^{A_1} \in U_R, \forall U_i^{A_2} \in U_R, \tag{4.11}$$

$$R_d = \left(F_1^{UR} : U_d \to R_1^d\right) \cup \left(F_2^{UR} : U_d \to R_2^d\right), \tag{4.12}$$

$$A_d = \left(\left(F_1^{AR}\right)^{-1} : R_d \to A_1^d\right) \cup \left(\left(F_2^{AR}\right)^{-1} : R_d \to A_2^d\right). \tag{4.13}$$

Перерозподіл ролей та (або) повноважень між різними версіями СРД здійснюється адміністраторами систем з урахуванням функціональних завдань користувачів. За потреби окремі повноваження користувачів можуть бути обмежені на період модернізації, після завершення якої відновлені.

Отже, розроблений метод узгодження різних версій рольових систем розмежування доступу дозволить формально описати процедуру спільного функціонування обох інформаційних систем з питань безпеки інформації та визначити умови, під час яких неможливе виникнення недозволених інформаційних потоків [66].

4.6 Методологічний базис узгодження моделей розмежування доступу інформаційних систем на стадії модернізації

Інформаційні системи суб’єктів національної безпеки України мають велику кількість підсистем, які розподілені на всій території держави. Особливістю таких систем є вимога функціонування в реальному масштабі часу, причому, навіть незначний збій або зупинка можуть призвести до серйозних збитків національного масштабу.

Адаптація інформаційних системи Держприкордонслужби до змін функціональних завдань прикордонного відомства потребує модернізації

відомчих систем, що призводить до спільного функціонування на загальному полі гетерогенної ІІС різних версій її складових. Побудова інформаційних систем, що взаємодіють у складі однієї суперсистеми, може здійснюватися як за однаковими, так і за різними моделями розмежування доступу. Під час здійснення модернізації однієї із них виникає проблема їх узгодження, що вимагає розробки єдиного підходу – методологічного базису узгодження.

Потреба в розробці теоретичної бази забезпечення властивостей інформації у разі колективної її обробки виникла в 70-х роках у зв'язку із впровадженням автоматизованих інформаційних систем. Відповідно до складових функціональних критеріїв інформації виникли три взаємопов'язаних напрями наукових розробок, які зосереджувались на конфіденційності, цілісності та доступності інформації. Найбільш актуальною стала проблема забезпечення конфіденційності інформації, тому на теперішній час розроблено вельми представницький арсенал математичних моделей розмежування доступу, стандартів безпеки комп'ютерних систем.

Відповідно до [67], загрози, що відносяться до несанкціонованого ознайомлення з інформацією, становлять загрози конфіденційності. Саме тому предметом дослідження систем розмежування доступом є забезпечення конфіденційності інформації. Суть поняття "загрози інформації" вимагає застосування суб'єктно-об'єктної моделі комп'ютерної системи з причини необхідності наявності суб'єкта як елемента системи який ознайомлюється з інформацією, та об'єкта – матеріального носія інформації. У разі відсутності хоча б однієї з двох складових втрачається сенс порушення конфіденційності. Для порушення конфіденційності є потреба у введенні третього поняття – потоку інформації від об'єкта до суб'єкта, у випадку відсутності якого загроза конфіденційності відсутня. На теперішній час є різні погляди на визначення поняття суб'єкта, об'єкта та потоку інформації. У роботі прийнято визначення яке наведено в [5], а саме:

суб'єкт – подання фізичного користувача в комп'ютерній системі, що створюється у процесі входження користувача в систему і повністю

характеризується своїм контекстом (псевдонімом, ідентифікаційним кодом, повноваженнями тощо);

об’єкт – елемент ресурсу комп’ютерної системи, що знаходиться під керуванням комплексу засобів захисту і характеризується певними атрибутами і поводженням;

потік інформації – передавання інформації від одного до іншого об’єкта комп’ютерної системи.

Водночас загроза конфіденційності передбачає визначення поняття "ознайомлення" суб’єкта з інформацією, що міститься в об’єкті. Відповідно до [5], ознайомлення – одержання користувачем або процесом інформації, що міститься в об’єкті. Іншими словами, виникнення потоку інформації від об’єкта до суб’єкта. Варто зазначити, що відповідно до прийнятих визначень порушення конфіденційності наступає не тільки тоді, коли користувач ознайомився з інформацією, а й коли процес від його імені отримав дану інформацію.

Під час розробки або модернізації ІС розробник реалізує СФБ на базі апробованих політик безпеки та забезпечує функціональну безпеку відповідно до встановлених замовником критеріїв. Разом із тим, впровадження модернізованих складових у загальну систему здійснюється поетапно та упродовж певного періоду часу при якому стара версія СРД функціонує одночасно з модернізованою СРД на загальному полі даних. Це спричиняє неконтрольовану однією із версій СРД дію над окремими об’єктами та виникнення інформаційних потоків, які можуть здійснюватися як в межах політики безпеки, так і виходити за них. У загальному випадку період модернізації характеризується виникненням недозволених в одній із версій інформаційних потоків, що призводить до порушення властивостей інформації. Забезпечивши рівність інформаційних потоків для спільних для обох версій суб’єктів та об’єктів системи, буде дотримано вимогу конфіденційності.

З метою доказу теореми безпеки узгодження різних версій СРД опишемо структурну модель їх спільного функціонування (рисунок 4.10):

S_1, S_2 – суб'єкти систем розмежування доступу;

$S_R = S_1 \cap S_2$ – спільні для обох версій суб'єкти;

O_1, O_2 – об'єкти систем розмежування доступу;

$O_R = O_1 \cap O_2$ – спільні для обох версій об'єкти;

Ω_1, Ω_2 – інформаційні потоки систем розмежування доступу;

$\Omega_1^{SO}, \Omega_2^{SO}$ – інформаційні потоки між суб'єктами та об'єктами СРД;

$\Omega_1^{RSO}, \Omega_2^{RSO}$ – інформаційні потоки між спільними суб'єктами та об'єктами СРД;

$\Omega_1^{OO}, \Omega_2^{OO}$ – інформаційні потоки між об'єктами СРД;

$\Omega_1^{ROO}, \Omega_2^{ROO}$ – інформаційні потоки між спільними об'єктами СРД;

Причому $\Omega_1^{RSO} \subseteq \Omega_1^{SO} \subseteq \Omega_1$, $\Omega_2^{RSO} \subseteq \Omega_2^{SO} \subseteq \Omega_2$, $\Omega_1^{ROO} \subseteq \Omega_1^{OO} \subseteq \Omega_1$, $\Omega_2^{ROO} \subseteq \Omega_2^{OO} \subseteq \Omega_2$.

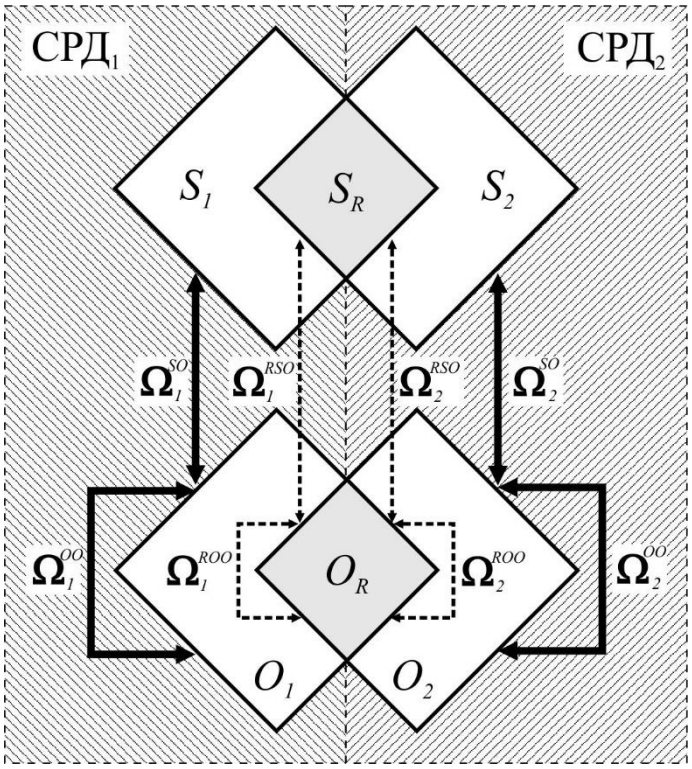


Рисунок 4.10 – Структурна модель спільного функціонування різних версій систем розмежування доступу

Зазначимо, що порушення властивостей інформації або правил політики безпеки СРД можливо тільки за умови наявності недозволеного (заборони дозволеного) інформаційного потоку між об’єктом, який містить інформацію, і суб’єктом. З цієї причини інформаційні потоки між суб’єктами в межах моделі не розглядаються. У випадку рівності всіх інформаційних потоків порушення властивостей інформаційного ресурсу відсутнє.

Визначимо необхідну та достатню умову, при якій неможливий недозволений інформаційний потік. З цією метою розглянемо вироджені варіанти спільного функціонування обох версій СРД за умови, що кожна із систем повністю забезпечує дотримання властивостей інформації відповідно до базових моделей СРД.

Варіант 1. У випадку, коли $S_R = \varnothing, O_R = \varnothing$ СРД не мають спільних елементів та функціонують незалежно одна від одної. Недозволені інформаційні потоки відсутні.

Варіант 2. У випадку, коли $S_R \neq \varnothing, O_R = \varnothing$ СРД мають тільки спільних користувачів. Необхідною умовою порушення властивостей інформації є наявність об’єкта, який містить інформацію, з якою не повинен ознайомитись користувач. Водночас політика безпеки СРД не допустить наявності такої інформації в об’єкті, який належить користувачу (має доступ). Отже, в такому варіанті порушення властивостей інформації відсутнє.

Варіант 3. У випадку, коли $S_R = \varnothing, O_R \neq \varnothing$ СРД мають тільки спільні об’єкти. Такий варіант передбачає можливість виникнення інформаційного потоку між об’єктами, який не передбачено в одній із версій СРД, що також призведе до недозволеного інформаційного потоку до певного суб’єкта. Отже, у такому варіанті можливе порушення властивостей інформації.

Варіант 4. У випадку, коли $S_R \neq \varnothing, O_R \neq \varnothing$ СРД мають спільні суб’єкти та об’єкти. Такий варіант об’єднує другий і третій випадки та передбачає можливість виникнення інформаційного потоку між об’єктами, який не

передбачено в одній із версій СРД. Отже, у такому варіанті можливе порушення властивостей інформації.

Аналіз варіантів спільного використання елементів СРД показав, що тільки у випадку наявності спільних об'єктів у різних версіях СРД можливе виникнення недозволеного інформаційного потоку. З метою заборони виникненню недозволених інформаційних потоків під час спільного функціонування обох версій СРД необхідно та достатньо забезпечити рівність інформаційних потоків між спільними об'єктами в кожній із версій СРД, що є формулюванням теореми безпеки спільного функціонування різних версій СРД. Доказ теореми можна здійснити з вищенаведеного.

Отже, методологічним базисом узгодження моделей розмежування доступу інформаційних систем на стадії модернізації є дотримання рівності інформаційних потоків між спільними об'єктами в кожній із версій СРД окремо [68, 69].

4.7 Оцінювання ефективності узгодження систем розмежування доступу

Модернізація інформаційних систем в окремих випадках вимагає функціонування на загальному полі даних різних версій систем розмежування доступу. З метою дотримання властивостей інформації на цій стадії життєвого циклу ІС здійснюється завдання узгодження обох версій цих систем, зокрема їх СРД. Вищенаведене обумовлює необхідність оцінювання ефективності узгодження різних СРД, які функціонують на загальному полі даних.

Ураховуючи ймовірнісний характер порушення властивостей інформації викликаних спільним функціонуванням різних версій ІС якість їх узгодження будемо оцінювати за допомогою імовірності виникнення недозволеного інформаційного потоку в різних версіях СРД – P_{IC}^{forb}. Врахуємо, що час обміну інформації між об'єктами ІС є набагато меншим ніж час модернізації, тобто $t_{obj} << t_M$. У даному випадку ймовірності виникнення

недозволених інформаційних потоків розглядатимемо у граничному стаціонарному процесі, тобто як фінальні ймовірності відповідних станів.

Показник ефективності спільного функціонування різних версій СРД розраховуватимемо так

$$P_{IC}^{forb} = 1 - \prod_{\forall i} \prod_{\forall j} \left(1 - P_{ij}^{forb}\right), \tag{4.14}$$

де P_{ij}^{forb} – імовірність наявності недозволеного інформаційного потоку між двома об’єктами системи.

У результаті дослідження доведено, що виникнення недозволеного інформаційного потоку можливе тільки між спільними для обох версій об’єктами. Ураховуючи, що СРД різних версій ІС окремо функціонують коректно, достатньо розглядати тільки спільні для обох версій об’єкти O_R.

Значення ймовірності недозволеного інформаційного потоку між двома спільними об’єктами системи визначається так

$$P_{ij}^{forb} = \begin{cases} 0, P_{ij}^1 > 0, P_{ij}^2 > 0 \\ 0, P_{ij}^1 = 0, P_{ij}^2 = 0 \\ P_{ij}^1, P_{ij}^1 > 0, P_{ij}^2 = 0 \\ P_{ij}^2, P_{ij}^1 = 0, P_{ij}^2 > 0 \end{cases}, \tag{4.15}$$

де P_{ij}^1, P_{ij}^2 – імовірності наявності інформаційного потоку між $o_i \in O_R$ та $o_j \in O_R$ об’єктами старої та нової ІС відповідно.

Проведені дослідження характеристик інформаційних потоків в інформаційних системах [70–73] показали, що в більшості випадків він є найпростішим. Вищенаведене є підґрунтям до застосування під час розрахунку ймовірності наявності інформаційного потоку між двома

об’єктами ІС методу диференціальних рівнянь для ймовірностей станів (рівнянь Чепмена-Колмогорова) [74].

Визначимо ймовірність наявності інформаційного потоку P_{sd} між s-м та d-м об’єктами СРД. Для цього опишемо матрицею величин інформаційних потоків $\Lambda = \{\lambda_{ij}\}$ навантажений граф станів системи (рисунок 4.11).

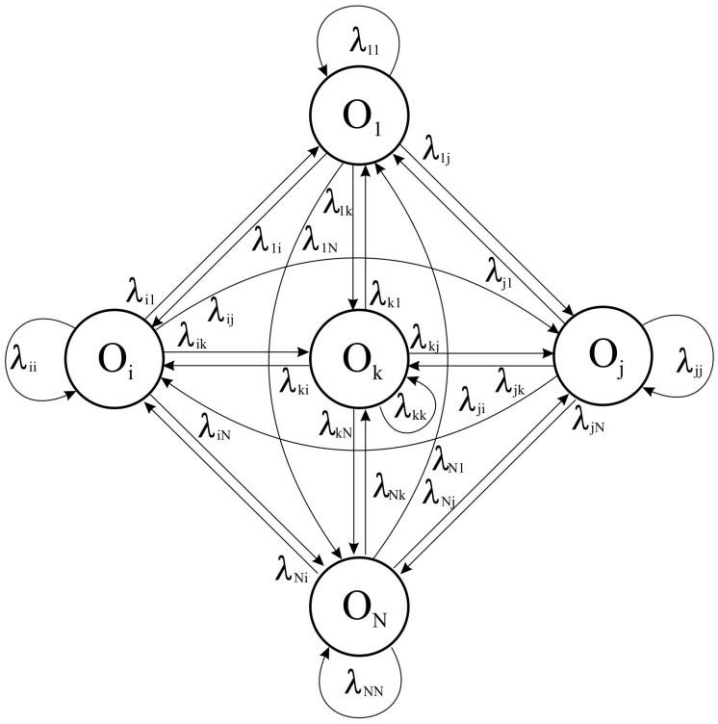


Рисунок 4.11 – Граф станів системи

Для опису значень імовірностей приймемо: $P_1(t),\ldots,P_i(t),\ldots,P_N(t)$ – як імовірності наявності інформації в певному об’єкті, який позначений індексом. Для будь-якого моменту часу виконується умова:

$$\sum_{i=1}^{N} P_i(t) = 1. \qquad (4.16)$$

Відповідно до графу станів, опишемо систему диференційних рівнянь першого порядку [75]:

$$\begin{cases} \dfrac{dP_1(t)}{dt} = \sum\limits_{k=1}^{N} \lambda_{k1} P_k(t) - P_1(t) \sum\limits_{k=1}^{N} \lambda_{1k} \\ \ldots \\ \dfrac{dP_i(t)}{dt} = \sum\limits_{k=1}^{N} \lambda_{ki} P_k(t) - P_i(t) \sum\limits_{k=1}^{N} \lambda_{ik} \\ \ldots \\ \dfrac{dP_N(t)}{dt} = \sum\limits_{k=1}^{N} \lambda_{kN} P_k(t) - P_N(t) \sum\limits_{k=1}^{N} \lambda_{Nk} \end{cases} . \quad (4.17)$$

Для визначення значення імовірності наявності інформаційного потоку між s-м та d-м об’єктами необхідно задати початкові умови

$$P_s(0) = 1, P_i(0) = 0, \forall i \neq s . \quad (4.18)$$

Семантичним навантаженням моделі є опис міграції даних від s-го об’єкта до d-го. Отже, значення $P_d(t)$ показує, з якою імовірністю дані, що містяться в s-му об’єкті, знаходитимуться в d-му об’єкті в момент часу t.

Зазначимо, що вирішення в загальному вигляді системи диференційних рівнянь (4.17) при достатньо великих значеннях N є проблемним [73]. Тому з метою визначення чисельних значень імовірностей використаємо широковідомий чисельний метод розв’язування систем диференціальних рівнянь – класичний метод Рунге – Кутти 4-го порядку [76].

Узагальнена структура методики оцінювання ефективності узгодження систем розмежування доступу наведена на рисунку 4.12.

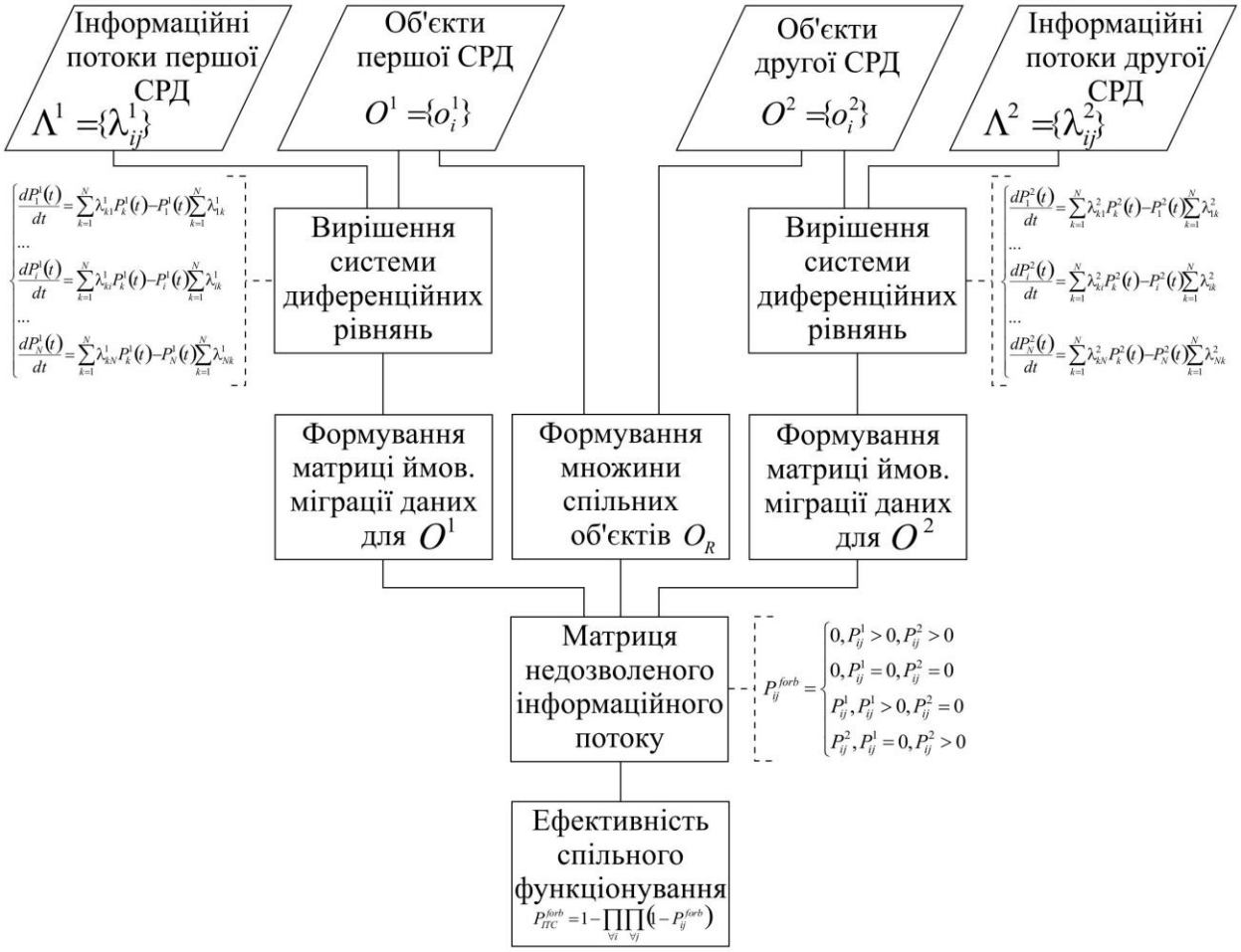


Рисунок 4.12 – Узагальнена структура методики оцінювання ефективності узгодження систем розмежування доступу

4.8 Висновки до розділу 4

1. Під час розробки складових ІІС формалізується та реалізовується певна політика безпеки, яка базується на відомих моделях інформаційної безпеки. Їх використання в окремих ІС та підсистемах забезпечує виконання функцій забезпечення дотримання властивостей інформаційного ресурсу. Водночас під час модернізації наявних складових ІІС або інтеграції нових виникає ситуація спільного функціонування систем розмежування доступу на загальному полі даних.

2. Для дослідження спільного функціонування різних версій моделей безпеки комп’ютерних системи обрано такі види моделей: дискреційного, рольового, мандатного та тематичного розмежування доступу; безпеки

інформаційних потоків; суб'єктно-орієнтовану модель ізольованого програмного середовища. Показано, що спільне функціонування різних версій систем розмежування доступу, які побудовані на розглянутих моделях безпеки комп'ютерних систем, передбачає наявність можливих шляхів виникнення інформаційних потоків в обхід політики безпеки однієї із версій системи розмежування доступу.

3. Моделі дискреційного розмежування доступу оперують матрицею доступу, а мандатного – решіткою рівнів конфіденційності, які у разі спільного функціонування різних версій СРД потребують узгодження. Для моделей рольового та тематичного розмежування доступу сформульовані гіпотези дотримання політики безпеки у випадку спільного функціонування різних версій систем розмежування доступу.

4. Аналіз моделей розмежування доступу дозволив розробити метод узгодження решіток рівнів конфіденційності систем мандатного розмежування доступу інформаційних систем на стадії модернізації, призначення якого полягає у формуванні спільної для обох версій СРД решітки рівнів конфіденційності на стадії модернізації ІС.

Суть методу узгодження решіток рівнів конфіденційності різних версій систем мандатного розмежування доступу полягає у формуванні спільної для обох версій єдиної решітки рівнів конфіденційності, в якій неможливо реалізувати недозволений інформаційний потік у кожній з версій СРД окремо.

У межах методу сформульована та доказана теорема безпеки спільної решітки конфіденційності, яка є математичним підґрунтям розробленого методу, що дозволить формально описати процедуру спільного функціонування обох інформаційних систем з питань забезпечення дотримання властивостей інформації та визначити умови, при яких неможливе виникнення недозволених інформаційних потоків.

5. Крім того, розроблений метод узгодження матриць доступу систем дискреційного розмежування доступу інформаційних систем на стадії модернізації, який призначений для формування спільної для обох версій СРД

матриць доступу на етапі модернізації інформаційних систем. Суть методу узгодження матриць доступу різних версій систем розмежування доступу полягає у формуванні спільної для обох версій єдиної матриці доступу, в якій неможливо реалізувати недозволений інформаційний потік у кожній з версій СРД окремо. Науковою основою методу є формулювання та доказ теореми безпеки спільного функціонування різних версій систем дискреційного розмежування доступу. Розроблений метод узгодження матриць доступу різних версій систем дискреційного розмежування доступу дозволить формально описати процедуру спільного функціонування обох інформаційних систем з питань дотримання властивостей інформації та визначити умови, за яких неможливе виникнення недозволених інформаційних потоків.

6. Подальшим дослідженням у розділі є розробка методу узгодження систем рольового розмежування доступу інформаційних систем на стадії модернізації. Метод узгодження систем рольового розмежування доступу призначений для визначення параметрів обох версій СРД за яких відсутнє порушення властивостей інформації під час їх функціонування на загальному полі даних. Суть методу полягає у формуванні таких параметрів СРД, в якій неможливо реалізувати недозволений інформаційний потік у кожній з версій окремо.

Розроблений метод узгодження різних версій рольових систем розмежування доступу дозволить формально описати процедуру спільного функціонування обох інформаційних систем з питань безпеки інформації та визначити умови, за яких неможливе виникнення недозволених інформаційних потоків.

7. Завершенням теоретичних досліджень узгодження моделей розмежування доступу інформаційних систем на стадії модернізації є формування методологічного базису, як науково-обґрунтованого фундаменту для розробки методів узгодження СРД. Варто зазначити, що розроблений базис є інваріантним до самих моделей розмежування доступу, що дає

можливість узгодження не тільки однотипних систем, а й систем, побудованих за різними моделями розмежування доступу.

8. Для оцінювання якості спільного функціонування різних СРД, які функціонують на загальному полі даних, розроблено методику оцінювання ефективності їх узгодження. Ураховуючи ймовірнісний характер порушення властивостей інформації, викликаних спільним функціонуванням різних версій ІС, якість їх узгодження оцінено за допомогою імовірності виникнення недозволеного інформаційного потоку в різних версіях СРД. В основу методики покладено метод диференціальних рівнянь для імовірностей станів, що дозволяє описати моделі міграції даних між спільними об'єктами СРД. Наведені моделі формують елементи матриці недозволеного інформаційного потоку, на підставі якої визначається імовірність виникнення недозволеного інформаційного потоку в різних версіях СРД.

Список використаних джерел у четвертому розділі

1. Блинов А.М. Информационная безопасность: Учебное пособие. Часть 1. – СПб.: Изд-во СПбГУЭФ, 2010. – 96 с.

2. Мясіщев О. А. Напрямки вирішення проблем захисту інформації в мережах / О. А. Мясіщев, А. В. Джулій // Вісник ХНУ – № 4. – 2009. – С. 107-111.

3. Оксіюк О. Г. Особливості забезпечення захисту інформації в системах управління навчанням / О. Г. Оксіюк // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка – № 49. – 2015. – С. 210-213.

4. Сташевський З. П. Впровадження політики рольового розмежування доступу до інформаційних ресурсів у системі дистанційного навчання / З. П. Сташевський, О. І. Лозинський, Н. Є. Бурак // Вісник Львівського державного університету безпеки життєдіяльності – № 6. – 2012. – С. 29-35.

5. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу : НД ТЗІ 1.1-003-99 ДСТСЗІ СБ України /

Затверджено наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від “28” квітня 1999 р. № 22.

6. Микитин Г. В. Системна, нормативна, комплексна моделі захисту інформаційних технологій / Г. В. Микитин // Вісник Національного університету "Львівська політехніка". – 2011. – № 695 : Автоматика, вимірювання та керування. – С. 126–132.

7. Мирошник М. А. Разработка средств защиты информации в распределенных компьютерных системах и сетях / М. А. Мирошник // Інформаційно-керуючі системи на залізничному транспорті – № 1. – 2015. – С. 18-25.

8. Юдін О. К. Аналіз класифікацій типів систем захисту інформації / О. К. Юдін, С. С. Бучик // Проблеми інформатизації та управління – № 3.51 – 2015. – С. 115-124.

9. Барсуков В.С. Современные автоматизированные средства контроля доступа / В.С. Барсуков, С.В. Дворянкин //Монитор-Аспект – №2. – 1993.

10. Цирлов, В. Л. Основы информационной безопасности автоматизированных систем. М.: Феникс (2008): 173.

11. Герасименко В. А. Защита информации в АСОД (в 2-х томах). – М.: Энергоатомиздат, 1994. – 400 с.

12. Замула О. А. Аналіз міжнародних стандартів в галузі оцінювання ризиків інформаційної безпеки / О. А. Замула, В. І. Черниш // Системи обробки інформації – № 2. – 2011. – С. 53-56.

13. Гнатюк С. О. Теоретичні основи побудови та функціонування систем управління інцидентами інформаційної безпеки / С. О. Гнатюк, Ю. Є. Хохлачова, А. О. Охріменко, А. К. Гребенькова // Захист інформації, – Т 14. – № 1 (54). –2012.

14. Нестеряк Ю. В. Міжнародні критерії інформаційної безпеки держави: теоретико-методологічний аналіз / Ю. В. Нестеряк // Публічне управління: теорія та практика – №1. – 2014. – С. 62-67.

15. Сікорський Д. О. Побудова процесу захисту інформації на основі міжнародного стандарту з інформаційної безпеки / Д. О. Сікорський // Держава та регіони. Сер.: Економіка та підприємництво – № 2. – 2014. – С. 32-35.

16. Юдін О. К. Концептуальна модель інформаційної безпеки державних інформаційних ресурсів / О. К. Юдін, С. С. Бучик // Наукоємні технології – № 24.4. – 2014. – С. 462-466.

17. Корченко А. Г. Метод формування кортежів для аналітико-синтетичної кортежної моделі інформаційної безпеки / А. Г. Корченко, С. В. Казмирчук, Б. Б. Ахметов // Захист інформації – № 19.2. – 2017. – С. 148-154.

18. Дудатьев А. В. Аналіз та забезпечення інформаційної безпеки в умовах конфліктів / А. В. Дудатьев, О. П. Войтович, І. А. Дудатьєв. // Вісник Інженерної академії України –№ 2. – 2010. – С. 83-88.

19. Завгородний В. И. Комплексная защита информации в компьютерных системах: Учебное пособие. М.: Логос 264 (2001):

20. Гайкович В. Ю., Ершов Д. В. Основы безопасности информационных технологий. М.: МИФИ 1 (1995).

21. Елисеев Н. И. Модель угроз безопасности информации при ее обработке в системе защищенного электронного документооборота / Н. И. Елисеев // Известия Южного федерального университета. Технические науки №12 (137). –2012.

22. Родионова З. В. Технология управления изменениями прав доступа на основе анализа бизнес-процессов / З. В. Родионова // Вестник НГУЭУ – №1. –2011.

23. Заборовский В. С. Защищенная платформа облачных вычислений для задач компьютерного инжиниринга. / В. С. Заборовский, А. А. Лукашин, А. С. Ильяшенко // Научный сервис в сети Интернет: все грани параллелизма: Труды Международной суперкомпьютерной конференции (23-28 сентября 2013 г., г. Новороссийск). 2013.

24. Косяков С. В. Разработка автоматизированной информационной системы учета и анализа аренды недвижимого имущества в учреждениях Рособразования / С. В. Косяков, Е. Б. Игнатьев, С. С. Машин. // Вестник Ивановского государственного энергетического университета – № 3. –2008. – С. 70-75.

25. Бречка Д. М. Алгоритмы анализа безопасности состояний компьютерной системы для модели Take-Grant / Д. М Бречка. // Математические структуры и моделирование – №2 (20). – 2009.

26. Косачев, А. С., В. Н. Пономаренко. Анализ подходов к верификации функций безопасности и мобильности. М.: Триумф (2004).

27. Варлатая С. К. Анализ методов описания политики безопасности при разработке информационно-безопасных технологий / С. К. Варлатая, М. В. Шаханова // Доклады Томского государственного университета систем управления и радиоэлектроники – № 1-1 (21). – 2010.

28. Стрельбіцький М.А. Аналіз спільного функціонування моделей розмежування доступу на стадії модернізації інформаційно-телекомунікаційних систем / М.А. Стрельбіцький // Збірник наукових праць Національної академії Державної прикордонної служби імені Б. Хмельницького. Серія військові та технічні науки – № 4(70). – 2016.

29. Стрельбіцький М. А. Приховані канали витоку інформації в інформаційно-телекомунікаційних системах Державної прикордонної служби України та шляхи їх ліквідації / М. А. Стрельбіцький, О. А. Ваврічен // Матеріали всеукраїнської науково-практичної конференції "Кібербезпека в Україні: правові та організаційні питання" (м. Одеса, 2016).

30. Мазулевський О. Є. Аналіз прихованих каналів витоку інформації в телекомунікаційних системах військового застосування / О. Є. Мазулевський // Збірник наукових праць Військового інституту телекомунікацій та інформатизації Національного технічного університету України Київський політехнічний інститут – № 2. – 2013. – С. 39-47.

31. Стрельбіцький М. А. Аналіз загроз інформаційної безпеки при використанні у державній прикордонній службі України геоінформаційних систем / М. А. Стрельбіцький, Р. В. Рачок, Д. А. Мул, Є. В. Прокопенко // Збірник наукових праць Національної академії Державної прикордонної служби імені Б. Хмельницького. Серія військові та технічні науки – №1(71). – 2017. – С. 394-403

32. Девянин П.Н. Модели безопасности компьютерных систем: Учеб. пособие для студ. высш. учеб. заведений. – М.: Издательский центр "Академия", 2005. – 144 с.

33. Зегжда Д. П., Ивашко А. М. Основы безопасности информационных систем. – М.: Горячая линия. – Телеком, 2000. – 452 с.

34. Богданов А. М., Корнейко А. В. и др. Моделирование безопасной обработки информации в компьютерных системах. – К.: Наукова думка, 2000. – 160 с.

35. Denning D. E. A lattice model of secure information flow // Coinroun. ACM. – 1976. – V. 19, № 5. – P. 236 – 243

36. Карасик И.Ш. Доклад на конференции “Антивирус-90”, Киев, 1990.

37. Веселов В. Математические аспекты компьютерных вирусов. Компьютер-Пресс, 1992, №10,11.

38. Тимофеев Ю. А. Комплексный подход к защите информации: почему и как надо защищать компьютерные системы / Ю. А. Тимофеев // Защита информации – 1992. Вып. 1 с. 62-80.

39. Кент С. Обеспечение безопасности в вычислительных сетях: Протоколы и методы управления в сетях передачи данных / Пер.с англ.; Под ред. Ф.Ф.Куо. М.: Радио и связь. 1985. с. 358-424.

40. Гайдамакин Н. А. Теоретические основы компьютерной безопасности: учеб. пособие / Н. А. Гайдамакин // Екатеринбург: изд-во Урал. Ун-та –2008. –212 с.

41. Докучаев А. А., Мошенский С. А. Защита данных в системах обработки экономической и финансовой информации: Учебн. пособие. - Спб., 1994, - 25с.

42. Баришев Ю. В. Дискреційна модель та метод розмежування прав доступу до розподілених інформаційних ресурсів / Ю. В. Баришев, В. А. Каплун, К. В. Неуйміна. // Наукові праці Вінницького національного технічного університету –№ 2. – 2017.

43. Семенов С. Г. Порівняльні дослідження технологій розмежування доступу для захисту даних в комп'ютерній системі / С. Г. Семенов, В. М. Зміївська, А. В. Голубенко // Системи обробки інформації –№3. – 2015. – С. 99-102.

44. Потенко О. С. Аналіз моделей безпеки в аспекті експертизи спеціалізованих інформаційних систем / О. С. Потенко // Моделювання та інформаційні технології – 2009.

45. Жора В. Підхід до моделювання рольової політики безпеки / В. Жора // Правове, нормативне та метрологічне забезпечення системи захисту інформації в України.–2003.–Вип. 7 (2003): 45-49.

46. Бабенко Л. К. Мандатный доступ в СУБД / Л. К. Бабенко, А. С. Басан, О. Б. Макаревич // Известия Южного федерального университета. Технические науки – № 48.4. – 2005.

47. Баранов П. А. Проблемы реализации мандатного доступа (модель Белла-ЛаПадулы) к ресурсам вычислительных систем / П. А. Баранов // Проблемы информационной безопасности. Компьютерные системы –№ 1. – 2005. – С. 7-14.

48. Яковів І. Класифікація і аналіз моделей систем захисту інформації в комп’ютерних системах / І. Яковів, О. Корнейко, О. Черноног // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні: науково-технічний збірник. – 2001. – Вип. 3. – С. 71-76.

49. Кононович І. В. Динаміка кількості інцидентів інформаційної безпеки / І. В. Кононович // Інформатика та математичні методи в моделюванні, –№ 1. – 2014. – С. 35-43.

50. Про Державну прикордонну службу України : Закон України Відомості Верховної Ради України (ВВР), 2003 р., № 27, стаття 208

51. Шинкарук О. М. Аналіз досвіду створення та використання інтегрованих телекомунікаційних систем "Гарт" в Державній прикордонній службі України / О. М. Шинкарук, А. В. Федорченко // Збірник наукових праць Національної академії Державної прикордонної служби України. Сер.: Військові та технічні науки – №2. – 2015. – С. 221-233.

52. Грушо А. А. Ценность информации / А. А. Грушо, Е. Е. Тимонина // Теоретические основы защиты информации. – М.: Издательство Агентства "Яхтсмен", 1996

53. Кузавков В.В. Метод узгодження решіток рівнів конфіденційності систем мандатного розмежування доступу інформаційно-телекомунікаційних систем на стадії модернізації / В. В. Кузавков, М. А. Стрельбіцький, В. О. Данько // ВІТІ Збірник наукових праць Випуск –№ 1, – 2017.

54. Weissman, Clark. "Security controls in the ADEPT-50 time-sharing system." Proceedings of the November 18-20, 1969, fall joint computer conference. ACM, 1969.

55. Linde, Richard R., Clark Weissman, and Clay E. Fox. "The ADEPT-50 time-sharing system." Proceedings of the November 18-20, 1969, fall joint computer conference. ACM, 1969.

56. Hartson, H. Rex, and David K. Hsiao. "A semantic model for data base protection languages." Proceedings of the second international conference on Systems for Large Data Bases. VLDB Endowment, 1976.

57. Harrison, M.H., Ruzzo, W.L. and Ullman, J.D. "Protection in Operating Systems." Communications of ACM 19(8), 1976, pages 461-471.

58. Домнин Л.Н. Элементы теории графов: учеб. пособие. – Пенза: Изд-во Пенз. гос. ун-та, 2007. – 144 с.

59. Стрельбіцький М. А. Метод узгодження матриць доступу систем дискреційного розмежування доступу інформаційно-телекомунікаційних систем на стадії модернізації / М. А. Стрельбіцький // Сучасні інформаційні технології у сфері безпеки та оборони. Національний університет оборони України імені Івана Черняховського – № 1(28). – 2017.

60. Киреенко А. Е. Модели разграничения доступа в компьютерных системах: реализация, особенности, сравнительный анализ / А. Е. Киреенко // Социальная политика и социология – №2. –2012. – С. 222-239.

61. Landwehr, Carl E., Constance L. Heitmeyer, and John McLean. "A security model for military message systems." ACM Transactions on Computer Systems (TOCS) 2.3 (1984): 198-222.

62. Ferraiolo, David, Janet Cugini, and D. Richard Kuhn. "Role-based access control (RBAC): Features and motivations." Proceedings of 11th annual computer security application conference. 1995.

63. Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах : постанова КМУ від 29 березня 2006 р. № 373, Київ.

64. Хусаінов П. В. Показник кібернетичної безпеки для виділеної автоматизованої системи / П. В. Хусаінов // Сучасний захист інформації – № 1. – 2015. – С. 68-73.

65. Максименко С. Защита и беззащитность информации в банке / С. Максименко, Л. Осовецкий // Банковские технологии. - М.: №7; 1995.

66. Стрельбіцький М. А. Метод узгодження систем рольового розмежування доступу інформаційно-телекомунікаційних систем на стадії модернізації / М. А. Стрельбіцький, Д. А. Мул, Є. В. Прокопенко // Збірник наукових праць Національної академії Державної прикордонної служби імені Б. Хмельницького. Серія військові та технічні науки –№2 (72). –2017. – С 330–339

67. Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу : НД ТЗІ 2.5-004-99. Затверджено наказом

Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від “28” квітня 1999 р. № 22 із змінами згідно наказу Адміністрації Держспецзв'язку від 28.12.2012 № 806

68. Стрельбіцький М.А. Методологічний базис узгодження моделей розмежування доступу інформаційно-телекомунікаційних систем на стадії модернізації / М.А. Стрельбіцький // Збірник наукових праць Національної академії Державної прикордонної служби імені Б. Хмельницького. Серія військові та технічні науки – № 3 (73). – 2017.

69. Стрельбіцький М.А. Методологія узгодження моделей розмежування доступу інформаційно-телекомунікаційних систем на стадії модернізації / Стрельбіцький М.А. // Матеріали X Всеукраїнської науково-практичної конференції "Освітньо-наукове забезпечення діяльності правоохоронних органів і військових формувань України" (м. Хмельницький, 2017).

70. Н. И. Головко, В. О. Каретник, В. Е. Танин, И. И. Сафонюк, Исследование моделей систем массового обслуживания в информационных сетях, Сиб. журн. индустр. матем., 2008, том 11, номер 2, 50–64

71. Степанов С. Н. Алгоритм оценки показателей качества обслуживания заявок в иерархических сетях доступа / С. Н. Степанов, Д. Л. Осия // T-Comm. 2012. №7. [Електронний ресурс]. – Режим доступу: http://cyberleninka.ru/article/n/algoritm-otsenki-pokazateley-kachestva-obsluzhivaniya-zayavok-v-ierarhicheskih-setyah-dostupa

72. Шелухин О. И. Разработка марковской модели потока ошибок в информационных системах при воздействии помех импульсного типа / О. И. Шелухин, М. В. Арсеньев // Электротехнические и информационные комплексы и системы. 2006. №1. [Електронний ресурс]. – Режим доступу: http://cyberleninka.ru/article/n/razrabotka-markovskoy-modeli-potoka-oshibok-v-informatsionnyh-sistemah-pri-vozdeystvii-pomeh-impulsnogo-tipa

73. Мухарлямов Р.К., Панкратьєва Т.Н. Системы обыкновенных дифференциальных уравнений. – Казань: КФУ, 2013.

74. Колмогоров А. Н. Основные понятия теории вероятностей. – М. : Наука, 1974.– 120 с.

75. Гардинер К. В. Стохастические методы в естественных науках. – М. : Мир, 1986. – 528 с.

76. В.Й. Чабан. Вибрані чисельні методи. – Львів: В–во Національного ун-ту “Львівська політехніка”, 2001. – 186 с

РОЗДІЛ 5
ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ ФУНКЦІОНАЛЬНОЇ БЕЗПЕКИ ІНФОРМАЦІЙНИХ СИСТЕМ НА СТАДІЇ МОДЕРНІЗАЦІЇ

Забезпечення надійності державних інформаційних ресурсів в умовах стрімкого розвитку інформаційних технологій вимагає наявності високоефективних систем функціональної безпеки. Зазначені системи являють собою складні організаційно-технологічні структури, створення яких вимагає вирішення комплексу системних задач.

Визначення кількісних та якісних оцінок ефективності СФБ як об’єктивного підтвердження якості СФБ є достатньо складним завданням, що залежить від: призначення ІС, умов її функціонування, типу інформації яка циркулює в ній, тощо.

Наявні засоби забезпечення функціональної безпеки ІІС прикордонного відомства можна розділити на окремі групи, які забезпечують:

- розмежування доступу;
- забезпечення безпеки інформації при передаванні каналами зв’язку;
- захист від інформаційних дестабілізаційних впливів;
- захист від шкідливого програмного забезпечення тощо.

Разом із тим, окремі засоби не в змозі забезпечити захист від значної кількості наявних ІІДФ, а проста комбінація засобів захисту може навіть знизити ефективність їх застосування з причини їх конфліктності.

Загалом ефективність СФБ як складного комплексу програмно-апаратних засобів, технічних, організаційних та інших методів і заходів – це здатність системи протистояти негативним впливам дестабілізаційних факторів, що передбачались, як в рамках проектування, так і іншим загрозам функціональній безпеці.

Отже, розробка інструменту визначення ефективності СФБ дозволить обґрунтувати шляхи вдосконалення такого типу систем.

5.1 Підходи до оцінювання ефективності систем функціональної безпеки

На сучасному етапі розвитку інформація є одним з найцінніших ресурсів, який визначає рівень національної безпеки держави. З розвитком інформаційних технологій і зростанням значущості технічних засобів зв'язку ІС піддаються все більшій кількості інформаційних дестабілізаційних впливів, які за умови їх реалізації можуть призвести до збитків національного масштабу. У цих умовах ефективність функціонування правоохоронних органів значною мірою залежить від можливості системи функціональної безпеки запобігти реалізації загроз ІДФ. Це особливо актуально для прикордонного відомства, яке пов'язано з особливостями організації захисту державного кордону України, процесу пропуску через державний кордон осіб і транспортних засобів та вантажів, специфікою функціонування на адміністративній межі та на лінії розмежування в зоні проведення антитерористичної операції. Однак упровадження та обслуговування комплексних систем забезпечення функціональної безпеки потребують значних витрат ресурсів. Аналогічні дослідження, проведені в цивільних організаціях, показують, що витрати коштів тільки на захист інформації досягають 20-30 % усього бюджету організації на інформаційні технології [1]. У цих умовах актуальною є проблема аналізу ефективності функціонування систем, спрямованих на забезпечення інформаційної безпеки.

Над розв’язанням зазначеної проблеми у сфері оцінювання ефективності систем інформаційної та функціональної безпеки працюють О. Є. Архипов, С. А. Архипова, І. Т. Бородавко, В. П. Ворожко, О. Г. Голубничий, Г. Ф. Конахович, А. Г. Корченко, С. А. Носок, В. Г. Потапов, О. Ю. Пузиренко, В. А. Риндюк [2–7]. Разом із тим на теперішній момент залишаються дискусійними методологічні підходи до оцінювання ефективності такого типу систем.

Наявні підходи до оцінювання ефективності базуються на двох категоріях: кількісних та якісних оцінок. Якісні методи оцінювання

застосовуються в умовах достатньо значної невизначеності та базуються, як правило, на досвіді експертів у даній галузі. З метою формалізації такого типу оцінок використовуються вітчизняні [8] та міжнародні стандарти [9, 10].

Вітчизняні стандарти оцінювання установлюють критерії оцінки безпеки інформації, оброблюваної в комп'ютерних системах, від несанкціонованого доступу та являє собою методологічну базу для визначення вимог з безпеки властивостей інформації. У зазначеному стандарті сформовані критерії, які надають порівняльну шкалу для оцінки надійності механізмів захисту інформації від несанкціонованого доступу, реалізованих у комп'ютерних системах.

Міжнародні стандарти оцінювання пропонують деталізований перелік таких аспектів інформаційної безпеки як політика безпеки, організація інформаційної безпеки, керування ресурсами тощо. Інший стандарт ISO/IEC 15408 "Загальні критерії оцінки безпеки інформаційних технологій" описує інфраструктуру, у якій користувачі системи описують вимоги, розробники заявляють про властивості безпеки, а експерти визначають ступінь відповідності. Базою для зазначеного стандарту є "Критерії оцінки безпеки інформаційних технологій". Стандарт містить два основних види вимог безпеки: функціональні, що висуваються до функцій безпеки і реалізують їх механізми, і вимоги довіри, які висуваються до технології та процесу розробки та експлуатації [11].

Точнішими є кількісні методи оцінювання, як результат глибокого опису предметної області дослідження, детального моделювання процесів систем інформаційної безпеки. Використання зазначених методів дає можливість визначити конкретне значення оцінки процесу, який досліджується, та в подальшому здійснити його оптимізацію.

У роботі [12] проведений аналіз типів критеріїв, які зустрічаються на практиці, а саме:

– критерії типу "ефект-витрати", що дозволяє оцінити досягнення мети функціонування системи безпеки при заданих витратах, іншими словами – економічна ефективність;

– критерії, які дозволяють оцінити якість системи безпеки за заданими показниками та виключити варіанти, що не задовольняють задані обмеження, при цьому використовуються методи багатокритеріальної оптимізації, методи дискретного програмування;

– штучно сформовані критерії, що дозволяють оцінити інтегральний ефект.

Вищенаведені критерії формують різноманітні методи та методики, які описують процес оцінювання ефективності систем забезпечення функціональної безпеки, що свідчить про відсутність єдиного методологічного підходу до вирішення завдання такого класу. Крім того, складові системи функціональної безпеки являють собою складні підсистеми, ефективність функціонування яких залежить від її елементів та описується, як правило, множиною критеріїв з антагоністичними характеристиками.

Аналіз підходів [12–17] до оцінювання ефективності систем інформаційної та функціональної безпеки дозволив сформувати їх класифікацію (рисунок 5.1).

Перший підхід до оцінювання ефективності функціонування системи функціональної безпеки включає якісні оцінки, які оперують категоріями "краще - гірше". Одним із методів даного підходу є методи експертних оцінок як способи прогнозування та оцінки майбутніх результатів дій на основі прогнозів фахівців [18]. Ефективність використання зазначеного методу залежить від ступеня опанування експертом проблем у досліджуваній галузі, професійного рівня та рівня ерудованості, уміння висловлювати чіткі відповіді на поставлені запитання. Експерти можуть сформулювати найкращу, на їх думку, структуру системи функціональної безпеки, визначити необхідні засоби її забезпечення, надати рекомендації з її організації.

Методи експертних оцінок поділяються на дві групи: індивідуальні та колективні.

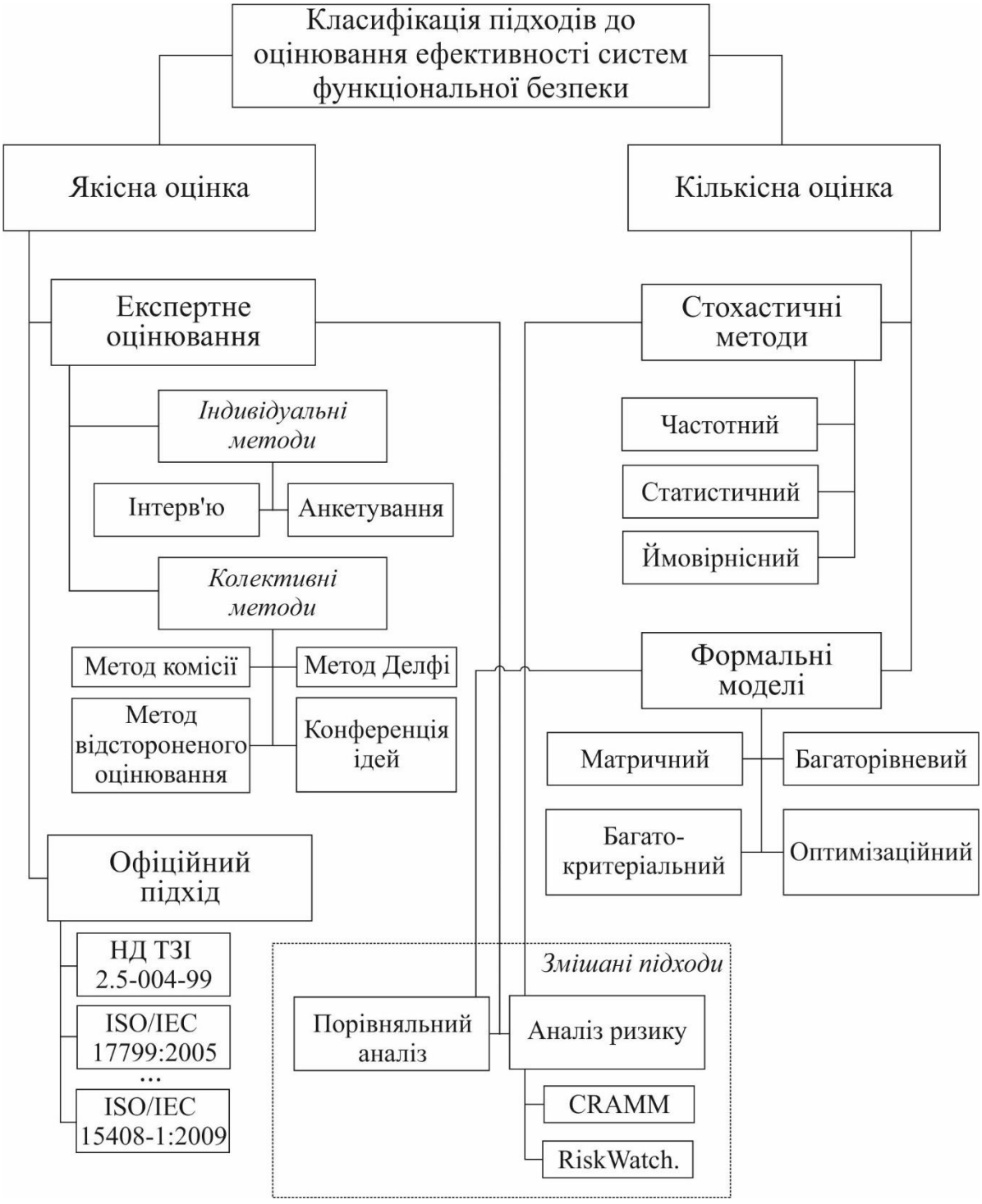


Рисунок 5.1 – Класифікація підходів до оцінювання ефективності систем функціональної безпеки

Індивідуальні методи використовують думку експертів без урахування думок інших. До таких методів належать: інтерв'ю та анкетування. Метод

інтерв'ю ґрунтується на взаємодії аналітика та експерта, де останній дає відповіді на запитання аналітика. Позитивним у даному методі є спілкування аналітика з експертом, де експерт може задати уточнювальні запитання, які, з погляду аналітика, є несуттєвими, хоча експерт може вважати їх значущими.

У результаті співбесіди визначаються фактори впливу на системи функціональної безпеки, очікуваний ефект від упровадження запропонованих рішень, напрямів підвищення ефективності функціонування системи функціональної безпеки тощо.

Метод анкетування полягає у письмовій відповіді експерта на запитання анкети. Разом із тим, даний метод має окремі недоліки, зокрема питання в анкеті можуть бути сформульовані некоректно, то ж і відповіді будуть не точними, тощо.

Іншою групою методів експертної оцінки є колективні експертні методи, які забезпечують формування єдиної спільної думки в результаті взаємодії залучених фахівців-експертів [19]. Серед зазначених методів виділяють методи: комісії, Дельфі, відстороненого оцінювання, конференція ідей та інші. Перевагою зазначених методів є можливість залучення фахівців з широким діапазоном знань з теорії та практики. Ступінь забезпечення безпеки системи визначається як [20]:

$$SR = \frac{1}{n_{i=1}^{n}} W_i G_i ,$$

де W_i – суб’єктивний коефіцієнт важливості i-ї характеристики;

G_i – призначене експертом значення кожної з характеристик;

n – кількість характеристик.

Ще одною групою якісної оцінки є офіційний підхід. На підставі розроблених раніше стандартів з оцінювання системи функціональної безпеки, практичного досвіду експлуатації такого типу систем, появи нових

загроз інформаційному ресурсу та способів протидії розробляються нормативні документи, які регламентують порядок оцінювання системи функціональної безпеки.

Порядок оцінювання комп'ютерної системи на предмет відповідності критеріям, які наведені в [8], визначається відповідними нормативними документами. Експертна комісія, яка проводить оцінку комп'ютерної системи, визначає, які послуги і на якому рівні реалізовані в даній комп'ютерній системі і як дотримані вимоги гарантій. Результатом оцінки є рейтинг, що являє собою упорядкований ряд (перелічення) буквено-числових комбінацій, що позначають рівні реалізованих послуг у поєднанні з рівнем гарантій. Комбінації упорядковуються в порядку опису послуг у критеріях. Для того, щоб до рейтингу комп'ютерної системи міг бути включений певний рівень послуги чи гарантій, повинні бути виконані всі вимоги, перелічені в критеріях для даного рівня послуги або гарантій [8].

Іще одним підходом до оцінювання системи функціональної безпеки є кількісний підхід, який реалізовується залученням стохастичних методів та формальних моделей. Використання такого підходу дозволяє об’єктивно визначити значення показників якості системи.

Серед стохастичних методів можна виокремити: частотний, статистичний, ймовірнісний. Частотний метод оцінювання системи функціональної безпеки базується на аналізі статистичного матеріалу та використовується для визначення збитку від реалізації певної загрози та визначається як [20]

$$R = 10^{(S+V-4)},$$

де: S – показник частоти виникнення загрози (обирається в інтервалі від 0 (загроза майже не виникає) до 7 (висока ймовірність виникнення загрози);

V – показник збитку, обирається в залежності від S.

Недоліком зазначеного методу є потреба у значному обзязі статистичного матеріалу.

Статистичний метод визначає виникнення певної загрози за визначений період часу, тобто статистична обробка потенційних загроз.

Ймовірнісний метод стохастичної групи визначає ймовірність відмови системи в результаті дії дестабілізаційних факторів.

Іншою групою якісного оцінювання системи функціональної безпеки є використання формальних моделей, а саме матричних, багаторівневих, багатокритеріальних, оптимізаційних.

Окремі автори [21] пропонують застосувати матричні або формальні моделі захисту. Відповідно до цього підходу стан системи описується трійкою параметрів: суб’єкти, об’єкти та права доступу. Аналогом такого підходу є модель дискреційного розмежування доступу, де аналогічним чином описується порядок надання доступу користувачам системи, які виступають в рамках даної моделі як суб’єкти або процеси, запущені від їхнього імені, а також модель Грехема-Денінга [22]. Спосіб визначення показників ефективності агреговано в [12, 20]. Суть його полягає: у визначенні параметрів; складанні тривимірної матриці відношень; перетворенні матриці відношень в двовимірну таблицю; визначенні якісних та кількісних значень показників.

Черговим підходом є використання моделей розмежування доступу, в яких вводиться функція рівня безпеки та визначається решітка рівнів безпеки (конфіденційності), які в сукупності визначають допустимі відношення доступу між сутностями системи. Показники ефективності визначаються відповідно до елементів моделі кінцевих станів Белла – Ла Падули.

Ще одним підходом до оцінки ефективності системи функціональної безпеки є застосування нечітких показників, таких як "абсолютно незахищена", "недостатньо захищена", "захищена", "достатньо захищена", "абсолютно захищена". Запропонована в [23] методика використовує поняття "рівень безпеки", який нормовано на проміжку [0, 1]. Показники надійності є

функцією $\mu^A(x_i)$, де x_i – елемент множини вимог безпека, A – множина значень, яка визначає виконання вимог безпеки. Оцінка ефективності за даною методикою здійснюється за попередньо чітко визначеними критеріями безпеки (багатокритеріальний підхід), що є головним недоліком даної методики.

Оптимізаційний або комбінаторний підхід використовує методи дискретного програмування (дискретної оптимізації), де значення функції $\sum_{j=1}^{n} c_j x_j$ необхідно максимізувати (мінімізувати) за умови: $\sum_{j=1}^{n} a_{ij} x_j \le b_i$, $i = \overline{1,m}$. При даному підході використовуються інструменти лінійного, випуклого програмування тощо.

Використання тільки одного із запропонованих підходів має недоліки. Наприклад, при використанні тільки методів експертних оцінок є великий ризик впливу певних шаблонів та стереотипів на кінцеве рішення. З іншого боку, використання тільки математичних методів вимагає чітких вихідних даних, які, як правило, відсутні. З метою визначення якості функціонування системи функціональної безпеки в умовах невизначеності вихідних даних запропоновано використати змішані методи. Одним із таких методів є метод порівняльного багатовимірного аналізу, суть якого полягає у визначенні ступеня взаємного впливу загроз та причин їх виникнення [15]. Загальна схема методу являє собою послідовність операцій, а саме:

- складення переліку об’єктів та вибір ознак оцінювання;
- формування матриці ознак;
- нормалізація елементів матриці ознак;
- визначення середнього арифметичного за усіма об’єктами;
- визначення стандартного відхилення;
- визначення матриці відстаней між показниками захищеності.

Отримана матриця відстаней дозволяє попарно зіставити між собою показники захищеності, здійснити їх ранжування, визначити ступінь

взаємного впливу. Використання цього методу вимагає формування матриці ознак, для чого застосовується метод експертних оцінок. Метод дозволяє оцінити вплив та взаємодію сформованих експертами загроз та на цій підставі раціоналізувати політику безпеки об’єкта інформаційної діяльності.

Одним із підходів змішаного характеру є управління ризиками як діяльність, що спрямована на прийняття і виконання управлінських рішень з метою зниження ймовірності виникнення негативного результату і мінімізації можливих втрат, які викликані її реалізацією [24]. Найбільш відомими алгоритмами, що сприяють оптимізації сил та засобів при управлінні ризиками, є методи CRAMM і RiskWatch.

Метод CRAMM був розроблений Центральним агентством з комп’ютерів та комунікації Великої Британії. Окремі версії методу спрямовані на вирішення завдань міністерства оборони, цивільних закладів, фінансових структур, приватних організацій. Метою розробки методу було створення формалізованої процедури, яка дозволяє впевнитись, що всі вимоги, які пов’язані з безпекою, повністю проаналізовані та задокументовані; уникнути зайвих витрат, які пов’язані із суб’єктивною оцінкою ризику; надавати допомогу при плануванні і здійсненні захисту на всіх стадіях життєвого циклу інформаційних систем; забезпечити проведення робіт у стислі терміни; автоматизувати процес аналізу вимог безпеки; надати обґрунтування для заходів протидії; оцінювати ефективність контрзаходів, порівнювати різні варіанти.

Метод складається із трьох етапів [15]. На першому етапі здійснюється формалізований опис інформаційної системи, її основних функцій, категорій користувачів, персоналу, який здійснює дослідження системи. Другим етапом методу є ідентифікація та оцінювання ресурсів. Третім етапом є оцінювання загроз і уразливостей. Оцінка ризику визначається через ймовірність реалізації та величину збитку

$$P_{изик} = P_{реалізації} \cdot З_{биток}.$$

У подальшому здійснюється деталізація ймовірності реалізації

$$P_{реалізації} = P_{загрози} P_{вразливості}.$$

Наведений метод дає підстави для прийняття рішення керівниками організації щодо впровадження нових механізмів безпеки або про модернізацію існуючої СІБ.

Ще одним із методів аналізу ризиків є метод RiskWatch, перевагами якого є детально опрацьована методика аналізу ризиків, яка добре зарекомендувала себе в багатьох державних організацій США; наявність як кількісної, так і якісної оцінки ризиків; достатньо велика база знань щодо загроз, уразливостей та контрзаходів; можливість редагування і вдосконалення бази знань. Структурно метод RiskWatch складається з трьох етапів, на першому з яких здійснюється формалізований опис системи, яка досліджується [15]. На другому етапі визначають конкретні характеристики системи. На третьому етапі здійснюється оцінка ризиків, де встановлюються зв’язки між втратами, ресурсами, загрозами та уразливостями та розраховуються математичні очікування втрат за рік

$$L = PV,$$

де L – сума втрат від загроз за рік;

P – частота виникнення загроз протягом року;

V – вартість ресурсу.

Використання описаних методів для оцінювання системи функціональної безпеки вимагає отримання об’єктивних вихідних даних, зокрема статистичних, що може бути проблематичним. Разом із тим, характер дії ІДФ на функціонування СФБ носить ймовірнісний характер. З цієї причини даний підхід є найбільш коректним для опису процесу оцінювання ефективності СФБ.

Дослідженням такого підходу присвячено низку робіт [12, 14, 15, 17, 23], але тільки в окремих [25, 26] запропоновано використати підхід теорії ефективності цілеспрямованих процесів. Як на наш погляд, такий підхід найбільш точно описує загалом поняття ефективності системи як ступінь досягнення мети цією системою. Проте використання такого підходу обмежується такими причинами: висока ступінь невизначеності вихідних даних, складність формалізації процесів функціонування [27].

Наявність проблем у формуванні й оцінюванні показників ефективності функціонування СФБ вимагає розробки методу оцінювання ефективності функціональної безпеки ІС на стадії модернізації.

В умовах модернізації ІІС, якщо апріорно в старій і новій версіях програмного забезпечення реалізуються функції забезпечення функціональної безпеки, необхідно врахувати потік інтегрованих інформаційних дестабілізаційних факторів, які викликані процесом спільного функціонування різних версій ІС.

Декомпозицію завдання узгодження з урахуванням ІІДФ на стадії модернізації може бути подано так:

– узгодження параметрів системних даних різних версій СФБ;

– доповнення системних даних обох версій необхідними значеннями;

– захист від ІДФ;

– контроль за станом програмних об’єктів, які реалізують тимчасове збереження даних та потребують синхронізації з іншими об’єктами за умови різної продуктивності пов'язаних компонентів, тобто забезпечення "прозорості" в гетерогенній ІС.

Кожна з функцій при декомпозиції на складові повинна поєднувати базові функції, систематизовані вище. Разом із тим зміна кількісного та якісного складу функціональних завдань СФБ пов'язана з додатковими витратами ресурсів ІІС.

5.2 Семантичні аспекти методу оцінювання ефективності функціональної безпеки

Міжнародним стандартом [50] визначено поняття функціональної безпеки як коректне функціонування як системи управління, так і керованого нею обладнання. Варто зазначити, що система управління відомчої інтегрованої інформаційної системи оперує критичним для прийняття рішення персоналом прикордонного відомства ресурсом. Дотримання властивостей інформаційного ресурсу та властивостей ІС загалом є головним завданням системи функціональної безпеки. В окремих джерелах [28] під поняттям дотримання властивостей інформаційного ресурсу ІС або забезпечення його безпеки розуміють діяльність, спрямовану на запобігання несанкціонованих дій щодо зазначеної інформації в системі. Вищенаведене дозволяє сформулювати поняття функціональної безпеки ІІС прикордонного відомства як цілеспрямований процес з єдиною (що є принциповим) метою – недопущення порушень властивостей інформаційної системи та інформаційного ресурсу в ньому під час усього життєвого циклу ІІС. Окремі нормативно-правові документи дають визначення систем забезпечення безпеки інформаційного ресурсу в ІС як взаємопов'язаної сукупності організаційних та інженерно-технічних заходів, засобів і методів забезпечення властивостей інформаційного ресурсу та інформаційної системи. Варто зазначити, що у цьому визначенні наведена система розглядається ізольовано від зовнішнього середовища, а саме від умов функціонування та умов застосування системи.

У роботах [29–31] використовується поняття зовнішнього середовища як основної умови забезпечення функціонування ІС, якість якої залежить не тільки від ступеня дотримання властивостей ІС та інформаційного ресурсу, який циркулює в ній, а й від здатності запобігання негативному впливу зовнішнього середовища та шкідливого програмного забезпечення. В основному всі автори, які розглядають у своїх роботах поняття "зовнішнє середовище", оцінюють тільки його негативний вплив на якість

функціонування системи. Зовнішнє середовище розглядається як джерело загроз: діяльність організацій (окремих осіб), вплив стихійного лиха, тощо. Такий підхід до розгляду зазначеного поняття має раціональне підґрунтя, а саме є сенс розглядати тільки негативний вплив, оскільки позитивний не призводить до зниження якості функціонування ІС загалом. Разом із тим вплив зовнішнього середовища може здійснювати і позитивний вплив на функціонування ІС або компенсувати негативні дії на її якість. У рамках такого підходу зовнішнє середовище ІС розглядається не тільки з негативної сторони, а і як неконтрольований вплив на функціонування всієї системи.

На наш погляд, варто розширити поняття "несанкціоновані дії щодо інформації в системі" в рамках системи забезпечення функціональної безпеки. Інформаційні системи ДПСУ є чутливими, у першу чергу, до таких властивостей інформації, як доступність та достовірність. Саме якість виконання цих послуг суттєво впливає на функціональну безпеку ІС прикордонного відомства та, у свою чергу, на національну безпеку держави. Особливостями функціонування інформаційних систем ДПСУ є використання орендованих каналів зв’язку для передачі даних до органів та підрозділів охорони кордону. Тому, наприклад, зменшення пропускної здатності каналу або його тимчасове відключення власником не можна класифікувати як несанкціоновані дії щодо інформації в системі, але такого типу порушення є інформаційним дестабілізаційним впливом на функціональну безпеку системи. Такі дії належать до категорії "навколишнього середовища".

Дамо визначення поняттю "навколишнє середовище" в рамках терміну "функціональна безпека", а саме: сукупність об’єктів, які не входять до СФБ та безпосередньо не беруть участь у процесі функціонування ІС, але впливають на досягнення мети СФБ. У подальшому поняття "навколишнє середовище" будемо розуміти як сукупність умов функціонування та умов застосування системи функціональної безпеки.

Загалом, функціонування системи функціональної безпеки можна представити як складну людино-машинну (ергатичну) систему з множиною

можливих станів, яка взаємодіє із зовнішнім середовищем та оперує власними ресурсами із завданням досягнення мети (рисунок 5.2).

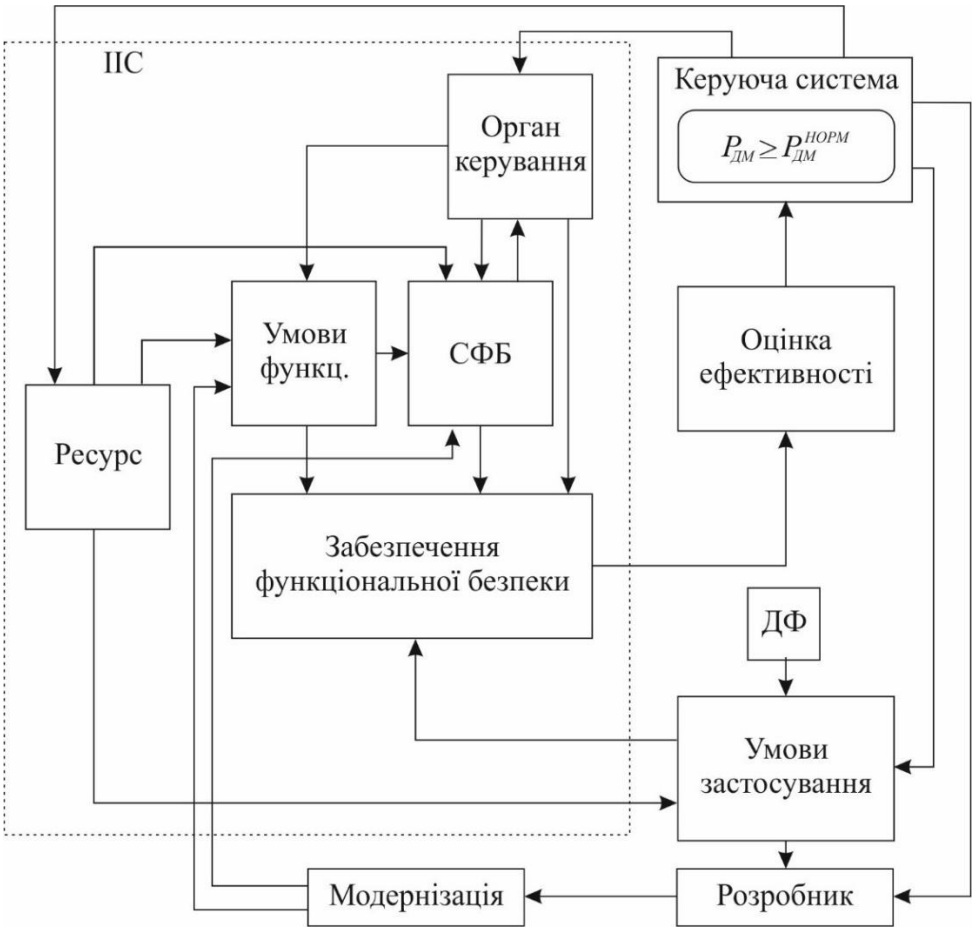


Рисунок 5.2 – Узагальнена структура функціонування СФБ

Стосовно до ІС "зовнішнім середовищем" вважаються умови застосування системи, на які діють різного типу дестабілізаційні фактори об’єктивного характеру, а також керуюча система та процес модернізації розробником.

Керуюча система (розпорядник ІІС) безпосередньо не входить до складу СФБ як підсистеми ІС, але чинить безпосередній вплив на наявність ресурсів системи, визначає умови застосування та через орган керування умови функціонування ІІС. Наприклад, у прикордонному відомстві розпорядником ІС є Адміністрація ДПСУ. При створенні ІС визначаються технічні умови розгортання зазначеної системи, розпорядник виділяє ресурси на її створення.

Реалізуючи розпорядчу функцію, Адміністрація через відповідні керівні документи формує порядок застосування СФБ в органах охорони державного кордону. Наявність зворотного зв’язку через оцінювання ефективності СФБ дозволяє Адміністрації здійснювати корегування умов функціонування та застосування системи загалом. У разі потреби модернізації наявної системи розпорядник надсилає розробнику технічне завдання на її модернізацію. Розробник, ув свою чергу, отримавши завдання на модернізацію системи ураховує умови застосування та здійснює зміни в системі, у тому числі стосовно СФБ. Модернізація складових ІІС приводить до зміни показника ефективності процесу функціональної безпеки, який після її оцінки порівнюється з нормативним значенням, та на цій підставі приймається рішення керуючою системою щодо запровадження внесених змін, зміни умов функціонування системи чи визначення допустимих умов застосування ІІС або регулювання ресурсів, які виділяються на процес забезпечення функціональної безпеки з метою дотримання відповідності показника ефективності заданому критерію. Такий підхід передбачає вирішення зворотної задачі оцінювання ефективності СФБ, а саме задачу синтезу СФБ при заданих умовах застосування та функціонування. Вищенаведене вимагає використання інших критеріїв: переваги й оптимальності, що виходить за межі дисертаційного дослідження.

На систему функціональної безпеки ІС впливають: орган керування, який визначає умови функціонування ІС та СФБ, зокрема; наявний ресурс, що забезпечує функціонування СФБ та визначає умови функціонування ІС загалом. Безпосередньо на сам процес впливають умови функціонування (внутрішній фактор) та умови застосування (зовнішній фактор), структура та організація СФБ, орган керування.

Аналіз узагальненої структури функціонування ІС показав, що вплив дестабілізаційних факторів на процес забезпечення функціональної безпеки здійснюється опосередковано через умови застосування системи. Керуюча

система з метою дотримання заданого (нормативного) рівня захисту має можливість визначати допустимі умови застосування.

Під умовами функціонування СФБ будемо розуміти сукупність факторів, які впливають на характеристики СФБ (стабільність, надійність, відновлюваність, керованість тощо). До умов функціонування віднесемо також природні та техногенні умови, в яких функціонує система, способи її застосування (постійний, періодичний), структуру та організацію СФБ, кількість та якість ресурсів. Як приклад умов функціонування СФБ наведемо мобільний ПТК АПК "Гарт 1/П", який базується на легковому автомобілі та застосовується відповідно до рішення начальника органу охорони кордону на різних ділянках відповідальності та в різний період. Тобто умови функціонування такого комплексу є різними (погодні умови, спосіб електроживлення, наявність каналів зв’язку тощо), спосіб застосування – періодичний.

Умови застосування СФБ – сукупність факторів організаційно-ситуаційного характеру, які впливають на ситуацію, у якій СФБ виконує свої завдання та визначає допустимі результати виконання завдань функціонального характеру. До умов застосування ІС ДПСУ належить оперативно-стратегічна обстановка як некерований фактор, що визначається дійсним розвитком прикордонного відомства і впливом ризиків та загроз його розвитку. Крім того, стратегія майбутнього використання ІС визначає основний характер їх цільового застосування. Зазначені фактори за своєю суттю є випадковими, тобто до моменту запуску в експлуатацію ІС (або після модернізації) їх значення невідомі. Це призводить до неможливості отримання розрахункового значення показника ефективності. Тому з метою усунення цієї невизначеності необхідно визначити ймовірнісні характеристики всіх випадкових факторів

Відповідно до визначення, поняття "функціональна безпека" можна розглядати як сукупність (послідовність) узгоджених протягом певного часу дій, які спрямовані на досягнення мети цього процесу. Оцінюючи

ефективність необхідно звернути увагу на те, що це властивість процесу, а не самої системи. Тому в подальшому під поняттям ефективності функціональної безпеки будемо розуміти комплексну властивість цілеспрямованого процесу, який характеризується ступенем досягнення мети, а саме функціональної безпеки.

Оцінюючи якість СФБ, яка описується n-вимірним векторним показником $Y_{\langle n\rangle}$, необхідно визначити сукупність критеріїв, які належать класу критеріїв придатності $\{G\}$, математичне формулювання якого має вигляд [32]

$$G:\left(Y_{\langle n\rangle}\in\left\{Y^{A}_{\langle n\rangle}\right\}\right), \tag{5.1}$$

де $Y_{\langle n\rangle}$ – показник якості СФБ;

$\left\{Y^{A}_{\langle n\rangle}\right\}$ – множина допустимих значень показника якості СФБ.

Отже, система функціональної безпеки, для якої виконується умова (5.1), придатна до використання за призначенням та виконує свої функції.

Серед множини властивостей системи функціональної безпеки істотними є ті, які визначають якість процесу функціональної безпеки. Визначені функціональні критерії [8], які описують вимоги до послуг, що забезпечують захист від загроз одного із чотирьох основних типів: конфіденційності, цілісності, доступності, спостереженості, що визначає множину типів показників якості СФБ (властивостей інформаційного ресурсу):

$$p=\{i,c,a,u\}, \tag{5.2}$$

де i – цілісність (**i**ntegrity);

c – конфіденційність (**c**onfidentiality);

a – доступність (**a**vailability);

u – спостереженість (acco**u**ntability).

Разом із тим у процесі забезпечення функціональної безпеки витрачаються ресурси задля підтримання функціонування системи на заданому рівні ефективності. Отже, СФБ у будь-який момент часу можна охарактеризувати трійкою властивостей:

– результативністю – властивістю системи забезпечити надійність інформації;

– ресурсоємністю, яка характеризується витратою ресурсів системи (матеріально-технічних, часових, енергетичних, фінансових, людських тощо);

– оперативністю – властивістю системи забезпечувати надійність інформації протягом зазначеного терміну часу.

Із зазначеного вище можна зробити висновок, що якість системи функціональної безпеки не може бути охарактеризована окремими властивостями, а визначається тільки їх сукупністю, тобто трійкою властивостей.

Введемо позначення цих властивостей:

$V_{\langle n_1 \rangle}$ – показник результативності;

$R_{\langle n_2 \rangle}$ – показник витрат ресурсів;

$T_{\langle n_3 \rangle}$ – показник часу.

Тоді, показником якості СФБ буде n-вимірний вектор, що містить три групи властивостей:

$$Y_{\langle n \rangle} = \left\langle V_{\langle n_1 \rangle}, R_{\langle n_2 \rangle}, T_{\langle n_3 \rangle} \right\rangle, \tag{5.3}$$

де: $n = n_1 + n_2 + n_3$

Усередині груп можливо згортання часткових показників шляхом введення узагальнених показників. Так, у більшості випадків витрати ресурсів можна привести до витрат коштів, тоді (5.3) набуде вигляду:

$$Y = \langle v_i, v_c, v_a, v_u; r; \tau \rangle, \tag{5.4}$$

де v_i – показник цілісності;

v_c – показник конфіденційності;

v_a – показник доступності;

v_u – показник спостереженості;

$r = \sum_{r_i \in R} r_i$ – показник витрат ресурсів;

τ – показник часу.

Необхідно врахувати, що при згортанні різнорідних показників узагальнений показник губить фізичний сенс, тому при багатокритеріальному аналізі коректним є згортання показників тільки всередині груп показників результатів. Згортання показників якості функціонування систем із різних груп є неприпустимим.

Фізичний сенс показників результативності забезпечення властивостей інформаційного ресурсу полягає у визначенні часу, протягом якого його властивість не буде порушена.

Фізичний сенс показника часу полягає у визначенні часу роботи всіх засобів забезпечення безпеки, за якого забезпечується нормативний рівень їх функціонування. З точки зору надійності, це напрацювання до відмови та описується відомими функціональними залежностями теорії надійності. Даний показник є складовим у формуванні показників результативності та може бути згорнутий у них.

Аналогічно показник витрат ресурсів також залежить від часу функціонування системи. Разом із тим розгортання об’єкта інформаційної діяльності передбачає витрату певних ресурсів та за їх відсутності або недостатній кількості дозвіл на функціонування ОІД не надається. Отже, даний показник не потребує дослідження і може бути виключений із вектора

показників якості СФБ та враховуватись окремо при порівнянні двох систем з однаковими значеннями показника якості.

Таким чином, вектор показників якості функціонування СФБ (5.4) прийме вигляд

$$Y = \langle v_i, v_c, v_a, v_u \rangle . \quad (5.5)$$

Варто зазначити, що компоненти вектора Y є кількісними характеристиками кількісних результатів самого процесу функціональної безпеки. Будемо вважати, що їх якісна характеристика завчасно забезпечується ще до початку експлуатації СФБ. Аналогічне зауваження застосуємо до якісної характеристики ресурсного забезпечення.

5.3 Обґрунтування показника ефективності функціонування системи функціональної безпеки

Система функціональної безпеки як взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів і методів забезпечення безпеки [28] повинна мати властивості системи, а не бути просто сукупністю певних засобів. Крім того, системний підхід повинен застосовуватись на всіх етапах життєвого циклу – від підготовки технічного завдання до експлуатації СФБ. Зазначимо, що система такого типу повинна мати чітке призначення, причому чим конкретніше сформульована мета системи, тим адекватніше буде її описувати показник ефективності. Складність формулювання мети СФБ ІІС полягає у її значній розосередженості та багатофункціональності, причому кожна із підсистем постійно підлягає модернізації. При такому підході значущість властивостей окремих елементів СФБ зменшується, а загальносистемні завдання збільшуються. Наприклад, визначення раціональної структури і режимів функціонування, організація взаємодії між складовими системи, вплив умов застосування та функціонування системи.

Системне об’єднання складових СФБ створює ефект емерджентності, тобто появу властивостей, які не притаманні жодному елементу окремо [33].

Аналіз ефективності функціонування СФБ вимагає формування та вирішення завдання кількісного оцінювання характеристик системи. Зазначені дані, які отримані або математичним моделюванням, або експериментальним шляхом, повинні описувати властивості системи, основною з яких є ефективність функціонування СФБ. Дана властивість системи агрегує в собі інші системні властивості, такі як надійність, керованість, оперативність відновлення після збоїв тощо. Разом із тим кількісна оцінка ефективності дозволяє здійснити порівняння системи при експлуатації в різних умовах та визначити допустимі межі експлуатаційних умов, за яких дотримується нормативне значення показника забезпечення функціональної безпеки.

У більшості випадків при проектуванні СФБ застосовують емпірично-інтуїтивний підхід, що наглядно показано в оцінюванні рівня безпеки інформаційних систем, коли оперують нечіткими поняттями, наприклад "достатньо захищений" [34, 35]. Нечітке визначення стосовно функціональної безпеки пов’язане з нечіткою постановкою завдання, вимог до забезпечення безпеки в умовах стохастичних впливів дестабілізаційних факторів. Як правило, це пояснюється тим, що СФБ проектується після розробки основного функціоналу ІС та не є складовою системи на стадії проектування.

Для оцінювання ефективності функціонування системи функціональної безпеки необхідно розробити показник ефективності процесу функціональної безпеки, який повинен відповідати основним вимогам [32]: показовість (адекватність), критичність (чутливість), комплексність (повнота), стохастичність, простота.

Показовість дозволяє оцінити ефективність функціонування СФБ з точки зору виконання нею основного завдання. Отже, мета системи повинна явно міститись у показникові ефективності системи.

Критичність показника показує, наскільки він чутливий до змін у характеристиках процесу забезпечення функціональної безпеки.

Комплексність показника дозволяє вирішити завдання визначення ефективності системи без залучення інших її характеристик.

Стохастичність дозволить урахувати невизначеність умов функціонування системи, впливу ДФ, які мають випадковий характер.

Простота показника ефективності сприяє доступності його сприйняття, а також аналізу якості функціонування СФБ.

На показники результативності системи функціональної безпеки впливають зовнішні та внутрішні фактори, які визначаються середовищем її функціонування.

Кожна з компонент вектора Y залежить від характеристик СФБ та її організації, умов функціонування та умов застосування системи.

$$Y = Y(A_1, A_2, B_1, B_2), \tag{5.6}$$

де A_1 – характеристики СФБ;

A_2 – характеристики організації процесу забезпечення безпеки;

B_1 – характеристики умов функціонування СФБ;

B_2 – характеристики умов застосування СФБ.

У свою чергу компоненти вектора Y^A допустимих значень теж залежать від умов застосування системи і визначаються керуючою системою

$$Y^A = Y^A(B_2). \tag{5.7}$$

У загальному випадку на характеристики СФБ, її організації, умови функціонування та застосування СФБ діє множина випадкових факторів, що визначає зазначені величини як випадкові. Разом із тим апріорі випадковими є і допустимі значення вектора Y^A, який залежить від умов застосування системи, оскільки завчасно невідомо, які повинні бути результати роботи СФБ, щоб забезпечити необхідний рівень функціональної безпеки. Окремі

дослідження при визначенні умов застосування та функціонування системи приймають припущення про найгірший їх варіант (з точки зору забезпечення функціональної безпеки), тобто величини B_1 та B_2 є не випадковими. Зазначене припущення призводить до неправомірно великих витрат ресурсів.

Усі складові вектора показників якості функціонування СФБ носять ймовірнісний характер, тому

$$\hat{Y} = Y\left(\hat{A}_1, \hat{A}_2, \hat{B}_1, \hat{B}_2\right), \qquad (5.8)$$
$$\hat{Y}^A = Y^A\left(\hat{B}_2\right).$$

У результаті реальних умов експлуатації СФБ критерій придатності (5.1) прийме вигляд

$$G : \left(\hat{Y} \in \left\{\hat{Y}^A\right\}\right). \qquad (5.9)$$

З виразу (5.9) можна зробити висновок, що придатність процесу функціональної безпеки – випадкова подія, яка безпосередньо не може відображати якість процесу. Тому характеристикою якості СФБ є ймовірність випадкової події

$$P_{ДМ} = P\left(\hat{Y} \in \left\{\hat{Y}^A\right\}\right). \qquad (5.10)$$

Отже, ймовірність $P_{ДМ}$ – це показник ефективності СФБ, який визначає ступінь виконання СФБ своїх функціональних завдань. На її основі формується критерій придатності системи, тобто $P_{ДМ} \geq P_{ДМ}^{НОРМ}$.

5.4 Методика формування моделі інформаційних дестабілізаційних факторів на стадії модернізації

Відповідно до [36] за результатами обстеження середовищ функціонування ІС визначаються потенційні ІДФ для ІС і розробляється їх модель. Побудова моделі здійснюється відповідно до положень [37–39].

Для створення моделі ІДФ складається перелік суттєвих факторів, описуються методи і способи їхнього здійснення. На підставі сформованих способів необхідно виокремити ті, які можуть їх реалізовувати в ІС. Прикладами такого типу ІДФ може бути взаємодія з каналом передавання даних, а саме отримування певних даних, які виникають у результаті різного виду випромінювань каналу або спеціальний вплив на нього з метою порушення функціонування системи функціональної безпеки чи цілісності інформаційного ресурсу. Ще одним шляхом отримання порушення властивостей інформаційного ресурсу є підключення до мереж, технічної апаратури або ліній зв'язку, здійснення різного виду маскувань під авторизовані процеси чи користувачів, інтеграція в систему програмних та/або апаратних закладних пристроїв (вірусів).

Інформаційні дестабілізаційні фактори для ІнР, що обробляється в ІС, залежать від її структури та складових, а саме: операційної системи, видів каналів передачі даних, фахового рівня персоналу, методів обробки даних та багатьох інших чинників. При формуванні моделі ІДФ повинні бути визначені їх основні види з метою забезпечення надійності інформації. Зазначені загрози можуть бути реалізовані стосовно ІС, яка модернізується, наприклад:

– зміна умов функціонування системи;

– зміна умов застосування ІС;

– збої і відмови при спільному функціонуванні обладнання та технічних засобів ІС;

– помилки під час упровадження компонентів ІС нової версії;

– помилки персоналу (користувачів) ІС під час модернізації;

– навмисні дії (спроби) потенційних порушників.

Формування моделі передбачає визначення переліку всіх ІДФ і проведення їх класифікації за результатом впливу на інформаційний ресурс відповідно до властивостей, на які вони спрямовані, а саме: конфіденційності, цілісності, доступності та спостережності.

Необхідно врахувати випадкові загрози суб’єктивного характеру (дії персоналу, користувачів з різних причин, наприклад: неуважності, недбалості, незнання тощо, але без навмисного наміру) [40]. Такого виду загрозами можуть бути:

– дії, що призводять до відмови ІС або її окремих компонентів з причини порушення порядку та правил, наведених розробником щодо здійснення модернізації;

– пошкодження носіїв інформації при здійсненні помилкових дій;

– зміна режимів роботи ІС або її окремих компонентів (переведення в тестовий режим, ініціювання процесу початкового налаштування, що може призвести до незворотних змін у системі);

– неумисне пошкодження СПЗ;

– невиконання вимог організаційних заходів при здійсненні модернізації;

– ненавмисне введення недостовірних даних у систему з метою перевірки якості функціонування;

– виведення даних за відсутніми в новій версії ІС адресами пристроїв, внутрішніх і зовнішніх абонентів тощо;

– розголошення конфіденційних відомостей із вилучених на заміну носіїв інформації;

– ненавмисне знищення атрибутів розмежування доступу тощо;

– використання з метою налаштування забороненого політикою безпеки програмного забезпечення;

– наслідки некомпетентного налаштування та застосування засобів захисту різних версій ІС та ін.

З іншого боку, загрозам суб’єктивної природи, що спрямовані на дезорганізацію роботи ІС, але за характером навмисні, можуть бути:

– порушення цілісності апаратної складової ІС або окремих компонентів під виглядом модернізації;

– порушення режимів функціонування систем захисту ІС;

– упровадження і використання недозволеного програмного та/або апаратного забезпечення;

– використання засобів перехоплення побічного випромінювання під час монтажу, заміни, встановлення СПЗ;

– крадіжки носіїв інформації під виглядом заміни, тощо;

– несанкціоноване копіювання носіїв інформації;

– одержання вищих прав доступу, ніж це передбачено функціональними обов’язками;

– отримання облікових даних інших користувачів;

– неправомірне підключення до каналів зв’язку з метою перехоплення даних тощо.

Перелік визначених суттєвих ІДФ повинен бути якомога повнішим і деталізованішим. Кожна загроза повинна бути класифікована стосовно:

– порушень властивостей інформаційного ресурсу;

– ймовірності виникнення ІДФ та факту їх залежності від процесу модернізації. Значення ймовірності визначається відомими статистичними методами або методом експертних оцінок;

– інших характеристик, які необхідні для розроблення, побудови, викладення та оформлення моделі ІДФ для інформації, що наведені в [41].

Зазначений перелік разом із характеристиками формується за результатами експертних оцінок (додаток Г). Варто зазначити, що наведена класифікація ІДФ і оцінки ймовірностей наведена для експериментального зразка ПТК АПС. Для конкретних ОІД ці величини повинні бути визначеними відповідними фахівцями.

У результаті аналізу множини загроз та їх характеристик визначаються можливі контрзаходи, які дають можливість сформувати структуру СФБ відомчої інформаційної системи відповідно до розробленого в попередніх розділах методу розподілу засобів забезпечення функціональної безпеки

інтегрованої інформаційної системи на стадії модернізації. Визначається склад, характеристики та можливості застосування тих чи інших заходів, засобів, способів, механізмів, функцій, здатних протистояти чи зменшити вплив кожного із впливів, а також вартість та термін функціонування кожного засобу.

Після визначення структури здійснюється повторний аналіз ІДФ з урахуванням функціонування системи функціональної безпеки та формування уточненої таблиці характеристик ІДФ.

Узагальнену структуру методики формування моделі ІДФ ІС на стадії модернізації наведено на рисунку 5.3.

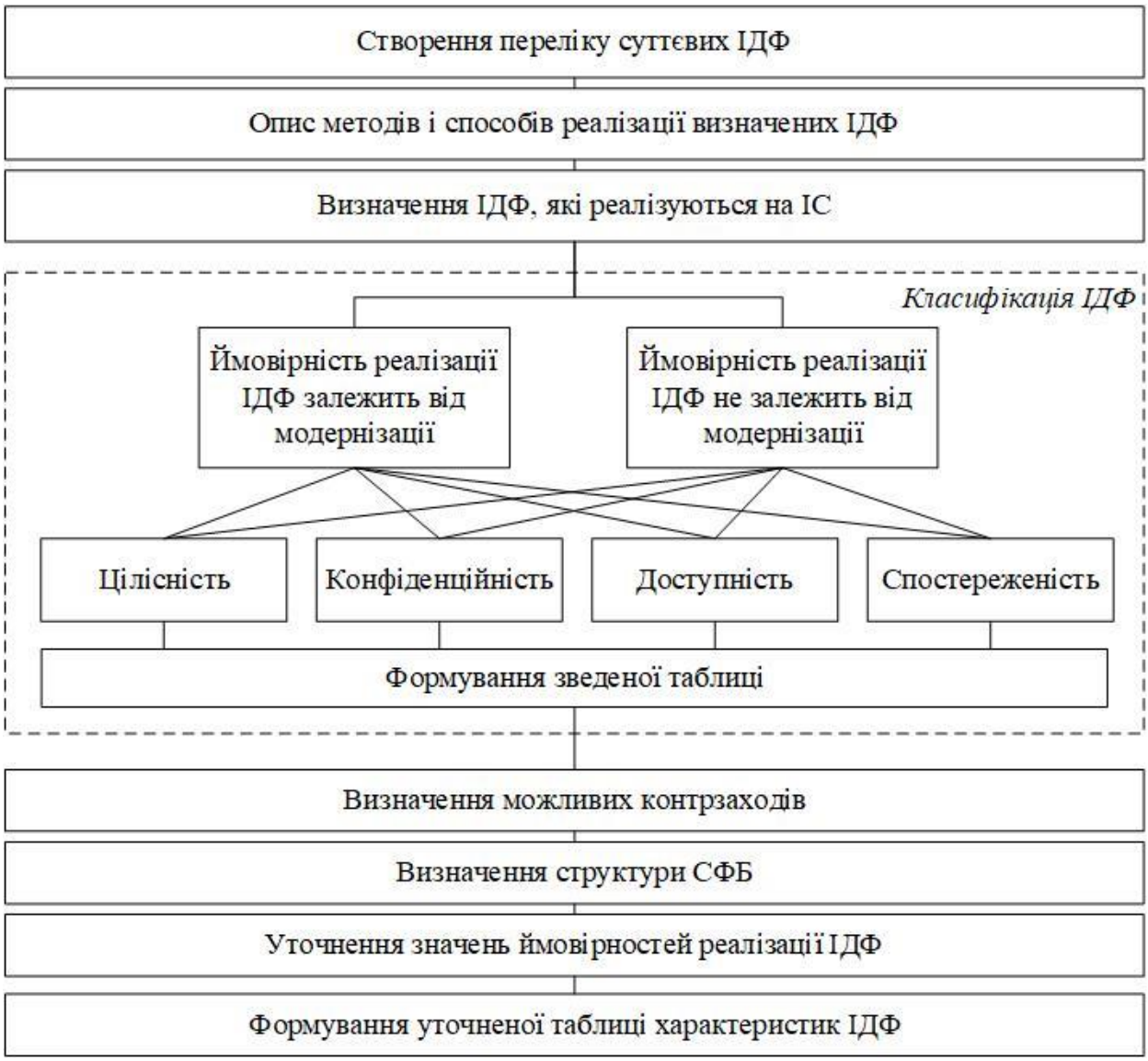


Рисунок 5.3 – Узагальнена структура методики формування ІДФ ІС на стадії модернізації

Уточнені характеристики ІДФ формуються за дві ітерації. Перша – визначення базових значень ймовірностей реалізації ІДФ, друга – на підставі сформованої структури СФБ та її можливостей із запобігання реалізації ІДФ, визначених у першій ітерації, формування уточнених значень допустимої ймовірності порушення властивостей інформаційного ресурсу.

Для визначення залишкового ризику загроз інформаційного ресурсу на стадії модернізації інформаційних систем пропонується розглянути ймовірності подолання СФБ відносно кожної властивості інформації [42].

На підставі сформованої уточненої характеристики ІДФ складовим інформаційного ресурсу в ІС формуються функціональні залежності залишкового ризику за властивостями інформаційного ресурсу.

Нехай P_p – значення залишкового ризику інформаційного ресурсу (ймовірність подолання засобів СФБ), яке залежить від ймовірності реалізації загрози, де $p \in \{i, c, a, u\}$ – властивості інформаційного ресурсу. Множина ІДФ складається із двох груп: група ІДФ, ймовірність виникнення яких не залежить від модернізації ІС, та група ІДФ, ймовірність виникнення яких залежить від модернізації ІС.

У загальному випадку функція залежності залишкового ризику інформаційному ресурсу від часу експлуатації для кожної загрози має вигляд

$$P_p^k(t) = \begin{cases} F_{p,k}^{ind}(t) - \textit{незалежить від модернізації}. \\ F_{p,k}^{dep}(t) - \textit{залежить від модернізації}, \end{cases} \quad (5.11)$$

де $F_{p,k}^{ind}(t)$ – функція розподілу ймовірності реалізації p–ї властивості та k–го ІДФ, ймовірність виникнення якого не залежить від модернізації ІС;

$F_{p,k}^{dep}(t)$–функція розподілу ймовірності реалізації p–ї властивості та k–го ІДФ, ймовірність виникнення якого залежить від модернізації ІС.

Ймовірність порушення властивості інформаційного ресурсу становить:

$$P_p = 1 - \prod_{k=1}^{N} \left(1 - P_p^k(t)\right), \tag{5.12}$$

де N – кількість складових ІДФ (додаток Д).

Визначимо ймовірність виникнення ІДФ, яка не залежить від модернізації ІС та може бути описана законом розподілу:

$$F_{p,k}^{ind}(t) = \begin{cases} 0, t < 0 \\ P_{p,k}^{ind} \\ 1, t > t_{експл} \end{cases}, \tag{5.13}$$

де $P_{p,k}^{ind}$ – значення ймовірності виникнення ІДФ, яка не залежить від модернізації ІС; $t_{експл}$ – час експлуатації СФБ.

Визначимо ймовірність виникнення ІДФ, яка залежить від модернізації ІС, тобто від потоку дестабілізаційних факторів, викликаних етапом приробітку модернізованої складової.

У загальному випадку найбільш повно описує ймовірність виникнення ІДФ функція розподілу цієї випадкової величини. Разом із тим при конкретному формуванні множини ІДФ та визначенні експертами самого факту функціональної залежності ДФ від модернізації формування виду та параметрів функції розподілу є малоймовірним. Тому пропонується як оцінку значення цієї ймовірності використовувати експертне значення величини ймовірності виникнення ІДФ з урахуванням ймовірності виникнення дестабілізаційного фактору, яка описується розподілом Вейбула, що описує час безвідмовної роботи та застосовується для оцінки надійності програмних засобів [43].

Отже, ймовірність виникнення ІДФ, який залежить від модернізації ІС, залежить від ймовірності безвідмовної роботи модернізованої ІС, а саме:

$$F_{p,k}^{dep}(t)=1-e^{-\left(\frac{t}{\beta_{p,k}}\right)^{\alpha_{p,k}}}. \qquad (5.14)$$

На практиці аналітичне визначення параметрів розподілу Вейбула за статистичними даними достатньо складне. Використовуючи наближений метод та дані випробувань, можливо визначити значення параметрів α та β для кожної складової кожного ІДФ [44].

Вищенаведені аналітичні дослідження дозволяють сформувати узагальнене значення величини залишкового ризику загроз інформаційному ресурсу Q на стадії модернізації інформаційних систем через складові ІДФ:

$$Q=1-\prod_{\forall p}\left(1-P_p\right). \qquad (5.15)$$

Варто зазначити, що значення величини залишкового ризику ІДФ виконане з припущенням про незалежність ймовірностей порушень властивостей інформаційного ресурсу. Разом із тим наведена функціональна залежність дозволить оцінити ступінь ризику інформаційному ресурсу при функціонуванні СФБ на об’єкті інформаційної діяльності.

5.5 Формування множини допустимих значень показника якості системи функціональної безпеки

Застосування ймовірнісного підходу теорії ефективності складних систем вимагає розробки аналітичного апарату формування множини допустимих значень.

Необхідно зазначити, що однобічність вимог до характеристик СФБ носить принциповий характер. Це дозволяє описати множину допустимих значень показника якості придатності СФБ 4-х вимірним гіпероктантом:

$$\left\{\hat{Y}^A\right\}=\left(\hat{\nu}_i^A,\infty\right)\times\left(\hat{\nu}_c^A,\infty\right)\times\left(\hat{\nu}_a^A,\infty\right)\times\left(\hat{\nu}_u^A,\infty\right) \tag{5.16}$$

з вершиною в точці $\hat{Z}=\left\langle\hat{\nu}_i^A,\hat{\nu}_c^A,\hat{\nu}_a^A,\hat{\nu}_u^A\right\rangle$.

Отже, опис множини допустимих значень показника якості придатності СФБ зводиться до відшукання законів розподілу компонент вектора $\hat{Z}$.

Відповідно до [36] за результатами обстеження середовищ функціонування ІС визначаються потенційні ІДФ та розробляється їх модель. Побудова моделі здійснюється відповідно до положень [37–39]. Після побудови системи забезпечення функціональної безпеки сформуємо уточнену множину ДІФ $\{\mathrm{T}\}$ складовим інформації в ІС, на підставі яких формуються компоненти вектора Y^A допустимих значень.

Нехай P_p^A – ймовірність порушення p–ї $\left(p\in\{i,c,a,u\}\right)$ властивості інформаційного ресурсу, яка залежить від ймовірності реалізації ІДФ:

$$P_p^A\left(\nu_p^A\right)=1-P\left(\hat{\nu}_p^A\le\nu_p^A\right). \tag{5.17}$$

Множину ІДФ $\{\mathrm{T}\}$ розділимо за властивостями інформаційного ресурсу p – $\{\mathrm{T}^p\}$. Кожну із цих підмножин, у свою чергу, розділимо на дві підмножини: $\{\mathrm{T}_{ind}^p\}$ – групу ІДФ, ймовірність виникнення яких не залежить від модернізації ІС та $\{\mathrm{T}_{dep}^p\}$ – групу ІДФ, ймовірність виникнення яких залежить від модернізації ІС за умови

$$\begin{gathered}\{\mathrm{T}_{dep}^p\}\cup\{\mathrm{T}_{ind}^p\}=\{\mathrm{T}^p\},\\ \{\mathrm{T}_{dep}^p\}\cap\{\mathrm{T}_{ind}^p\}=\varnothing.\end{gathered} \tag{5.18}$$

Отже, ймовірність порушення властивості інформаційного ресурсу становить

$$P_p^A\left(v_p^A\right)=1-\prod_{\forall k\in\left\{\Gamma_{ind}^p\right\}}\left(1-P_{p,k}^{ind}\right)\prod_{\forall k\in\left\{\Gamma_{dep}^p\right\}}\left(1-P_{p,k}^{dep}(\hat{v}_p^A\le v_p^A)\right), \quad (5.19)$$

де $P_{p,k}^{ind}$ – ймовірність порушення p –ї властивості інформаційного ресурсу при реалізації k – го ІДФ; $P_{p,k}^{dep}(t)$ – ймовірність порушення p –ї властивості інформаційного ресурсу при реалізації k – го ІДФ при модернізації ІС протягом часу t.

Ймовірність порушення p –ї властивості інформаційного ресурсу при реалізації k – го ІДФ яка не залежить від модернізації ІС та може бути описана законом розподілу (5.14). Ймовірність порушення властивостей інформаційного ресурсу, яка залежить від модернізації ІС, тобто від потоку дестабілізаційних факторів, викликаних етапом приробітку модернізованої складової та може бути описана законом розподілу (5.14).

Таким чином, (5.17) прийме вигляд:

$$P_p^A\left(v_p^A\right)=1-\prod_{\forall k\in\left\{\Gamma_{ind}^p\right\}}\left(1-F_{p,k}^{ind}\left(v_p^A\right)\right)\prod_{\forall k\in\left\{\Gamma_{dep}^p\right\}}e^{-\left(\frac{v_p^A}{\beta_{p,k}}\right)^{\alpha_{p,k}}}. \quad (5.20)$$

Отримані функціональні залежності дозволять сформувати закон розподілу випадкового вектора $\hat{Z}$:

$$F_{\hat{Z}}\left(Y^A\right)=P\left[\left(\hat{v}_i^A\le v_i^A\right)\wedge\left(\hat{v}_c^A\le v_c^A\right)\wedge\left(\hat{v}_a^A\le v_a^A\right)\wedge\left(\hat{v}_u^A\le v_u^A\right)\right]. \quad (5.21)$$

У загальному випадку події, пов’язані з порушенням властивостей інформаційного ресурсу, є взаємозалежними. Тому для формування закону розподілу випадкового вектора $\hat{Z}$ не достатньо знати закони розподілу кожної

із випадкових величин, а потрібно ще знати закони зв'язку між ними. Цей зв'язок характеризують за допомогою умовних законів розподілу. Маючи вид та характеристики умовних законів розподілу, не важко сформувати загальну функціональну залежність (5.21).

Разом із тим отримання умовних законів розподілу при формуванні СФБ є проблемним. З метою оцінки ступеня залежності показників якості системи функціональної безпеки пропонується використати метод експертних оцінок або статистичне значення ймовірностей виникнення події порушення властивості інформації при умові порушення іншої (через наявності такої).

Значення умовних ймовірностей сформуємо у вигляді таблиці (таблиця 5.1).

Таблиця 5.1 – Значення умовних ймовірностей порушення властивостей інформаційного ресурсу

Властивість інформаційного ресурсу	Умовна ймовірність порушення властивості ІнР			
	ціл.	конф.	дост.	спост.
Цілісність	1	$P_i(c)$	$P_i(a)$	$P_i(u)$
Конфід.	$P_c(i)$	1	$P_c(a)$	$P_c(u)$
Доступність	$P_a(i)$	$P_a(c)$	1	$P_a(u)$
Спостереж.	$P_u(i)$	$P_u(c)$	$P_u(a)$	1

Визначимо множину гіпотез

$$\mathrm{H} = \{H_i, H_c, H_a, H_u, H_d\}, \tag{5.22}$$

де H_i – порушення цілісності інформаційного ресурсу;

H_c – порушення конфіденційності інформаційного ресурсу;

H_a – порушення доступності інформаційного ресурсу;

H_u – порушення спостереженості інформаційного ресурсу;

H_d – дотримання властивостей інформаційного ресурсу;

Де

$$(1-P(H_i))\cdot(1-P(H_c))\cdot(1-P(H_a))\cdot(1-P(H_u))+(1-P(H_d))=1, \qquad (5.23)$$

звідки

$$P(H_d)=(1-P(H_i))\cdot(1-P(H_c))\cdot(1-P(H_a))\cdot(1-P(H_u)). \qquad (5.24)$$

Визначимо аналітичні залежності для гіпотези H_i за умови порушення тільки конфіденційності $P_c(i)$. Для цього сформуємо повну групу подій

$$\Omega=\{\omega_1,\omega_2,\omega_3\}, \qquad (5.25)$$

де ω_1 – порушення конфіденційності інформаційного ресурсу, яке не призвело до порушення цілісності;

ω_2 – порушення конфіденційності інформаційного ресурсу, яке призвело до порушення цілісності;

ω_3 – порушення конфіденційності інформаційного ресурсу відсутнє.

Отже, порушення цілісності інформаційного ресурсу за умови порушення конфіденційності становить

$$P^c_{H_1}=P_i(v_i^A)+(1-P_i(v_i^A))\cdot(1-[(1-P_c(v_i^A))+P_c(v_i^A)\cdot(1-P_c(i))]). \qquad (5.26)$$

Використовуючи цей підхід, розширимо множину подій на решту властивостей. Таким чином, порушення цілісності інформаційного ресурсу є зворотна подія до події не порушення цілісності з урахуванням ймовірностей порушень інших властивостей

$$\begin{aligned} P_{H_i}(v_i^A) &= P_i(v_i^A)+(1-P_i(v_i^A))\times \\ &\times(1-[(1-P_c(v_i^A))+P_c(v_i^A)(1-P_c(i))])\times \\ &\times(1-[(1-P_a(v_i^A))+P_a(v_i^A)(1-P_a(i))])\times \\ &\times(1-[(1-P_u(v_i^A))+P_u(v_i^A)(1-P_u(i))]) \end{aligned} \qquad (5.27)$$

Аналогічно для інших гіпотез

$$\begin{aligned} P_{H_c}\left(v_c^A\right) &= P_c(v_c^A) + (1 - P_c(v_c^A)) \times \\ &\times \left(1 - \left[\left(1 - P_i(v_c^A)\right) + P_i(v_c^A)(1 - P_i(c))\right]\right) \times \\ &\times \left(1 - \left[\left(1 - P_a(v_c^A)\right) + P_a(v_c^A)(1 - P_a(c))\right]\right) \times \\ &\times \left(1 - \left[\left(1 - P_u(v_c^A)\right) + P_u(v_c^A)(1 - P_u(c))\right]\right) \end{aligned}. \quad (5.28)$$

$$\begin{aligned} P_{H_a}\left(v_a^A\right) &= P_a(v_a^A) + (1 - P_a(v_a^A)) \times \\ &\times \left(1 - \left[\left(1 - P_i(v_a^A)\right) + P_i(v_a^A)(1 - P_i(a))\right]\right) \times \\ &\times \left(1 - \left[\left(1 - P_c(v_a^A)\right) + P_c(v_a^A)(1 - P_c(a))\right]\right) \times \\ &\times \left(1 - \left[\left(1 - P_u(v_a^A)\right) + P_u(v_a^A)(1 - P_u(a))\right]\right) \end{aligned}. \quad (5.29)$$

$$\begin{aligned} P_{H_u}\left(v_u^A\right) &= P_u(v_u^A) + (1 - P_u(v_u^A)) \times \\ &\times \left(1 - \left[\left(1 - P_i(v_u^A)\right) + P_i(v_u^A)(1 - P_i(u))\right]\right) \times \\ &\times \left(1 - \left[\left(1 - P_c(v_u^A)\right) + P_c(v_u^A)(1 - P_c(u))\right]\right) \times \\ &\times \left(1 - \left[\left(1 - P_a(v_u^A)\right) + P_a(v_u^A)(1 - P_a(u))\right]\right) \end{aligned}. \quad (5.30)$$

Ураховуючи (5.21, 5.27–5.30) отримаємо аналітичну форму закону розподілу випадкового вектора $\hat{Z}$

$$F_{\hat{Z}}\left(Y^A\right) = \left(1 - P_{H_i}\left(v_i^A\right)\right) \cdot \left(1 - P_{Hc}\left(v_c^A\right)\right) \cdot \left(1 - P_{H_a}\left(v_a^A\right)\right) \cdot \left(1 - P_{H_u}\left(v_u^A\right)\right). \quad (5.31)$$

Отримані функціональні залежності дозволяють описати множину допустимих значень показника якості системи функціональної безпеки.

Запропонований підхід до формування множини допустимих значень показника якості системи функціональної безпеки враховує динамічний потік дестабілізаційних факторів, викликаних процесом модернізації складових ІС при оцінці ефективності СФБ у реальних умовах [45]. При формуванні закону розподілу випадкового вектора вершини гіпероктанта допустимих значень

ураховані умовні ймовірності порушення властивостей інформаційного ресурсу. Отримана функціональна залежність дозволить аналітично описати показник ефективності функціонування СФБ.

5.6 Розробка методу оцінювання ефективності функціональної безпеки на стадії модернізації

5.6.1. Структурний опис методу оцінювання ефективності. Семантичні аспекти методу описують компоненти вектора $V_{\langle n_1 \rangle}$ як показники результативності СФБ, що являють собою кількісні характеристики тільки кількісних результатів системи. Зазначимо, що така інтерпретація допустима тільки за умови дотримання якісних характеристик складових результативності СФБ. Тобто якість процесу забезпечення функціональної безпеки забезпечується ще до "запуску" системи. Таким чином, тільки за якістю результатів процесу СФБ безпосередньо приймати рішення про її якість є некоректним з причини необхідності врахування ймовірнісного характеру процесу оцінювання. Вищезазначене вимагає оцінювати ефективність процесу забезпечення безпеки в два етапи (рисунок 5.4).

На етапі оцінювання якості результатів функціонування СФБ:

– визначається показник якості результатів функціонування СФБ через вектор показників якості функціонування;

– визначаються вимоги до якості результатів функціонування СФБ через множину допустимих значень показника якості СФБ;

– обґрунтовується критерій оцінювання якості результатів функціонування СФБ.

На етапі оцінювання ефективності функціонування СФБ:

– визначається показник ефективності функціонування СФБ як ймовірність досягнення мети системи;

– визначається вимоги до ефективності функціонування СФБ через мінімально допустиме значення ймовірності досягнення мети системи;

– реалізується критерій оцінювання ефективності функціонування СФБ як критерій придатності;

– здійснюється безпосереднє оцінювання ефективності функціонування СФБ.

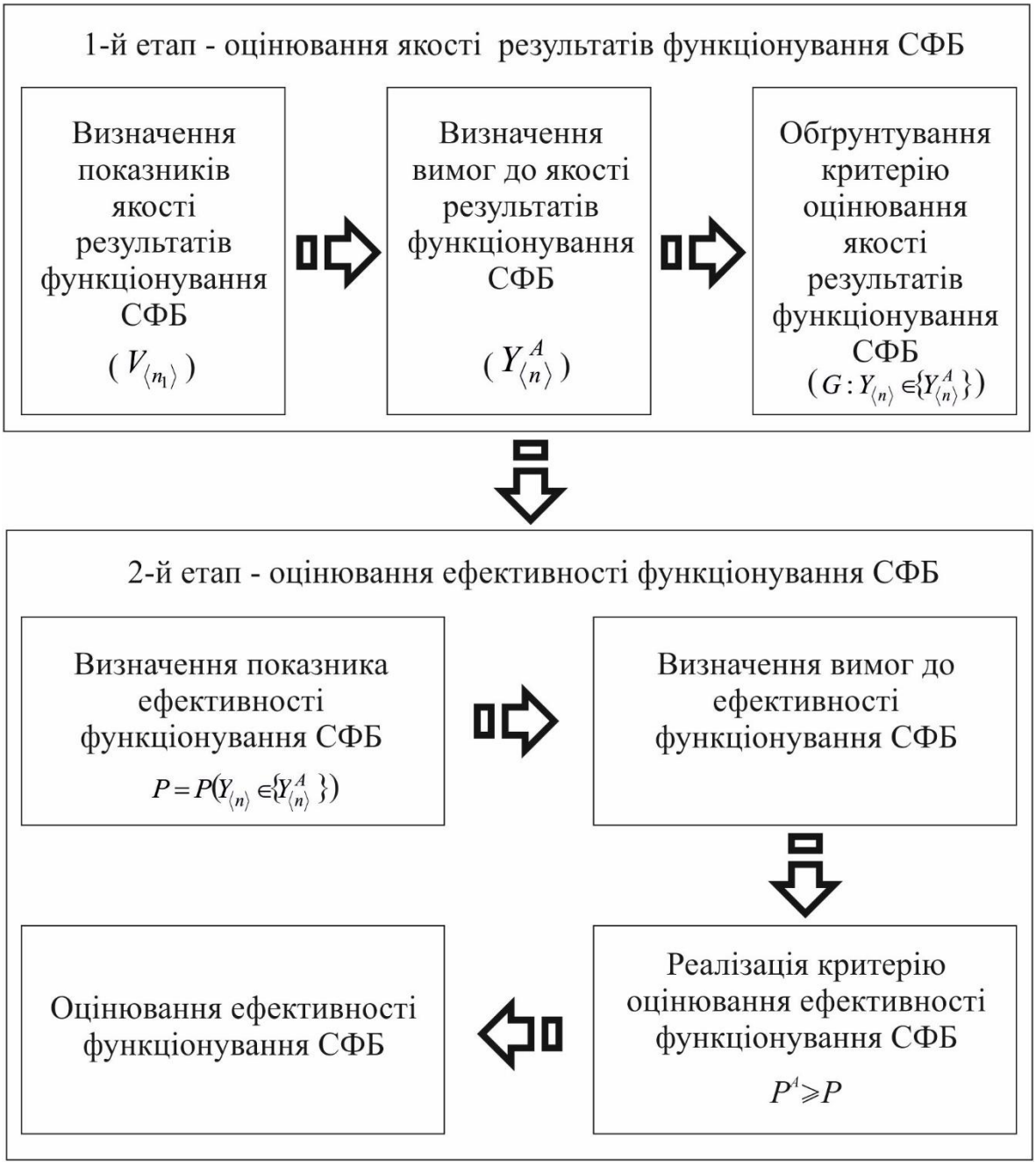


Рисунок 5.4 – Етапи оцінювання ефективності процесу функціонування системи функціональної безпеки

У загальному випадку ефективність СФБ пропонується визначати через ймовірність виконання системою функціональних задач в умовах впливу як

зовнішніх, так і внутрішніх дестабілізаційних факторів (5.1). Визначення вектора значень показників якості здійснюється залежно від структури ІС та наявної СФБ.

5.6.2. Аналітичний опис методу оцінювання ефективності. Для визначення показника ефективності повинна бути задана функція розподілу випадкового вектора $\hat{Y}$, універсальна форма, яка має вигляд:

$$F_{\hat{Y}}(Y) = P[(\hat{\nu}_i \le \nu_i) \wedge (\hat{\nu}_c \le \nu_c) \wedge (\hat{\nu}_a \le \nu_a) \wedge (\hat{\nu}_u \le \nu_u)]. \quad (5.32)$$

Стосовно до даної проблеми, а саме до складових вектора показників якості СФБ, фізичний сенс яких є час, протягом якого властивості інформаційного ресурсу не будуть порушені, більш зручною та інформативною є така форма інтегрального закону розподілу:

$$\Phi_{\hat{Y}}(Y) = P[(\hat{\nu}_i > \nu_i) \wedge (\hat{\nu}_c > \nu_c) \wedge (\hat{\nu}_a > \nu_a) \wedge (\hat{\nu}_u > \nu_u)], \quad (5.33)$$

фізичний сенс якого полягає у ймовірності дотримання властивостей інформації протягом визначених термінів.

У розділі 3 наведені аналітичні залежності для визначення ймовірності порушення цілісності інформаційного ресурсу та модель процесу порушення цілісності інформаційного ресурсу на елементі ІС (3.37, 3.38, 3.54), урахування яких дозволяє сформувати узагальнений вигляд закону розподілу ймовірності дотримання цілісності інформаційного ресурсу в ІС на стадії модернізації

$$P(\hat{\nu}_i > \nu_i) = 1 - P(\hat{\nu}_i \le \nu_i) = 1 - (1 - P_i(\nu_i))^N, \quad (5.34)$$

де N – кількість блоків даних, які обробляються в ІС, при чому складова ймовірності порушення цілісності інформаційного ресурсу k змінюється за експоненційним законом (додаток В), який свідчить про зміну кількості

елементів старої версії відносно загальної кількості елементів протягом періоду модернізації, та становить

$$k(\nu_i) = a_k e^{-w\nu_i} + b_k, \tag{5.35}$$

де w, a_k, b_k – параметри швидкості здійснення модернізації складових ІС.

Функціональна залежність (3.38), ймовірність того, що дані надходять в елемент ІС з іншої версії СПЗ, враховуючи (5.35), набуде вигляду

$$P_н(t) = \frac{\lambda_{old}\left(a_k e^{-wt} + b_k\right)}{\lambda_{new} a_k \left(1 - e^{-wt}\right) + \lambda_{old}\left(a_k e^{-wt} + b_k\right)}, \tag{5.36}$$

де λ_{old} – величина інформаційного потоку старої версії ІС;

λ_{new} – величина інформаційного потоку нової версії ІС.

На рисунку 5.5 показана динаміка зміни ймовірності того, що дані надходять в елемент ІС з іншої версії СПЗ.

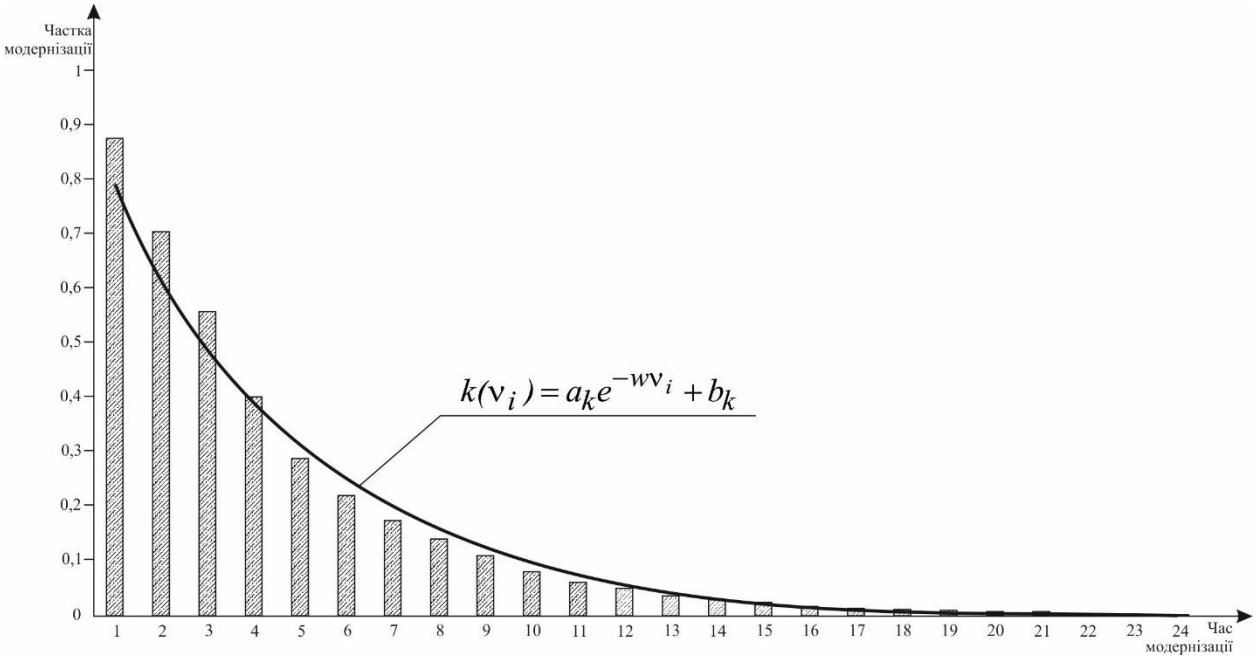


Рисунок 5.5 – Динаміка зміни ймовірності надходження даних в елемент ІС з іншої версії СПЗ

Аналіз (5.36) показав інваріантність значень ймовірності надходження даних в елемент ІС з іншої версії СПЗ від кількості елементів в ІС при рівності інформаційних потоків старої і нової версій. Разом із тим у загальному випадку таке припущення не є обов'язковим. За відмінностей інформаційних потоків різних версій ІС значення $P_н$ змінюється відповідно до рисунку 5.6.

Аналіз динаміки зміни ймовірності надходження даних в елемент ІС з іншої версії СПЗ при відмінностях інформаційних потоків різних версій ІС показав більш швидке зменшення зазначеної ймовірності у разі збільшення інформаційних потоків нової версії.

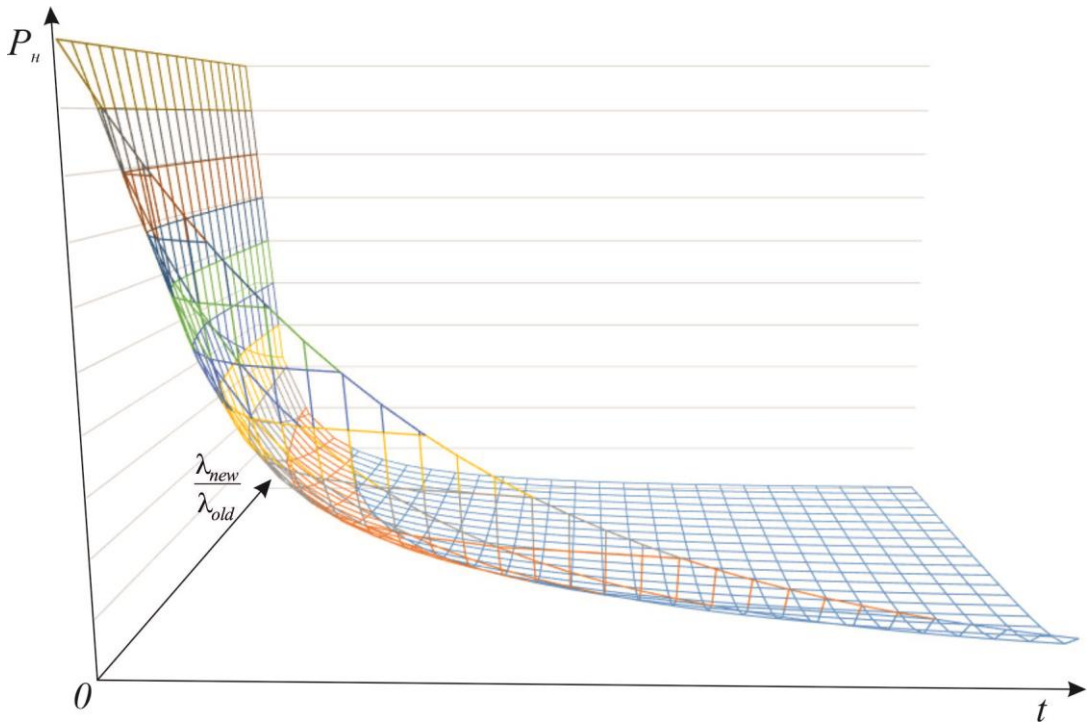


Рисунок 5.6 – Динаміка зміни ймовірності надходження даних в елемент ІС іншої версії СПЗ при відмінностях інформаційних потоків різних версій ІС

Таким чином, впровадження нових версій СПЗ із зменшеною величиною інформаційного потоку, у порівнянні із старою версією, призводить до збільшення ймовірності порушення властивостей інформаційного ресурсу, що необхідно враховувати при модернізації ІС. Разом із тим зворотна ситуація веде до зменшення інтенсивності дестабілізаційних факторів порушення

властивостей інформаційного ресурсу, викликаних невідповідностями версій СПЗ на стадії модернізації ІС.

Ураховуючи (3.37, 3.38, 3.54, 5.34, 5,35), отримаємо

$$P(\hat{\nu}_i > \nu_i) = 1 - \left(1 - P_{вх} + (1 - P_{вх}) P_н(\nu_i) P_{нв} \left(1 - \prod_{j=1}^{J} (1 - P_j)\right)\right)^N . \qquad (5.37)$$

З урахуванням (3.40, 5.35) закон розподілу ймовірності дотримання конфіденційності інформаційного ресурсу в ІС на стадії модернізації становить

$$P(\hat{\nu}_C > \nu_C) = 1 - \left(\prod_{i=1}^{m} (1 - P_д \cdot P_{кнсд} \cdot P_{дост} \cdot P_{нд} \cdot P_{нв} \cdot P_н(\nu_C))\right)^N . \qquad (5.38)$$

З урахуванням (3.42, 5.35) закон розподілу ймовірності дотримання доступності інформаційного ресурсу в ІС на стадії модернізації становить

$$P(\hat{\nu}_a > \nu_a) = 1 - \left(\prod_{i=1}^{m} (1 - P_д \cdot P_{кнсд} \cdot P_{дост} \cdot P_{нд} \cdot P_{нв} \cdot P_н(\nu_a))\right)^N \qquad (5.39)$$

З урахуванням (3.43, 5.35) закон розподілу ймовірності дотримання спостереженості інформаційного ресурсу в ІС на стадії модернізації становить

$$P(\hat{\nu}_u > \nu_u) = 1 - \left(\begin{array}{l} 1 - P_н(\nu_u) \cdot P_{нв} \cdot P_p \cdot (1 - (1 - P_i) \cdot (1 - P_c)) \times \\ \times \prod_{m=1}^{M} P_m^{ia} \cdot P_{дк} \cdot \left(1 - \prod_{j=1}^{J} (1 - P_j^{цкзз})\right) \end{array}\right)^N \qquad (5.40)$$

Вид інтегрального закону розподілу випадкового вектора $\hat{Y}$ з урахуванням (5.37-5.40) становить

$$\Phi_{\hat{Y}}(Y)=\left(\begin{array}{l}1-P_{вх}+(1-P_{вх})P_{н}(\nu_i)\times\\ \times P_{нв}\left(1-\prod_{j=1}^{J}\left(1-P_j^i(\nu_i)\right)\right)\end{array}\right)^N\times$$

$$\times\left(1-\left(\prod_{k=1}^{m}\left(1-P_{д}^k\cdot P_{кнсд}^k\cdot P_{дост}^k\cdot P_{нд}^k\cdot P_{нв}^k\cdot P_{н}(\nu_c)\left(1-\prod_{j=1}^{J}\left(1-P_j^c(\nu_c)\right)\right)\right)\right)^N\right)\times$$

$$\times\left(1-\left(\prod_{k=1}^{m}\left(1-P_{д}^k\cdot P_{кнсд}^k\cdot P_{дост}^k\cdot P_{нд}^k\cdot P_{нв}^k\cdot P_{н}(\nu_a)\left(1-\prod_{j=1}^{J}\left(1-P_j^a(\nu_a)\right)\right)\right)\right)^N\right)\times \quad (5.41)$$

$$\times\left(1-\left(\begin{array}{l}1-P_{н}(\nu_u)\cdot P_{нв}\cdot P_{р}\cdot(1-(1-P_i)\cdot(1-P_c))\times\\ \times\prod_{m=1}^{M}P_m^{ia}\cdot P_{дк}\cdot\left(1-\prod_{j=1}^{J}\left(1-P_j^{цкзз}(\nu_u)\right)\right)\end{array}\right)^N\right)$$

Вищезазначене дозволяє сформувати за формулою повної ймовірності ймовірність досягнення мети СФБ як:

$$P_{ДМ}=P\left(\hat{Y}\in\left\{\hat{Y}^A\right\}\right)=\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}\Phi_{\hat{Y}}(Z)dF_{\hat{Z}}(Z), \quad (5.42)$$

або

$$P_{ДМ}=\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}\Phi_{\hat{Y}}(Z)f_{\hat{Z}}(Z)d\nu_i^A d\nu_c^A d\nu_a^A d\nu_u^A, \quad (5.43)$$

де $f_{\hat{Z}}(Z)$ – щільність розподілу ймовірності випадкового вектораy $\hat{Z}$.

5.6.2.1 Середня ймовірність досягнення мети операції із забезпечення функціональної безпеки ІС. Оцінювання ефективності полягає у порівнянні значення показника ефективності СФБ, який визначає ступінь виконання СФБ своїх функціональних завдань з нормативним значенням. Першим етапом оцінювання ефективності СФБ є визначення значення показника

ефективності. Для визначення числового значення показника необхідно отримати закон розподілу випадкового вектора $\hat{Y}$ та випадкової множини $\left\{\hat{Y}^A\right\}$, що є завершальним етапом побудови математичної моделі процесу оцінювання ефективності СФБ.

Аналіз виразу (5.42) показав, що ймовірність $P_{ДМ}$ являє собою математичне очікування випадкової величини

$$\hat{\xi} = \Phi_{\hat{Y}}\left(\hat{Z}\right). \tag{5.44}$$

Величина $\hat{\xi}$ відповідно основних положень теорії стохастичної індикації називається стохастичним суперіндикатором [46].

Крім того, співвідношення (5.42) являють собою формулу повної ймовірності в інтегральній формі відносно подій $\hat{Z} = Z$ та $\hat{Y} = Y$. Функція розподілу випадкової величини $\hat{\xi}$ визначається як

$$F_{\hat{\xi}}(\xi) = P\left(\hat{\xi} \le \xi\right) = P\left(\hat{Z} \in \{Y\}\right) = \int\limits_{\{Y\}}\int\int\int dF_{\hat{Z}}(Z), \tag{5.45}$$

де $\{Y\}$ – область значень вектора Y, межа якого $Y^b(\xi) = \Phi_{\hat{Y}}^{-1}(\xi)$, та $\Phi_{\hat{Y}}^{-1}$ – зворотна функція до $\Phi_{\hat{Y}}$.

Ураховуючи (5.42, 5.44, 5.45), отримаємо

$$P_{ДМ} = \int\limits_0^1 \xi dF_{\hat{\xi}}(\xi). \tag{5.46}$$

Вираз (5.46) дозволяє стверджувати, що ймовірність досягнення мети операції із забезпечення функціональної безпеки є математичне очікування

його умовної ймовірності, тобто середньої умовної ймовірності досягнення мети операції із забезпечення функціональної безпеки інформаційної системи.

В окремих випадках функція розподілу нормативних вимог до результатів забезпечення функціональної безпеки може бути невідомою. З цієї причини керуюча система задає максимально можливі значення результатів операції із забезпечення функціональної безпеки. У даному випадку значення $\hat{Z}$ перестають бути випадковими, тобто $\hat{Z} = Z^{НОРМ}$. Отже, закон розподілу випадкового вектора набуває такого вигляду:

$$F_{\hat{Z}}(Z) = \prod_{\forall p} \Delta\left(\nu_p - \nu_p^{НОРМ}\right), \tag{5.47}$$

тоді $dF_{\hat{Z}}(Z) = \prod_{\forall p} \delta\left(\nu_p - \nu_p^{НОРМ}\right) d\nu_p$

то співвідношення (5.42) набуде вигляду

$$P_{ДМ} = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} \Phi_{\hat{Y}}(Z) \prod_{\forall p} \delta\left(\nu_p - \nu_p^{НОРМ}\right) d\nu_i^A d\nu_c^A d\nu_a^A d\nu_u^A, \tag{5.48}$$

або

$$P_{ДМ} = \Phi_{\hat{Y}}\left(\nu_i^{НОРМ}, \nu_c^{НОРМ}, \nu_a^{НОРМ}, \nu_u^{НОРМ}\right). \tag{5.49}$$

Отже, при детермінованих вимогах до результатів функціонування СФБ достатньо отримати закон розподілу їх випадкового вектора.

З метою наочності динаміки змін значень ймовірності виконання функціональних завдань із забезпечення функціональної безпеки зафіксуємо окремі складові функціональної залежності (5.41). На рисунку 5.7 показано вплив нормативних значень показників результативності на ефективність виконання СФБ функціональних завдань.

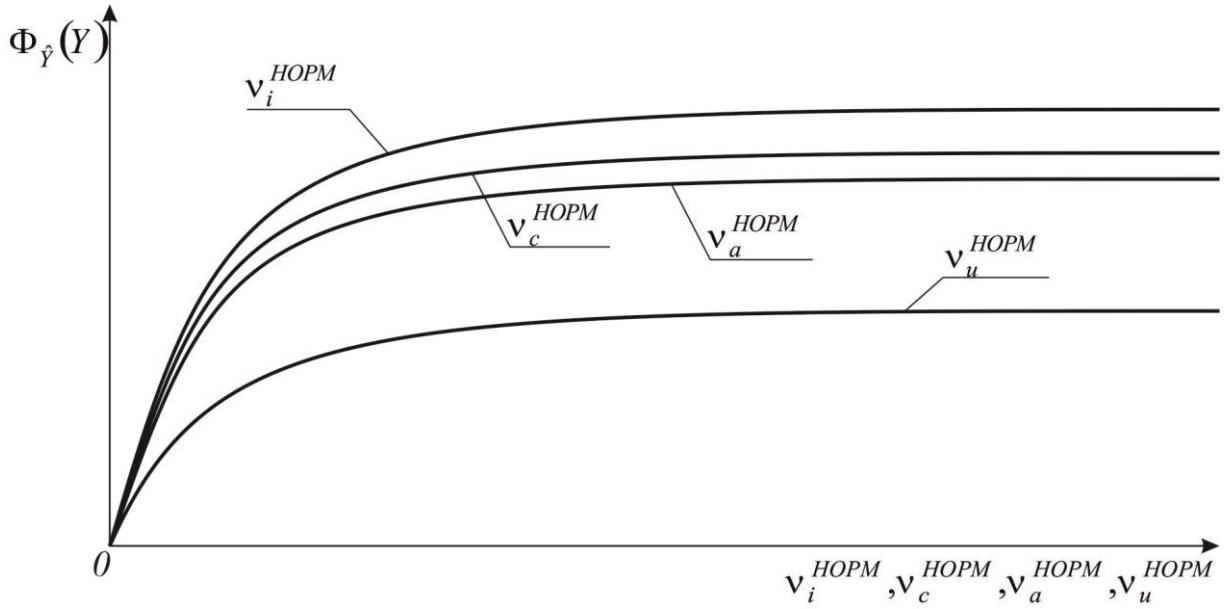


Рисунок 5.7 – Динаміка змін значень ймовірності виконання функціональних завдань при часткових змінах нормативних значень

Нормативне значення показника цілісності найбільше впливає на результативність системи з причини більшого впливу на показник спостереженості. Наступними за рівнем впливу є показники конфіденційності та доступності, які мають близькі значення. Найменший вплив чинить показник спостереженості.

Отже, при збільшенні значень нормативних показників результативності середнє значення ймовірності виконання завдання із забезпечення надійності інформації на стадії модернізації збільшується. Фізичний сенс такого явища пояснюється поступовим зменшенням потоку дестабілізаційних факторів, викликаних процесом модернізації.

Динаміку зміни середнього значення ймовірності виконання завдання із забезпечення функціональної безпеки на стадії модернізації при зафіксованих значеннях нормативних результатів та зміні кількості функціональних блоків інформації, яка опрацьовується системою, показано на рисунку 5.8.

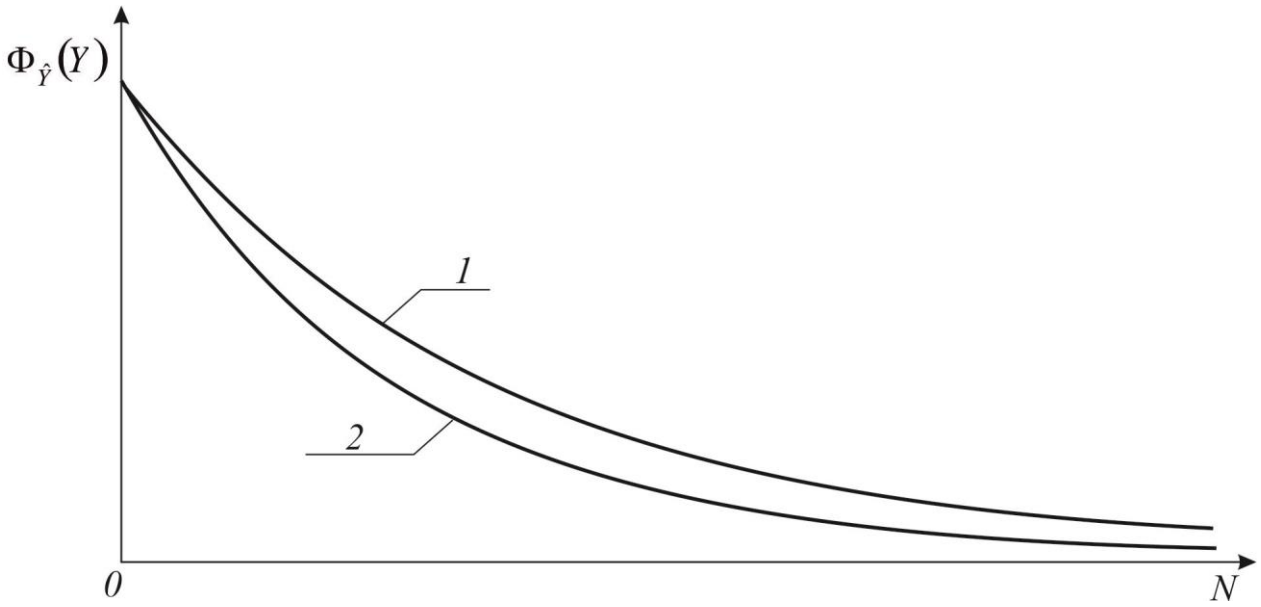


Рисунок 5.8 – Динаміка зміни значень ймовірності виконання функціональних завдань із забезпечення функціональної безпеки при зміні кількості функціональних блоків інформації (1) та кількості АРМ (2)

Аналіз впливу кількості блоків інформації показав експоненційний вплив на ефективність системи, тобто збільшення кількості інформації, яка обробляється на АРМ ІС, призводить до значного зменшення ймовірності виконання завдань СБФ. Вищенаведене дозволить сформувати рекомендації щодо проведення модернізації інформаційних систем, а саме нормативне зменшення кількості інформаційних блоків або проведення модернізації під час їх мінімальних значень. Причому збільшення кількості АРМ в ІС має менший вплив ніж саме кількість інформації.

Аналіз впливу зміни ймовірностей невідповідності версій ($P_{нв}$), ймовірності наявності даних певної категорії в ІС ($P_{нв}$) та ймовірність того, що дані певної категорії надходять у загальне поле елементу ІС із старої або нової версій СПЗ з порушеною властивістю ($P_{вх}$) на кінцеву ефективність СФБ (рисунок 5.9), показав, що збільшення значень ймовірностей $P_{нв}$ та $P_{нв}$ не призводить до повної втрати ефективності системи, а тільки до зниження до певного порогового значення.

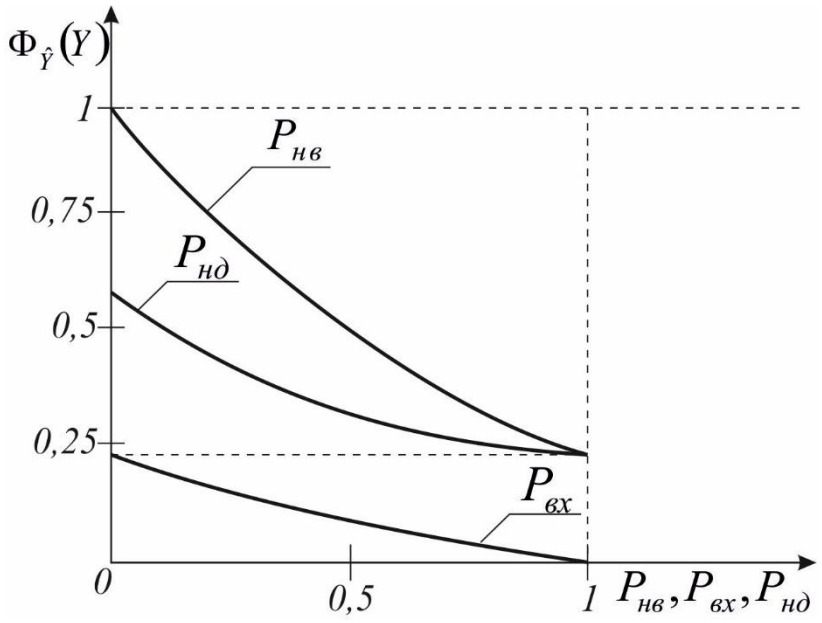


Рисунок 5.9 – Динаміка зміни значень ймовірності виконання функціональних завдань із захисту інформації при зміні окремих складових

Як видно із рисунку 5.7, мінімальне значення ефективності СФБ при максимальних значеннях $P_{нв}$ та $P_{нв}$ відповідає мінімальному значенню $P_{вх}$ та при збільшенні останнього призводить до невиконання СФБ своїх функціональних завдань. Фізичний сенс зазначених висновків полягає в тому, що при надходженні у загальне поле елементу ІС із старої або нової версій СПЗ даних із порушеною властивістю СФБ не має можливості виконати своє завдання за призначенням, оскількик властивості інформаційного ресурсу вже було порушено. Це призводить до втрати ймовірнісної складової факту порушення властивостей інформаційного ресурсу і робить цей факт детермінованим.

5.6.2.2 Гарантована ймовірність досягнення мети операції із забезпечення функціональної безпеки. Ймовірнісні характеристики випадкових величин надають можливість здійснити прогнозування значень їх властивостей. Наприклад, математичне очікування визначає середнє значення випадкової величини [47]. Дисперсія визначає міру відхилення значень випадкової величини від центру розподілу [48]. Найбільш повно описує властивості випадкової величини її закон розподілу, який ураховує всі

ймовірнісні властивості у взаємозв'язку. Варто звернути увагу на суттєву відмінність властивостей прогнозування і можливостей зазначених характеристик. Числові характеристики випадкових величин дають прогноз тільки середніх результатів для великої кількості майбутніх дослідів, причому закони їх розподілу дозволяють прогнозувати результати одиничних дослідів [49].

У попередньому пункті визначено функцію розподілу стохастичного суперіндикатора $\hat{\xi}$, тому можливо визначити ще один показник ефективності – гарантовану ймовірність досягнення мети операції із захисту інформації:

$$\xi^{\Gamma}(\omega) = F_{\hat{\xi}}(1-\omega), \tag{5.50}$$

де ω – рівень гарантії.

З урахуванням того, що при визначенні гарантованої ймовірності використовується закон розподілу суперіндикатора, цей показник дозволяє оцінити ефективність одиничних операцій, на відміну від середньої ймовірності $P_{ДМ}$, яка дійсна тільки при достатньо великих кількостях дослідів.

При дослідженні ефективності функціонування СФБ в умовах невизначеності, які викликані впливом дестабілізаційних факторів зовнішнього та внутрішнього характеру, їх вплив при тривалому терміні експлуатації системи буде в середньому компенсуватись. Проте, при одноразовому застосуванні системи значення показника $\hat{\xi}$ може мати відхилення від середнього значення на досить значну величину.

Відповідно до (5.50) гарантована ймовірність виконання завдання СФБ є функцією, у якій аргумент (рівень гарантії) не зростає, тобто чим вище рівень гарантії, тим нижче на цьому рівні значення $\xi^{\Gamma}(\omega)$. Семантикою функції (5.50) є мінімально можлива частка (з ймовірністю ω) значення умовних

ймовірностей виконання функціональних завдань із забезпечення функціональної безпеки. Причому кількісні значення цієї величини є достатньо малими у відношенні до середньої ймовірності досягнення мети із забезпечення надійності інформації. Разом із тим поняття гарантованої ймовірності, як правило, використовується не для оцінювання ефективності, а для порівняння якості функціонування різних систем.

У випадку наявності детермінованих вимог до результатів роботи СФБ, у яких функція розподілу описана в (5.47), тоді і стохастичні суперіндикатори являють собою невипадкові величини і їх розподіл є виродженим (рисунок 5.10) [32].

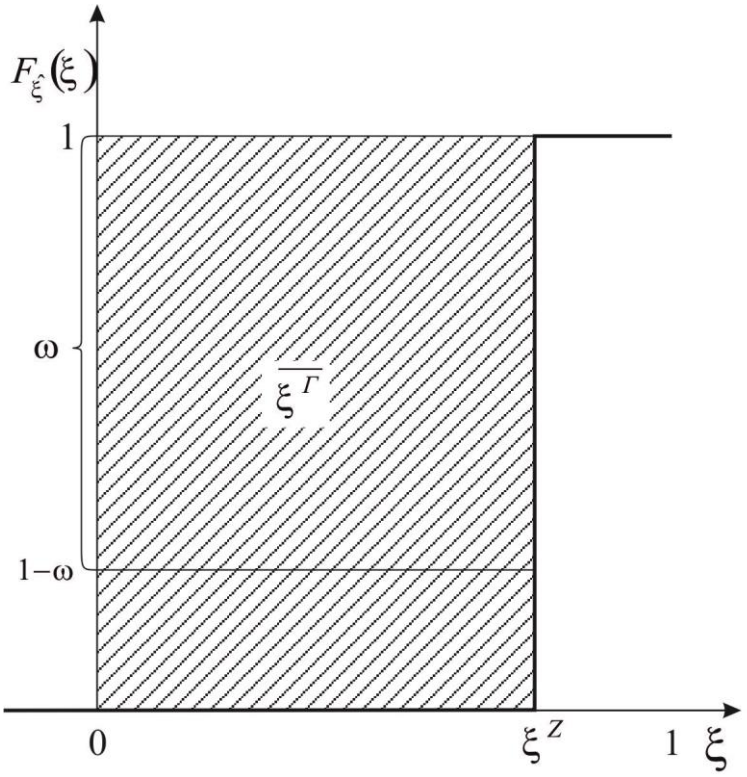


Рисунок 5.10 – До пояснення розподілу стохастичного суперіндикатора у випадку детермінованих вимог до результатів роботи СФБ

Таким чином, при детермінованих вимогам до результатів операції всі показники її ефективності дорівнюють один одному при будь-якому рівні гарантії [32].

5.7 Висновки до розділу 5

1. У розділі проведений аналіз наявних підходів до оцінювання ефективності систем функціональної безпеки, які базуються на двох категоріях: кількісних та якісних оцінок. Якісні методи оцінювання застосовуються в умовах достатньо значної невизначеності та базуються, як правило, на досвіді експертів у даній галузі. Кількісні методи оцінювання – це результат глибокого опису предметної області дослідження, детального моделювання процесів систем функціональної безпеки. Використання зазначених методів дає можливість визначити конкретне значення оцінки процесу, який досліджується, та в подальшому здійснити його оптимізацію.

2. На підставі проведеного аналізу запропоновано використати підхід теорії ефективності цілеспрямованих процесів, що найбільш точно описує загалом поняття ефективності системи як ступінь досягнення мети цією системою. Проте його використання обмежується такими причинами: висока ступінь невизначеності вихідних даних, складність формалізації процесів функціонування.

3. Наведені семантичні аспекти методу оцінювання ефективності. З’ясовано, що у наведеному визначенні система функціональної безпеки розглядається ізольовано від зовнішнього середовища, а саме від умов функціонування та умов застосування системи. Саме тому це поняття підлягало визначенню та врахуванню у функціонуванні системи забезпечення функціональної безпеки.

4. Аналіз узагальненої структури функціонування СФБ показав, що вплив дестабілізаційних факторів на процес забезпечення функціональної безпеки здійснюється опосередковано через умови застосування системи. Керуюча система з метою дотримання заданого (нормативного) рівня забезпечення функціональної безпеки має можливість визначати допустимі умови застосування.

5. Обґрунтовано поняття ефективності забезпечення функціональної безпеки як властивості цілеспрямованого процесу, який характеризується

ступенем досягнення мети. Дане поняття носить стохастичних характер та залежить від сукупності зовнішніх і внутрішніх чинників, які у свою чергу, у будь-який момент можна охарактеризувати трійкою властивостей: результативністю, ресурсоємністю, оперативністю.

6. Вищенаведене дозволило розробити показник ефективності процесу забезпечення функціональної безпеки, який відповідає основним вимогам: показовості, критичності, комплексності, стохастичності, простоті. На підставі розробленого показника сформовано критерій придатності системи.

7. Одним із основних складових показника ефективності забезпечення функціональної безпеки є визначення множини ІДФ властивостей інформаційного ресурсу ІС на стадії модернізації. З цією метою в даному розділі розроблено методику формування моделі ІДФ на стадії модернізації. Результатом є визначення узагальненого значення величини залишкового ризику властивостям інформаційного ресурсу на стадії модернізації інформаційних систем через складові ІДФ та формування їх переліку з урахуванням впливу саме на стадії модернізації. Використання зазначеної методики дозволить оцінити ступінь ризику інформаційного ресурсу при функціонуванні СФБ на об’єкті інформаційної діяльності. Результати методики є базисом для подальшого формування множини допустимих значень складових показника ефективності системи загалом.

8. Запропонований підхід до формування множини допустимих значень показника якості системи забезпечення функціональної безпеки дозволить врахувати динамічний потік дестабілізаційних факторів, викликаних процесом модернізації складових ІС при оцінці ефективності СФБ в реальних умовах. При формуванні закону розподілу випадкового вектора вершини гіпероктанта допустимих значень ураховані умовні ймовірності порушення властивостей інформаційного ресурсу.

9. Дослідження дозволили сформувати структурну схему методу оцінювання ефективності, яка складається з двох етапів: оцінювання якості результатів функціонування СФБ та оцінювання ефективності

функціонування СФБ. У загальному випадку ефективність СФБ пропонується визначати через ймовірність виконання системою функціональних задач в умовах впливу як зовнішніх, так і внутрішніх дестабілізаційних факторів. Визначення вектора значень показників якості здійснюється залежно від структури ІС та наявної СФБ.

10. При аналітичному описі моделі методу оцінки ефективності забезпечення функціональної безпеки на стадії модернізації проаналізовано динаміку зміни ймовірності надходження даних в елемент ІС з іншої версії СПЗ при відмінностях інформаційних потоків різних версій ІС, який показав більш швидке зменшення зазначеної ймовірності при збільшенні інформаційних потоків нової версії. Отже упровадження нових версій СПЗ із зменшеною величиною інформаційного потоку, у порівнянні із старою версією, призводить до збільшення ймовірності порушення властивостей інформаційного ресурсу, що необхідно враховувати при модернізації ІС. Разом із тим зворотна ситуація приводить до зменшення інтенсивності дестабілізаційних факторів порушення властивостей інформаційного ресурсу, викликаних невідповідностями версій СПЗ на стадії модернізації ІС.

11. Розроблений інтегральний закон розподілу випадкового вектора показників результативності функціонування СФБ, який дозволив сформувати за формулою повної ймовірності ймовірність досягнення мети системою функціональної безпеки. Аналіз функціональних залежностей дозволив визначити такі поняття, як середня та гарантована ймовірність виконання завдання із забезпечення функціональної безпеки. У результаті досліджень з’ясовано, що при збільшенні значень нормативних показників результативності середнє значення ймовірності виконання завдання із забезпечення функціональної безпеки на стадії модернізації збільшується. Фізичний сенс такого явища пояснюється поступовим зменшенням потоку дестабілізаційних факторів, викликаних процесом модернізації.

12. Аналіз впливу кількості блоків інформації на ефективність безпеки показав експоненційний характер дії на ефективність системи, тобто

збільшення кількості інформації, яка обробляється на АРМ ІС, призводить до значного зменшення ймовірності виконання завдань СФБ. Вищенаведене дозволить сформувати рекомендації щодо проведення модернізації інформаційних систем, а саме нормативного зменшення кількості інформаційних блоків або модернізації під час їх мінімальних значень.

13. У результаті досліджень ефективності функціонування СФБ в умовах невизначеності, які викликані впливом дестабілізаційних факторів зовнішнього та внутрішнього характеру, з'ясовано, що їх вплив при тривалому терміні експлуатації системи буде в середньому компенсуватись, проте при одноразовому застосуванні системи значення показника ефективності може мати відхилення від середнього значення на досить значну величину.

14. Визначено поняття гарантованої ймовірності виконання завдання СФБ, семантикою якої є мінімально можлива частка (з ймовірністю ω) значення умовних ймовірностей виконання функціональних завдань із забезпечення функціональної безпеки. Причому кількісні значення цієї величини є достатньо малими у відношенні до середньої ймовірності досягнення мети із забезпечення надійності інформації. Разом із тим поняття гарантованої ймовірності, як правило, використовується не для оцінювання ефективності, а для порівняння якості функціонування різних систем.

15. Розглянуто окремий випадок, при якому функція розподілу нормативних вимог до результатів забезпечення функціональної безпеки є невідомою. З цієї причини керуюча система задає максимально можливі значення результатів операції із забезпечення функціональної безпеки. Для вирішення цієї задачі наведені функціональні залежності закону розподілу випадкового вектора показників результативності СФБ.

Список використаних джерел у п’ятому розділі

1. Петренко С. А. Информационная безопасность: экономические аспекты / С. Петренко, С. Симонов, Р. Кислов // Jet Info Online. - 2003. - №10. [Электронный ресурс]. - Режим доступа: http://citforum.ru/security/articles/sec/index.shtml.

2. Архипов А. Е. Технологии експертного оценивания в задачах защиты информации / А. Е. Архипов, С. А. Архипова, С. А. Носок // Інформаційні технології та комп’ютерна інженерія : міжнар. наук.-техн. журн. – № 1. – 2005. – С. 89-94.

3. Архипов О. Є. Оцінювання ефективності системи охорони державної таємниці : монографія / О. Є. Архипов, І. Т. Бородавко, В. П. Ворожко. – К., 2007. – 63 с.

4. Архипов О. Є. Системні аспекти оцінювання рівня важливості секретної інформації / О. Є. Архипов, В. П. Ворожко // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні : наук.-техн. зб. – К., 2007. – Вип. 2 (15). – С. 10-12.

5. Корченко А. Г. Построение систем защиты информации на нечетких множествах. Теория и практические решения / А. Г. Корченко. – К. : "МК-Прес", 2006. – 320 с.

6. Корченко А. Г. Экспертиза в системе ТЗИ на основе нечетких множеств / А. Г. Корченко, В. Г. Потапов, В. А. Рындюк // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – К., 2003. – Вип. 7. – С. 118-127.

7. Конахович Г. Ф. Оцінка ефективності систем захисту інформації в телекомунікаційних системах / Г. Ф. Конахович, О. Г. Голубничий, О. Ю. Пузиренко // Проблеми інформатизації та управління– № 3.21. –2007. – С. 75-83.

8. Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу НД ТЗІ 2.5-004-99. Затверджено наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації

Служби безпеки України від “28” квітня 1999 р. № 22 із змінами згідно наказу Адміністрації Держспецзв'язку від 28.12.2012 № 806

9. ISO/IEC 17799:2005 Information technology -- Security techniques -- Code of practice for information security management [Электронный ресурс]. - Режим доступа: https://www.iso.org/standard/39612.html

10. ISO/IEC 15408-1:2009 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model [Электронный ресурс]. - Режим доступа: https://www.iso.org/standard/50341.html

11. Міжнародні стандарти забезпечення інформаційної безпеки підприємста (СР№1) [Электронный ресурс]. – Режим доступа: https://nikitenko11.wordpress.com/2012/11/23/міжнародні-стандарти-забезпечення-і/

12. Маслова Н. А. Методы оценки эффективности систем защиты информационных систем / Н. А. Маслова // Искусственный интеллект. – 2008. – № 4. –С. 253–264.

13. Павлов І.М. Неформальний підхід в методиці оцінки ефективності ескізного проектування комплексних систем захисту інформації / І. М. Павлов // Захист інформації –Том 12, –№ 1 (46) (2010)

14. Пігур, Н. В., В. Д. Погребенник. "Оцінювання ефективності комплексних систем захисту інформації." (2013). [Электронный ресурс]. - Режим доступа: http://ena.lp.edu.ua:8080/bitstream/ntb/23063/1/45-61-61.pdf

15. Гарасимчук О. І. Оцінка ефективності систем / О. І. Гарасимчук, Ю. М. Костів //Вісник КНУ ім. М. Остроградського.– Кременчук: КНУ ім. М. Остроградського –№1/2011 (66). Частина 1

16. Власов О. М. Комплексний підхід оцінки ефективності систем захисту інформації в інфокомунікаційних мережах нового покоління / О. М. Власов, С. В. Толюпа // Наукові записки Наукові записки УНДІЗ. Науково-вироб. зб 3 (2011): 19.

17. Янчук, В. О. "Методика оцінювання стану захисту інформації локальних об’єктів системи електронного врядування." [Электронный ресурс]. - Режим доступа: http://academy.gov.ua/ej/ej11/txts/10ivoseu.pdf

18. International Carnahan Conference on Security Technology, October 10-12, 1990.

19. Теорія економічного аналізу: Навч. посіб. / Купалова Г.І. - К., 2008. 639 с.

20. Домарев В.В. "Безопасность информационных технологий. Методология создания систем защиты" – К.: ООО "ТИД "ДС", 2002 – 688 с.

21. А. В. Артемов Информационная безопасность. Курс лекций [Электронный ресурс]. - Режим доступа: http://fictionbook.ru/static/trials/09/06/63/09066361.a4.pdf

22. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа. – М: Наука и техника, 2003. – 384 с

23. Чипига А.Ф. Оценка эффективности защищённости автоматизированных систем от несанкционированного доступа / А.Ф. Чипига, В.С. Пелешенко // Вестник СевКавГТУ / Серия "Физико- химическая" –2004, № 1(8)

24. Алексеев А. "Управление рисками. Метод CRAMM." IT Expert.– Электрон. дан.–М.: ЗАО “ИТ Эксперт (2010). [Электронный ресурс]. - Режим доступа: http://www.itexpert.ru/rus/ITEMS/ITEMS_CRAMM.pdf

25. Грибунин В. Г. Комплексная система защиты информации на предприятии : учеб. пособие для студ. высш. учеб. заведений / В. Г. Грибунин, В.В.Чудовский. — М. : Издательский центр "Академия", 2009. — 416 с.

26. Пігур Н. В. Показники та критерії оцінювання якості комплексної системи захисту інформації / Н. В. Пігур, В. Д. Погребеник // Вісник Національного університету "Львівська політехніка". – 2013. – № 774 : Автоматика, вимірювання та керування. – С. 88–93

27. Юдін О.К., Стрельбіцький М.А. Підходи до оцінювання ефективності захисту інформації в інформаційно-телекомунікаційних

системах на стадії модернізації Наукоемкие технологии в инфокоммуникациях: обработка информации, кибербезопасность, информационная борьба : Монография / под общей редакцией В. М. Безрука, В. В. Баранника. – Х. : Издательство "Лидер", 2017. – 600 с.

28. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України // Відомості Верховної Ради України (ВВР), –1994, – № 31, ст.286

29. Гончарова Л.Л., Возненко А.Д., Стасюк О.І., Коваль Ю.О. Основи захисту інформації в телекомунікаційних та комп'ютерних мережах. – К., 2013. – 435 с., іл.160.

30. Основы информационной безопасности. Учебное пособие для вузов / Е. Б. Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов. -М.: Горячая линия - Телеком, 2006. - 544 с.: ил.

31. Кавун С.В. Інформаційна безпека. Навчальний посібник. Ч.1 / С.В. Кавун, В.В. Носов, О.В. Мажай. – Харків: Вид. ХНЕУ, 2008. – 352 с.

32. Петухов Г.Б., Якунин В.И. Методологические основы внешнего проектирования целенаправленных процессов и целеустремлённых систем. М.: АСТ, 2006. – 504 с.

33. Стрельбіцький М. А. Обґрунтування показника ефективності функціонування системи захисту інформації на стадії модернізації / М. А. Стрельбіцький // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – 2017. – Вип. 56. – С. 166-177.

34. Хмелев, Л. "Оценка эффективности мер безопасности, закладываемых при проектировании электронно-информационных систем." Безопасность информационных технологий": Труды научно-технической конференции, Пенза, июнь 2001. 2001.

35. Толюпа С. В. Комплексні системи захисту інформації спеціальних об'єктів та методика їх оцінки / С. В. Толюпа, Ю. Я. Самохвалов, Н. В. Цьопа. // Сучасний захист інформації 1 (2014).

36. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі : НД ТЗІ 3.7-003-05

37. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу : НД ТЗІ 1.1-002. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999 № 22.

38. Типове положення про службу захисту інформації в автоматизованій системі : НД ТЗІ 1.4-001. Затверджено наказом ДСТСЗІ СБ України від 04.12.2000 № 53.

39. Створення комплексів технічного захисту інформації на об’єктах інформаційної діяльності. Правила розроблення, побудови, викладення та оформлення моделі загроз для інформації : НД ТЗІ 1.6-003.

40. Будько М. Методика оцінки загроз для інформації автоматизованих систем / М. Будько // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, 10 вип., 2005 р.

41. Порядок з організації та забезпечення режиму секретності в державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях : Постанова КМУ № 1561-12 від 2.10.03

42. Стрельбіцький М. А. Визначення залишкового ризику загроз інформації на стадії модернізації інформаційно-телекомунікаційних систем / М. А. Стрельбіцький // Збірник наукових праць Національної академії Державної прикордонної служби імені Б. Хмельницького. Серія військові та технічні науки –№3(69) 2016

43. Усенко О.А. Модели и методы оценки надежности программного обеспечения информационных систем: Учебное пособие. – Таганрог: Изд-во ТТИ ЮФУ, 2008. – 40 с.

44. П.Ф. Овчинников, Б.М. Лисицын, В.М. Михайленко Высшая математика: Учеб. Пособие. – К.: Выща шк., 1989. – 679 с.

45. Стрельбіцький М. А. Формування множини допустимих значень показника якості системи захисту інформації інформаційно-телекомунікаційних систем на стадії модернізації / М. А. Стрельбіцький

// Збірник наукових праць Національної академії Національної гвардії України. - 2017. - Вип. 1. - С. 27-32.16.

46. Горбачев И. Е. Моделирование процессов нарушения информационной безопасности критической инфраструктуры / И. Е. Горбачев, А. П. Глухов // Труды СПИИРАН. 2015. Вып. 38. С. 112-135.

47. В.Феллер. Глава XI. Целочисленные величины. Производящие функции // Введение в теорию вероятностей и её приложения = An introduction to probability theory and its applicatons, Volume I second edition / Перевод с англ. Р. Л. Добрушина, А. А. Юшкевича, С. А. Молчанова Под ред. Е. Б. Дынкина с предисловием А. Н. Колмогорова. 2-е изд. - М.: Мир, 1964. - С. 270-272.

48. Смирнов Н. В., Дунин-Барковский И. В. (1965). Курс теории вероятности и математической статистики. Москва: Наука.

49. Вероятностные методы в прикладной кибернетике / Под ред. Р.М. Юсупова. – МО СССР, 1976. – 426 с.

50. IEC 61508-1 Edition 2.0 2010-04 International Standard // Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements) [Електронний ресурс]. - Режим доступу: https://webstore.iec.ch/p-preview/info_iec61508-1%7Bed1.0%7Den_d.pdf

51. Стрельбіцький М. А. Оцінка ефективності методів отримання та обробки діагностичної інформації / М. А. Стрельбіцький, В. В. Кузавков // Збірник наукових праць № 2 (62) Частина ІІ. – Хмельницький: НАДПСУ, 2014. С. 277-289

РОЗДІЛ 6
ЗАСТОСУВАННЯ ІНФОРМАЦІЙНОЇ ТЕХНОЛОГІЇ ЗАБЕЗПЕЧЕННЯ ФУНКЦІОНАЛЬНОЇ БЕЗПЕКИ В ІНТЕГРОВАНІЙ ІНФОРМАЦІЙНІЙ СИСТЕМІ НА СТАДІЇ МОДЕРНІЗАЦІЇ

6.1 Створення інформаційної технології забезпечення функціональної безпеки інтегрованої інформаційної системи на стадії модернізації

Технології обробки даних залежать від цільового призначення інформаційних систем, наявних апаратних і програмних засобів та режимів роботи. Введення до складу ІС нових апаратних засобів, спеціального програмного забезпечення може бути здійснено тільки за умови узгодження їх спільного функціонування на загальному полі даних із наявним програмно-апаратним забезпеченням.

При сполученні наявної ІС із більш досконалими ЗОТ і спеціальним програмним забезпеченням розпоряднику інформаційної системи необхідно чітко визначитися з величиною допустимих витрат, необхідною захищеністю даних, аспектами сумісності. Важливим аргументом на користь тієї чи іншої версії може бути: розроблене спеціальне програмне забезпечення, що є розвитком уже відпрацьованих функціональних завдань; наявна функціональна безпека для цієї платформи.

Першочерговим етапом технології забезпечення функціональної безпеки інформаційних систем на стадії модернізації є визначення розпорядником ІС базових засад, а саме:

стратегії функціональної безпеки;

завдання на модернізацію конкретних ІС;

критеріїв ефективності щодо кожної складової узгодження;

умов функціонування модернізованих ІС.

Загальну структуру технології забезпечення функціональної безпеки інформаційних систем на стадії модернізації наведено на рисунку 6.1.

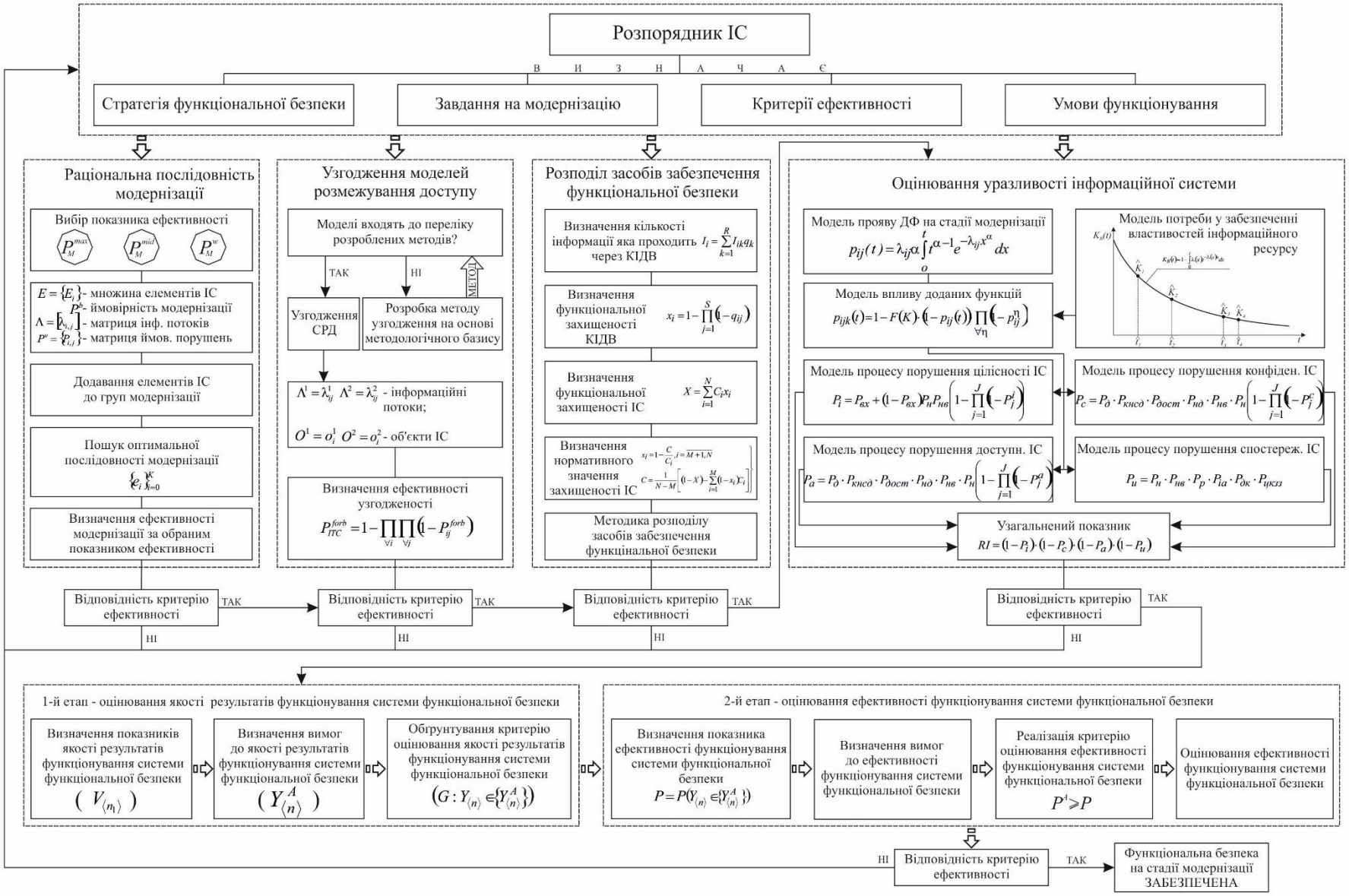


Рисунок 6.1 – Інформаційна технологія забезпечення функціональної безпеки ІС на стадії модернізації

На другому етапі технології залежно від визначених на попередньому етапі засад здійснюються заходи узгодження різних версій спеціального програмного забезпечення та апаратних засобів забезпечення функціональної безпеки. Особливістю цього етапу є можливість паралельного їх проведення. З урахуванням стратегії функціональної безпеки, завдання на модернізацію та умов функціонування обирається показник ефективності процесу модернізації. Відповідно до розробленого методу визначається раціональна послідовність модернізації та оцінюється її ефективність за обраним показником. Відповідність показника обраному критерію ефективності свідчить про успішне виконання частини другого етапу. В іншому випадку пропонується розпоряднику ІС змінити базові засади з причини неможливості їх дотримання.

Разом із тим здійснюється узгодження моделей розмежування доступу модернізованих ІС. У випадку відсутності розроблених методів узгодження моделей розмежування доступу на основі сформованого методологічного базису провадиться розробка необхідного методу. Після узгодження СРД оцінюється ефективність цього процесу. При невідповідності показника ефективності пропонується розпоряднику змінити умови функціонування ІС, завдання на модернізацію або сам критерій ефективності.

Третьою складовою етапу є розподіл засобів забезпечення функціональної безпеки ІС. Провадиться за потреби їх розподіл та оцінюється загальна функціональна безпека системи. У випадку відповідності всіх розглянутих показників ефективності критеріям здійснюється перехід до третього етапу технології – оцінювання уразливості даних.

На третьому етапі, ґрунтуючись на визначених базових засадах, визначають вплив дестабілізаційних факторів, які викликані стадією модернізації, на властивості інформаційної системи: цілісності, доступності, конфіденційності та спостереженості. Моделювання зазначених процесів дозволяє провести оцінювання уразливості ІС, викликаних стадією

модернізації. При відповідності узагальненого показника визначеному розпорядником ІС критерію здійснюється перехід до четвертого етапу технології – оцінювання ефективності системи функціональної безпеки.

На четверному етапі здійснюються оцінювання ефективності функціонування системи функціональної безпеки. Результатом цього етапу є значення ймовірності виконання системою функціональних завдань. За умови дотримання значення цієї ймовірності у визначених розпорядником ІС межах функціональну безпеку на стадії модернізації забезпечено. В іншому випадку пропонується змінити умови функціонування системи або критерії оцінювання.

6.2 Застосування методу визначення раціональної послідовності модернізації елементів інформаційної системи

Досвід застосування програмно-технічних комплексів ІС прикордонного відомства показав, що процес їх модернізації здійснюється достатньо інтенсивно (декілька модернізацій на місяць). Така частота спричинена динамікою функціональних завдань ДПСУ. Разом із тим сам процес модернізації в більшості випадків стосується тільки окремих елементів ІС або їх ПТК. Зазначимо, що співвідношення кількості апаратних модернізацій систем до кількості програмних є досить малим. У більшості випадків Адміністрація ДПСУ ставить завдання щодо вдосконалення саме програмної складової ІС. Як правило, модернізація здійснюється з метою усунення недоліків у функціоналі програмного забезпечення або впровадження нових функцій з відповідними доданими елементами користувацького інтерфейсу.

Для опису застосування методу визначення раціональної послідовності модернізації елементів ІС оберемо експериментальний зразок програмно-технічного комплексу автоматизації прикордонної служби "Гарт-3/П" та розглянемо раціональну послідовність модернізації.

Топологічно даний комплекс являє собою "зірку", але обмін інформації (інформаційні потоки) здійснюється між усіма елементами ПТК через серверну частину. Структура зазначеного комплексу формується відповідно до потреб конкретного відділу прикордонної служби. Для прикладу розглянемо ПТК, який складається з одного екземпляра кожного АРМ та серверної частини (рисунок 6.2). Для зручності кожний елемент проіндексовано.

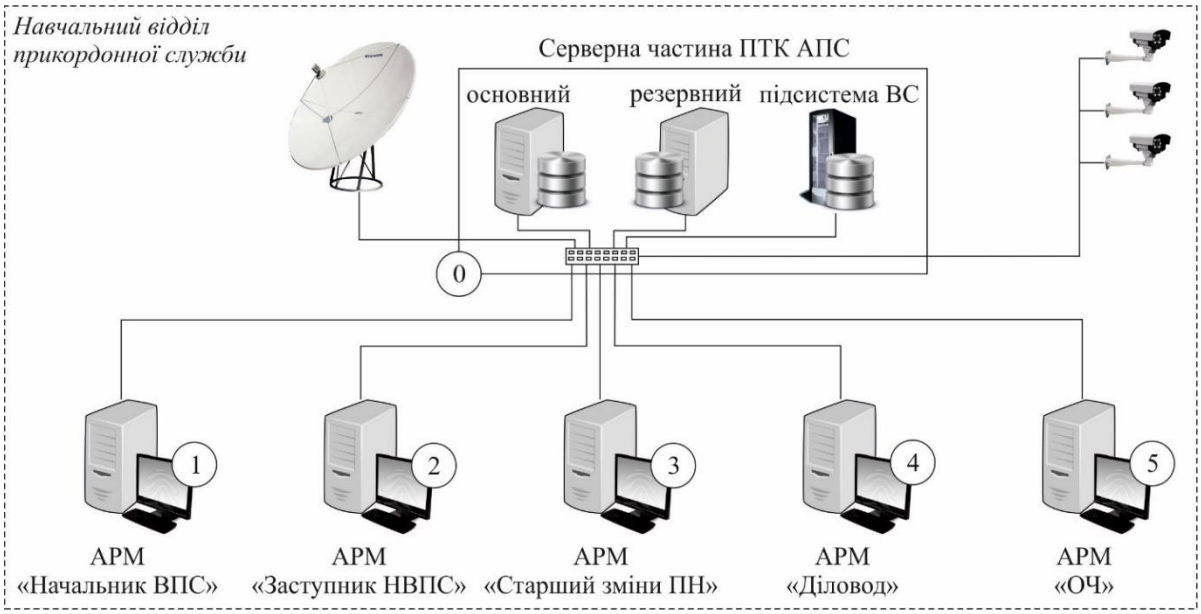


Рисунок 6.2 – Структура експериментального ПТК АПС "Гарт-3/П"

Дослідження, проведені на експериментальному зразку, дозволили визначити інформаційний потік між елементами ПТК АПС, які зведені в таблицю 6.1.

Таблиця 6.1 – Матриця інформаційних потоків між елементами ПТК АПС ($\Lambda = \lfloor \lambda_{i,j} \rfloor$ – Кб/с)

Індекс	**0**	**1**	**2**	**3**	**4**	**5**
0	0	1	1	0,3	0,2	0,1
1	1	0	1	0,3	0,2	0,1
2	0,5	0,2	0	0,3	0,2	0,1
3	0,3	0,2	0,1	0	0,05	0,05
4	0,2	0,2	0,2	0,05	0	0,02
5	0,1	0,5	0,5	0,05	0,02	0

Визначення елементів матриці ймовірностей порушення властивостей елементів ІС при здійсненні обміну між ними у разі невідповідності версій спеціального програмного забезпечення повинні здійснювати експерти із розробників СПЗ. Для прикладу приймемо, що ймовірність порушення властивостей елементу ІС при надсиланні даних на серверну частину становить одиницю, а при отриманні даних – 0,8. Причому значення ймовірності при взаємодії з іншими елементами становитиме – 0.5. Зведені дані наведено в таблиці 6.2.

Таблиця 6.2 – Матриця ймовірностей порушення властивостей елементів ІС при здійсненні обміну між ними у разі невідповідності версій спеціального програмного забезпечення

Індекс	**0**	**1**	**2**	**3**	**4**	**5**
0	0	0,8	0,8	0,8	0,8	0,8
1	1	0	0,5	0,5	0,5	0,5
2	1	0,5	0	0,5	0,5	0,5
3	1	0,5	0,5	0	0,5	0,5
4	1	0,5	0,5	0,5	0	0,5
5	1	0,5	0,5	0,5	0,5	0

Ураховуючи дані таблиць 6.1 та 6.2, сформуємо матрицю величин ймовірностей порушення властивостей елементів ІС при заданому інформаційному потоці (таблиця 6.3).

Таблиця 6.3 – Матриця величин ймовірностей порушення властивостей елементів ІС при заданому інформаційному потоці

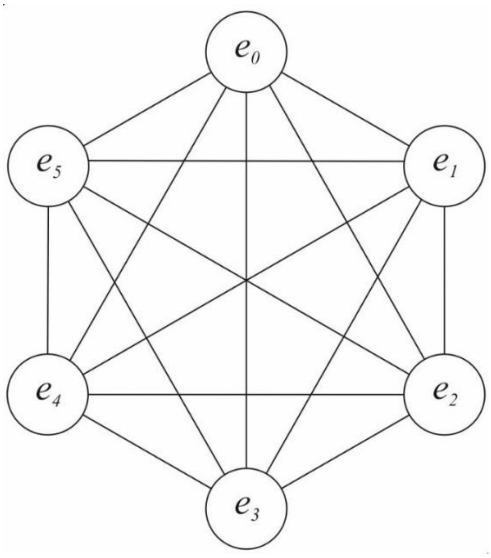
Індекс	**0**	**1**	**2**	**3**	**4**	**5**
0	0	0,8	0,8	0,382966	0,27522	0,14866
1	1	0	0,5	0,187748	0,129449	0,066967
2	1	0,129449	0	0,187748	0,129449	0,066967
3	1	0,129449	0,066967	0	0,034064	0,034064
4	1	0,129449	0,129449	0,034064	0	0,013767
5	1	0,292893	0,292893	0,034064	0,013767	0

На підставі таблиці 6.3 сформуємо матрицю суміжностей навантаженого графу факту порушень властивостей елементів ІС (таблиця 6.4)

Таблиця 6.4 – Матриця суміжностей навантаженого графу факту порушень властивостей елементів ІС

Індекс	**0**	**1**	**2**	**3**	**4**	**5**
0	0	1	1	1	1	1
1	1	0	1	1	1	1
2	1	1	0	1	1	1
3	1	1	1	0	0	1
4	1	1	1	1	0	1
5	1	1	1	1	1	0

Базуючись на матриці суміжностей, сформуємо навантажений граф ймовірностей порушень властивостей елементів ІС (рисунок 6.3).



де: e_0 – серверна частина ПТК АПС; e_1 – АРМ начальника ВПС; e_2 – АРМ заступника начальника ВПС; e_3 – АРМ старшого зміни прикордонних нарядів; e_4 – АРМ діловода; e_5 – АРМ оперативного чергового;

Рисунок 6.3 – Граф ймовірностей порушень властивостей елементів ІС

Для визначення часу початку модернізації кожного елементу припустимо однакову швидкість заміни СПЗ персоналом відділу

прикордонної служби, яка становитиме 6 од/год. Дане значення визначено в ході проведення експерименту на дослідному зразку програмно-технічного комплексу. Параметр модернізації залежить у кожному конкретному випадку від виду та складності модернізації СПЗ, типу засобів обчислювальної техніки, кваліфікації персоналу, який проводить обслуговування, та може визначатись як експериментально, так і розробником СПЗ. За величину ймовірності завершення модернізації приймемо значення 0,95 як достовірної події. У результаті обчислень за формулою (2.13) час модернізації чергового елементу становитиме 0,5 год.

З метою підтвердження адекватності методики визначення раціональної послідовності модернізації достатньо провести розрахунок для всіх можливих варіантів. Зазначимо, що для 5 елементів у дослідному зразку кількість варіантів модернізації становить 5!=720. Результати для всіх варіантів послідовності модернізації (додаток Д) розраховані за допомогою програми (додаток Е).

Результатом методу є раціональна послідовність модернізації ПТК АПС "Гарт-1/П" $\{e_4, e_0, e_3, e_5, e_2, e_1\}$, при якій максимальна ймовірність порушення властивостей ІС становить 0,052. На рисунку 6.4 зображено динаміку зміни поточного значення ймовірності протягом терміну модернізації при різних послідовностях модернізації.

Аналіз динаміки зміни ймовірності порушення властивостей ІС на стадії модернізації при різних послідовностях показав, що, незважаючи на загальне достатньо низьке значення ймовірності, пікові значення можуть бути достатньо високими (послідовність $\{e_3, e_4, e_2, e_0, e_1, e_5\}$). Крім того, при середньому значенні ймовірності, меншому за визначене, максимальне значення є більшим за оптимальну послідовність $\{e_5, e_4, e_0, e_3, e_2, e_1\}$.

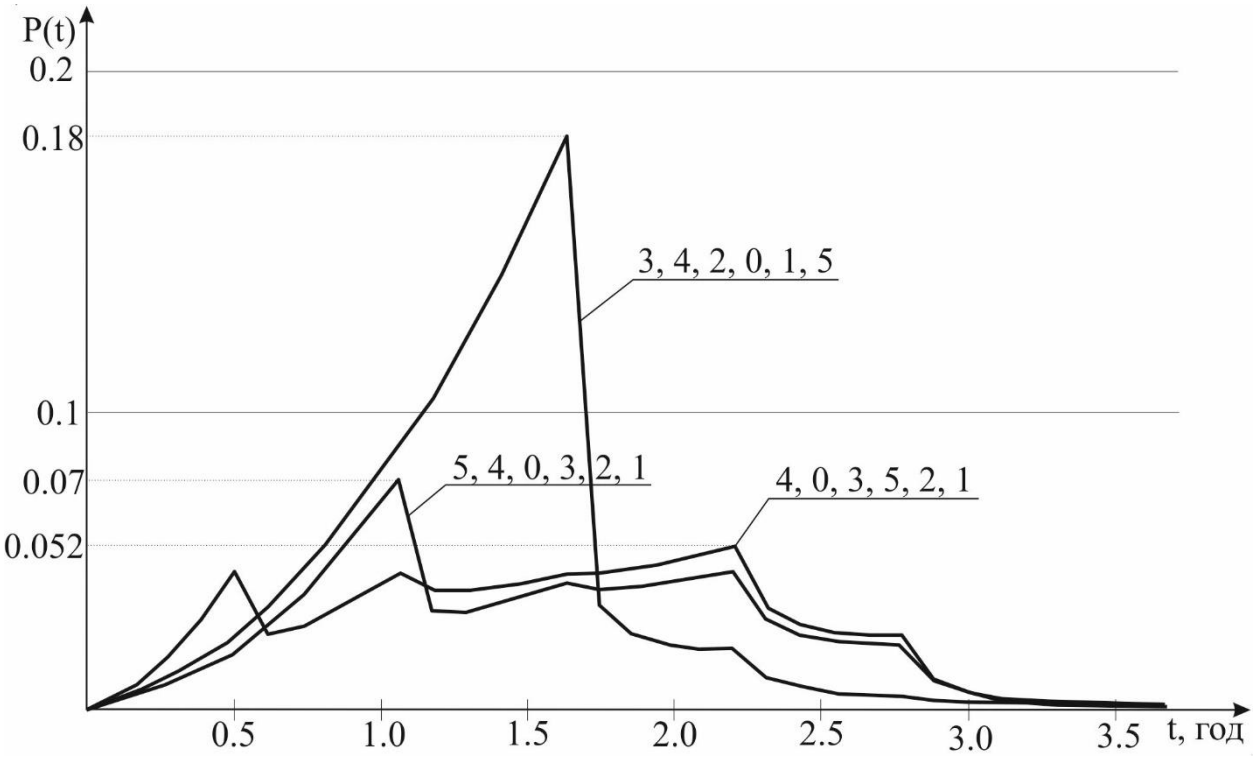


Рисунок 6.4 – Динаміка зміни поточного значення ймовірності при різних послідовностях модернізації

Отже відповідно до обраних стратегії модернізації та режиму роботи ІС визначено раціональні послідовності модернізації елементів ІС.

6.3 Застосування методу розподілу засобів забезпечення функціональної безпеки інформаційних систем на стадії модернізації

Практична реалізація завдання узгодження технічних (апаратних, програмно-технічних) засобів забезпечення функціональної безпеки на стадії модернізації ІС вимагає адаптації теоретичних положень до реалізації конкретних систем. З цією метою розглянемо розподіл засобів забезпечення функціональної безпеки при модернізації експериментального зразка ПТК АПС «Гарт-3/П».

Першочерговим завданням є формування групи експертів, які на підставі технічної документації про порядок функціонування ПТК, схеми розгортання (рисунок 6.5) та власного досвіду виявляють множину каналів інформаційних дестабілізаційних впливів.

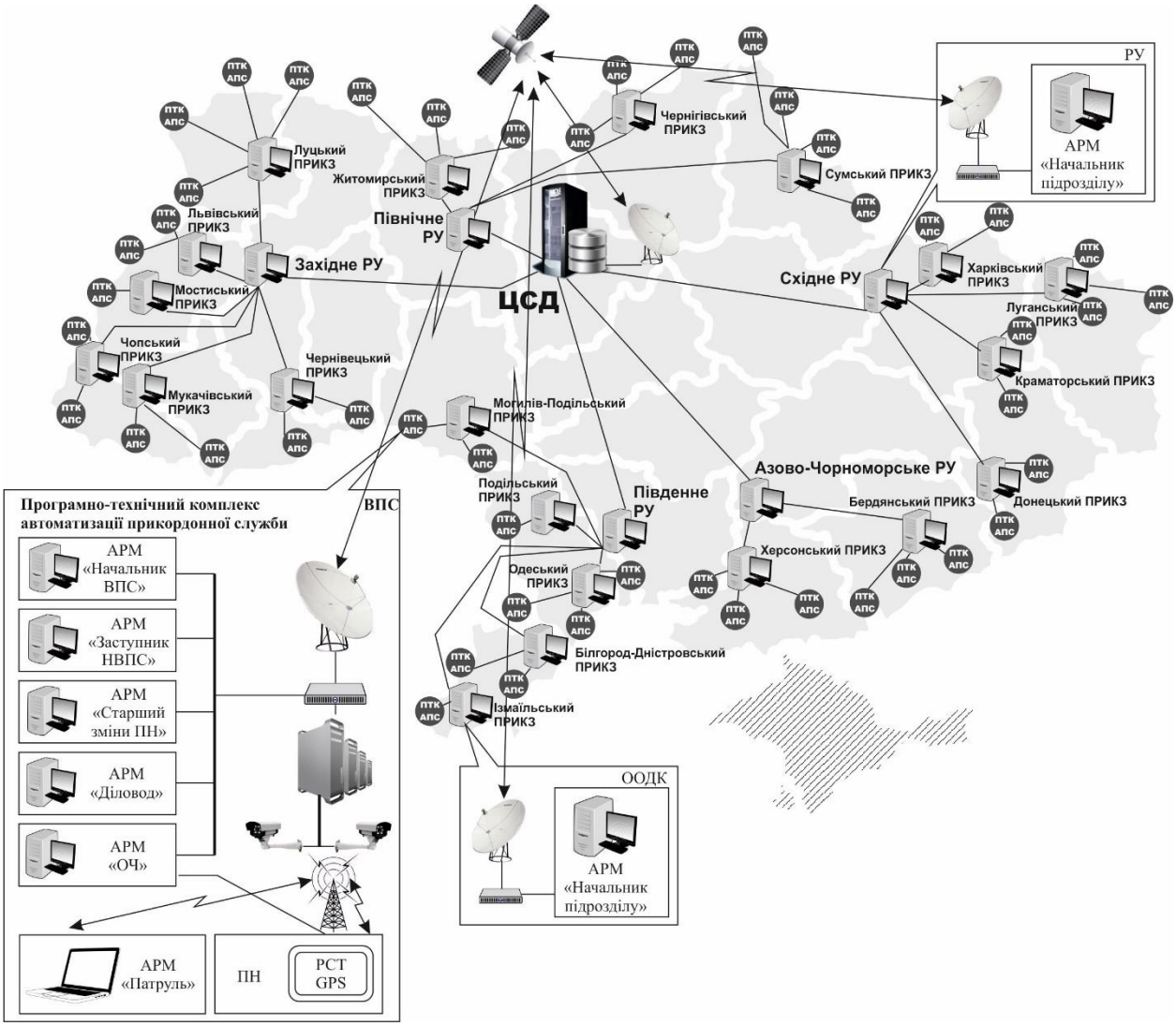


Рисунок 6.5 – Узагальнена схема розгортання ІС «Гарт-3»

У Державній прикордонні службі України, як правило, каналом зв’язку для підпорядкованих підрозділів забезпечує підрозділ вищого рівня. Таким чином, інформаційні потоки з нижніх рівнів об’єднуються на вищих рівнях.

Визначимо типові можливі канали інформаційних дестабілізаційних впливів. У кожному конкретному випадку КІДВ визначаються експертами для кожного об’єкта інформаційної діяльності. Разом із тим таке узагальнення не змінює принциповий підхід до оцінювання величини надійності інформації в ІС загалом. Відповідно до узагальненої схеми розгортання ІТС «Гарт-3» визначимо декілька груп КІДВ, які стосуються різних об’єктів ІС:

1– ПТК АПС;

2 – АРМ ООДК;

3 – АРМ РУ;

4 – ЦСД;

5 – каналу передачі даних від ПТК АПС до ООДК;

6 – каналу передачі даних від ООДК до РУ;

7 – каналу передачі даних від РУ до ЦСД.

Для розрахунків приймемо декілька припущень, а саме: кількість інформації, яка передається до ЦСД від ПТК АПС, однакова; кількість інформації, яку отримують автоматизовані робочі місця від ЦСД, на кожному рівні автоматизації однакова; кількість ПТК АПС в ООДК однакова; у кожному ООДК та РУ кількість АРМ становить одиницю.

Приймемо, що:

I_{ik} – величина інформаційного потоку i–го елементу k–го рівня автоматизації;

C_i^l – вага i–го КІДВ l–ї групи;

N_j – кількість ПТК АПС в ООДК.

Ураховуючи вищенаведене припущення $N_1 = N_2 = N_j = N$, приймемо, що кількість ПТК АПС відділу прикордонної служби в ООДК становить 3 одиниці.

Визначимо, що інформація, яка циркулює в ІТС «Гарт-3» є службовою. Крім того, джерелами інформації є ПТК АПС, а споживачами – АРМ різних рівнів автоматизації. Це дозволить визначити сумарну величину інформаційного потоку, який циркулює в ІС. З урахуванням сталого характеру планування прикордонної служби у ВПС (щоденне, щотижневе, щомісячне тощо) величина інформаційного потоку теж є сталою; приймемо її як одиницю за одиницю часу. Зазначимо, що реальне визначення цієї величини є достатньо простою процедурою.

Отже величина інформаційного потоку «Гарт-3» з урахуванням організаційної структури ДПСУ (додаток Ж), у Східному РУ 5 ООДК, які мають ВПС, Північному РУ – 3, Західному РУ – 5, Південному РУ – 5, Азово-Чорноморському РУ – 2, становить $I = 3 \cdot (5 + 3 + 5 + 5 + 2) = 60$.

Об'єднаємо ваги всіх КІДВ в таблицю з урахуванням вимог 3.1 та 3.2, зважаючи, що кількість КІДВ у «Гарт-3» становить 111 одиниць (таблиця 6.5).

Таблиця 6.5 – Ваги КІДВ за групами

Назва	**К-сть**	**Номер групи КІДВ**						
		1	2	3	4	5	6	7
ЦСД	1				0,2647			
ПТК АПС	60	0,0015				0,0015		
АРМ ООДК	20		0,0015					
Східне регіональне управління	1							0,0662
АРМ РУ	1			0,0221				
Донецький прикордонний загін	1						0,0088	
Краматорський прикордонний загін	1						0,0088	
Луганський прикордонний загін	1						0,0088	
Харківський прикордонний загін	1						0,0088	
Сумський прикордонний загін	1						0,0088	
Північне регіональне управління	1							0,0397
АРМ РУ	1			0,0132				
Чернігівський прикордонний загін	1						0,0088	
Житомирський прикордонний загін	1						0,0088	
Луцький прикордонний загін	1						0,0088	
Західне регіональне управління	1							0,0662
АРМ РУ	1			0,0221				
Львівський прикордонний загін	1						0,0088	
Мостиський прикордонний загін	1						0,0088	

Продовження таблиці 6.5

Назва	**К-сть**	**Номер групи КІДВ**						
		1	2	3	4	5	6	7
Мукачівський прикордонний загін	1						0,0088	
Чопський прикордонний загін	1						0,0088	
Чернівецький прикордонний загін	1						0,0088	
Південне регіональне управління	1							0,0662
АРМ РУ	1			0,0221				
Одеський прикордонний загін	1						0,0088	
Котовський прикордонний загін	1						0,0088	
Білгород-Дністровський прикордонний загін	1						0,0088	
Ізмаїльський прикордонний загін	1						0,0088	
Могилів-Подільський прикордонний загін	1						0,0088	
Азово-Чорноморське РУ	1							0,0265
АРМ РУ	1			0,0088				
Бердянський прикордонний загін	1						0,0088	
Херсонський прикордонний загін	1						0,0088	

Припустимо, що коефіцієнт захисту x сукупності ЗЗ, які забезпечують захист кожного із наведених КІДВ, становить 0.95 (у кожному конкретному випадку ці значення вираховуються окремо). Отже загальна захищеність ІС «Гарт-3» визначається через функціональну залежність 3.20 і становить

$$X = x\sum_{i=1}^{N} C_i = 0{,}95.$$

При здійсненні модернізації ІС «Гарт-3» Державною прикордонною службою прийнято рішення щодо розгортання додаткових двох ВПС на ділянці Білгород-Дністровського прикордонного загону (придністровський сегмент) із встановленням на них ПТК АПС «Гарт-3/П» та інтеграції в ІС «Гарт-3». Причому розробнику системи в технічному завдання на

модернізацію вказано, що рівень функціональної безпеки системи загалом не повинен зменшитись.

Вищенаведена модернізація вимагає перерахунку ваг КІДВ для дотримання умови (3.1).

Таблиця 6.5 набуде такого вигляду (таблиця 6.6).

Таблиця 6.6 – Ваги КІДВ за групами після модернізації

Назва	**К-сть**	**Номер групи КІДВ**						
		1	2	3	4	5	6	7
ЦСД	1				0,2650			
ПТК АПС	62	0,0014				0,0014		
АРМ ООДК	20		0,0014					
Східне регіональне управління	1							0,0641
АРМ РУ	1			0,0214				
Донецький прикордонний загін	1						0,0085	
Краматорський прикор-донний загін	1						0,0085	
Луганський прикордонний загін	1						0,0085	
Харківський прикордонний загін	1						0,0085	
Сумський прикордонний загін	1						0,0085	
Північне регіональне управління	1							0,0385
АРМ РУ	1			0,0128				
Чернігівський прикордонний загін	1						0,0085	
Житомирський прикордонний загін	1						0,0085	
Луцький прикордонний загін	1						0,0085	
Західне регіональне управління	1							0,0641
АРМ РУ	1			0,0214				
Львівський прикордонний загін	1						0,0085	
Мостиський прикордонний загін	1						0,0085	
Мукачівський прикордонний загін	1						0,0085	
Чопський прикордонний загін	1						0,0085	

Продовження таблиці 6.6

Назва	**К-сть**	**Номер групи КІДВ**						
		1	2	3	4	5	6	7
Чернівецький прикордонний загін	1						0,0085	
Південне регіональне управління	1							0,0726
АРМ РУ	1			0,0242				
Одеський прикордонний загін	1						0,0085	
Котовський прикордонний загін	1						0,0085	
Білгород-Дністровський прикордонний загін	1						0,0142	
Ізмаїльський прикордонний загін	1						0,0085	
Могилів-Подільський прикордонний загін	1						0,0085	
Азово-Чорноморське РУ	1							0,0256
АРМ РУ	1			0,0085				
Бердянський прикордонний загін	1						0,0085	
Херсонський прикордонний загін	1						0,0085	

Для проведення розрахунків використаємо функціональну залежність (3.29). Загалом кількість КІДВ після модернізації становить 113, разом із тим, модернізованими є елементи доданих ПТК АПС на двох ВПС та канали зв'язку. Кількість модернізованих КІДВ становить 4 одиниці. З урахуванням цього значення $C = \frac{1}{2}\left[(1-0{,}95)-0{,}05\cdot(1-0{,}0014)\cdot 2\right] = 0{,}00007$, звідки захищеність доданих КІДВ повинна бути $x_i = 1-\frac{0{,}00007}{0{,}0014} = 0{,}95$.

Отримане значення узгоджується з попередніми розрахунками. Оскільки всі КІДВ мають однакову ступінь захищеності 0,95 (з урахуванням прийнятих припущень), то і додані повинні мати таке ж значення для забезпечення захищеності ІС «Гарт-3» загалом.

Нормативні значення захищеності КІДВ є базовими для вибору засобів забезпечення функціональної безпеки ІС. Відповідно до функціональної

залежності (3.35) необхідно забезпечити сукупний рівень захищеності для доданих КІДВ, у результаті модернізації не менший за значення захищеності самого КІДВ.

6.4 Методика експертного оцінювання ступеня впливу дестабілізаційних факторів на інформаційні системи на стадії модернізації

Необхідність проведення експертного оцінювання обумовлюється відсутністю числових значень ступеня впливу дестабілізаційних факторів та їхніх основних характеристик на елементи конкретної ІС.

Загалом структура методики експертного оцінювання ступеня впливу дестабілізаційних факторів на ІС на стадії модернізації являє собою поетапний процес, а саме:

1. Визначення переліку суттєвих дестабілізаційних факторів та формування таблиці опитування.

2. Формування шкали оцінювання ступеня впливу ДФ на елементи конкретної ІС.

3. Формування складу робочої групи експертів.

4. Оцінювання експертами наведених у таблицях ДФ відповідно до запропонованої шкали.

5. Обробка результатів опитування.

Розглянемо кожний із етапів.

Етап 1. Визначення переліку суттєвих дестабілізаційних факторів.

Аналіз нормативних документів з питань забезпечення безпеки інформації та інформаційних систем дозволив визначити суттєві ІДФ ІС на стадії модернізації експериментального зразка ПТК АПС. Перелік визначених загроз формується у вигляді таблиці 6.7.

Таблиця 6.7 – Вигляд таблиці переліку ІДФ з урахуванням впливу процесу модернізації

№ з/п	Вид ІДФ	Властивість ІС				Вплив процесу модернізації			
		к	ц	д	с	к	ц	д	с
1									

Етап 2. Формування шкали оцінювання ступеня впливу ДФ на елементи конкретної ІС.

Зважаючи на те, що вплив дестабілізаційних факторів на складові властивостей ІС є достатньо малим, при формуванні характеристик загроз методом експертних оцінок пропонується ймовірність оцінювати за наступною градацією, яка розподілена за експоненційним законом (таблиця 6.8):

Таблиця 6.8 – Шкала оцінювання ступеня впливу дестабілізаційних факторів на елементи конкретної ІС

№	Ступінь впливу	Значення ймовірності	Кількість балів
1	Постійний	1	10
2	Занадто високий	0,95	9
3	Дуже високий	0,6	8
4	Високий	0,4	7
5	Більше середнього	0,25	6
6	Середній	0,18	5
7	Менше середнього	0,1	4
8	Низький	0,05	3
9	Дуже низький	0,01	2
10	Занадто низький	0,005	1
11	Неможливий	0	0

При визначенні експертами факту зміни ймовірності виникнення ІДФ при модернізації ІІС або її складових значення заноситься в другу частину таблиці 6.8 у вигляді двох варіантів: 1 – вплив наявний, 0 – вплив відсутній.

Етап 3. Формування складу робочої групи експертів.

Проблема вибору експертів завжди залишається актуальною та складною в теорії експертного оцінювання. Аналіз робіт у цій галузі [1–15]

дозволив сформувати підхід до визначення ступеня впливу ДФ на елементи певної ІС.

У роботах [1, 6–9, 11–13] визначено, що вибір складу експертної групи є поетапним процесом з такою послідовністю:

1. Вибір кількості експертів у складі робочої групи з визначення ступеня впливу дестабілізаційних факторів та їх основних характеристик на елементи конкретної ІС.

2. Формування попереднього переліку експертів та визначення ступеня їх компетентності.

4. Формування складу робочої групи.

Аналіз наявних джерел показав різний підхід до визначення кількості експертів у складі групи. Відповідно [10] кількість експертів повинна бути не менша від кількості факторів, які підлягають ранжуванню. У роботах [9, 13] автори пропонують визначати за такою формулою:

$$m \geq 0{,}5\left(0{,}33/b + 5\right), \tag{6.1}$$

де b – помилка результату експертного аналізу ($0 < b < 1$).

Окремі автори [5] пропонують брати не менше 10 та не більше 30 осіб, а в [6] – не менше 7 та не більше 20 осіб, обґрунтовуючи своє рішення тим, що менша кількість експертів призводить до недостовірності оцінювання, а занадто більша – до складності опитування.

У [13] автори пропонують визначати кількість експертів за формулою:

$$m \leq \frac{3}{2Q_{max}} \sum_{i=1}^{m^*} Q_i \,, \tag{6.2}$$

де m^* – кількість експертів;

Q_i – компетентність i-го експерта;

Q_{max} – максимально можлива компетентність i-го експерта;

У [15] автори для визначення кількості експертів пропонують використати ймовірнісний підхід та елементи математичної статистики. З курсу статистики [16] відомо, ще середня помилка вибірки (μ) – це середнє квадратичне відхилення всіх можливих значень вибіркового середнього від свого математичного очікування. Таким чином, μ^2 – дисперсія можливих значень вибіркового середнього. У курсі математичної статистики показно, що зазначена величина в n разів менша дисперсії σ^2 генеральної сукупності, де n – обсяг вибірки. Варто мати на увазі, що вищенаведене має місце при нормальному розподілі генеральної сукупності. Отже, за великої кількості елементів генеральної сукупності вірний такий вираз:

$$\mu = \sqrt{\frac{\sigma^2}{n}}. \tag{6.3}$$

При малому обсягу вибірки, якщо $n < 30$, вираз (6.3) визначається як

$$\mu = \sqrt{\frac{\sigma^2}{n-1}}. \tag{6.4}$$

Після перетворень (6.1) та (6.2) і заміни вибірки на кількість експертів отримуємо

$$m = \frac{\sigma^2}{\mu^2}, m \geq 30, \tag{6.5}$$

$$m = \frac{\sigma^2}{\mu^2} + 1, m < 30. \tag{6.6}$$

Рекомендовану кількість експертів у складі робочої групи для окремих співвідношень дисперсій зведемо в таблицю 6.9

Таблиця 6.9 – Кількісний склад робочої групи експертів

μ^2/σ^2	0,05	0,06	0,07	0,08	0,09	0,1	0,2
n	21	18	16	14	12	11	6

Ураховуючи достатньо прості формулювання набору альтернатив визначимо, що мінімальний рівень похибки 0,05. Відповідно до таблиці 6.9 кількісний склад робочої групи становитиме 21 особа.

Визначимо коефіцієнт компетентності складу робочої групи за формулою [9]

$$M = \frac{1}{m}\sum_{i=1}^{m} K_i \,, \tag{6.7}$$

де K_i – рівень компетентності i-го експерта робочої групи, який визначається відповідно таблиці 6.10.

Таблиця 6.10 – Визначення рівня компетентності та інформованості експертів

№ з/п	Кваліфікація	Значення коефіцієнта компетентності	Кількість
1	Доктор технічних наук	1	2
2	Здобувач наукового ступеня доктора технічних наук	0,95	2
3	Кандидат технічних наук	0,9	7
4	Здобувач наукового ступеня кандидата технічних наук	0,85	2
5	Фахівець у галузі зв’язку, автоматизації та захисту інформації зі стажем роботи більше 20 років	0,8	3
6	Фахівець у галузі зв’язку, автоматизації та захисту інформації зі стажем роботи від 15 до 20 років	0,7	1
7	Фахівець у галузі зв’язку, автоматизації та захисту інформації зі стажем роботи від 10 до 15 років	0,6	1
8	Фахівець у галузі зв’язку, автоматизації та захисту інформації зі стажем роботи від 5 до 10 років	0,5	1
9	Фахівець у галузі зв’язку, автоматизації та захисту інформації зі стажем роботи до 5 років	0,4	2

З метою визначення ступеня впливу ДФ на елементи експериментальної ІС до складу експертної групи залучались фахівці кафедри зв'язку, автоматизації та захисту інформації та відділу зв'язку, автоматизації та захисту інформації Національної академії Державної прикордонної служби імені Б. Хмельницького у кількості 21 особа.

Сформована робоча група експертів вважається компетентною, якщо загальний рівень компетентності лежить у межах [11]

$$0.67 \le M \le 1. \tag{6.8}$$

Провівши відповідні розрахунки, отримаємо значення коефіцієнта компетентності складу робочої групи, яке становить 0,8, що відповідає умові (6.8).

Етап 4. Оцінювання експертами наведених в таблицях ДФ відповідно до запропонованої шкали.

Для виконання 4-го етапу розроблено анкету, яка наведена у вигляді таблиці (додаток Г) з указанням категорії експерта.

Етап 5. Обробка результатів опитування.

Найбільш поширеним серед діючих методів обробки експертної інформації є статистичні методи.

Результуюча оцінка i-ї загрози x_i^p за окремими властивостями $p = \{i, c, a, u\}$ інформації становитиме:

$$x_i^p = \frac{\sum_{j=1}^{m} x_{ij}^p k_j}{\sum_{j=1}^{m} k_j}, \tag{6.9}$$

де x_{ij}^p – оцінка i-ї властивості j-м експертом.

З метою визначення ступеня узгодженості результатів експертної оцінки кожної загрози необхідно визначити середнє квадратичне відхилення кожного фактора з урахуванням кваліфікації експерта:

$$\tilde{\sigma}_i^p = \sqrt{\frac{\sum_{i=1}^{m}\left(x_{ij}^p - x_i^p\right)\cdot k_j}{\sum_{i=1}^{m} k_j}}. \qquad (6.10)$$

Визначене значення середньоквадратичного відхилення дозволить визначити коефіцієнт варіації, який характеризує ступінь узгодженості експертів з питань кожного типу загрози

$$V_i^p = \frac{\tilde{\sigma}_i^p}{x_i^p}. \qquad (6.11)$$

Показники середнього квадратичного відхилення та середнього значення експертних оцінок дозволяють прогнозувати величину довірчого інтервалу, в якому із заданою ймовірністю знаходиться значення величини. Зазначена область визначається як

$$\tilde{x}_i^p - \varepsilon \le x_i^p \le \tilde{x}_i^p + \varepsilon. \qquad (6.12)$$

Ураховуючи, що кількість експертів достатньо велика, а саме більше 20 осіб, можна зробити припущення про нормальний розподіл величини x_i^p. Величина ε визначається таким чином:

$$\varepsilon_i^p = t_\beta \frac{\sigma_i^p}{\sqrt{m}}, \qquad (6.13)$$

де $t_\beta = arg\left[\Phi\left(\frac{1+\beta}{2}\right)\right]$ – величина, яка обернена нормальній функції розподілу $\Phi(x)$, обчислюється для заданого значення імовірності β.

Для визначення значення t_β приймемо значення ймовірності потрапляння в довірчий інтервал як $\beta = 0{,}95$. Відповідно до табличних значень нормальної функції розподілу значення $t_\beta = 1{,}96$.

Відповідно до наведеної методики проводиться експертне оцінювання за кожною властивістю ІС та фактом впливу процесу модернізації на них. Результати експертного оцінювання наведено в додатку Г.

6.5 Визначення уразливості інформаційних систем на стадії модернізації

З метою перевірки ступеня уразливості експериментального зразка програмно-технічного комплексу автоматизації прикордонної служби, який розгорнуто на кафедрі зв'язку, автоматизації та захисту інформації Національної академії Державної прикордонної служби України імені Б. Хмельницького, визначимо складові комплексного показника (3.36).

Величину ймовірності порушення цілісності ПТК АПС визначимо за формулою (3.37). Структуру експериментального ПТК АПС "Гарт-1/П" наведено на рисунку 6.1. Припустимо, що у новій версії СПЗ ймовірність того, що цілісність елементу ІС буде порушено в результаті неузгодженості версій, дорівнює нулю з причини врахування функціонування попередньої версії. Крім того, за умовою експерименту першою модернізувалась серверна частина ПТК АПС. Приймемо, що ймовірність того, що цілісність даних буде порушено в результаті неузгодженості версій на всіх АРМ, становить 0,05. Таким чином, ймовірності $P_0^i = 0$, $P_j^i = 0{,}05, j = \overline{1{,}5}$ (індекси наведено відповідно до рисунку 6.1). Варто зазначити, що співвідношення потоку даних нової та попередньої версій на вхід АРМ ІС від серверної частини становить 1 (формула 3.38).

Проведемо розрахунки для кожного елементу ПТК АПС: $P_0^i = 0$, $P_j^i = 0.01, j = \overline{1{,}5}$. Для визначення загальної ймовірності порушення цілісності

ПТК АПС використаємо відомі співвідношення теорії ймовірностей

$$P^i = 1 - \prod_{j=0}^{5}\left(1 - P_j^i\right) = 1 - (1 - 0{,}01)^5 = 0{,}049.$$

Для визначення ймовірності порушення конфіденційності на експериментальному зразку ПТК АПС введемо певні припущення. Нехай ймовірність доступу порушника до елементу ІС становить 0,05. Таке низьке значення ймовірності обґрунтоване виконанням організаційних заходів щодо доступу сторонніх осіб у приміщення відділу прикордонної служби. Ймовірність наявності каналу інформаційного дестабілізаційного впливу в елементі ІС визначимо за результатами експертного оцінювання, які наведено в додатку Д. Результати обчислень становлять $P_{кідф} = 0{,}27$. Приймемо, що ймовірність доступу порушника до самого каналу буде максимальною, тобто дорівнюватиме одиниці. Ймовірність наявності даних певної категорії на елементі ІС теж приймемо рівною одиниці. Таким чином, ймовірність порушення конфіденційності на експериментальному зразку ПТК АПС становитиме $P^c = 1 - \prod_{j=0}^{6}\left(1 - P_j^c\right) = 1 - (1 - 0{,}013)^6 = 0{,}058$.

Для визначення ймовірності порушення доступності ІС при умові надходження даних іншої версії СПЗ застосуємо залежність (3.41) та зазначені вище припущення щодо ймовірності решти подій, а саме:

$$P^a = 1 - \prod_{j=0}^{6}\left(1 - P_j^a\right) = 1 - (1 - 0{,}006)^6 = 0{,}037.$$

Використовуючи аналогічний підхід, визначимо ймовірність порушення спостереженості ІС. Зазначимо, що даний показник залежить від значень ймовірності порушення цілісності та конфіденційності. У складі ПТК АПС "Гарт-3/П" упроваджено один тип ідентифікації і автентифікації, ймовірність порушення якого приймемо за 0,5. Таким чином, ймовірність порушення ідентифікації і автентифікації порушником визначається за формулою (3.34) і становить $P_{ia} = \left(1 - (1 - 0{,}049)\cdot(1 - 0{,}058)\right)\cdot 0{,}5 = 0{,}05$.

Відповідно до функціональної залежності та прийнятих припущень, загальна ймовірність порушення спостереженості ПТК АПС становитиме

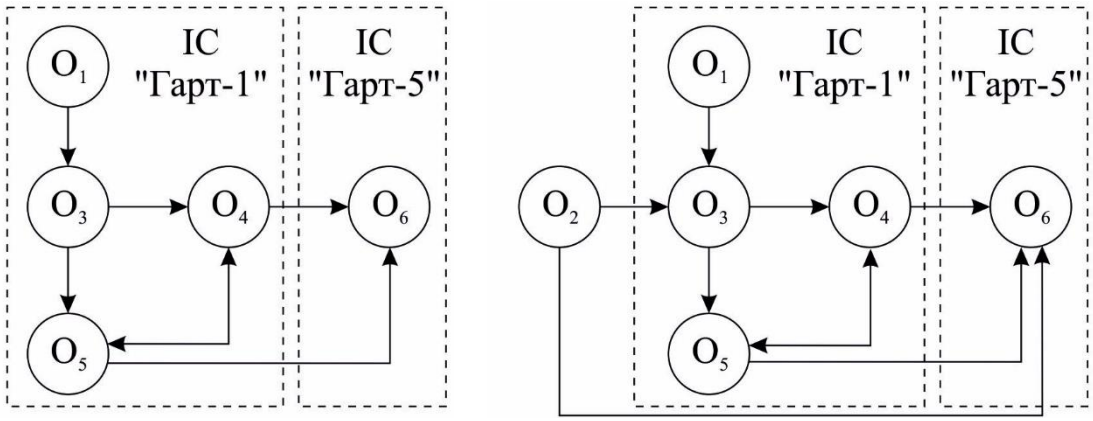
$$P^{u} = 1 - \prod_{j=0}^{6}\left(1 - P_j^{u}\right) = 1 - (1 - 0{,}0004)^{6} = 0{,}003$$

Вищенаведені розрахунки дозволяють визначити показник уразливості експериментальному зразку ПТК АПС "Гарт-3/П", який становить 0,14. Зазначений показник описує дотримання властивості ІС без урахування динаміки зміни потоку дестабілізаційних факторів у часі. Разом із тим його значення дає можливість оцінити стан системи функціональної безпеки.

6.6 Визначення ефективності узгодження систем розмежування доступу інформаційних систем "Гарт-1" та "Гарт-5"

Проведемо оцінювання ефективності узгодження систем розмежування доступу на прикладі взаємодії двох ІС у складі інтегрованої інформаційної системи "Гарт-1" та "Гарт-5". Структуру інформаційних потоків обох ІС подано у додатку Б. Вищенаведене обумовлює можливість спільного функціонування різних версій СРД на загальному полі даних при модернізації ІС. Для дослідження було розгорнуто дві експериментальних ІС з реалізацією їх взаємодії та обрано окремі елементи, які підлягали модернізації (рисунок 6.6).

Особливістю функціонування ІС автоматизації прикордонного контролю "Гарт-1" до модернізації є відсутність можливості здійснення перевірки особи за базами даних Інтерполу. Після модернізації такий доступ надано особам, що здійснюють контроль пропуску осіб через державний кордон. Разом із тим доступ до баз даних Інтерполу персоналу, який використовує "Гарт-5", не передбачався.



а) до модернізації б) після модернізації

де: O_1 – дані про особу; O_2 – БД Інтерполу; O_3 – перевірка документів; O_4 – журнал в'їзду/виїзду; O_5 – журнал спрацювань; O_6 – статистичні дані

Рисунок 6.6 – Інформаційні потоки ІС "Гарт–1" та "Гарт–5"

На рисунку 6.5 (б) показані додані інформаційні потоки, аналіз яких показує можливість міграції відомостей до елементів ІС "Гарт-5". Без надання права доступу елементу "Гарт-5" до відомостей Інтерполу порушення надійності даних здійснюватиметься постійно з причини наявності доданого інформаційного потоку. Зазначимо, що в дослідженні передбачається коректна робота СРД окремо в обох версіях, тому основним завданням модернізації передбачається підключення ІІС (у тому числі надання прав доступу "Гарт–5") до баз даних Інтерполу.

З метою дослідження ефективності узгодження систем розмежування доступу обох ІС на експериментальних зразках визначені величини інформаційних потоків між розглянутими елементами, загальні відомості яких зведені в таблицю 6.11 та 6.12. Одиницею інформаційного потоку прийнято вважати блок інформації стосовно однієї особи, розрахунок здійснювався за допомогою програми, що наведена в додатку И.

Таблиця 6.11 – Матриця інформаційних потоків до модернізації між елементами обох ІС ($\Lambda = \lfloor \lambda_{i,j} \rfloor$ – 1/с)

Індекс	**1**	**2**	**3**	**4**	**5**	**6**
1	0	0	0,005	0	0	0
2	0	0	0	0	0	0
3	0	0	0	0,004	0,001	0
4	0	0	0	0	0,001	0,14
5	0	0	0	0,001	0	0,014
6	0	0	0	0	0	0

Таблиця 6.12 – Матриця інформаційних потоків після модернізації між елементами обох ІС ($\Lambda = \lfloor \lambda_{i,j} \rfloor$ – 1/с)

Індекс	**1**	**2**	**3**	**4**	**5**	**6**
1	0	0	0,005	0	0	0
2	0	0	0,005	0	0	0,14
3	0	0	0	0,004	0,001	0
4	0	0	0	0	0,001	0,14
5	0	0	0	0,001	0	0,014
6	0	0	0	0	0	0

Аналіз інформаційних потоків дозволив визначити множину спільних об’єктів обох версій СРД $O_R = \{o_2, o_4, o_5\}$.

Сформуємо матриці ймовірностей міграції даних для об’єктів СРД до та після модернізації (таблиця 6.13, 6.14).

Таблиця 6.13 – Матриця ймовірностей міграції даних для об’єктів СРД до модернізації

Об’єкти	o_2	o_4	o_5
o_2	0	0	0
o_4	0	0	$1{,}2 \cdot 10^{-10}$
o_5	0	$1{,}2 \cdot 10^{-10}$	0

Таблиця 6.14 – Матриця ймовірностей міграції даних для об’єктів СРД після модернізації

Об’єкти	o_2	o_4	o_5
o_2	0	$2{,}6 \cdot 10^{-6}$	$9{,}1 \cdot 10^{-6}$
o_4	0	0	$1{,}2 \cdot 10^{-10}$
o_5	0	$1{,}2 \cdot 10^{-10}$	0

На підставі отриманих значень ймовірностей сформуємо матрицю недозволеного інформаційного потоку (таблиця 6.51).

Таблиця 6.15 – Матриця недозволеного інформаційного потоку

Об’єкти	o_2	o_4	o_5
o_2	0	$2{,}6 \cdot 10^{-6}$	$9{,}1 \cdot 10^{-6}$
o_4	0	0	0
o_5	0	0	0

Отже ефективність спільного функціонування обох версій СРД для одного елементу даних становитиме 0,9999883. В експериментальних зразках ІС вхідний потік передбачався 20 осіб на годину та часом модернізації систем 20 хв. Таким чином, ймовірність порушення властивостей хоча б одного елементу даних становитиме 0,00024.

6.7 Застосування методу оцінювання ефективності функціональної безпеки в інформаційних системах на стадії модернізації

Модернізація програмно-технічних комплексів Державної прикордонної служби України як основних елементів ключових ІС провадиться досить інтенсивно. Варто зазначити, що розпорядженнями Адміністрації ДПСУ на модернізацію окремих ІС виділяється достатньо тривалий термін часу (2–3 доби). Вищенаведене обумовлює спільне функціонування різних версій СПЗ. Для визначення рівня ризику надійності

інформації під час модернізації необхідно провести оцінювання ефективності функціональної безпеки.

Відповідно до методики формування моделі інформаційних дестабілізаційних факторів проведено експертне опитування щодо визначення їх переліку для експериментального зразка ПТК АПС (додаток Г). Після визначення структури та складу елементів системи забезпечення функціональної безпеки експертами проведено повторне оцінювання значень допустимої ймовірності порушення властивостей інформаційного ресурсу, яке наведено в додатку Г (таблиця Г.15). За результатами експертного оцінювання (додаток К) сформовані функції розподілу для ІДФ щодо складових інформаційного ресурсу, основу яких складало статистичне спостереження на експериментальному ПТК АПС "Гарт-З/П".

Вищенаведені розрахунки дозволяють сформувати функції розподілу ймовірностей ІДФ за її складовими. Аналіз подій, що спричинені процесом модернізації, показав, що вони стосуються тільки цілісності та доступності даних. У зв’язку із тим приймемо, що функції розподілу для зазначених складових однакові, а для решти не залежать від модернізації. Зведені дані щодо функцій розподілу ймовірностей реалізації ІДФ за її складовими наведено в таблиці 6.16.

Для формування загального вигляду закону розподілу випадкового вектора множини допустимих значень показника якості придатності СФБ необхідно врахувати взаємний вплив ймовірностей порушень властивостей інформації одна на одну, тобто отримати умовні закони розподілу. У розділі 5 наведено підхід до оцінювання ступеня залежності показників якості системи методом експертних оцінок.

Таблиця 6.16 – Функції розподілу ймовірностей реалізації ІДФ за її складовими

№ з/п	Вид ІДФ	Властивість інформаційного ресурсу			
		к	ц	д	с
1.	Порушення режимів функціонування систем життєзабезпечення ІС або її складових	$F_{c,1}^{ind}(t)=\begin{cases}0, t\le t_{експл}\\1, t>t_{експл}\end{cases}$	$F_{i,1}^{ind}(t)=\begin{cases}0, t<0\\0{,}05\\1, t>t_{експл}\end{cases}$	$F_{a,1}^{ind}(t)=\begin{cases}0, t<0\\0{,}01\\1, t>t_{експл}\end{cases}$	$F_{u,1}^{ind}(t)=\begin{cases}0, t<0\\0{,}005\\1, t>t_{експл}\end{cases}$
2.	Неправомірне підключення до каналів зв'язку, перехоплення даних, що передаються, зміна (модифікація) інформації повідомлень	$F_{c,2}^{ind}(t)=\begin{cases}0, t<0\\0{,}05\\1, t>t_{експл}\end{cases}$	$F_{i,2}^{ind}(t)=\begin{cases}0, t<0\\0{,}01\\1, t>t_{експл}\end{cases}$	$F_{a,2}^{ind}(t)=\begin{cases}0, t<0\\0{,}005\\1, t>t_{експл}\end{cases}$	$F_{u,2}^{ind}(t)=\begin{cases}0, t<0\\0{,}005\\1, t>t_{експл}\end{cases}$
3.	Несанкціоноване копіювання носіїв інформації	$F_{c,3}^{ind}(t)=\begin{cases}0, t<0\\0{,}05\\1, t>t_{експл}\end{cases}$	$F_{i,3}^{ind}(t)=\begin{cases}0, t\le t_{експл}\\1, t>t_{експл}\end{cases}$	$F_{a,3}^{ind}(t)=\begin{cases}0, t\le t_{експл}\\1, t>t_{експл}\end{cases}$	$F_{u,3}^{ind}(t)=\begin{cases}0, t<0\\0{,}01\\1, t>t_{експл}\end{cases}$
4.	Крадіжки носіїв інформації	$F_{c,4}^{ind}(t)=\begin{cases}0, t<0\\0{,}01\\1, t>t_{експл}\end{cases}$	$F_{i,4}^{ind}(t)=\begin{cases}0, t<0\\0{,}01\\1, t>t_{експл}\end{cases}$	$F_{a,4}^{ind}(t)=\begin{cases}0, t<0\\0{,}01\\1, t>t_{експл}\end{cases}$	$F_{u,4}^{ind}(t)=\begin{cases}0, t<0\\0{,}01\\1, t>t_{експл}\end{cases}$
5.	Фальсифікація (приховування) фактів формування та видачі даних	$F_{c,5}^{ind}(t)=\begin{cases}0, t\le t_{експл}\\1, t>t_{експл}\end{cases}$	$F_{i,5}^{ind}(t)=\begin{cases}0, t\le t_{експл}\\1, t>t_{експл}\end{cases}$	$F_{a,5}^{ind}(t)=\begin{cases}0, t\le t_{експл}\\1, t>t_{експл}\end{cases}$	$F_{u,5}^{ind}(t)=\begin{cases}0, t<0\\0{,}01\\1, t>t_{експл}\end{cases}$

Продовження таблиці 6.16

№ з/п	Вид загрози	Властивість інформаційного ресурсу			
		к	ц	д	с
6.	Переривання передачі потоку даних	$F_{c,7}^{ind}(t)=\begin{cases}0, t\le t_{експл}\\ 1, t>t_{експл}\end{cases}$	$F_{i,7}^{ind}(t)=\begin{cases}0, t<0\\ 0{,}01\\ 1, t>t_{експл}\end{cases}$	$F_{a,7}^{ind}(t)=\begin{cases}0, t<0\\ 0{,}005\\ 1, t>t_{експл}\end{cases}$	$F_{u,7}^{ind}(t)=\begin{cases}0, t<0\\ 0{,}005\\ 1, t>t_{експл}\end{cases}$
7.	Порушення фізичної цілісності ІС (її окремих компонентів)	$F_{c,8}^{ind}(t)=\begin{cases}0, t<0\\ 0{,}05\\ 1, t>t_{експл}\end{cases}$	$F_{i,8}^{ind}(t)=\begin{cases}0, t<0\\ 0{,}05\\ 1, t>t_{експл}\end{cases}$	$F_{a,8}^{ind}(t)=\begin{cases}0, t<0\\ 0{,}005\\ 1, t>t_{експл}\end{cases}$	$F_{u,8}^{ind}(t)=\begin{cases}0, t<0\\ 0{,}005\\ 1, t>t_{експл}\end{cases}$
8.	Дії, що призводять до відмови ІС чи окремих її елементів, руйнування окремих складових обчислювальних систем та іншого обладнання (телекомунікаційного, засобів вводу/виводу тощо)	$F_{c,9}^{ind}(t)=\begin{cases}0, t<0\\ 0{,}005\\ 1, t>t_{експл}\end{cases}$	$F_{i,9}^{ind}(t)=\begin{cases}0, t<0\\ 0{,}005\\ 1, t>t_{експл}\end{cases}$	$F_{a,9}^{ind}(t)=\begin{cases}0, t<0\\ 0{,}005\\ 1, t>t_{експл}\end{cases}$	$F_{u,9}^{ind}(t)=\begin{cases}0, t<0\\ 0{,}01\\ 1, t>t_{експл}\end{cases}$
9.	Ненавмисне пошкодження носіїв інформації	$F_{c,10}^{ind}(t)=\begin{cases}0, t\le t_{експл}\\ 1, t>t_{експл}\end{cases}$	$F_{i,10}^{ind}(t)=\begin{cases}0, t<0\\ 0{,}01\\ 1, t>t_{експл}\end{cases}$	$F_{a,10}^{ind}(t)=\begin{cases}0, t<0\\ 0{,}01\\ 1, t>t_{експл}\end{cases}$	$F_{u,10}^{ind}(t)=\begin{cases}0, t<0\\ 0{,}005\\ 1, t>t_{експл}\end{cases}$

Продовження таблиці 6.16

№ з/п	Вид загрози	Властивість інформаційного ресурсу			
		к	ц	д	с
10.	Невиконання організаційних заходів щодо порядку і правил експлуатації чи використання ресурсів ІС, передбачених керівними документами та технологічними інструкціями	$F_{c,11}^{ind}(t)=\begin{cases}0, t<0\\0{,}01\\1, t>t_{експл}\end{cases}$	$F_{i,11}^{ind}(t)=\begin{cases}0, t<0\\0{,}01\\1, t>t_{експл}\end{cases}$	$F_{a,11}^{ind}(t)=\begin{cases}0, t<0\\0{,}01\\1, t>t_{експл}\end{cases}$	$F_{u,11}^{ind}(t)=\begin{cases}0, t<0\\0{,}01\\1, t>t_{експл}\end{cases}$
11.	Використання персоналом ІС з корисливою метою	$F_{c,12}^{ind}(t)=\begin{cases}0, t<0\\0{,}005\\1, t>t_{експл}\end{cases}$	$F_{i,12}^{ind}(t)=\begin{cases}0, t<0\\0{,}01\\1, t>t_{експл}\end{cases}$	$F_{a,12}^{ind}(t)=\begin{cases}0, t<0\\0{,}01\\1, t>t_{експл}\end{cases}$	$F_{u,12}^{ind}(t)=\begin{cases}0, t<0\\0{,}01\\1, t>t_{експл}\end{cases}$
12.	Некомпетентне застосування засобів забезпечення функціональної безпеки	$F_{c,13}^{ind}(t)=\begin{cases}0, t<0\\0{,}005\\1, t>t_{експл}\end{cases}$	$F_{i,13}^{ind}(t)=\begin{cases}0, t<0\\0{,}005\\1, t>t_{експл}\end{cases}$	$F_{a,13}^{ind}(t)=\begin{cases}0, t<0\\0{,}005\\1, t>t_{експл}\end{cases}$	$F_{u,13}^{ind}(t)=\begin{cases}0, t<0\\0{,}005\\1, t>t_{експл}\end{cases}$
13.	Зміна умов фізичного середовища	$F_{c,14}^{ind}(t)=\begin{cases}0, t\le t_{експл}\\1, t>t_{експл}\end{cases}$	$F_{i,14}^{ind}(t)=\begin{cases}0, t<0\\0{,}005\\1, t>t_{експл}\end{cases}$	$F_{a,14}^{ind}(t)=\begin{cases}0, t<0\\0{,}005\\1, t>t_{експл}\end{cases}$	$F_{u,14}^{ind}(t)=\begin{cases}0, t<0\\0{,}005\\1, t>t_{експл}\end{cases}$
14.	Збої та відмови у роботі ІС, аварійне відключення живлення та інше	$F_{c,15}^{ind}(t)=\begin{cases}0, t\le t_{експл}\\1, t>t_{експл}\end{cases}$	$F_{i,15}^{ind}(t)=\begin{cases}0, t<0\\0{,}005\\1, t>t_{експл}\end{cases}$	$F_{a,15}^{ind}(t)=\begin{cases}0, t<0\\0{,}005\\1, t>t_{експл}\end{cases}$	$F_{u,15}^{ind}(t)=\begin{cases}0, t<0\\0{,}01\\1, t>t_{експл}\end{cases}$

Продовження таблиці 6.16

№ з/п	Вид загрози	Властивість інформаційного ресурсу			
		к	ц	д	с
15.	Впливи природних та технологічних завад (грозові розряди, електрозварювальні роботи тощо)	$F_{c,16}^{ind}(t)=\begin{cases}0, t\le t_{експл}\\1, t>t_{експл}\end{cases}$	$F_{i,16}^{ind}(t)=\begin{cases}0, t<0\\0{,}005\\1, t>t_{експл}\end{cases}$	$F_{a,16}^{ind}(t)=\begin{cases}0, t<0\\0{,}005\\1, t>t_{експл}\end{cases}$	$F_{u,16}^{ind}(t)=\begin{cases}0, t<0\\0{,}05\\1, t>t_{експл}\end{cases}$
16.	Помилки при введенні даних в систему	$F_{c,17}^{ind}(t)=\begin{cases}0, t<0\\0{,}01\\1, t>t_{експл}\end{cases}$	$F_{i,17}^{dep}(t)=1-e^{-\left(\frac{t}{13}\right)^{1.31}}$	$F_{a,17}^{dep}(t)=1-e^{-\left(\frac{t}{13}\right)^{1.31}}$	$F_{u,17}^{ind}(t)=\begin{cases}0, t<0\\0{,}01\\1, t>t_{експл}\end{cases}$
17.	Помилки при розробці або модернізації ІІТС та її складових	$F_{c,18}^{ind}(t)=\begin{cases}0, t<0\\0{,}005\\1, t>t_{експл}\end{cases}$	$F_{i,18}^{dep}(t)=1-e^{-\left(\frac{t}{18}\right)^{2}}$	$F_{a,18}^{dep}(t)=1-e^{-\left(\frac{t}{18}\right)^{2}}$	$F_{u,18}^{ind}(t)=\begin{cases}0, t<0\\0{,}005\\1, t>t_{експл}\end{cases}$

В додатку Л проведено експертизу такої залежності, результати якої зведено до таблиці 6.17.

Таблиця 6.17 – Значення умовних ймовірностей порушення властивостей інформаційного ресурсу на експериментальному ПТК АПС "Гарт-1П"

Властивість інформаційного ресурсу	Умовна ймовірність порушення властивості інформаційного ресурсу			
	цілісність	конфід.	доступність	спостереж.
Цілісність	1	0,05	0,8	0,6
Конфід.	0,05	1	0,05	0,05
Доступність	0,2	0,05	1	0,4
Спостереж.	0,05	0,5	0,2	1

Складовою функцій розподілу ймовірностей порушення властивостей інформаційного ресурсу є ймовірність того, що дані надходять в елемент ІС з іншої версії СПЗ. У додатку В наведені розрахунки параметрів швидкості здійснення модернізації складових ІС "Гарт-1". Разом із тим параметрами також є величини інформаційних потоків старої і нової версій ІС. З урахуванням конкретного типу модернізації, який здійснювався на експериментальному зразку ІТС "Гарт-1", аналіз величин інформаційного потоку нової версії показав його збільшення в середньому на 8 %. Отже функціональна залежність (5.36) набуде вигляду:

$$P_н(t) = \frac{e^{-wt}}{c \cdot \left(1 - e^{-wt}\right) + e^{-wt}}, \qquad (6.14)$$

де $c = \frac{\lambda_{new}}{\lambda_{old}}$ – величина зміни інформаційного потоку.

Варто зазначити, що величини інформаційних потоків різних версій "Гарт-1" залежать від пасажиропотоку пункту пропуску. Зміна величини блоку даних приводить до лінійної зміни величини інформаційного потоку у новій версії спеціального програмного забезпечення. На експериментальному

зразку "Гарт-1" величина пасажиропотоку була визначена як $\lambda = 38 осіб/год$.

Вищенаведені дані дозволяють сформувати аналітичний вигляд функції розподілу множини допустимих значень показника якості системи функціональної безпеки та вид інтегрального закону розподілу випадкового вектора $\hat{Y}$.

Відповідно до вихідних даних, які наведено в додатку К, сформуємо функції розподілу ймовірності порушення надійності інформації на ділянці терміну експлуатації ІС

$$P_i(v_i) = 1 - 0.83 \cdot e^{-\left(\left(\frac{v_i}{13}\right)^{1.3} + \left(\frac{v_i}{18}\right)^2\right)} = 1 - 0.83 \cdot f(v_i), \quad (6.15)$$

$$P_c(v_c) = 0.18, \quad (6.16)$$

$$P_a(v_a) = 1 - 0.91 \cdot e^{-\left(\left(\frac{v_a}{13}\right)^{1.3} + \left(\frac{v_a}{18}\right)^2\right)} = 1 - 0.91 \cdot f(v_a), \quad (6.17)$$

$$P_u(v_u) = 0.16, \quad (6.18)$$

де $f(x) = e^{-\left(\left(\frac{x}{13}\right)^{1.3} + \left(\frac{x}{18}\right)^2\right)}$,

звідки

$$P_{H_i}(v_i) = 1 - 0.83 f(v_i) + 0.00005976 f(v_i) \cdot (0.2 - 0.182 f(v_i)), \quad (6.19)$$

$$P_{H_c}(v_c) = 0.18 + 0.0656(0.05 - 0.0415 f(v_c)) \cdot (0.05 - 0.0455 f(v_c)), \quad (6.20)$$

$$P_{H_a}(v_a) = 1 - 0.91 f(v_a) + 0.00026208 f(v_a) \cdot (0.2 - 0.246 f(v_a)), \quad (6.21)$$

$$P_{H_u}(v_u) = 0.16 + 0.00756(0.6 - 0.498 f(v_u)) \cdot (0.4 - 0.364 f(v_u)). \quad (6.22)$$

Підставивши (6.19–6.22) у (5.31), отримаємо

$$F_{\hat{Z}}(Y)=\left(0.83f(v_i)+0.00005976f(v_i)\cdot(0.2-0.182f(v_i))\right)\times$$
$$\times\left(0.82-0.0656(0.05-0.0415f(v_c))\cdot(0.05-0.0455f(v_c))\right)\times$$
$$\times\left(0.91f(v_a)+0.00026208f(v_a)\cdot(0.2-0.246f(v_a))\right)\times$$
$$\times\left(0.84-0.00756(0.6-0.498f(v_u))\cdot(0.4-0.364f(v_u))\right) \quad (6.23)$$

Після певних перетворень (6.23) отримаємо

$$F_{\hat{Z}}(v_i,v_c,v_a,v_u)=\left(0.83f(v_i)+0.0000109f^2(v_i)\right)\times$$
$$\times\left(0.82+0.00028f(v_c)-0.000123f^2(v_c)\right)\times$$
$$\times\left(0.908f(v_a)+0.00174f^2(v_a)\right)\times \quad (6.24)$$
$$\times\left(0.838+0.00316f(v_u)-0.00137f^2(v_u)\right)$$

Для використання (6.24) в розрахунку функціональної залежності (5.43) необхідно знайти щільність розподілу $F_{\hat{Z}}(Y)$, яка визначається як

$$f_{\hat{Z}}(Y)=\frac{\partial^4 F_{\hat{Z}}(v_i,v_c,v_a,v_u)}{dv_i dv_c dv_a dv_u}. \quad (6.25)$$

Відшукання щільності розподілу (6.25) наведено в додатку М.

Ці розрахунки дозволяють сформувати вид інтегрального закону розподілу випадкового вектора $\hat{Y}$ для експериментального зразка ПТК АПС Гарт-1/П" з урахуванням (5.41) , а саме:

$$\Phi_{\hat{Y}}(Y)=\left(1-0.05P_н(v_i)(1-0.83\cdot f(v_i))\right)^6\times$$
$$\times\left(1-(0.0243\cdot P_н(v_c))^6\right)\cdot\left(1-P_н(v_a)(1-0.91\cdot f(v_a))^6\right)\times \quad (6.26)$$
$$\times\left(1-(0.0455P_н(v_u)f(v_u)(1-(1-0.83\cdot f(v_u))\cdot(1-0.1494\cdot f(v_u))))^6\right)$$

Визначення аналітичного виразу формули повної ймовірності в інтегральній формі з урахуванням (6.25) та (6.26) є проблемним. Для обчислення значень використаємо чисельні методи знаходження інтегралу за

допомогою квадратурних методів обчислення [17]. З цією метою використаємо метод прямокутників, суть якого зводиться до знаходження визначеного інтегралу як суми об’ємів фігур, які обмежені заданою функцією [18], тобто:

$$P_{ДМ} = \frac{V_i}{N_i}\frac{V_c}{N_c}\frac{V_a}{N_a}\frac{V_u}{N_u}\sum_{k_1=0}^{N_i}\sum_{k_2=0}^{N_c}\sum_{k_3=0}^{N_a}\sum_{k_4=0}^{N_u}\left[\begin{array}{l}\Phi_{\hat{Y}}\left(v_{k_1}^{i},v_{k_2}^{c},v_{k_3}^{a},v_{k_4}^{u}\right)\times\\ \times f_{\hat{Z}}\left(v_{k_1}^{i},v_{k_2}^{c},v_{k_3}^{a},v_{k_4}^{u}\right)\end{array}\right]. \qquad (6.27)$$

Обчислення здійснено за допомогою ЕОМ, відповідно до програми, код якої наведено в додатку Н. Результати обчислень подано в додатку П.

Аналіз результатів визначення ймовірності порушення властивостей інформаційного ресурсу за умови дотримання їх значень у допустимих межах проведемо поетапно за кожною із його властивостей. На рисунках 6.7–6.9 показано динаміку зміни ймовірності порушення властивостей інформаційного ресурсу при зміні нормативного значення цілісності та інших властивостей інформаційного ресурсу.

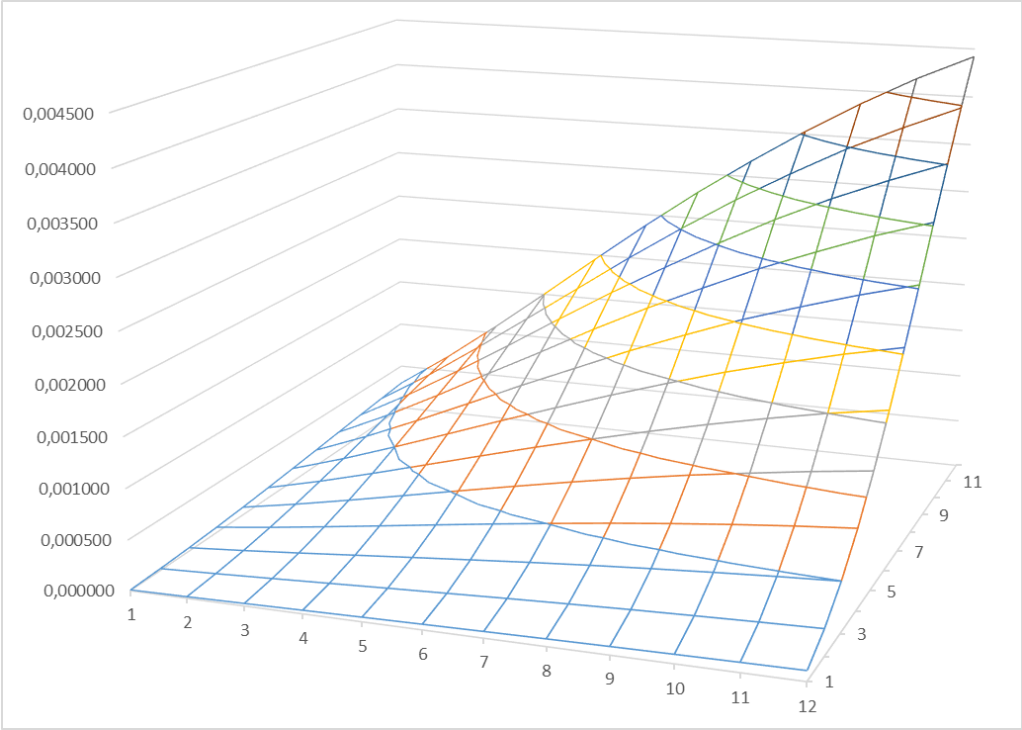


Рисунок 6.7 – Ймовірності порушення властивостей інформаційного ресурсу при фіксованих нормативних значеннях доступності та спостережності

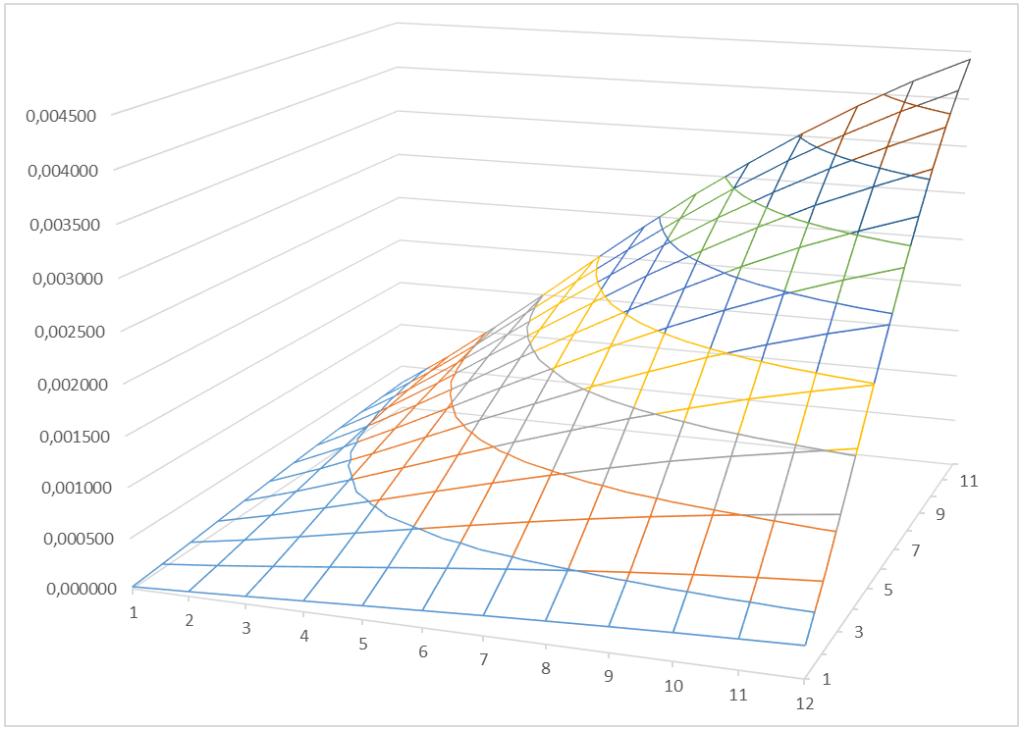


Рисунок 6.8 – Ймовірності порушення властивостей інформаційного ресурсу при фіксованих нормативних значеннях конфіденційності та спостережності

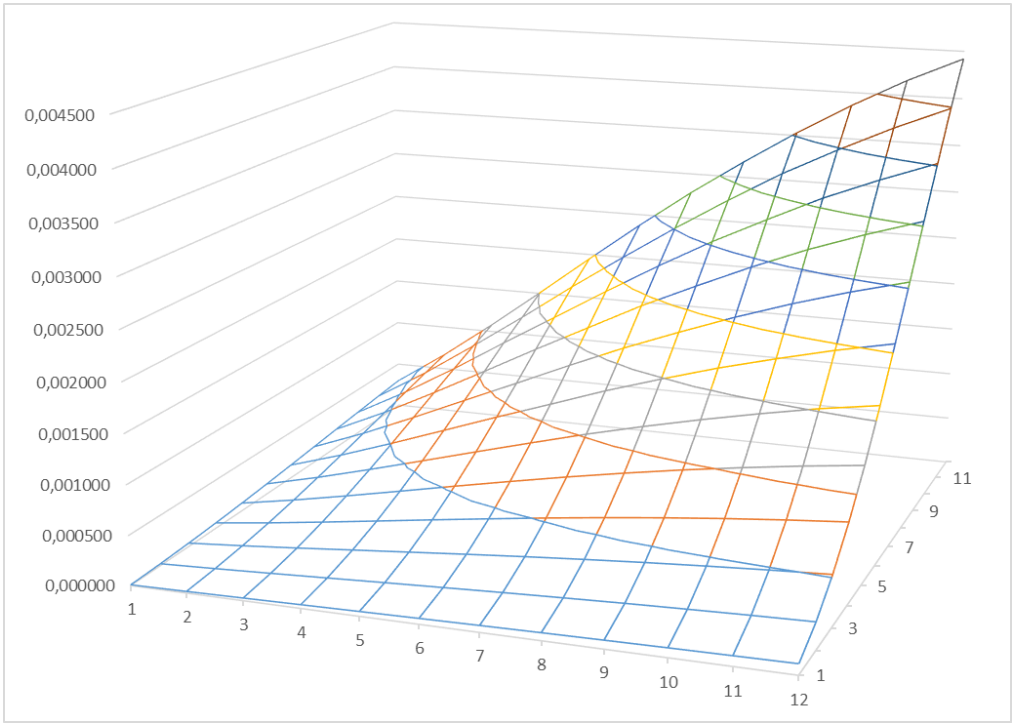


Рисунок 6.9 – Ймовірності порушення властивостей інформаційного ресурсу при фіксованих нормативних значеннях конфіденційності та доступності

З метою порівняння значень ймовірностей у різних умовах для якісного оцінювання ступеня впливу наведемо графік різниці двох ймовірностей.

Позитивне значення свідчить про перевагу першого параметра, негативне – другого (рисунок 6.10).

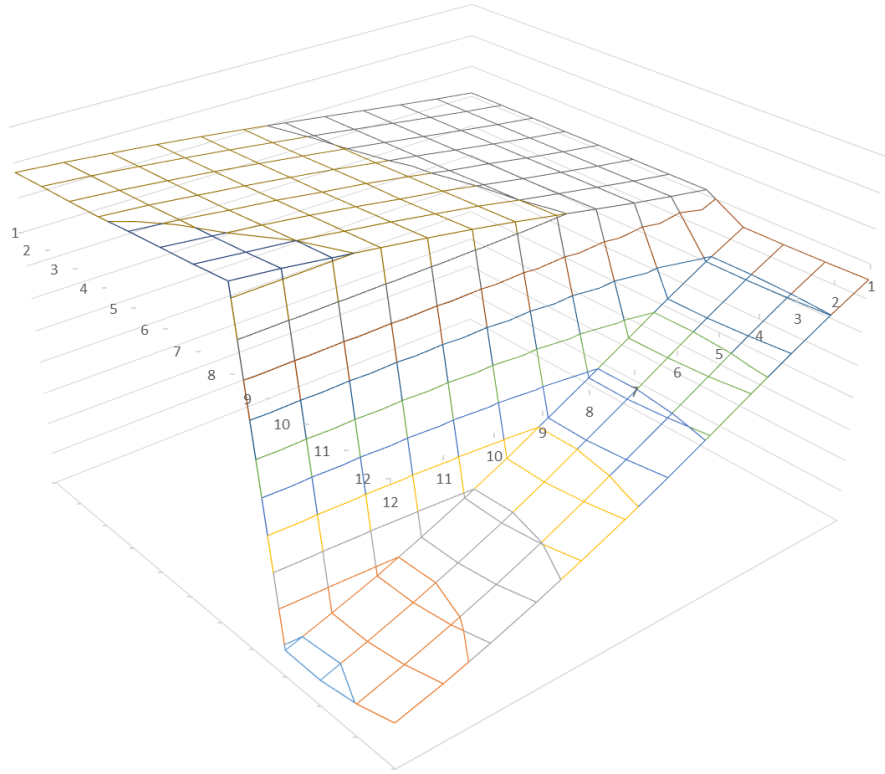


Рисунок 6.10 – Різниця ймовірностей порушення властивостей інформаційного ресурсу за параметрами цілісності та конфіденційності

Аналіз різниці ймовірностей порушення властивостей інформаційного ресурсу за параметрами цілісності та конфіденційності показав, що на початку модернізації більший вплив на $P_{ДМ}$ має складова цілісності, а при збільшенні нормативного часу кожного із них характерна різка зміна ступеня впливу конфіденційності (стрибок площини в межах 8 год модернізації). Причому така зміна відбувається незалежно від нормативного значення цілісності.

Аналогічний аналіз за іншими властивостям, а саме цілісності та спостереженості, показав аналогічну тенденцію (рисунок 6.11). Варто зазначити певне зростання впливу цілісності на значення $P_{ДМ}$ у порівнянні із параметром конфіденційності.

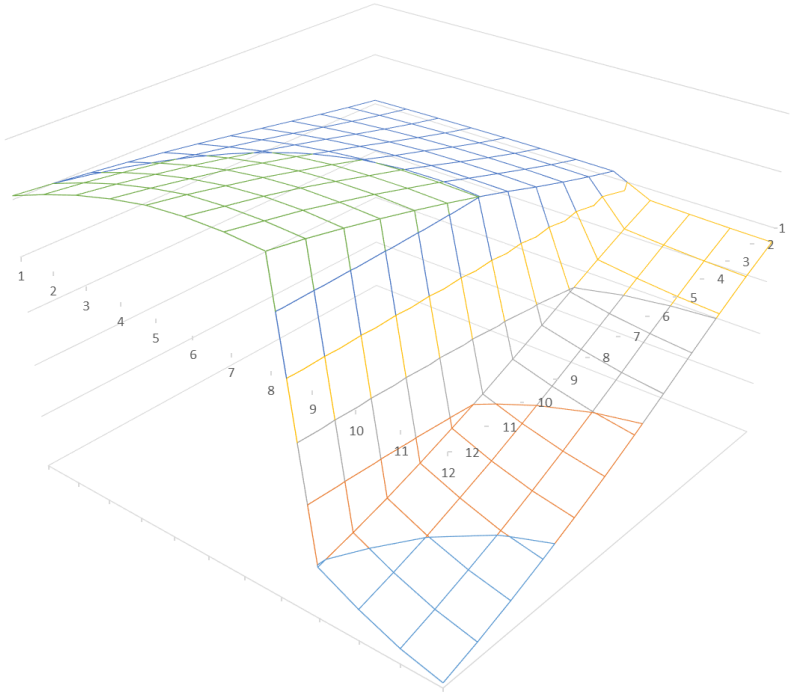


Рисунок 6.11 – Різниця ймовірностей порушення властивостей інформаційного ресурсу за параметрами цілісності та спостереженості

Проведемо аналогічне порівняння за параметрами конфіденційності (рисунок 6.12, 6.13).

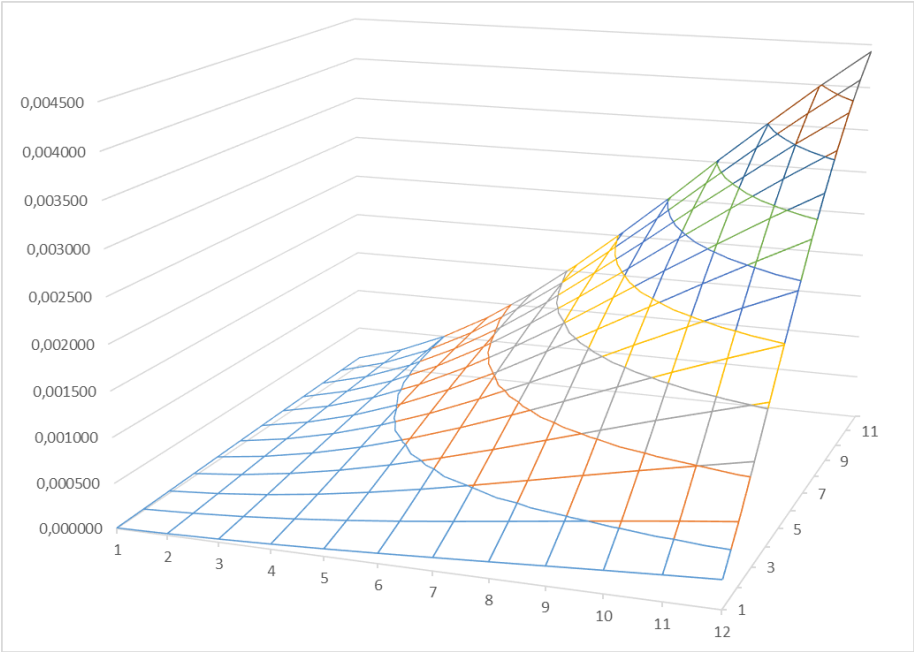


Рисунок 6.12 – Ймовірності порушення властивостей інформаційного ресурсу при фіксованих нормативних значеннях цілісності та спостереженості

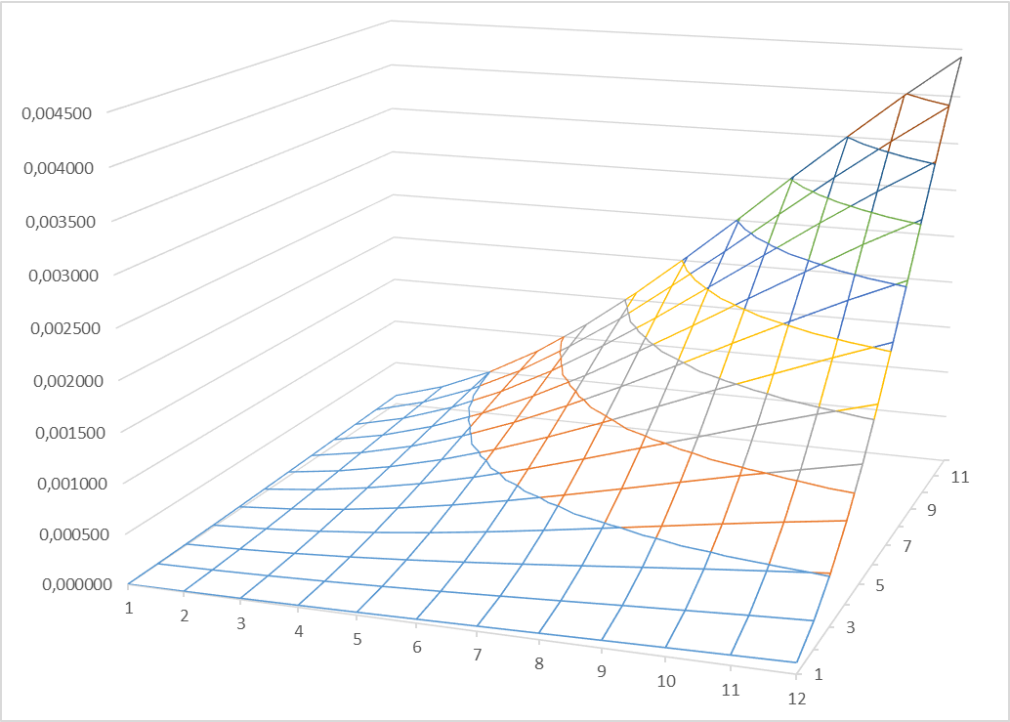


Рисунок 6.13 – Ймовірності порушення властивостей інформаційного ресурсу при фіксованих нормативних значеннях цілісності та доступності

Аналіз за властивостям доступності та спостереженості показав аналогічну тенденцію (рисунок 6.14). Варто зазначити вид функції зростання значення $P_{ДМ}$ у порівнянні із параметром конфіденційності (рисунок 6.11). У цьому випадку зростання ймовірності порушення властивості інформаційного ресурсу при зростанні нормативного часу конфіденційності у разі зміни параметрів цілісності та доступності має лінійний характер. У випадку аналогічного дослідження в умовах зміни параметрів доступності та спостереженості характер зміни значення $P_{ДМ}$ за параметром конфіденційності має тенденцію степеневого зростання. Такий самий вплив має характер зміни стрибка впливу обох параметрів. Аналогічно до зростання за степеневим видом зростання ймовірності за параметром конфіденційності, вплив другого параметра, а саме доступності, має подібний вплив на етапі стрибка ступеня впливу параметру спостереженості.

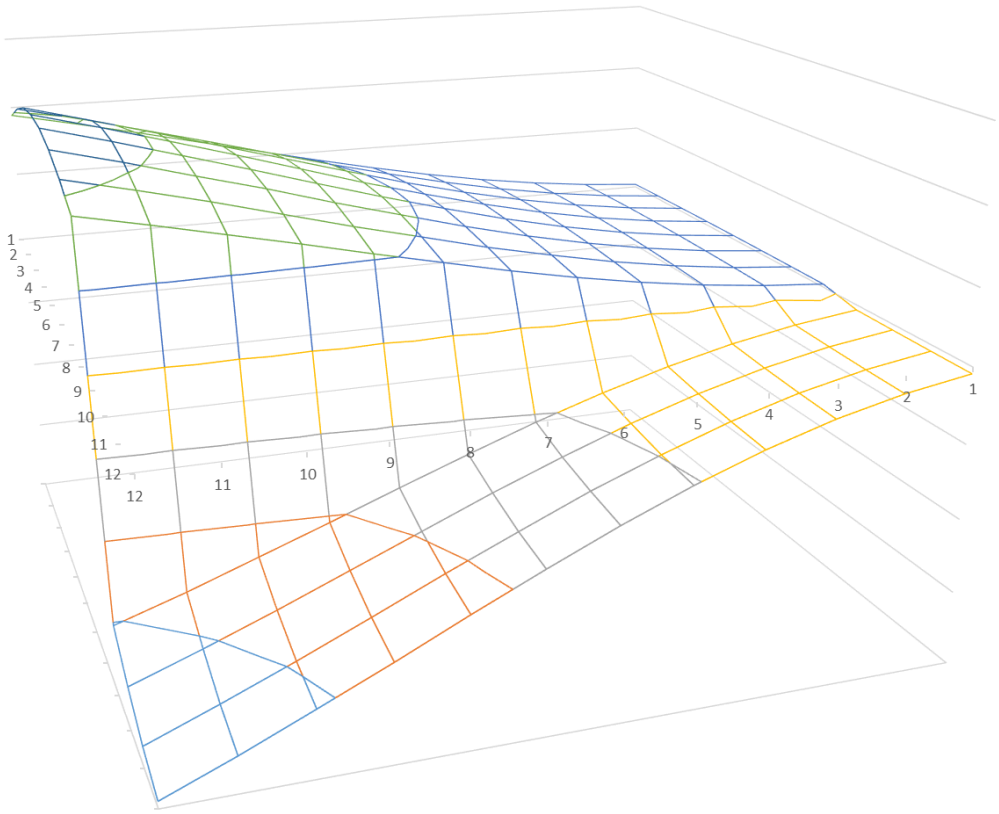


Рисунок 6.14 – Різниця ймовірностей порушення властивостей інформаційного ресурсу за параметрами доступності та спостереженості

Отже аналіз впливу нормативних значень властивостей інформаційного ресурсу при дослідженні ймовірності порушення властивостей інформаційного ресурсу на експериментальному програмно-технічному комплексі автоматизації прикордонної служби показав загальну тенденцію до зростання у разі зростання нормативних значень. Зазначена тенденція є прогнозованою з причини збільшення часу дотримання кожної властивості інформаційного ресурсу. Разом із тим аналіз динаміки впливу окремих властивостей на результуючу функцію показав наявність стрибка зміни впливу окремих параметрів, причому для різних параметрів у межах одного і того ж значення. Вищенаведене дозволить визначити спільне для всіх нормативних параметрів значення, за яких їх вплив на загальну ймовірність порушення властивостей інформаційного ресурсу буде однаковий.

6.8 Висновки до розділу 6

1. Для дослідження застосування технології підвищення якості функціонування інтегрованої інформаційної системи Держприкордонслужби обрано найбільш поширені в прикордонному відомстві інформаційні системи, які містять програмно-технічні комплекси. Визначення окремих характеристик здійснювалось із використанням експериментальних зразків програмно-технічних комплексів автоматизації прикордонного контролю ("Гарт-1-П") та прикордонної служби ("Гарт-3/П"). Топологічно дані комплекси являють собою "зірку", але обмін інформації (інформаційні потоки) здійснюються між всіма їхніми елементами через серверну частину. Структура зазначених комплексів формується відповідно до потреб конкретного відділу прикордонної служби.

2. Визначення раціональної послідовності модернізації елементів ІС здійснювалось на базі експериментального зразка програмно-технічного комплексу автоматизації прикордонного контролю ("Гарт-1-П"). Аналіз динаміки зміни ймовірності порушення його властивостей на стадії модернізації при різних послідовностях показав, що незважаючи на загальне достатньо низьке значення ймовірності, пікові значення можуть бути достатньо високими. Крім того, при середньому значенні ймовірності меншому за визначене максимальне значення є більшим за оптимальну послідовність. Отже відповідно до обраних стратегії модернізації та режиму роботи ІС визначено раціональні послідовності модернізації елементів ІС.

3. За розробленим методом здійснено розподіл засобів забезпечення функціональної безпеки при модернізації інформаційної системи прикордонної служби "Гарт-3". Визначені вагові коефіцієнти можливих каналів ІДФ для зазначеного зразка. Проведено дослідження щодо зміни ваг можливих КІДФ при модернізації інформаційної системи у разі розгортання додаткових відділів прикордонної служби та визначені нормативні значення захищеності доданих каналів за умови дотримання заданого значення функціональної безпеки ІС «Гарт-3» загалом.

4. Розроблено методику експертного оцінювання ступеня впливу дестабілізаційних факторів на ІС на стадії модернізації. Наведено етапи зазначеної методики та сформовано шкали оцінювання ступеня впливу дестабілізаційних факторів на елементи конкретної ІС. Проведено аналіз наявних підходів до порядку проведення експертного оцінювання. Обрано ймовірнісний підхід та елементи математичної статистики для здійснення обробки результатів експертного опитування. Відповідно розробленої методики проведено експертне оцінювання за кожною властивістю інформації та фактом впливу процесу модернізації на них.

5. Визначено ступінь уразливості експериментального зразка програмно-технічного комплексу автоматизації прикордонної служби, який розгорнуто на кафедрі зв’язку, автоматизації та захисту інформації Національної академії Державної прикордонної служби України імені Б. Хмельницького. Розрахунки дозволяють визначити показник уразливості експериментального зразка ПТК АПС "Гарт-3/П", який становить 0,86. Зазначений показник описує дотримання властивостей інформаційного ресурсу ІС без урахування динаміки зміни потоку дестабілізаційних факторів у часі. Разом із тим, його значення дає можливість оцінити стан системи функціональної безпеки.

6. Проведено оцінювання ефективності узгодження систем розмежування доступу на прикладі взаємодії двох ІС у складі інтегрованої інформаційної системи "Гарт-1" та "Гарт-5". Ефективність спільного функціонування обох версій систем розмежування доступу для одного елементу даних становитиме 0,9999883. В експериментальних зразках ІС вхідний потік передбачався 20 осіб на годину та часом модернізації систем 20 хв. Отже ймовірність порушення властивостей хоча б одного елементу даних становитиме 0,00024.

7. Оцінено ефективність функціонування системи функціональної безпеки в експериментальному зразку програмно-технічного комплексу автоматизації прикордонної служби "Гарт-1/П" на стадії модернізації. Аналіз

впливу нормативних значень властивостей інформаційного ресурсу при дослідженні ймовірності порушення властивостей інформаційного ресурсу показав загальну тенденцію до зростання при зростанні нормативних значень. Разом із тим аналіз динаміки впливу окремих властивостей на результуючу функцію показав наявність стрибка зміни впливу окремих параметрів, причому для різних параметрів у межах одного і того ж значення. Це дозволить визначити спільне для всіх нормативних параметрів значення, за якого їх вплив на загальну ймовірність порушення властивостей інформаційного ресурсу буде однаковий.

Список використаних джерел у шостому розділі

1. Афоничкин А. И. Управленческие решения в экономических системах / А. И. Афоничкин, Д. Г. Михаленко. – СПб.: Питер. 2009. – 480 с.

2. Бешелев С. Д. Математико-статистические методы экспертных оценок / С.Д, Бешелев, Ф.Г. Гурвич. – М.: Статистика. 1974. – 160 с.

3. Гапоненко Т.В. Управленческие решения. - Ростов Н/Д: Феникс. 2008. – 284 с.

4. Горбашко Е.А. Управление качеством. – Спб.: Питер. 2008. – 384 с.

5. Жуков Б. М. Исследование систем управления / Б. М. Жуков, Е. Н. Ткачева. - М.: Дашков и К, 2011.- 208 с.

6. Зерный Ю. В. Управление качеством в приборостроении. / Ю. В. Зерный, А. Г. Полываный, А. А. Якушин.- М.: Новый центр. 2011. – 479 с.

7. Кошелев О. С. Управление проектами / О. С. Кошелев, И. О. Леушин, О. В. Федоров – М.: КНОРУС, 2011.- 254 с.

8. Крылов А. В. О проблемах организации экспертизы / А. В. Крылов // Проблемы полиграфии и издательского дела. – 2006. - №4. – С.117- 122.

9. Лукичева Л.И., Егорычев Д.Н. Управленческие решения – М.: Омега-Л. 2009 – 383 с.

10. Марголин Е. Методика обработки данных экспертного опроса / Е. Марголин // Полиграфия . – 2006. - №5 - С. 14 – 16.

11. Михненко П. Секреты эффективных бизнес-решений. – М. NTPress. -2007. – 288 с.

12. Орлов А.И. Организационно-экономическое моделирование. Теория принятия решений. – М.: КНОРУС. 2011. – 568 с.

13. Петров А.Ю. Интегральная методика оценки коммерческого потенциала инвестиционного продукта. – М.: Московский печатник, 2010.- 23с.

14. Сышикова Е.Н. Теория и методы повышения эффективности систем управления на предприятии. – Воронеж. ГОУВПО ВГТУ. 2010. - 206 с.

15. Шевченко С. А. Выбор комплекта допечатного оборудования, отвечающего заданным условиям / С. А. Шевченко, Ю. Н. Самарин // Проблемы полиграфии и издательского дела. – 2006. - №4. – С.3 -12.

16. Теория статистики / под. ред. Громыко Г.Л. – М.: ИНФРА-М, 2009.- 476 с.

17. Ляшенко М.Я., Головань М.С. Чисельні методи: Підручник. Либідь. 1996. – 288 с.

18. Щуп Т. Решение инженерных задач на ЭВМ. – М.: Мир, 1982. – 235с.

ВИСНОВКИ

Результатом виконаної роботи є вирішення актуальної і важливої науково-технічної проблеми створення інформаційної технології забезпечення функціональної безпеки відомчої ІІС на стадії модернізації.

У процесі виконання дисертаційної роботи отримані такі основні результати:

1. Проведено формалізований опис процесу модернізації інтегрованої інформаційної системи. Розроблені раціональні стратегії функціональної безпеки, на базі яких розроблено загальну концепцію забезпечення функціональної безпеки на стадії модернізації, як інструментально-методологічну базу, що забезпечує виконання розглянутих стратегій. Концепцією передбачено три завдання узгодження спільного функціонування ІС: спеціального програмного забезпечення, програмних і технічних засобів. В подальшому здійснюється визначення величини уразливості ІС під час проведення заходів з модернізації та оцінювання ефективності системи функціональної безпеки ІС на стадії модернізації. Результатом є отримання оцінки ефективності проведених заходів, яка використовується власником системи для прийняття рішення стосовно проведення модернізації та визначення організаційних заходів щодо особливості проведення самого процесу оновлення складових ІС.

2. Розроблена математична модель інформаційних потоків ІС на стадії модернізації та метод визначення раціональної послідовності модернізації елементів інформаційних систем, що дозволило раціоналізувати процес модернізації елементів інформаційних систем довільної структури за обраною стратегією модернізації. Використання розробленого методу дозволило зменшити ймовірність порушення властивостей ІС за обраною стратегією модернізації до восьми разів від максимального та до трьох разів від середнього значення.

3. Розроблені моделі каналу інформаційного дестабілізаційного впливу і функціональної захищеності ІС та метод розподілу засобів забезпечення функціональної безпеки інформаційних систем на стадії модернізації, що дозволило забезпечити нормативний рівень функціональної безпеки системи в цілому.

4. Сформований метод оцінювання уразливості ІС в інтегрованій інформаційній системі на стадії модернізації на базі розроблених аналітичних моделей порушення властивостей ІС, що дозволило визначити інтегральну величину уразливості ІС. Розроблений метод враховує фактори, викликані процесом модернізації інформаційної системи та до двох разів підвищує точність порівняно з наявними методами.

5. Розроблено комплекс методів узгодження систем розмежування доступу в інформаційних системах на стадії модернізації, сформульовані та доказані базові теореми безпеки. Зазначена сукупність методів дозволила сформувати їх методологічний базис. У межах методології розроблена методика оцінювання ефективності узгодження систем розмежування доступу у разі наявності недозволених інформаційних потоків. Проведене оцінювання на прикладі взаємодії двох ІС у складі інтегрованої інформаційної системи "Гарт-1" та "Гарт-5" показало ймовірність порушення хоча б одного елемента даних під час модернізації на рівні до 0,0003.

6. Розроблена модель ІДФ на стадії модернізації та метод оцінювання ефективності забезпечення функціональної безпеки інформаційних систем на стадії модернізації дозволив визначити ймовірність виконання системою функціональних завдань в умовах впливу як зовнішніх, так і внутрішніх дестабілізаційних факторів.

7. Розроблено інформаційну технологію забезпечення функціональної безпеки інтегрованої інформаційної системи на стадії модернізації, що дозволить здійснювати поетапне вдосконалення інформаційних систем реального часу критичного застосування. Розроблена інформаційна

технологія дозволила забезпечити нормативний рівень порушення функціональної безпеки під час модернізації ІС "Гарт-1/П" на рівні до 0,005.

8. Розроблений програмний комплекс, що базується на створених технології, методах та моделях, дозволив підвищити до трьох разів оперативність формування практичних рекомендацій із адаптації засобів забезпечення функціональної безпеки інформаційних систем на стадії модернізації.

ДОДАТКИ

А – Взаємозв’язок інформаційного ресурсу з функціями прикордонного відомства та складовими національної безпеки України

Б – Функціональна структура відомчої інтранет мережі та її інформаційні потоки

В – Визначення параметрів швидкості здійснення модернізації складових інформаційної системи "Гарт-1"

Г – Експертне оцінювання ступеня впливу дестабілізаційних факторів на стадії модернізації експериментального програмно-технічного комплексу автоматизації прикордонної служби

Д – Максимальні значення ймовірностей порушення властивостей ПТК АПС при різних варіантах модернізації

Е – Код програми для розрахунку раціональної послідовності модернізації елементів інформаційних систем

Ж – Організаційна структура ДПСУ

И – Код програми для розрахунку ефективності спільного функціонування обох версій системи розмежування доступу

К – Формування функцій розподілу для загроз складовим інформаційного ресурсу в експериментальному програмно–технічному комплексі АПС "Гарт-3/П"

Л – Експертне оцінювання ступеня взаємного впливу ймовірностей порушення властивостей інформаційного ресурсу

М – Пошук щільності розподілу випадкового вектору множини допустимих значень показника якості функціонування системи функціональної безпеки

Н – Код програми визначення значень ймовірності порушення властивостей інформаційного ресурсу на експериментальному програмно-технічному комплексі автоматизації прикордонного контролю "Гарт-3/П"

П – Результати обчислень значень ймовірності порушення властивостей інформаційного ресурсу на експериментальному програмно-технічному комплексі автоматизації прикордонного контролю "Гарт-3/П"

Р – Список публікацій за темою дисертації та відомості про апробацію результатів дисертації

С – Акти впровадження та реалізації результатів наукових досліджень

ДОДАТОК А

Взаємозв’язок інформаційного ресурсу з функціями прикордонного відомства та складовими національної безпеки України

Таблиця А.1 – Взаємозв’язок впроваджених підсистем, інформаційних та інформаційно-комунікаційних систем з основними функціями ДПСУ

№ з/п	Основні функції ДПСУ	Складові інформаційного ресурсу
1.	Охорона державного кордону України на суші, морі, річках, озерах та інших водоймах з метою недопущення незаконної зміни проходження його лінії, забезпечення дотримання режиму державного кордону та прикордонного режиму	Інформаційнні системи: оперативно-чергової служби "Гарт-2"; прикордонної служби "Гарт-3"; інформаційно-аналітичної служби "Гарт-5"; контролю та висвітлення обстановки "Гарт-14"; Підсистеми: центральне сховище даних; "Ризик"; "Порушник"; Аналіз та профілювання ризиків; "Патруль"; Оперативні повідомлення
2.	Здійснення в установленому порядку прикордонного контролю і пропуску через державний кордон України осіб, транспортних засобів, вантажів, а також виявлення і припинення випадків незаконного їх переміщення	Інформаційні системи: прикордонного контролю "Гарт-1"; інформаційно-аналітичної служби "Гарт-5"; Підсистеми: центральне сховище даних; "Ризик"; "Аркан" Аналіз та профілювання ризиків
3.	Охорона суверенних прав України в її виключній (морській) економічній зоні та контроль за реалізацією прав і виконанням зобов'язань у цій	Інформаційні системи: морської охорони "Гарт-12"; Підсистеми: центральне сховище даних

№ з/п	Основні функції ДПСУ	Складові інформаційного ресурсу
	зоні інших держав, українських та іноземних юридичних і фізичних осіб, міжнародних організацій	
4.	Ведення розвідувальної, інформаційно-аналітичної та оперативно-розшукової діяльності в інтересах забезпечення захисту державного кордону України згідно із законами України "Про розвідувальні органи України" та "Про оперативно-розшукову діяльність"	Інформаційні системи: інформаційно-аналітичної служби "Гарт-5"; оперативно-розшукової діяльності "Гарт-10"; Підсистеми: центральне сховище даних; "Ризик"; Аналіз та профілювання ризиків
5.	Участь у боротьбі з організованою злочинністю та протидія незаконній міграції на державному кордоні України та в межах контрольованих прикордонних районів	Інформаційні системи: оперативно-чергової служби "Гарт-2"; інформаційно-аналітичної служби "Гарт-5"; контролю та висвітлення обстановки "Гарт-14"; Підсистеми: центральне сховище даних; "Ризик"; "Порушник"; Аналіз та профілювання ризиків; "Патруль"; Оперативні повідомлення
6.	Участь у здійсненні державної охорони місць постійного і тимчасового перебування Президента України та посадових осіб, визначених у Законі України "Про державну	Забезпечення підготовки персоналу за допомогою ТІС професійної підготовки "Гарт-8"

№ з/п	Основні функції ДПСУ	Складові інформаційного ресурсу
	охорону органів державної влади України та посадових осіб"	
7.	Охорона закордонних дипломатичних установ України	Забезпечення підготовки персоналу за допомогою ТІС професійної підготовки "Гарт-8"
8.	Координація діяльності військових формувань та відповідних правоохоронних органів, пов'язаної із захистом державного кордону України, а також діяльності державних органів, що здійснюють різні види контролю при перетинанні державного кордону України або беруть участь у забезпеченні режиму державного кордону, прикордонного режиму і режиму в пунктах пропуску через державний кордон України	Інтегрована міжвідомча інформаційно-телекомунікаційна система "Аркан"

Таблиця А.2 - Взаємозалежність завдань ДПСУ із загрозами національної безпеки у прикордонній сфері

№ з/п	Основні реальні та потенційні загроз національній безпеці України	№ з/п (табл. Б.1) основних завдань ДПСУ
1	**Зовнішньополітична сфера**	
1.1	Посягання на державний суверенітет України та її територіальну цілісність, територіальні претензії з боку інших держав	1, 4
1.2	Спроби втручання у внутрішні справи України з боку інших держав	4, 7, 8
1.3	Воєнно-політична нестабільність, регіональні та локальні війни (конфлікти) в різних регіонах світу, насамперед поблизу кордонів України	1-5, 8
2	**Сфера державної безпеки**	
2.1	Розвідувально-підривна діяльність іноземних спеціальних служб	4
2.2	Загроза посягань з боку окремих груп та осіб на державний суверенітет, територіальну цілісність, економічний, науково-технічний і оборонний потенціал України, права і свободи громадян	1-4, 8
2.3	Поширення корупції, хабарництва в органах державної влади, зрощення бізнесу і політики, організованої злочинної діяльності	4, 5
2.4	Злочинна діяльність проти миру і безпеки людства, насамперед поширення міжнародного тероризму	4, 8
2.5	Загроза використання з терористичною метою ядерних та інших об'єктів на території України	2, 8

№ з/п	Основні реальні та потенційні загроз національній безпеці України	№ з/п (табл. Б.1) основних завдань ДПСУ
2.6	Можливість незаконного ввезення в країну зброї, боєприпасів, вибухових речовин і засобів масового ураження, радіоактивних і наркотичних засобів	2, 8
2.7	Спроби створення і функціонування незаконних воєнізованих збройних формувань та намагання використати в інтересах певних сил діяльність військових формувань і правоохоронних органів держави	4
2.8	прояви сепаратизму, намагання автономізації за етнічною ознакою окремих регіонів України	1, 8
3	**Воєнна сфера та сфера безпеки державного кордону України**	
3.1	Поширення зброї масового ураження і засобів її доставки	2, 8
3.2	Недостатня ефективність існуючих структур і механізмів забезпечення міжнародної безпеки та глобальної стабільності	-
3.3	Нелегальна міграція	2, 4, 5, 8
3.4	Можливість втягування України в регіональні збройні конфлікти чи у протистояння з іншими державами	4, 8
3.5	Нарощування іншими державами поблизу кордонів України угруповань військ та озброєнь, які порушують співвідношення сил, що склалося	4
3.6	Небезпечне зниження рівня забезпечення військовою та спеціальною технікою та озброєнням нового покоління Збройних Сил України, інших військових формувань, що загрожує зниженням їх боєздатності	-

№ з/п	Основні реальні та потенційні загроз національній безпеці України	№ з/п (табл. Б.1) основних завдань ДПСУ
3.7	Повільність у здійсненні та недостатнє фінансове забезпечення програм реформування Воєнної організації та оборонно-промислового комплексу України	-
3.8	Накопичення великої кількості застарілої та не потрібної для Збройних Сил України військової техніки, озброєння, вибухових речовин	-
3.9	Незавершеність договірно-правового оформлення і недостатнє облаштування державного кордону України	1
3.10	Незадовільний рівень соціального захисту військовослужбовців, громадян, звільнених з військової служби, та членів їхніх сімей	-
4	**Внутрішньополітична сфера**	
4.1	Порушення з боку органів державної влади та органів місцевого самоврядування Конституції і законів України, прав і свобод людини і громадянина, в тому числі при проведенні виборчих кампаній, недостатня ефективність контролю за дотриманням вимог Конституції і виконання законів України	-
4.2	Можливість виникнення конфліктів у сфері міжетнічних і міжконфесійних відносин, радикалізації та проявів екстремізму в діяльності деяких об'єднань національних меншин та релігійних громад	4, 8
4.3	Загроза проявів сепаратизму в окремих регіонах України	1, 4, 8

№ з/п	Основні реальні та потенційні загроз національній безпеці України	№ з/п (табл. Б.1) основних завдань ДПСУ
4.4	Структурна та функціональна незбалансованість політичної системи суспільства, нездатність окремих її ланок до оперативного реагування на загрози національній безпеці	-
5	**Економічна сфера**	
5.1	Істотне скорочення внутрішнього валового продукту, зниження інвестиційної та інноваційної активності і науково-технічного та технологічного потенціалу, скорочення досліджень на стратегічно важливих напрямах інноваційного розвитку	-
5.2	Ослаблення системи державного регулювання і контролю у сфері економіки	-
5.3	Нестабільність у правовому регулюванні відносин у сфері економіки, в тому числі фінансової (фіскальної) політики держави; відсутність ефективної програми запобігання фінансовим кризам; зростання кредитних ризиків	-
5.4	Критичний стан основних виробничих фондів у провідних галузях промисловості, агропромисловому комплексі, системах життєзабезпечення; загострення проблеми підтримання в належному технічному стані ядерних об'єктів на території України	-
5.5	Недостатні темпи відтворювальних процесів та подолання структурної деформації в економіці	-
5.6	Критична залежність національної економіки від кон'юнктури зовнішніх ринків, низькі темпи розширення внутрішнього ринку	-

№ з/п	Основні реальні та потенційні загроз національній безпеці України	№ з/п (табл. Б.1) основних завдань ДПСУ
5.7	Нераціональна структура експорту з переважно сировинним характером та низькою питомою вагою продукції з високою часткою доданої вартості	-
5.8	Велика боргова залежність держави, критичні обсяги державних зовнішнього і внутрішнього боргів	-
5.9	Небезпечне для економічної незалежності України зростання частки іноземного капіталу у стратегічних галузях економіки	-
5.10	Неефективність антимонопольної політики та механізмів державного регулювання природних монополій, що ускладнює створення конкурентного середовища в економіці	-
5.11	Критичний стан з продовольчим забезпеченням населення	-
5.12	Неефективність використання паливно-енергетичних ресурсів, недостатні темпи диверсифікації джерел їх постачання та відсутність активної політики енергозбереження, що створює загрозу енергетичній безпеці держави	-
5.13	"Тінізація" національної економіки	-
5.14	Переважання в діяльності управлінських структур особистих, корпоративних, регіональних інтересів над загальнонаціональними	-
6	**Соціальна та гуманітарна сфера**	
6.1	Невідповідність програм реформування економіки країни і результатів їх здійснення визначеним соціальним пріоритетам	-

№ з/п	Основні реальні та потенційні загроз національній безпеці України	№ з/п (табл. Б.1) основних завдань ДПСУ
6.2	Неефективність державної політики щодо підвищення трудових доходів громадян, подолання бідності та збалансування продуктивної зайнятості працездатного населення	-
6.3	Криза системи охорони здоров'я і соціального захисту населення і, як наслідок, небезпечне погіршення стану здоров'я населення; поширення наркоманії, алкоголізму, соціальних хвороб	-
6.4	Загострення демографічної кризи;	-
6.5	Зниження можливостей здобуття якісної освіти представниками бідних прошарків суспільства	-
6.6	Прояви моральної та духовної деградації суспільства	-
6.7	Зростання дитячої та підліткової бездоглядності, безпритульності, бродяжництва	-
7	**Науково-технологічна сфера**	
7.1	Наростаюче науково-технологічне відставання України від розвинутих країн	-
7.2	Неефективність державної інноваційної політики, механізмів стимулювання інноваційної діяльності	-
7.3	Низька конкурентоспроможність продукції	-
7.4	Нерозвиненість внутрішнього ринку високотехнологічної продукції та відсутність його ефективного захисту від іноземної технічної і технологічної експансії	-

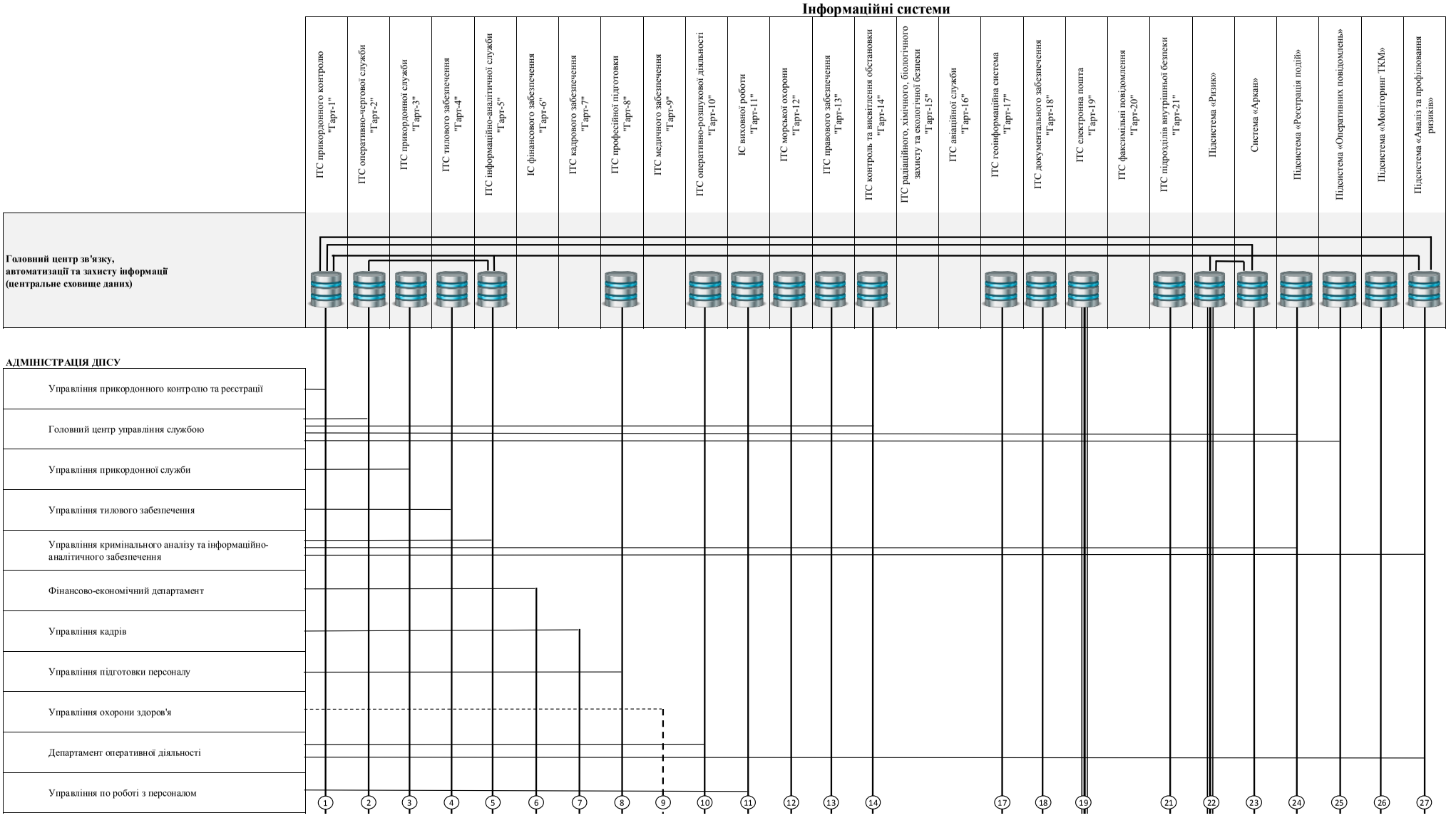
№ з/п	Основні реальні та потенційні загроз національній безпеці України	№ з/п (табл. Б.1) основних завдань ДПСУ
7.5	Зниження внутрішнього попиту на підготовку науково-технічних кадрів для наукових, конструкторських, технологічних установ та високотехнологічних підприємств, незадовільний рівень оплати науково-технічної праці, падіння її престижу, недосконаліть механізмів захисту прав інтелектуальної власності	-
7.6	Відплив учених, фахівців, кваліфікованої робочої сили за межі України	-
8	**Екологічна сфера**	
8.1	Значне антропогенне порушення і техногенна перевантаженість території України, зростання ризиків виникнення надзвичайних ситуацій техногенного та природного характерів	4
8.2	Нераціональне, виснажливе використання мінерально-сировинних природних ресурсів як невідновлюваних, так і відновлюваних	-
8.3	Неподоланність негативних соціально-екологічних наслідків Чорнобильської катастрофи	-
8.4	Погіршення екологічного стану водних басейнів, загострення проблеми транскордонних забруднень та зниження якості води	-
8.5	Загострення техногенного стану гідротехнічних споруд каскаду водосховищ на р. Дніпро	-

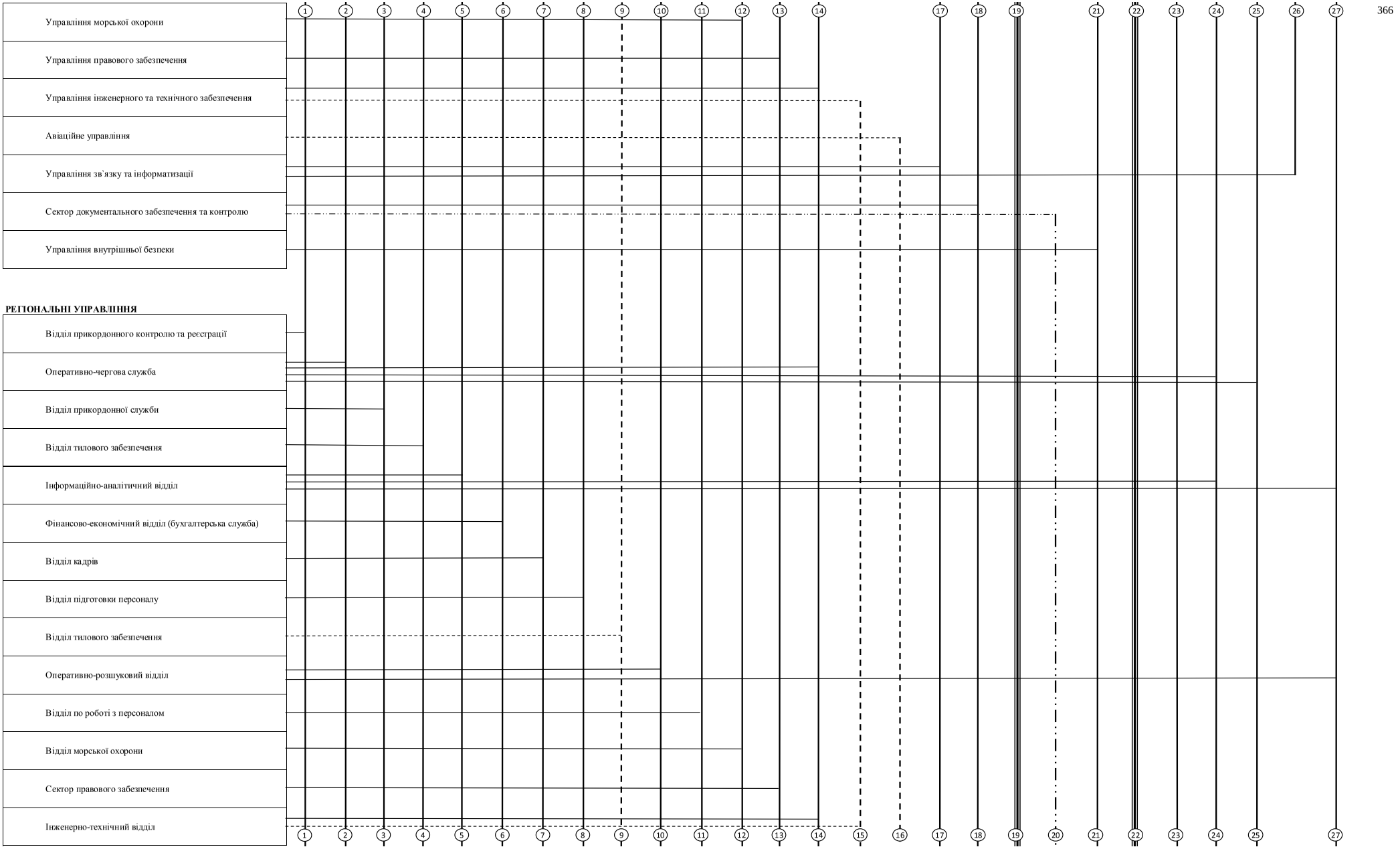
№ з/п	Основні реальні та потенційні загроз національній безпеці України	№ з/п (табл. Б.1) основних завдань ДПСУ
8.6	неконтрольоване ввезення в Україну екологічно небезпечних технологій, речовин, матеріалів і трансгенних рослин, збудників хвороб, небезпечних для людей, тварин, рослин і організмів, екологічно необґрунтоване використання генетично змінених рослин, організмів, речовин та похідних продуктів	2, 4, 8
8.7	Неефективність заходів щодо подолання негативних наслідків військової та іншої екологічно небезпечної діяльності	-
8.8	Небезпека техногенного, у тому числі ядерного та біологічного, тероризму	2, 4, 5, 8
8.9	Посилення впливу шкідливих генетичних ефектів у популяціях живих організмів, зокрема генетично змінених організмів, та біотехнологій	-
8.10	Застарілість та недостатня ефективність комплексів з утилізації токсичних і екологічно небезпечних відходів	-
9	**Інформаційна сфера**	
9.1	Прояви обмеження свободи слова та доступу громадян до інформації	-
9.2	Поширення засобами масової інформації культу насильства, жорстокості, порнографії	-
9.3	Комп'ютерна злочинність та комп'ютерний тероризм	4, 8
9.4	Розголошення інформації, яка становить державну та іншу, передбачену законом, таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави	2-8

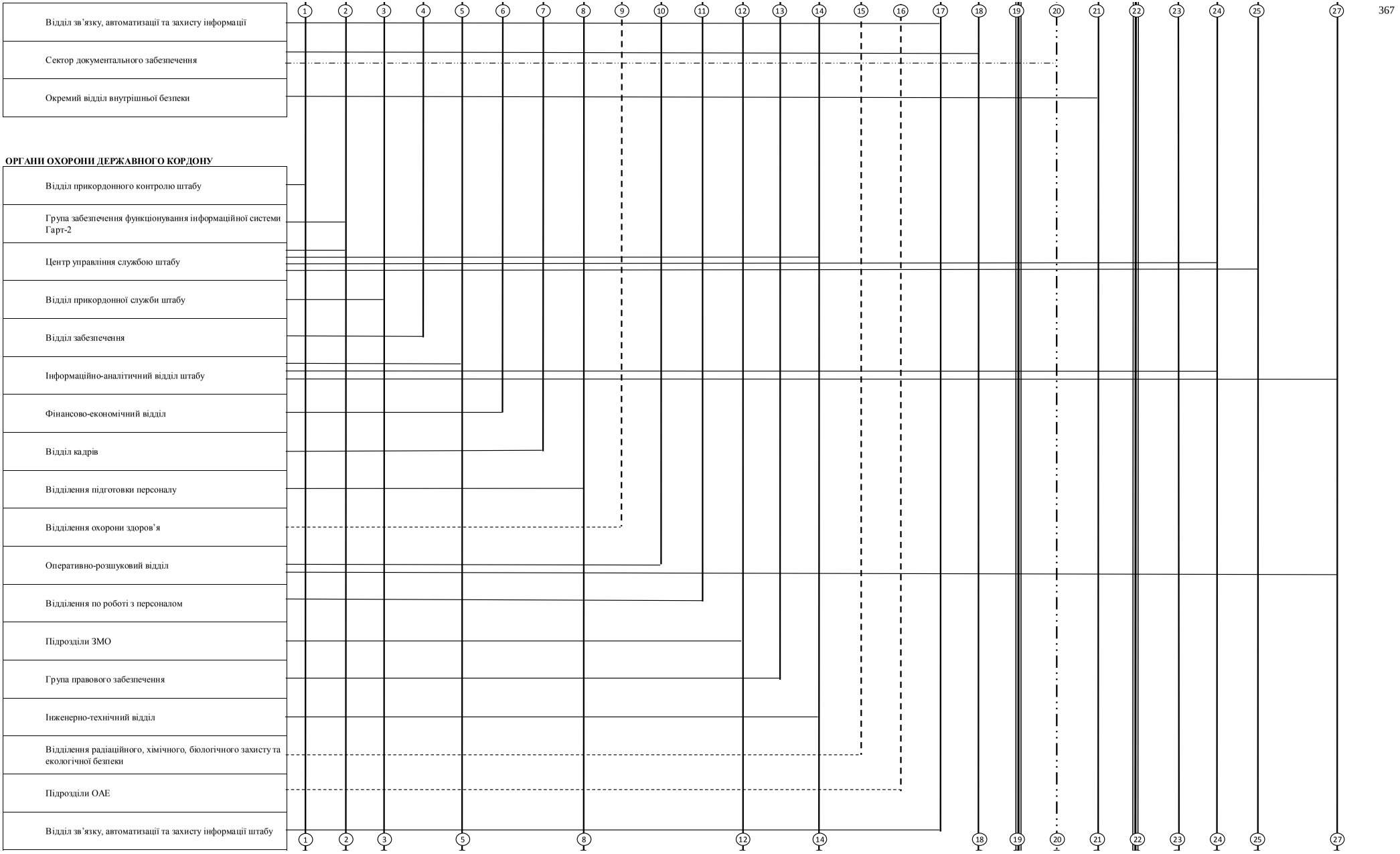
№ з/п	Основні реальні та потенційні загроз національній безпеці України	№ з/п (табл. Б.1) основних завдань ДПСУ
9.5	Намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації	-

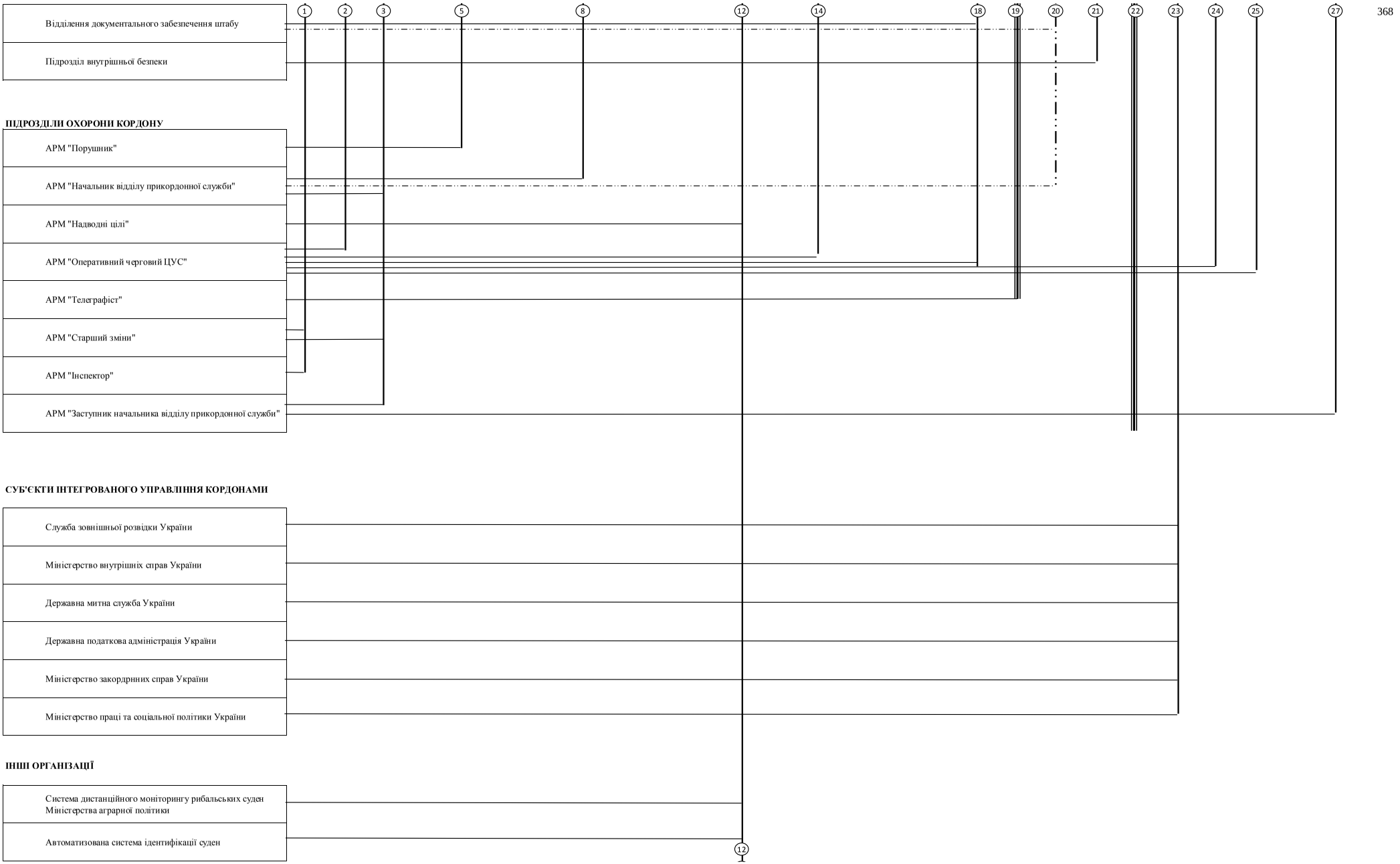
ДОДАТОК Б

Функціональна структура відомчої інтранет мережі та її інформаційні потоки




Управління морської охорони
Управління правового забезпечення
Управління інженерного та технічного забезпечення
Авіаційне управління
Управління зв'язку та інформатизації
Сектор документального забезпечення та контролю
Управління внутрішньої безпеки
РЕГІОНАЛЬНІ УПРАВЛІННЯ
Відділ прикордонного контролю та реєстрації
Оперативно-чергова служба
Відділ прикордонної служби
Відділ тилового забезпечення
Інформаційно-аналітичний відділ
Фінансово-економічний відділ (бухгалтерська служба)
Відділ кадрів
Відділ підготовки персоналу
Відділ тилового забезпечення
Оперативно-розшуковий відділ
Відділ по роботі з персоналом
Відділ морської охорони
Сектор правового забезпечення
Інженерно-технічний відділ
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27


Відділ зв'язку, автоматизації та захисту інформації
Сектор документального забезпечення
Окремий відділ внутрішньої безпеки
ОРГАНИ ОХОРОНИ ДЕРЖАВНОГО КОРДОНУ
Відділ прикордонного контролю штабу
Група забезпечення функціонування інформаційної системи Гарт-2
Центр управління службою штабу
Відділ прикордонної служби штабу
Відділ забезпечення
Інформаційно-аналітичний відділ штабу
Фінансово-економічний відділ
Відділ кадрів
Відділення підготовки персоналу
Відділення охорони здоров'я
Оперативно-розшуковий відділ
Відділення по роботі з персоналом
Підрозділи ЗМО
Група правового забезпечення
Інженерно-технічний відділ
Відділення радіаційного, хімічного, біологічного захисту та екологічної безпеки
Підрозділи ОАЕ
Відділ зв'язку, автоматизації та захисту інформації штабу
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 27
1 2 3 5 8 12 14 18 19 20 21 22 23 24 25 27


Відділення документального забезпечення штабу
Підрозділ внутрішньої безпеки
ПІДРОЗДІЛИ ОХОРОНИ КОРДОНУ
АРМ "Порушник"
АРМ "Начальник відділу прикордонної служби"
АРМ "Надводні цілі"
АРМ "Оперативний черговий ЦУС"
АРМ "Телеграфіст"
АРМ "Старший зміни"
АРМ "Інспектор"
АРМ "Заступник начальника відділу прикордонної служби"
СУБ'ЄКТИ ІНТЕГРОВАНОГО УПРАВЛІННЯ КОРДОНАМИ
Служба зовнішньої розвідки України
Міністерство внутрішніх справ України
Державна митна служба України
Державна податкова адміністрація України
Міністерство закордрнних справ України
Міністерство праці та соціальної політики України
ІНШІ ОРГАНІЗАЦІЇ
Система дистанційного моніторингу рибальських суден Міністерства аграрної політики
Автоматизована система ідентифікації суден
1
2
3
5
8
12
14
18
19
20
21
22
23
24
25
27
12

Примітки

інформаційні потоки

плануються до введення

при наявності доступу

резервний інформаційний потік

ДОДАТОК В

Визначення параметрів швидкості здійснення модернізації складових інформаційної системи "Гарт-1"

Для визначення параметрів швидкості здійснення модернізації проведено збір статистичних даних з органів охорони державного кордону при здійсненні модернізації ІС "Гарт-1/П", результати якої зведено в таблицю В.1. Відповідно керівних документів на проведення модернізації було визначено 24 години.

Таблиця В.1 – Зведені дані щодо модернізації ІС "Гарт-1"

ООДК	Відсоток модернізованих автоматизованих робочих місць за годинами (від початку модернізації)																							
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Львівський прикордонний загін	18	39	53	62	71	80	84	87	90	93	94	95	97	97	98	99	99	99	99	100	100	100	100	100
Мостиський прикордонний загін	13	27	53	64	72	78	83	86	89	93	94	96	97	97	98	99	99	99	99	100	100	100	100	100
Мукачівський прикордонний загін	15	39	53	66	73	79	84	88	91	93	94	96	97	98	98	99	99	99	99	100	100	100	100	100
Чопський прикордонний загін	8	31	31	54	66	75	85	87	89	91	94	95	96	97	97	98	99	99	99	99	99	100	100	100
Чернівецький прикордонний загін	12	42	56	66	74	80	85	88	91	93	95	96	97	98	98	99	99	99	99	100	100	100	100	100
Чернігівський прикордонний загін	5	15	55	62	64	75	80	86	88	90	94	94	96	97	98	98	99	99	99	99	100	100	100	100

Продовження таблиці В.1

ООДК	Відсоток модернізованих автоматизованих робочих місць за годинами (від початку модернізації)																							
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Житомирський прикордонний загін	21	30	30	55	74	80	82	84	84	92	94	95	97	98	98	99	99	99	99	100	100	100	100	100
Луцький прикордонний загін	6	11	22	53	74	78	79	82	90	92	93	95	96	96	98	98	99	99	99	100	100	100	100	100
Середнє значення	12,2	29,2	44,1	60,2	71	78,1	82,7	86	89	92,1	94	95,2	96,6	97,2	97,8	98,6	99	99	99	99,7	99,8	100	100	100
Відсоток немодернізованих АРМ	87,8	70,8	55,9	39,8	29	21,9	17,3	14	11	7,9	6	4,8	3,4	2,8	2,2	1,4	1	1	1	0,3	0,2	0	0	0

Відповідно результатів зведеної таблиці, кількість модернізованих автоматизованих робочих місць наведена у відсотках. Разом із тим, величина залишку немодернізованих елементів в кінці періоду модернізації становить нулю. На підставі вищенаведеного можна зробити висновок про числові значення функції швидкості здійснення модернізації складових ІТС "Гарт-1", а саме: $a_k = 1, b_k = 0$.

Для визначення числового значення параметру w використаємо метод найменших квадратів:

$$\sum_{i=1}^{24} \left(x_i - e^{-wi} \right)^2 \to min$$

де: x_i – частка немодернізованих АРМ

Для обчислення значень скористаємось відомими програмними пакетами пошуку рішень, результат роботи яких зведено в таблицю В.2.

Таблиця В.1 – Результати обчислень параметру w

№ з/п	Параметр x_i	Параметр e^{-wi}	$\left(a_i - e^{-wi}\right)^2$
1	0,8775	0,794023	0,006968
2	0,7075	0,630473	0,005933
3	0,55875	0,50061	0,00338
4	0,3975	0,397496	1,63E-11
5	0,29	0,315621	0,000656
6	0,21875	0,25061	0,001015
7	0,1725	0,19899	0,000702
8	0,14	0,158003	0,000324
9	0,11	0,125458	0,000239
10	0,07875	0,099617	0,000435
11	0,06	0,079098	0,000365
12	0,0475	0,062806	0,000234
13	0,03375	0,049869	0,00026
14	0,0275	0,039597	0,000146

Продовження таблиці В.1

№ з/п	Параметр x_i	Параметр e^{-wi}	$\left(a_i - e^{-wi}\right)^2$
15	0,02125	0,031441	0,000104
16	0,01375	0,024965	0,000126
17	0,01	0,019823	9,65E-05
18	0,01	0,01574	3,29E-05
19	0,01	0,012498	6,24E-06
20	0,0025	0,009923	5,51E-05
21	0,00125	0,007879	4,39E-05
22	0	0,006256	3,91E-05
23	0	0,004968	2,47E-05
24	0	0,003945	1,56E-05
			Сума: 0,021202

За результатами чисельних методів пошуку параметра w його значення становить -0,23 од/год. Графічне відображення наведено на рисунку В.1

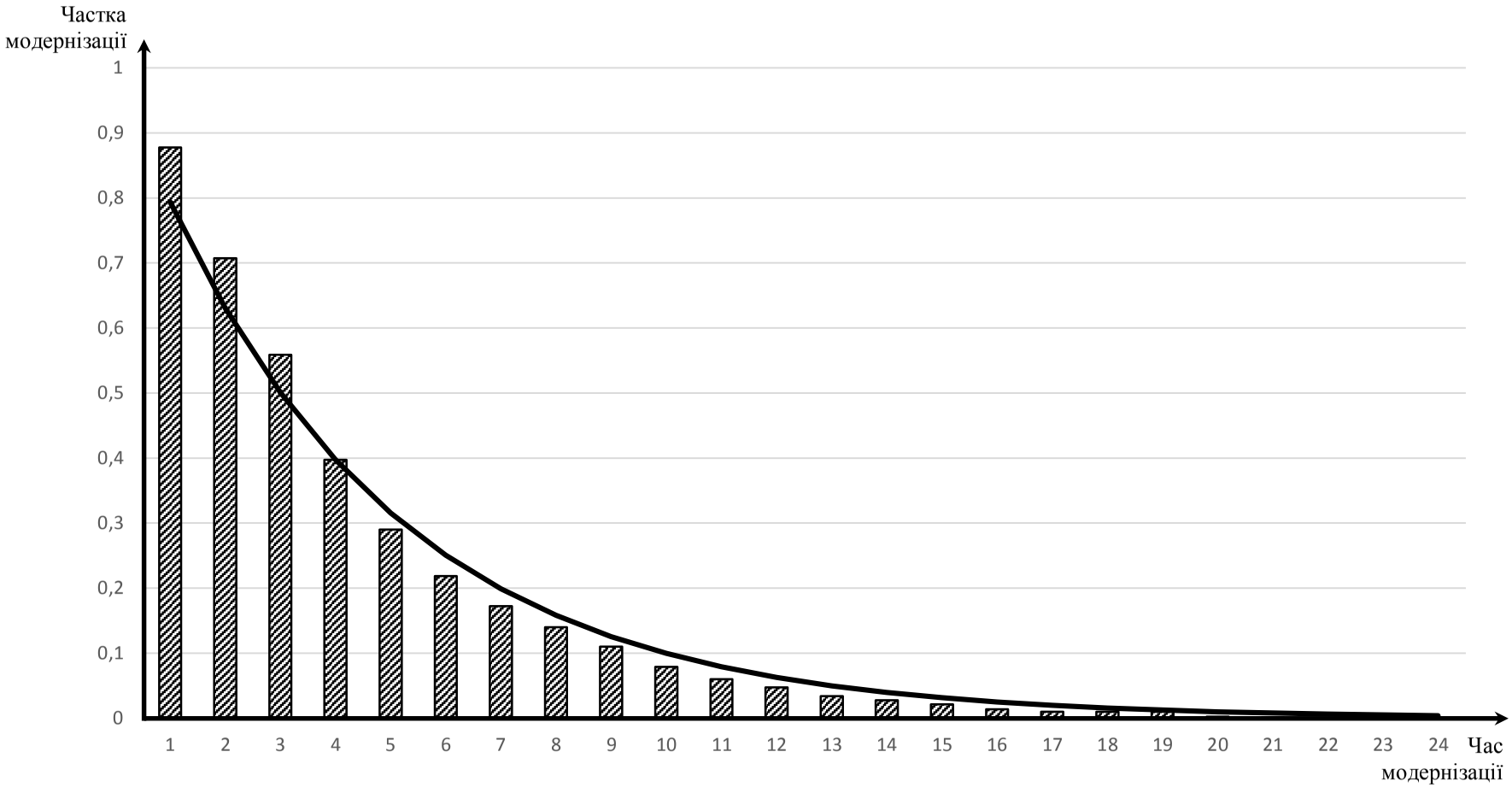


Рисунок В.1 – Експериментальні та теоретичні значення швидкості модернізації елементів ІС "Гарт-1"

ДОДАТОК Г

Експертне оцінювання ступеня впливу дестабілізаційних факторів на стадії модернізації експериментального програмно-технічного комплексу автоматизації прикордонної служби

Таблиця Г.1 – Структура анкети для проведення експертизи

Вкажіть кваліфікаційний індекс _____									
№ з/п	**Вид загрози**	**Властивість інф. ресурсу**				**Вплив процесу модернізації**			
		к	**ц**	**д**	**с**	**к**	**ц**	**д**	**с**
1.	Доступ до даних з порушенням політики безпеки								
2.	Модифікація спеціального та системного програмного забезпечення								
3.	Порушення режимів функціонування систем життєзабезпечення ІС або її складових.								
4.	Впровадження і використання шкідливого програмного забезпечення								
5.	Отримання захищених даних за допомогою санкціонованих запитів в обхід політики безпеки								
6.	Неправомірне підключення до каналів зв’язку, перехоплення даних, що передаються, зміна (модифікація) інформації повідомлень								
7.	Несанкціоноване копіювання носіїв інформації								
8.	Крадіжки носіїв інформації								
9.	Фальсифікація (приховування) фактів формування та видачі даних								

Продовження таблиці Г.1

№ з/п	Вид загрози	Властивість інф. ресурсу				Вплив процесу модернізації			
		к	ц	д	с	к	ц	д	с
10.	Виконання аналізу потоку даних (трафіку)								
11.	Переривання передачі потоку даних								
12.	Порушення фізичної цілісності ІС (її окремих компонентів).								
13.	Дії, що призводять до відмови ІС чи окремих її елементів, руйнування окремих складових обчислювальних систем та іншого обладнання (телекомунікаційного, засобів вводу/ виводу, тощо)								
14.	Ненавмисне пошкодження носіїв інформації								
15.	Неправомірна зміна режимів роботи СПЗ або загального ПЗ, яке призводить до незворотного знищення інформації на носіях ІС								
16.	Невмисне зараження програмних засобів комп’ютерними вірусами								
17.	Невиконання організаційних заходів щодо порядку і правил експлуатації чи використання ресурсів ІС, передбачених керівними документами, посадовими та технологічними інструкціями.								
18.	Використання персоналу ІС корисливою метою								
19.	Помилки при введені даних в систему								
20.	Некомпетентне застосування засобів забезпечення функціональної безпеки								
21.	Помилки при розробці або модернізації ІІС та її складових								
22.	Зміна умов фізичного середовища								
23.	Збої та відмови у роботі ІС, аварійне відключення живлення та інше.								
24.	Впливи природних та технологічних завад (грозові розряди, електрозварювальні роботи, тощо).								

Таблиця Г.2 – Зведені результати експертного оцінювання за властивістю "конфіденційність"

№ загрози	Експерт																					Сер. зважене	$\tilde{\sigma}$	ε
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21			
1	1	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0,92	0,28	0,12
2	0	0	1	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0,11	0,31	0,13
3	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,05	0,22	0,10
4	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	4	3	3	3	3,04	0,19	0,08
5	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	1	1	1	1	1,04	0,20	0,09
6	3	3	3	3	3	3	3	3	3	3	3	4	3	3	3	3	3	3	3	3	3	3,05	0,22	0,09
7	3	2	3	3	2	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	2,89	0,32	0,14
8	2	2	2	2	2	3	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2,05	0,22	0,10
9	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0,05	0,22	0,09
10	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,06	0,23	0,10
11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,00	0,00	0,00
12	3	3	2	3	3	3	3	3	3	3	3	3	3	3	4	3	3	3	3	3	3	2,99	0,32	0,14
13	2	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1,00	0,34	0,15
14	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0,13	0,34	0,14
15	1	1	1	2	1	1	1	1	1	1	1	0	1	2	1	1	1	1	1	1	1	1,05	0,39	0,17
16	4	3	3	2	3	4	3	3	3	3	3	4	3	3	2	3	3	3	3	3	3	3,06	0,51	0,22
17	2	2	2	2	2	2	2	2	2	2	2	2	1	2	2	2	2	2	2	2	2	1,95	0,22	0,09
18	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1,00	0,00	0,00
19	2	1	2	2	2	2	2	2	2	2	2	2	1	2	2	2	2	2	2	2	2	1,89	0,31	0,13
20	1	1	0	1	1	1	1	1	1	1	1	1	2	1	1	1	1	1	1	1	1	0,99	0,33	0,14
21	1	2	1	1	1	1	1	1	1	1	2	1	1	1	0	1	1	1	1	1	1	1,07	0,39	0,17
22	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,00	0,00	0,00
23	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0,11	0,31	0,13
24	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0,10	0,30	0,13

Таблиця Г.3 – Зведені результати експертного оцінювання за властивістю "цілісність"

№ загрози	Експерт																					Сер. зважене	$\tilde{\sigma}$	ε
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21			
1	1	1	1	1	1	1	1	1	1	2	1	1	1	1	2	1	1	1	1	1	1	1,10	0,30	0,13
2	1	1	0	1	1	1	1	1	1	1	1	1	1	0	2	1	1	1	1	1	1	0,94	0,38	0,16
3	3	3	3	4	3	3	3	3	3	4	3	3	3	4	4	3	3	3	3	3	2	3,18	0,44	0,19
4	2	2	2	2	2	2	2	2	2	2	2	1	2	2	2	2	2	2	2	2	2	1,95	0,22	0,09
5	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	1,02	0,15	0,07
6	2	2	2	2	2	2	2	2	2	2	2	2	1	2	2	2	2	2	2	2	2	1,95	0,22	0,09
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,00	0,00	0,00
8	2	2	2	2	2	2	2	2	2	2	1	2	2	2	2	1	2	2	2	2	2	1,90	0,30	0,13
9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,00	0,00	0,00
10	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	1	0,08	0,27	0,11
11	2	2	2	2	3	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2,05	0,22	0,10
12	3	3	2	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	2,94	0,23	0,10
13	1	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0,94	0,23	0,10
14	2	2	2	2	2	2	2	2	2	2	2	1	2	2	2	1	2	2	2	2	2	1,90	0,30	0,13
15	1	1	1	0	1	1	1	2	1	1	1	1	1	1	1	1	1	1	1	1	2	1,02	0,36	0,16
16	2	2	2	1	2	2	2	3	1	2	2	2	2	2	2	2	2	2	2	2	2	1,94	0,40	0,17
17	2	3	2	2	3	2	2	2	2	2	2	2	2	2	2	2	3	2	2	2	2	2,15	0,36	0,15
18	2	2	2	2	2	1	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	1,95	0,22	0,10
19	2	2	2	2	2	2	2	2	2	2	1	2	2	2	2	2	2	3	2	2	2	1,98	0,30	0,13
20	1	1	1	1	1	2	1	1	1	1	1	1	1	1	1	2	1	1	1	1	1	1,10	0,30	0,13
21	1	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1,06	0,24	0,10
22	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1,00	0,00	0,00
23	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1,00	0,00	0,00
24	1	1	0	1	1	1	1	1	1	1	1	1	2	1	1	1	1	0	1	1	1	0,96	0,37	0,16

Таблиця Г.4 – Зведені результати експертного оцінювання за властивістю "доступність"

№ загрози	Експерт																					Сер. зважене	$\tilde{\sigma}$	ε
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21			
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	1	1	1	1	2	1	0,98	0,27	0,11
2	1	0	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0,89	0,32	0,14
3	2	2	2	2	2	2	2	2	2	2	2	2	2	3	2	1	3	2	2	2	2	2,04	0,37	0,16
4	1	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1	2	1	1	1	1	0,99	0,31	0,13
5	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0,05	0,21	0,09
6	1	1	1	1	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1	0,95	0,21	0,09
7	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0,05	0,22	0,09
8	2	2	2	2	2	2	2	2	2	2	2	2	2	1	2	2	2	2	2	2	2	1,95	0,21	0,09
9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,00	0,00	0,00
10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0,03	0,17	0,07
11	1	2	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1	0	1	1	1	0,97	0,38	0,16
12	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1,00	0,00	0,00
13	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1	1	1	1	0,95	0,22	0,10
14	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	3	2	2	2	2,04	0,19	0,08
15	1	1	1	1	1	1	1	1	2	1	1	1	2	1	1	1	1	1	1	1	1	1,10	0,30	0,13
16	2	2	2	2	2	2	2	2	2	2	2	2	3	1	2	2	2	2	2	3	2	2,03	0,35	0,15
17	2	2	2	2	2	2	2	2	2	3	2	1	2	2	1	2	2	2	2	2	2	1,96	0,39	0,17
18	2	2	2	2	2	2	1	2	2	2	2	2	2	3	2	2	1	2	1	2	2	1,92	0,41	0,17
19	2	2	2	2	2	2	2	1	2	2	2	2	2	2	2	2	2	2	2	2	2	1,95	0,22	0,10
20	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0,98	0,15	0,07
21	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1,00	0,00	0,00
22	1	1	2	1	2	1	2	1	1	1	1	1	1	1	1	1	1	1	2	0	1	1,17	0,43	0,19
23	1	1	1	0	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1	1	1	0,89	0,31	0,13
24	1	1	1	1	1	1	1	1	1	1	1	2	1	1	0	1	1	1	1	1	1	1,00	0,31	0,13

Таблиця Г.5 – Зведені результати експертного оцінювання за властивістю "спостереженість"

№ загрози	Експерт																					Сер. зважене	$\tilde{\sigma}$	ε
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21			
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1,00	0,00	0,00
2	0	1	1	0	1	2	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0,99	0,47	0,20
3	1	2	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1,00	0,34	0,15
4	2	2	2	2	2	2	2	2	2	3	2	2	2	2	2	2	2	2	2	2	2	2,05	0,22	0,10
5	1	1	1	1	1	1	0	1	1	1	2	1	1	1	1	1	1	1	0	1	1	0,97	0,37	0,16
6	1	1	1	1	1	1	1	0	1	1	1	1	2	2	0	1	1	1	1	0	2	1,00	0,50	0,21
7	2	2	2	2	2	2	2	2	2	2	2	2	2	2	1	2	2	2	2	2	2	1,95	0,21	0,09
8	2	2	2	2	2	3	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2,05	0,22	0,10
9	3	2	2	2	2	2	2	2	2	2	2	2	2	2	1	2	2	2	2	2	2	2,01	0,33	0,14
10	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0,98	0,15	0,07
11	1	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0,94	0,24	0,10
12	1	1	1	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1,06	0,23	0,10
13	2	2	2	2	2	2	2	2	1	2	3	2	2	2	2	2	2	2	2	1	2	1,98	0,36	0,15
14	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	1	1	1	1	1,04	0,20	0,09
15	1	1	1	1	1	1	0	1	1	1	1	0	1	1	1	1	1	1	1	1	1	0,90	0,30	0,13
16	1	1	1	1	1	1	1	1	1	1	1	0	1	1	1	0	1	1	1	1	1	0,90	0,30	0,13
17	2	2	2	2	1	2	2	2	2	2	1	2	2	2	2	2	2	2	2	2	1	1,87	0,34	0,14
18	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2,00	0,00	0,00
19	2	2	2	3	2	2	3	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2,11	0,31	0,13
20	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1,00	0,00	0,00
21	1	1	1	1	1	1	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1,05	0,22	0,10
22	1	1	1	2	1	1	1	1	1	1	1	1	1	1	1	1	2	1	1	1	2	1,12	0,33	0,14
23	2	2	2	2	2	2	2	2	3	1	2	2	2	2	2	2	2	2	2	2	2	2,00	0,33	0,14
24	3	3	3	3	3	3	3	3	3	3	3	3	3	4	3	3	3	3	4	3	3	3,08	0,27	0,11

Таблиця Г.6 – Зведені результати експертного оцінювання за властивістю "Вплив процесу модернізації на конфіденційність"

№ загрози	Експерт																					Сер. зважене	$\tilde{\sigma}$	ε
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21			
1	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1	0,95	0,22	0,10
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,00	0,00	0,00
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,00	0,00	0,00
4	1	1	1	1	1	0	0	1	1	1	1	1	1	1	1	0	0	0	1	1	1	0,77	0,42	0,18
5	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1,00	0,00	0,00
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,00	0,00	0,00
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,00	0,00	0,00
8	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,06	0,24	0,10
9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,00	0,00	0,00
10	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1	0	0	0	1	0	0,12	0,33	0,14
11	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,05	0,22	0,10
12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0,04	0,19	0,08
13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0,05	0,21	0,09
14	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1	0	0	0,08	0,27	0,12
15	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1,00	0,00	0,00
16	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1,00	0,00	0,00
17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0,02	0,15	0,07
18	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0,05	0,22	0,09
19	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	0,95	0,21	0,09
20	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,00	0,00	0,00
21	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1,00	0,00	0,00
22	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0,05	0,22	0,10
23	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,12	0,32	0,14
24	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,06	0,23	0,10

Таблиця Г.7 – Зведені результати експертного оцінювання за властивістю "Вплив процесу модернізації на цілісність"

№ загрози	Експерт																					Сер. зважене	$\tilde{\sigma}$	ε
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21			
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1,00	0,00	0,00
2	1	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1	1	1	0,95	0,22	0,10
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,00	0,00	0,00
4	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1,00	0,00	0,00
5	1	1	0	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1	1	1	0,89	0,31	0,13
6	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0	0	0	0	0	0	0	0,10	0,30	0,13
7	0	0	1	0	0	1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0,16	0,36	0,16
8	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,06	0,23	0,10
9	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0,11	0,31	0,13
10	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0,05	0,22	0,09
11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,00	0,00	0,00
12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0,08	0,27	0,11
13	1	0	0	1	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0,22	0,42	0,18
14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,00	0,00	0,00
15	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1	1	0,95	0,22	0,10
16	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1,00	0,00	0,00
17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0,08	0,28	0,12
18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,00	0,00	0,00
19	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	1	1	1	1	0,96	0,20	0,09
20	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,00	0,00	0,00
21	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1,00	0,00	0,00
22	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,00	0,00	0,00
23	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,00	0,00	0,00
24	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0,05	0,22	0,09

Таблиця Г.8 – Зведені результати експертного оцінювання за властивістю "Вплив процесу модернізації на доступність"

№ загрози	Експерт																					Сер. зважене	$\tilde{\sigma}$	ε
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21			
1	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1	1	0	1	1	1	1	0,90	0,30	0,13
2	1	1	1	1	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1	0,95	0,21	0,09
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,00	0,00	0,00
4	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1,00	0,00	0,00
5	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1,00	0,00	0,00
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,00	0,00	0,00
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0,03	0,17	0,07
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,00	0,00	0,00
9	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0,05	0,22	0,09
10	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,05	0,22	0,10
11	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	1	0,08	0,27	0,11
12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0,04	0,20	0,09
13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0,05	0,21	0,09
14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,00	0,00	0,00
15	0	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1	0	1	0,86	0,34	0,15
16	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1,00	0,00	0,00
17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,00	0,00	0,00
18	0	0	1	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0,11	0,31	0,13
19	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	1	1	1	0,96	0,19	0,08
20	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,00	0,00	0,00
21	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1,00	0,00	0,00
22	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1	0,07	0,26	0,11
23	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0,10	0,30	0,13
24	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,00	0,00	0,00

Таблиця Г.9 – Зведені результати експертного оцінювання за властивістю "Вплив процесу модернізації на спостереженість"

№ загрози	Експерт																					Сер. зважене	$\tilde{\sigma}$	ε
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21			
1	1	1	1	1	1	1	0	1	0	1	1	1	1	1	1	1	1	1	1	1	1	0,89	0,31	0,13
2	1	1	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1	0	1	0,93	0,26	0,11
3	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0,05	0,22	0,09
4	1	1	1	1	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1	0,95	0,21	0,09
5	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1	0,95	0,21	0,09
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,00	0,00	0,00
7	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0,05	0,22	0,10
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,00	0,00	0,00
9	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0,05	0,21	0,09
10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,00	0,00	0,00
11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,00	0,00	0,00
12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,00	0,00	0,00
13	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0,05	0,22	0,10
14	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0,08	0,27	0,11
15	1	1	1	1	1	1	1	1	1	0	0	1	1	1	1	1	1	1	1	1	1	0,89	0,31	0,13
16	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1	0,95	0,21	0,09
17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,00	0,00	0,00
18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,00	0,00	0,00
19	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1,00	0,00	0,00
20	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0,05	0,22	0,10
21	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1	0,95	0,22	0,10
22	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,05	0,22	0,10
23	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,00	0,00	0,00
24	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0,05	0,22	0,10

Таблиця Г.10 – Зведені дані щодо визначення ступеня впливу дестабілізуючих факторів на стадії модернізації експериментального програмно-технічного комплексу автоматизації прикордонної служби

№ з/п	Вид загрози	Властивість інф. ресурсу				Вплив процесу модернізації			
		к	ц	д	с	к	ц	д	с
1.	Доступ до даних з порушенням політики безпеки	0,005	0,005	0,005	0,005	+	+	+	+
2.	Модифікація спеціального та системного програмного забезпечення	0	0,005	0,005	0,005	-	+	+	+
3.	Порушення режимів функціонування систем життєзабезпечення ІС або її складових.	0	0,05	0,01	0,005	-	-	-	-
4.	Впровадження і використання шкідливого програмного забезпечення	0,05	0,01	0,005	0,01	+	+	+	+
5.	Отримання захищених даних за допомогою санкціонованих запитів в обхід політики безпеки	0,005	0,005	0	0,005	+	+	+	+
6.	Неправомірне підключення до каналів зв’язку, перехоплення даних, що передаються, зміна (модифікація) інформації повідомлень	0,05	0,01	0,005	0,005	-	-	-	-
7.	Несанкціоноване копіювання носіїв інформації	0,05	0	0	0,01	-	-	-	-
8.	Крадіжки носіїв інформації	0,01	0,01	0,01	0,01	-	-	-	-
9.	Фальсифікація (приховування) фактів формування та видачі даних	0	0	0	0,01	-	-	-	-
10.	Виконання аналізу потоку даних (трафіку)	0	0	0	0,005	-	-	-	-
11.	Переривання передачі потоку даних	0	0,01	0,005	0,005	-	-	-	-
12.	Порушення фізичної цілісності ІС (її окремих компонентів).	0,05	0,05	0,005	0,005	-	-	-	-

13.	Дії, що призводять до відмови ІС чи окремих її елементів, руйнування окремих складових обчислювальних систем та іншого обладнання (телекомунікаційного, засобів вводу/ виводу, тощо)	0,005	0,005	0,005	0,01	-	-	-	-
14.	Ненавмисне пошкодження носіїв інформації	0	0,01	0,01	0,005	-	-	-	-
15.	Неправомірна зміна режимів роботи СПЗ або загального ПЗ, яке призводить до незворотного знищення інформації на носіях ІС	0,005	0,005	0,005	0,005	+	+	+	+
16.	Невмисне зараження програмних засобів комп’ютерними вірусами	0,05	0,01	0,01	0,005	+	+	+	+
17.	Невиконання організаційних заходів щодо порядку і правил експлуатації чи використання ресурсів ІС, передбачених керівними документами, посадовими та технологічними інструкціями.	0,01	0,01	0,01	0,01	-	-	-	-
18.	Використання персоналу ІС корисливою метою	0,005	0,01	0,01	0,01	-	-	-	-
19.	Помилки при введені даних в систему	0,01	0,01	0,01	0,01	+	+	+	+
20.	Некомпетентне застосування засобів забезпечення функціональної безпеки	0,005	0,005	0,005	0,005	-	-	-	-
21.	Помилки при розробці або модернізації ІІС та її складових	0,005	0,005	0,005	0,005	+	+	+	+
22.	Зміна умов фізичного середовища	0	0,005	0,005	0,005	-	-	-	-
23.	Збої та відмови у роботі ІС, аварійне відключення живлення та інше.	0	0,005	0,005	0,01	-	-	-	-
24.	Впливи природних та технологічних завад (грозові розряди, електрозварювальні роботи, тощо).	0	0,005	0,005	0,05	-	-	-	-

Таблиця Г.11 – Зведені результати експертного оцінювання за властивістю "конфіденційність" при застосуванні ЗЗФБ

№ загрози	Експерт																					Сер. зважене	$\tilde{\sigma}$	ε
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21			
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,00	0,00	0,00
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0,04	0,19	0,08
3	0	1	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0,17	0,37	0,16
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,00	0,00	0,00
5	0	1	0	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0,16	0,37	0,16
6	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	2	3	2	3	3	3	2,92	0,28	0,12
7	2	3	3	3	3	3	2	3	3	2	3	3	3	3	2	3	3	3	3	3	3	2,79	0,41	0,18
8	2	2	2	2	2	2	3	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2,05	0,22	0,10
9	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	1	0	0,08	0,27	0,11
10	0	0	0	0	0	0	0	0	1	0	0	1	1	0	0	0	0	0	1	0	0	0,18	0,39	0,17
11	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0,05	0,22	0,10
12	3	3	3	3	3	3	3	3	3	3	4	3	3	3	3	3	3	3	3	3	3	3,05	0,22	0,10
13	1	1	1	2	1	1	1	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1,01	0,31	0,13
14	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0,11	0,31	0,13
15	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0,11	0,31	0,13
16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,00	0,00	0,00
17	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2,00	0,00	0,00
18	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1,06	0,24	0,10
19	1	2	2	2	1	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	1,89	0,32	0,14
20	1	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0,94	0,23	0,10
21	1	1	1	1	1	1	1	1	1	1	2	1	1	1	2	1	2	1	1	1	1	1,14	0,35	0,15
22	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,00	0,00	0,00
23	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0,14	0,35	0,15
24	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,00	0,00	0,00

Таблиця Г.12 – Зведені результати експертного оцінювання за властивістю "цілісність" при застосуванні ЗЗФБ

№ загрози	Експерт																					Сер. зважене	$\tilde{\sigma}$	ε
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21			
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,00	0,00	0,00
2	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,06	0,23	0,10
3	3	4	3	3	3	3	3	4	3	3	3	3	3	4	3	3	3	3	3	3	3	3,16	0,37	0,16
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,00	0,00	0,00
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,00	0,00	0,00
6	2	2	2	2	2	2	2	2	1	2	2	2	2	2	2	2	2	2	2	3	2	1,97	0,28	0,12
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	0	0	0,08	0,27	0,11
8	2	2	2	2	1	2	2	2	2	2	2	2	2	2	2	2	2	1	2	1	2	1,89	0,32	0,14
9	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0,05	0,22	0,09
10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,00	0,00	0,00
11	2	2	2	3	2	2	2	1	2	2	2	2	3	2	2	2	2	2	2	1	2	2,03	0,43	0,18
12	3	3	3	3	3	2	3	3	3	3	3	3	3	3	3	3	3	2	3	3	3	2,91	0,28	0,12
13	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1	0,95	0,22	0,10
14	1	2	2	2	2	2	2	2	2	2	2	2	2	2	2	3	2	2	2	2	2	1,99	0,33	0,14
15	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,00	0,00	0,00
16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,00	0,00	0,00
17	2	3	2	2	2	2	2	3	3	2	2	2	2	3	2	2	2	2	3	2	2	2,24	0,43	0,18
18	3	2	2	2	2	2	2	2	2	1	2	2	2	2	2	2	1	2	2	2	2	1,96	0,39	0,17
19	2	2	2	2	2	2	2	2	2	2	1	2	2	2	2	2	2	2	2	2	2	1,95	0,22	0,10
20	2	1	1	1	1	1	1	1	2	1	1	1	1	1	1	2	1	1	1	1	1	1,16	0,37	0,16
21	1	1	1	1	1	1	1	1	1	1	1	2	1	1	1	1	1	1	1	1	1	1,05	0,22	0,09
22	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1,00	0,00	0,00
23	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	1	1	1	0,96	0,19	0,08
24	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1,00	0,00	0,00

Таблиця Г.13 – Зведені результати експертного оцінювання за властивістю "доступність" при застосуванні ЗЗФБ

№ загрози	Експерт																					Сер. зважене	$\tilde{\sigma}$	ε
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21			
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,00	0,00	0,00
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,00	0,00	0,00
3	2	2	2	2	2	2	3	2	3	2	2	2	2	2	3	2	2	2	2	2	3	2,18	0,38	0,16
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,00	0,00	0,00
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0,02	0,15	0,07
6	0	1	1	1	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1	0,89	0,31	0,13
7	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0,08	0,27	0,12
8	2	2	2	1	2	2	2	1	2	2	2	2	2	2	3	2	2	2	2	2	2	1,94	0,39	0,17
9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,00	0,00	0,00
10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0,02	0,15	0,07
11	1	1	2	1	1	1	1	1	1	1	1	1	2	1	1	1	2	0	1	1	0	1,09	0,45	0,19
12	1	1	1	2	1	1	1	0	1	1	1	1	1	1	0	1	1	1	1	1	1	0,96	0,39	0,17
13	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1,00	0,00	0,00
14	2	2	2	2	1	2	2	2	2	2	2	2	2	2	2	3	2	2	2	2	2	1,99	0,32	0,14
15	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,00	0,00	0,00
16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,00	0,00	0,00
17	2	1	1	2	2	1	3	2	2	2	2	2	2	2	2	2	2	2	2	2	3	1,91	0,49	0,21
18	2	2	2	2	1	2	2	2	2	2	2	2	2	2	1	2	2	2	2	2	2	1,90	0,30	0,13
19	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2,00	0,00	0,00
20	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	1	1	0	1,01	0,24	0,10
21	1	1	1	1	1	1	1	2	1	1	1	1	1	1	1	1	1	1	1	2	1	1,08	0,27	0,11
22	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	1	1	1,03	0,17	0,07
23	1	1	0	0	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0,79	0,41	0,18
24	1	1	1	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0,84	0,37	0,16

Таблиця Г.14 – Зведені результати експертного оцінювання за властивістю "спостереженість" при застосуванні ЗЗФБ

№ загрози	Експерт																					Сер. зважене	$\tilde{\sigma}$	ε
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21			
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,00	0,00	0,00
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,00	0,00	0,00
3	1	1	1	1	0	1	1	1	1	1	1	1	1	2	1	1	1	1	1	1	1	0,99	0,32	0,14
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,00	0,00	0,00
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,00	0,00	0,00
6	1	1	1	1	1	1	1	1	2	1	1	1	1	1	1	1	1	1	1	1	1	1,05	0,22	0,10
7	2	3	2	2	2	2	1	1	2	2	2	2	2	2	2	2	2	2	2	2	2	1,95	0,40	0,17
8	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2,00	0,00	0,00
9	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2,00	0,00	0,00
10	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1	1	0,95	0,22	0,10
11	1	1	1	1	1	1	1	1	1	1	1	2	1	1	0	1	0	1	1	1	2	0,99	0,40	0,17
12	1	1	1	1	0	1	2	1	1	1	1	2	1	1	1	1	1	1	1	1	1	1,05	0,39	0,17
13	2	2	2	2	3	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2,05	0,22	0,10
14	1	1	1	1	1	1	1	1	1	1	1	0	2	1	1	1	1	1	1	1	2	1,02	0,35	0,15
15	1	1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0,17	0,38	0,16
16	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,06	0,23	0,10
17	2	1	2	2	2	1	1	2	1	1	2	1	2	2	2	1	1	2	1	2	2	1,56	0,50	0,21
18	2	2	2	2	2	2	2	1	2	2	2	2	2	2	2	2	2	2	3	3	2	2,00	0,33	0,14
19	2	3	2	2	2	2	2	2	2	2	2	2	2	2	2	3	2	2	2	2	2	2,11	0,31	0,13
20	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	1	1	2	1	1	2	1,01	0,33	0,14
21	1	1	2	1	1	1	1	1	1	1	1	1	1	1	1	2	1	1	1	1	1	1,10	0,30	0,13
22	2	1	2	2	1	1	1	1	2	1	1	1	1	1	1	0	1	1	1	1	1	1,18	0,49	0,21
23	2	2	2	2	2	1	3	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2,00	0,33	0,14
24	3	3	3	3	3	3	3	4	3	4	3	3	3	3	3	3	4	3	3	4	3	3,17	0,38	0,16

Таблиця Г.15 – Зведені дані щодо визначення ступеня впливу дестабілізуючих факторів на стадії модернізації експериментального програмно-технічного комплексу автоматизації прикордонної служби при застосуванні ЗЗФБ

№ з/п	Вид загрози	Властивість інф. ресурсу			
		к	ц	д	с
1.	Доступ до даних з порушенням політики безпеки	0	0	0	0
2.	Модифікація спеціального та системного програмного забезпечення	0	0	0	0
3.	Порушення режимів функціонування систем життєзабезпечення ІС або її складових.	0	0,05	0,01	0,005
4.	Впровадження і використання шкідливого програмного забезпечення	0	0	0	0
5.	Отримання захищених даних за допомогою санкціонованих запитів в обхід політики безпеки	0	0	0	0
6.	Неправомірне підключення до каналів зв’язку, перехоплення даних, що передаються, зміна (модифікація) інформації повідомлень	0,05	0,01	0,005	0,005
7.	Несанкціоноване копіювання носіїв інформації	0,05	0	0	0,01
8.	Крадіжки носіїв інформації	0,01	0,01	0,01	0,01
9.	Фальсифікація (приховування) фактів формування та видачі даних	0	0	0	0,01
10.	Виконання аналізу потоку даних (трафіку)	0	0	0	0,005
11.	Переривання передачі потоку даних	0	0,01	0,005	0,005
12.	Порушення фізичної цілісності ІС (її окремих компонентів).	0,05	0,05	0,005	0,005
13.	Дії, що призводять до відмови ІС чи окремих її елементів, руйнування окремих складових обчислювальних систем та іншого обладнання (телекомунікаційного, засобів вводу/ виводу, тощо)	0,005	0,005	0,005	0,01
14.	Ненавмисне пошкодження носіїв інформації	0	0,01	0,01	0,005
15.	Неправомірна зміна режимів роботи СПЗ або загального ПЗ, яке призводить до незворотного знищення інформації на носіях ІС	0	0	0	0

Продовження таблиці Г.15

№ з/п	Вид загрози	Властивість інф. ресурсу			
		к	ц	д	с
16.	Невмисне зараження програмних засобів комп’ютерними вірусами	0	0	0	0
17.	Невиконання організаційних заходів щодо порядку і правил експлуатації чи використання ресурсів ІС, передбачених керівними документами, посадовими та технологічними інструкціями.	0,01	0,01	0,01	0,01
18.	Використання персоналу ІС корисливою метою	0,005	0,01	0,01	0,01
19.	Помилки при введені даних в систему	0,01	0,01	0,01	0,01
20.	Некомпетентне застосування засобів забезпечення функціональної безпеки	0,005	0,005	0,005	0,005
21.	Помилки при розробці або модернізації ІІС та її складових	0,005	0,005	0,005	0,005
22.	Зміна умов фізичного середовища	0	0,005	0,005	0,005
23.	Збої та відмови у роботі ІС, аварійне відключення живлення та інше.	0	0,005	0,005	0,01
24.	Впливи природних та технологічних завад (грозові розряди, електрозварювальні роботи, тощо).	0	0,005	0,005	0,05

ДОДАТОК Д

Максимальні значення ймовірностей порушення властивостей ПТК АПС при різних варіантах модернізації

Послідовність модернізації	Значення ймовірн.	Послідовність модернізації	Значення ймовірн.	Послідовність модернізації	Значення ймовірн.
12345	0,15786	102345	0,21425	201345	0,10963
12354	0,15642	102354	0,21403	201354	0,10938
12435	0,15498	102435	0,21380	201435	0,10912
12453	0,15208	102453	0,21335	201453	0,10861
12534	0,15063	102534	0,21313	201534	0,10836
12543	0,14918	102543	0,21290	201543	0,10810
13245	0,13526	103245	0,20793	203145	0,11065
13254	0,13471	103254	0,20770	203154	0,11040
13425	0,12643	103425	0,20429	203415	0,11065
13452	0,12143	103452	0,20223	203451	0,11040
13524	0,12477	103524	0,20360	203514	0,10989
13542	0,12031	103542	0,20178	203541	0,10989
14235	0,13196	104235	0,20656	204135	0,10912
14253	0,13085	104253	0,20611	204153	0,10861
14325	0,12421	104325	0,20337	204315	0,10963
14352	0,11919	104352	0,20132	204351	0,10938
14523	0,12087	104523	0,20200	204513	0,10810
14532	0,11696	104532	0,20040	204531	0,10836
15234	0,12809	105234	0,20497	205134	0,10733
15243	0,12754	105243	0,20474	205143	0,10708
15324	0,12031	105324	0,20178	205314	0,10784
15342	0,11583	105342	0,19994	205341	0,10784
15423	0,11863	105423	0,20109	205413	0,10708
15432	0,11471	105432	0,19949	205431	0,10733
21345	0,15048	120345	0,39281	210345	0,28551
21354	0,14995	120354	0,39226	210354	0,28487
21435	0,14941	120435	0,39172	210435	0,28422
21453	0,14833	120453	0,39062	210453	0,28293
21534	0,14779	120534	0,39007	210534	0,28229
21543	0,14724	120543	0,38952	210543	0,28164
23145	0,13526	123045	0,44051	213045	0,34330
23154	0,13471	123054	0,43973	213054	0,34239
23415	0,12643	123405	0,41023	213405	0,32610
23451	0,12143	123450	0,34228	213450	0,27311
23514	0,12477	123504	0,41038	213504	0,32627
23541	0,12031	123540	0,34156	213540	0,27231
24135	0,13196	124035	0,43956	214035	0,34219

Послідовність модернізації	Значення ймовірн.	Послідовність модернізації	Значення ймовірн.	Послідовність модернізації	Значення ймовірн.
24153	0,13085	124053	0,43797	214053	0,34032
24315	0,12421	124305	0,40798	214305	0,32353
24351	0,11919	124350	0,34009	214350	0,27069
24513	0,12087	124503	0,40832	214503	0,32392
24531	0,11696	124530	0,33864	214530	0,26909
25134	0,12809	125034	0,43788	215034	0,34021
25143	0,12754	125043	0,43706	215043	0,33926
25314	0,12031	125304	0,40590	215304	0,32115
25341	0,11583	125340	0,33717	215340	0,26746
25413	0,11863	125403	0,40609	215403	0,32137
25431	0,11471	125430	0,33645	215430	0,26666
31245	0,16949	130245	0,38675	230145	0,22673
31254	0,16831	130254	0,38637	230154	0,22625
31425	0,15014	130425	0,38051	230415	0,22606
31452	0,13907	130452	0,37699	230451	0,22526
31524	0,14651	130524	0,37937	230514	0,22464
31542	0,13662	130542	0,37623	230541	0,22430
32145	0,16854	132045	0,42725	231045	0,28487
32154	0,16736	132054	0,42660	231054	0,28406
32415	0,14868	132405	0,39744	231405	0,27368
32451	0,13734	132450	0,33122	231450	0,22943
32514	0,14504	132504	0,39743	231504	0,27367
32541	0,13489	132540	0,33047	231540	0,22856
34125	0,13011	134025	0,42773	234015	0,26235
34152	0,11261	134052	0,42260	234051	0,26087
34215	0,12931	134205	0,39090	234105	0,25006
34251	0,11138	134250	0,32455	234150	0,20860
34512	0,08910	134502	0,39421	234501	0,24319
34521	0,08854	134520	0,32186	234510	0,19987
35124	0,13495	135024	0,42656	235014	0,26083
35142	0,11887	135042	0,42157	235041	0,25956
35214	0,13415	135204	0,38855	235104	0,24717
35241	0,11765	135240	0,32153	235140	0,20507
35412	0,09068	135402	0,39217	235401	0,24065
35421	0,09012	135420	0,31963	235410	0,19724
41235	0,17222	140235	0,38136	240135	0,21906
41253	0,16980	140253	0,38055	240153	0,21804
41325	0,15486	140325	0,37549	240315	0,21935
41352	0,14353	140352	0,37170	240351	0,21847
41523	0,14740	140523	0,37302	240513	0,21627
41532	0,13850	140532	0,37005	240531	0,21641
42135	0,17222	142035	0,41932	241035	0,27487

Послідовність модернізації	Значення ймовірн.	Послідовність модернізації	Значення ймовірн.	Послідовність модернізації	Значення ймовірн.
42153	0,16980	142053	0,41791	241053	0,27312
42315	0,15486	142305	0,38859	241305	0,26301
42351	0,14353	142350	0,32337	241350	0,22039
42513	0,14740	142503	0,38867	241503	0,26310
42531	0,13850	142530	0,32186	241530	0,21864
43125	0,13081	143025	0,42121	243015	0,25357
43152	0,11304	143052	0,41583	243051	0,25202
43215	0,13044	143205	0,38435	243105	0,24196
43251	0,11247	143250	0,31889	243150	0,20197
43512	0,08939	143502	0,38790	243501	0,23507
43521	0,08911	143520	0,31621	243510	0,19317
45123	0,13758	145023	0,41838	245013	0,24960
45132	0,12308	145032	0,41363	245031	0,24905
45213	0,13758	145203	0,37965	245103	0,23614
45231	0,12308	145230	0,31281	245130	0,19484
45312	0,09334	145302	0,38360	245301	0,22958
45321	0,09334	145320	0,31169	245310	0,18783
51234	0,18138	150234	0,37707	250134	0,21364
51243	0,18015	150243	0,37663	250143	0,21309
51324	0,16277	150324	0,37007	250314	0,21257
51342	0,15202	150342	0,36610	250341	0,21149
51423	0,15897	150423	0,36874	250413	0,21092
51432	0,14946	150432	0,36521	250431	0,21039
52134	0,18138	152034	0,41084	251034	0,26429
52143	0,18015	152043	0,41009	251043	0,26335
52314	0,16277	152304	0,37970	251304	0,25229
52341	0,15202	152340	0,31467	251340	0,21036
52413	0,15897	152403	0,37979	251403	0,25240
52431	0,14946	152430	0,31391	251430	0,20949
53124	0,13980	153024	0,41402	253014	0,24431
53142	0,12288	153042	0,40830	253041	0,24239
53214	0,13943	153204	0,37544	253104	0,23099
53241	0,12231	153240	0,31013	253140	0,19171
53412	0,09352	153402	0,37985	253401	0,22501
53421	0,09324	153420	0,30828	253410	0,18382
54123	0,14172	154023	0,41237	254013	0,24185
54132	0,12664	154032	0,40714	254031	0,24073
54213	0,14172	154203	0,37310	254103	0,22807
54231	0,12664	154230	0,30706	254130	0,18811
54312	0,09570	154302	0,37758	254301	0,22205
54321	0,09570	154320	0,30599	254310	0,18110
301245	0,09042	401235	0,09296	501234	0,11268

Послідовність модернізації	Значення ймовірн.	Послідовність модернізації	Значення ймовірн.	Послідовність модернізації	Значення ймовірн.
301254	0,08985	401253	0,09164	501243	0,11195
301425	0,08058	401325	0,08318	501324	0,09980
301452	0,07503	401352	0,07691	501342	0,09255
301524	0,07883	401523	0,07917	501423	0,09759
301542	0,07385	401532	0,07422	501432	0,09106
302145	0,08819	402135	0,09296	502134	0,11268
302154	0,08761	402153	0,09164	502143	0,11195
302415	0,07718	402315	0,08318	502314	0,09980
302451	0,07104	402351	0,07691	502341	0,09255
302514	0,07543	402513	0,07917	502413	0,09759
302541	0,06986	402531	0,07422	502431	0,09106
304125	0,07516	403125	0,07643	503124	0,09258
304152	0,06575	403152	0,06587	503142	0,08064
304215	0,07345	403215	0,07603	503214	0,09219
304251	0,06495	403251	0,06527	503241	0,08005
304512	0,06495	403512	0,05280	503412	0,06217
304521	0,06468	403521	0,05251	503421	0,06189
305124	0,07950	405123	0,08211	504123	0,09391
305142	0,07022	405132	0,07305	504132	0,08302
305214	0,07779	405213	0,08211	504213	0,09391
305241	0,06764	405231	0,07305	504231	0,08302
305412	0,06495	405312	0,05467	504312	0,06249
305421	0,06468	405321	0,05467	504321	0,06236
310245	0,22252	410235	0,19092	510234	0,16298
310254	0,22230	410253	0,19031	510243	0,16258
310425	0,21847	410325	0,18617	510324	0,15496
310452	0,21621	410352	0,18317	510342	0,15052
310524	0,21780	410523	0,18432	510423	0,15376
310542	0,21576	410532	0,18193	510432	0,14972
312045	0,28140	412035	0,24707	512034	0,21128
312054	0,28091	412053	0,24584	512043	0,21053
312405	0,27340	412305	0,24260	512304	0,21036
312450	0,23069	412350	0,20592	512340	0,17942
312504	0,27301	412503	0,24202	512403	0,21018
312540	0,22978	412530	0,20408	512430	0,17848
314025	0,27773	413025	0,24625	513024	0,21398
314052	0,27411	413052	0,24178	513042	0,20749
314205	0,26506	413205	0,23701	513204	0,20478
314250	0,22298	413250	0,20064	513240	0,17397
314502	0,26578	413502	0,23853	513402	0,20906
314520	0,21956	413520	0,19720	513420	0,17162
315024	0,27602	415023	0,24216	514023	0,21158

Послідовність модернізації	Значення ймовірн.	Послідовність модернізації	Значення ймовірн.	Послідовність модернізації	Значення ймовірн.
315042	0,27226	415032	0,23792	514032	0,20549
315204	0,26179	415203	0,23040	514203	0,20146
315240	0,21947	415230	0,19342	514230	0,17026
315402	0,26326	415302	0,23308	514302	0,20612
315420	0,21699	415320	0,19188	514320	0,16887
320145	0,17411	420135	0,13874	520134	0,10899
320154	0,17388	420153	0,13809	520143	0,10857
320415	0,17259	420315	0,13765	520314	0,10457
320451	0,17159	420351	0,13645	520341	0,10193
320514	0,17188	420513	0,13569	520413	0,10330
320541	0,17112	420531	0,13514	520431	0,10108
321045	0,23636	421035	0,19969	521034	0,16165
321054	0,23585	421053	0,19839	521043	0,16085
321405	0,23355	421305	0,20106	521304	0,16705
321450	0,19795	421350	0,17213	521340	0,14450
321504	0,23314	421503	0,20044	521403	0,16686
321540	0,19701	421530	0,17021	521430	0,14352
324015	0,21322	423015	0,17778	523014	0,14258
324051	0,21146	423051	0,17577	523041	0,13849
324105	0,20872	423105	0,17840	523104	0,14370
324150	0,17628	423150	0,15259	523140	0,12432
324501	0,20168	423501	0,17129	523401	0,13922
324510	0,16721	423510	0,14328	523410	0,11598
325014	0,21136	425013	0,17297	524013	0,13960
325041	0,20945	425031	0,17140	524031	0,13614
325104	0,20519	425103	0,17125	524103	0,14008
325140	0,17256	425130	0,14494	524130	0,12039
325401	0,19894	425301	0,16522	524301	0,13588
325410	0,16447	425310	0,13760	524310	0,11304
340125	0,14740	430125	0,12016	530124	0,09190
340152	0,14670	430152	0,11906	530142	0,08909
340215	0,14635	430215	0,11966	530214	0,09138
340251	0,14512	430251	0,11831	530241	0,08831
340512	0,14424	430512	0,11636	530412	0,08292
340521	0,14372	430521	0,11610	530421	0,08266
341025	0,20195	431025	0,17666	531024	0,14183
341052	0,19938	431052	0,17350	531042	0,13633
341205	0,19913	431205	0,17741	531204	0,14244
341250	0,16938	431250	0,15259	531240	0,12430
341502	0,19839	431502	0,17721	531402	0,14537
341520	0,16557	431520	0,14876	531420	0,12164
342015	0,18432	432015	0,15780	532014	0,12217

Послідовність модернізації	Значення ймовірн.	Послідовність модернізації	Значення ймовірн.	Послідовність модернізації	Значення ймовірн.
342051	0,18233	432051	0,15563	532041	0,11765
342105	0,18280	432105	0,16057	532104	0,12489
342150	0,15541	432150	0,13834	532140	0,10957
342501	0,17570	432501	0,15341	532401	0,12065
342510	0,14613	432510	0,12888	532410	0,10112
345012	0,17369	435012	0,14718	534012	0,11449
345021	0,17292	435021	0,14679	534021	0,11408
345102	0,16879	435102	0,14685	534102	0,11721
345120	0,14013	435120	0,12280	534120	0,09785
345201	0,16315	435201	0,14061	534201	0,11076
345210	0,13473	435210	0,11726	534210	0,09214
350124	0,14269	450123	0,10639	540123	0,08275
350142	0,14124	450132	0,10441	540132	0,07982
350214	0,14163	450213	0,10639	540213	0,08275
350241	0,13966	450231	0,10441	540231	0,07982
350412	0,13729	450312	0,10045	540312	0,07393
350421	0,13676	450321	0,10045	540321	0,07393
351024	0,19181	451023	0,15393	541023	0,12920
351042	0,18826	451032	0,14972	541032	0,12365
351204	0,18682	451203	0,15206	541203	0,12940
351240	0,15863	451230	0,13053	541230	0,11299
351402	0,18775	451302	0,15446	541302	0,13323
351420	0,15589	451320	0,12882	541320	0,11137
352014	0,17395	452013	0,13387	542013	0,10855
352041	0,17098	452031	0,13105	542031	0,10441
352104	0,17024	452103	0,13464	542103	0,11151
352140	0,14448	452130	0,11590	542130	0,09806
352401	0,16477	452301	0,12959	542301	0,10775
352410	0,13622	452310	0,10844	542310	0,09058
354012	0,16556	453012	0,12867	543012	0,10408
354021	0,16479	453021	0,12848	543021	0,10389
354102	0,16077	453102	0,12966	543102	0,10803
354120	0,13301	453120	0,10817	543120	0,09032
354201	0,15508	453201	0,12306	543201	0,10127
354210	0,12757	453210	0,10251	543210	0,08454

ДОДАТОК Е

Код програми для розрахунку раціональної послідовності модернізації елементів інформаційних систем

```
<?php
const COUNT_ELEMENTS = 6;
const MODERNIZATION_VELOCITY = 6;
const MODERNIZATION_TIME_SHIFT = 0.5;

function P_ij($i, $j) {
    $P_ij = array(
        array(0, 0.8, 0.8, 0.8, 0.8, 0.8, 0.8, 0.8,
0.8, 0.8),
        array(1,   0, 0.5, 0.5, 0.5, 0.5, 0.5, 0.5,
0.5, 0.5),
        array(1, 0.5,   0, 0.5, 0.5, 0.5, 0.5, 0.5,
0.5, 0.5),
        array(1, 0.5, 0.5,   0, 0.5, 0.5, 0.5, 0.5,
0.5, 0.5),
        array(1, 0.5, 0.5, 0.5,   0, 0.5, 0.5, 0.5,
0.5, 0.5),
        array(1, 0.5, 0.5, 0.5, 0.5,   0, 0.5, 0.5,
0.5, 0.5),
        array(1, 0.5, 0.5, 0.5, 0.5, 0.5,   0, 0.5,
0.5, 0.5),
        array(1, 0.5, 0.5, 0.5, 0.5, 0.5, 0.5,   0,
0.5, 0.5),
        array(1, 0.5, 0.5, 0.5, 0.5, 0.5, 0.5, 0.5,
0, 0.5),
        array(1, 0.5, 0.5, 0.5, 0.5, 0.5, 0.5, 0.5,
0.5,  0 ),
    );

    return $P_ij[$i][$j];
}

function Lambda($i, $j) {
    $l = array(
        array(  0,   1,   1,  0.3,  0.2,  0.1, 0.3,
0.2,  0.3,  0.2),
        array(  1,   0,   1,  0.3,  0.2,  0.1, 0.3,
0.2,  0.3,  0.2),
        array(0.5, 0.2,   0,  0.3,  0.2,  0.1, 0.3,
0.2,  0.3,  0.2),
```

```
        array(0.3, 0.2, 0.1,    0, 0.05, 0.05, 0.3,
0.2,  0.3,  0.2),
        array(0.2, 0.2, 0.2, 0.05,    0, 0.02, 0.3,
0.2,  0.3,  0.2),
        array(0.1, 0.5, 0.5, 0.05, 0.02,    0, 0.3,
0.2,  0.3,  0.2),
        array(0.1, 0.5, 0.5, 0.05, 0.02,  0.2,   0,
0.3,  0.3,  0.2),
        array(0.1, 0.5, 0.5, 0.05, 0.02,  0.3, 0.2,
0, 0.3,  0.2),
        array(0.1, 0.5, 0.5, 0.05, 0.02,  0.3, 0.2,
0.3,    0, 0.2),
        array(0.1, 0.5, 0.5, 0.05, 0.02,  0.3, 0.2,
0.3,  0.2,   0),
    );
    return $l[$i][$j]*(1/3600);
}

function P_modernization_element($t, $tb) {
    if($t<$tb) return 0;
    return 1-exp(-1*MODERNIZATION_VELOCITY*($t-$tb));
}

function P_modernization_para($t, $i, $j, $sequence) {
    $tb_i = MODERNIZATION_TIME_SHIFT*array_search($i,
$sequence);
    $tb_j = MODERNIZATION_TIME_SHIFT*array_search($j,
$sequence);
    $tmp = P_modernization_element($t, $tb_i)*(1-
P_modernization_element($t, $tb_j))*P_ij($i, $j);

    return $tmp;
}

function P_modernization_para_potik($t, $i, $j,
$sequence) {
    $t1 = P_modernization_para($t, $i, $j, $sequence);
    $t2 = Lambda($i, $j)*$t;
    $tmp = 1-(1-$t1)**$t2;
    //echo '----------P_modernization_para: '.$i.
':'.$j.'='.$tmp.'<br>';
    return $tmp;
}

function P_porushennya($t, $i, $sequence) {
```

```
    $res = 1;
    foreach($sequence as $item) {
        $tmp = P_modernization_para_potik($t, $i,
$item, $sequence);

        $res *= $res * (1-$tmp);
    }
    return 1-$res;
}

function P_ITS($t, $sequence) {
    $res = 1;
    foreach($sequence as $item) {
        $tmp = P_porushennya($t, $item, $sequence);
                $res *= $res * (1-$tmp);
    }
    return 1-$res;
}

$sequence = array(3, 4, 2, 0, 1, 5);
for($t=0; $t <= 6; $t+=0.1) {
    $tmp = P_ITS($t, $sequence);
    echo $tmp.'<br>';
}

function Swap($a,$b, &$sequence) {
    $t = $sequence[$a];
    $sequence[$a] = $sequence[$b];
    $sequence[$b] = $t;
}

function Generate($k, $sequence) {
    if($k == count($sequence)) {
        $max = 0;
        $sum = 0;
        $i = 0;
        for($t=0; $t < 6; $t+=0.1) {
            $tmp = P_ITS($t, $sequence);
            //echo '-'.$tmp.'-';
            $sum += $tmp;
            $i++;
            if($tmp > $max) $max = $tmp;
        }
    } else {
        for($j=$k; $j<count($sequence); $j++) {
```

```
            Swap($k, $j, $sequence);
            Generate($k+1, $sequence);
            Swap($k, $j, $sequence);
        }
    }
}

function calculate($sequence) {
    $max = 0;
    $sum = 0;
    $i = 0;
    for($t=0; $t < 6; $t+=0.5) {
        $tmp = P_ITS($t, $sequence);
        $sum += $tmp;
         $i++;
         if($tmp > $max) $max = $tmp;
     }
    return $max;
}

class E {
    public $element = NULL;
    public $parent = NULL;
    public $child = array();
    public $value = NULL;
    public $sequence = array();

    public function hasElement($e) {
        if($e === $this->element) return TRUE;
        if(!is_null($this->parent)) return $this-
>parent->hasElement($e);
        return FALSE;
    }

    public function generate() {
        $is_add = FALSE;
        for($i = 0; $i < COUNT_ELEMENTS; $i++) {
            if(!$this->hasElement($i)) {
                $tmp = new E();
                $tmp->element = $i;
                $tmp->parent = $this;
                $is_add = TRUE;
                $tmp->setSequence($tmp->sequence);
                if(count($tmp->sequence) > 1) $tmp-
>value = calculate($tmp->sequence);
```

```
                $this->child[] = $tmp;
            }
        }

        return $is_add;
    }

    public function setSequence(&$seq) {
        if(!is_null($this->element))
array_unshift($seq, $this->element);
        if(!is_null($this->parent)) $this->parent-
>setSequence($seq);
        return $seq;
    }

    public function getMinLeaf(&$node) {
        if(count($this->child) == 0) {
            if(!is_null($this->value)) {
                if (is_null($node)) $node = $this;
                if ($node->value > $this->value) $node
= $this;
            }
        } else {
            foreach($this->child as $item) {
                $item->getMinLeaf($node);
            }
        }
    }
}
```

ДОДАТОК Ж

Організаційна структура ДПСУ

Назва об’єкту
Державна прикордонна служба України
Адміністрація Держприкордонслужби України
Частини центрального підпорядкування
Окремий контрольно-пропускний пункт «Київ»
Мобільний прикордонний загін
Навчальний центр підготовки молодших спеціалістів ДПСУ
Головний центр зв’язку, автоматизації та захисту інформації
Центральний клінічний госпіталь
Національна академія ДПСУ ім. Богдана Хмельницького
Науково-дослідний інститут
Клінічний санаторій „Аркадія”
Спорткомітет
Академічний ансамбль пісні і танцю ДПСУ
Центральний музей Державної прикордонної служби України
Інформаційне Агентство ДПСУ
Окрема комендатура охорони і забезпечення
Галузевий державний архів ДПС України
Головний експертно-криміналістичний центр
Східне регіональне управління
Донецький прикордонний загін
Краматорський прикордонний загін
Луганський прикордонний загін
Харківський прикордонний загін
Сумський прикордонний загін
Харківська окрема авіаційна ескадрилья
Маріупольський загін морської охорони
Північне регіональне управління
Чернігівський прикордонний загін
Житомирський прикордонний загін
Луцький прикордонний загін
Західне регіональне управління
Львівський прикордонний загін
Мостиський прикордонний загін
Мукачівський прикордонний загін
Чопський прикордонний загін
Чернівецький прикордонний загін
Клінічний госпіталь Державної прикордонної служби України
Кінологічний навчальний центр ДПСУ
Південне регіональне управління
Одеський прикордонний загін
Одеський загін морської охорони

Назва об’єкту
Котовський прикордонний загін
Білгород-Дністровський прикордонний загін
Ізмаїльський прикордонний загін
Могилів-Подільський прикордонний загін
Одеська окрема авіаційна ескадрилья
Клінічний госпіталь ДПСУ
Навчально-тренувальний загін морської охорони ДПСУ
Азово-Чорноморське регіональне управління
Бердянський прикордонний загін
Херсонський прикордонний загін

ДОДАТОК И

Код програми для розрахунку ефективності спільного функціонування обох версій системи розмежування доступу

```
<?php
const COUNT_ELEMENTS = 6;
const FROM = 5;

function Lambda($i, $j) {
    $l = array(
        //    1  2    3      4      5      6
        array(0, 0, 0.005,     0,     0,     0), // 1
        array(0, 0, 0.005,     0,     0,  0.14), // 2
        array(0, 0,     0, 0.004, 0.001,     0), // 3
        array(0, 0,     0,     0, 0.001,  0.14), // 4
        array(0, 0,     0, 0.001,     0, 0.014), // 5
        array(0, 0,     0,     0,     0,     0), // 6
    );
    return $l[$i][$j];
}

function F($vars, $index) {
    $res = 0;
    for($j = 0; $j < COUNT_ELEMENTS; $j++) $res +=
$vars[$j+1]*Lambda($j, $index);
    $sum_alpha = 0;
    for($j = 0; $j < COUNT_ELEMENTS; $j++) $sum_alpha
+= Lambda($index, $j);
    return $res - $vars[$index+1]*$sum_alpha;
}
```

```
function Runge_Kutt($first, $last, $steps, $initArray)
{
    $delt = ($last - $first) / $steps; // находим
величину шага разбиений
    $res = array();
    $vars = array();
    $vars2 = array();
    $vars3 = array();
    $vars4 = array();

    $coefs1 = array();
    $coefs2 = array();
    $coefs3 = array();
    $coefs4 = array();

    $vars[0] = $first;

    for($k = 0; $k <= COUNT_ELEMENTS-1; $k++)
$vars[$k+1] = $initArray[$k];

    for($j = 0; $j <= COUNT_ELEMENTS; $j++) $res[$j][0]
= $vars[$j];
    for($i = 0; $i <= $steps-1; $i++) { // начало цикла
иттераций
        for ($j = 0; $j <= COUNT_ELEMENTS - 1; $j++)
$coefs1[$j] = F($vars, $j) * $delt; // 1-й коэфф.
        $vars2[0] = $vars[0] + $delt / 2;
        for ($k = 1; $k <= COUNT_ELEMENTS; $k++)
$vars2[$k] = $vars[$k] + $coefs1[$k - 1] / 2;
```

```
        for ($j = 0; $j <= COUNT_ELEMENTS - 1; $j++)
$coefs2[$j] = F($vars2, $j) * $delt; // 2-й коэф.

        $vars3[0] = $vars[0] + $delt / 2;

        for ($k = 1; $k <= COUNT_ELEMENTS; $k++)
$vars3[$k] = $vars[$k] + $coefs2[$k - 1] / 2;

        for ($j = 0; $j <= COUNT_ELEMENTS - 1; $j++)
$coefs3[$j] = F($vars3, $j) * $delt; // 3 коэфф.

        $vars4[0] = $vars[0] + $delt;

        for ($k = 1; $k <= COUNT_ELEMENTS; $k++)
$vars4[$k] = $vars[$k] + $coefs3[$k - 1];

        for ($j = 0; $j <= COUNT_ELEMENTS - 1; $j++)
$coefs4[$j] = F($vars4, $j) * $delt; // 4 коэфф.

        $vars[0] = $vars[0] + $delt;

        for ($k = 1; $k <= COUNT_ELEMENTS; $k++)
$vars[$k] = $vars[$k] + (1 / 6) * ($coefs1[$k - 1] + 2
* ($coefs2[$k - 1] + $coefs3[$k - 1]) + $coefs4[$k -
1]);

        for ($j = 0; $j <= COUNT_ELEMENTS; $j++)
$res[$j][$i + 1] = $vars[$j];

    }

    return $res;

}


$f_d = array();

for($j = 0; $j < COUNT_ELEMENTS; $j++){

    $f_d[$j] = ($j == (FROM-1)) ? 1 : 0;

}

$s = 0; // початок

$f = 1200; // кінець

$st = 1200; // крок

$res = Runge_Kutt($s, $f, $st, $f_d);
```

```
echo "<table>";

echo "<tr>";

echo "<td>time</td>";

for($j = 1; $j <= COUNT_ELEMENTS; $j++) echo "<td>P-
".$j.'</td>';

echo '</tr>';

for($i = 0; $i <= $st; $i++) {

    echo "<tr>";

    for($j = 0; $j <= COUNT_ELEMENTS; $j++) echo
"<td>".$res[$j][$i].'</td>';

    echo '</tr>';

}

echo "<tr>";

echo "<td>time</td>";

for($j = 1; $j <= COUNT_ELEMENTS; $j++) echo "<td>P-
".$j.'</td>';

echo '</tr>';

echo "</table>";
```

ДОДАТОК К

Формування функцій розподілу для загроз складовим інформаційного ресурсу в експериментальному ПТК АПС "Гарт-3/П"

З метою визначення параметрів закону розподілу при здійсненні введення даних та помилки при модернізації в ПТК АПС "Гарт-1/П" здійснено збір статистичних даних при проведенні ділової гри в Національній академії Державної прикордонної служби України імені Б. Хмельницького. Результати зведені в таблиці К.1 та К.2.

Таблиця К.1 – Зведена таблиця даних щодо помилок введення даних в ПТК АПС "Гарт-1/П"

№ з/п	Час помилки від початку модернізації		Посадова особа	Зміст помилки
	год	хв		
1.	0	14	Старший зміни ПН	Помилка при введенні в поле окремого рішення старшого зміни
2.	0	38	Заступник начальника ВПС	Помилка при введенні в поле окремих рішень
3.	0	52	Діловод	Помилка при введенні в поле звіту
4.	1	04	Діловод	Помилка при введенні в поле звіту
5.	1	08	Заступник начальника ВПС	Помилка при введенні в реєстр плавзасобів
6.	1	37	Старший зміни ПН	Помилка при введенні в поле результатів перевірки служби
7.	2	10	Старший зміни ПН	Помилка при введенні в поле окреме рішення зміни ПН
8.	2	45	Старший зміни ПН	Помилка при введенні в поле окреме рішення зміни ПН
9.	2	55	Оперативний черговий	Помилка при введенні в поле фіксації події
10.	3	20	Діловод	Помилка при введенні в поле звіту
11.	3	37	Оперативний черговий	Помилка при введенні в поле статусу відміни дії
12.	3	52	Діловод	Помилка при введенні в поле звіту
13.	4	18	Начальник ВПС	Помилка при введенні в довідник "Штат"
14.	4	25	Начальник ВПС	Помилка при введенні в довідник сигналів тривог

Продовження таблиці К.1

№ з/п	Час помилки від початку модернізації		Посадова особа	Зміст помилки
	год	хв		
15.	4	48	Заступник начальника ВПС	Помилка при введенні в поле календарного плану
16.	5	05	Оперативний черговий	Помилка при введенні в поле статусу відміни дії
17.	5	27	Заступник начальника ВПС	Помилка при введенні в реєстр транспортних засобів
18.	5	32	Начальник ВПС	Помилка при введенні в поле календарного плану
19.	6	14	Оперативний черговий	Помилка при введенні в поле статусу відміни дії
20.	6	34	Оперативний черговий	Помилка при введенні в поле статусу відміни дії
21.	6	42	Діловод	Помилка при введенні в поле звіту
22.	7	05	Оперативний черговий	Помилка при введенні в поле фіксації події
23.	7	24	Начальник ВПС	Помилка при введенні в реєстр обліку даташтампів
24.	7	45	Заступник начальника ВПС	Помилка при введенні в поле інформації
25.	8	15	Діловод	Помилка при введенні в поле звіту
26.	8	28	Діловод	Помилка при введенні в поле звіту
27.	8	54	Начальник ВПС	Помилка при введенні в поле ділянки ВПС
28.	9	09	Заступник начальника ВПС	Помилка при введенні в довідник час служби
29.	9	27	Оперативний черговий	Помилка при введенні в поле статусу відміни дії
30.	9	42	Діловод	Помилка при введенні в поле звіту
31.	10	30	Старший зміни ПН	Помилка при введенні в поле окреме рішення зміни ПН
32.	10	55	Старший зміни ПН	Помилка при введенні в поле результатів перевірки служби
33.	11	10	Оперативний черговий	Помилка при введенні в поле статусу відміни дії
34.	11	37	Заступник начальника ВПС	Помилка при введенні в реєстр обліку пристроїв
35.	12	15	Заступник начальника ВПС	Помилка при введенні в реєстр обліку даташтампів
36.	12	40	Оперативний черговий	Помилка при введенні в поле статусу відміни дії
37.	13	30	Старший зміни ПН	Помилка при введенні в поле плану охорони ДК
38.	13	55	Оперативний черговий	Помилка при введенні в поле фіксації події
39.	14	05	Діловод	Помилка при введенні в поле звіту
40.	14	20	Начальник ВПС	Помилка при введенні в поле календарного плану

Продовження таблиці К.1

№ з/п	Час помилки від початку модернізації		Посадова особа	Зміст помилки
	год	хв		
41.	15	10	Оперативний черговий	Помилка при введенні в поле фіксації події
42.	15	38	Оперативний черговий	Помилка при введенні в поле фіксації події
43.	16	20	Старший зміни ПН	Помилка при введенні в поле розпізнавальні знаки
44.	17	58	Заступник начальника ВПС	Помилка при введенні в реєстр обліку пристроїв
45.	18	26	Заступник начальника ВПС	Помилка при введенні в поле графіку змін
46.	19	52	Оперативний черговий	Помилка при введенні в поле фіксації події
47.	20	46	Діловод	Помилка при введенні в поле звіту
48.	21	33	Оперативний черговий	Помилка при введенні в поле статусу відміни дії
49.	22	54	Старший зміни ПН	Помилка при введенні в поле результатів служби
50.	23	20	Заступник начальника ВПС	Помилка при введенні в поле графіку змін

Таблиця К.2 – Зведена таблиця даних щодо помилок при модернізації ПТК АПС "Гарт-1/П"

№ з/п	Час помилки від початку модернізації		Посадова особа	Зміст помилки
	год	хв		
1.	2	18	Старший зміни ПН	Помилка при відображенні позиції ПН
2.	3	13	Начальник ВПС	Помилка при збереженні реєстру плавзасобів
3.	4	49	Старший зміни ПН	Помилка при відображенні часу зміни ПН
4.	5	6	Заступник начальника ВПС	Помилка при введенні даних при відсутності запису в реєстрі
5.	6	4	Старший зміни ПН	Помилка при відображенні часу зміни ПН
6.	7	22	Начальник ВПС	Помилка при збереженні реєстру плавзасобів
7.	8	21	Начальник ВПС	Помилка при введенні даних при відсутності запису в реєстрі
8.	9	8	Оперативний черговий	Помилка при відображенні позиції ПН
9.	9	23	Оперативний черговий	Помилка при відображенні часу зміни ПН
10.	10	46	Начальник ВПС	Помилка при збереженні реєстру плавзасобів
11.	11	15	Начальник ВПС	Помилка при введенні даних при відсутності запису в реєстрі

Продовження таблиці К.2

№ з/п	Час помилки від початку модернізації		Посадова особа	Зміст помилки
	год	хв		
12.	11	58	Начальник ВПС	Помилка при збереженні реєстру плавзасобів
13.	12	17	Начальник ВПС	Помилка при введенні даних при відсутності запису в реєстрі
14.	12	56	Оперативний черговий	Помилка при відображенні позиції ПН
15.	13	29	Заступник начальника ВПС	Помилка при введенні даних при відсутності запису в реєстрі
16.	13	45	Заступник начальника ВПС	Помилка при збереженні реєстру плавзасобів
17.	14	3	Заступник начальника ВПС	Помилка при збереженні реєстру плавзасобів
18.	15	23	Начальник ВПС	Помилка при збереженні реєстру плавзасобів
19.	16	48	Заступник начальника ВПС	Помилка при збереженні реєстру плавзасобів
20.	17	29	Заступник начальника ВПС	Помилка при введенні даних при відсутності запису в реєстрі
21.	18	32	Начальник ВПС	Помилка при введенні даних при відсутності запису в реєстрі
22.	10	25	Оперативний черговий	Помилка при відображенні часу зміни ПН
23.	20	42	Оперативний черговий	Помилка при відображенні позиції ПН
24.	21	49	Оперативний черговий	Помилка при відображенні часу зміни ПН
25.	22	59	Начальник ВПС	Помилка при збереженні реєстру плавзасобів
26.	23	13	Начальник ВПС	Помилка при збереженні реєстру плавзасобів
27.	24	10	Начальник ВПС	Помилка при збереженні реєстру плавзасобів

Для визначення параметрів функції розподілу Вейбула при здійсненні помилок введення даних в ПТК АПС "Гарт-1/П" використаємо метод найменших квадратів. Числові значення параметрів функції розподілу визначимо за допомогою відомих програмних математичних пакетів, результати яких зведено в таблицю Л.3 при визначених параметрах $k = 1.31$ та $\lambda = 13$.

Таблиця К.3 – Розрахунок числових значень функції розподілу ймовірності здійснення помилок при введенні даних в ПТК АПС "Гарт-1/П"

№ інтервалу	Кількість елементів	Частота (x_i)	Теоретична ймовірність (p_i)	$(x_i - p_i)^2$
1	3	0,06	0,043946	0,000258
2	3	0,06	0,051752	6,8E-05
3	3	0,06	0,055246	2,26E-05
4	3	0,06	0,056483	1,24E-05
5	3	0,06	0,056295	1,37E-05
6	3	0,06	0,055145	2,36E-05
7	3	0,06	0,05333	4,45E-05
8	3	0,06	0,051056	8E-05
9	3	0,06	0,048478	0,000133
10	3	0,06	0,045712	0,000204
11	2	0,04	0,042845	8,1E-06
12	2	0,04	0,039947	2,76E-09
13	2	0,04	0,037071	8,58E-06
14	2	0,04	0,034256	3,3E-05
15	2	0,04	0,031532	7,17E-05
16	2	0,04	0,028922	0,000123
17	1	0,02	0,026441	4,15E-05
18	1	0,02	0,024098	1,68E-05
19	1	0,02	0,0219	3,61E-06
20	1	0,02	0,019848	2,3E-08
21	1	0,02	0,017943	4,23E-06
22	1	0,02	0,016181	1,46E-05
23	1	0,02	0,014558	2,96E-05
24	1	0,02	0,01307	4,8E-05
	Всього: 50			Сума: 0,001262

Для перевірки гіпотези про те, що дані статистичні дані розподілені за законом розподілу Вейбула проведемо ідентифікацію його за критерієм χ^2 (хі-квадрат) Пірсона. Процедура застосування χ^2 при оцінці узгодженості теоретичного і статистичного розподілів з врахуванням статистичних значень частот ν_i^* передбачає визначення ступеня розбіжності:

$$\chi^2 = m\sum_{i=1}^{k}\frac{\left(\nu_i^* - \nu_i\right)^2}{\nu_i},$$

де ν_i - теоретична частота; ν_i^* - статистична частота випадкової величини в *i*-му інтервалі; *k* - кількість інтервалів, на які розбитий час спостереження; *m* - об'єм вибірки.

Знаходження кількості степенів свободи: $r = k - (s+1)$, де *s* - кількість параметрів теоретичного розподілу.

Разом із тим, необхідно, щоб для класів які знаходяться на межі кількість елементів було більше одиниці, а для решти елементів груп, їх кількість повинна перевищувати 5. З цією метою згрупуємо зведені дані таблиці К.4.

Таблиця К.4 – Згруповані дані для перевірки гіпотез про вид функції розподілу ймовірності здійснення помилок при введенні даних в ПТК АПС "Гарт-1/П"

№ інтервалу	Статистична частота	Теоретична частота	$\frac{(\nu_i^* - \nu_i)^2}{\nu_i}$
1	0,18	0,167434	0,000943
2	0,18	0,180401	8,9E-07
3	0,18	0,15921	0,002715
4	0,14	0,12966	0,000825
5	0,12	0,100452	0,003804
6	0,08	0,075043	0,000327
7	0,06	0,054468	0,000562
8	0,06	0,038597	0,011869
			Сума: 0,021
			$\chi^2 = 50 \cdot 0.021 = 1.05$

Обчислене значення χ^2 порівняємо з табличним значенням які відповідають вибраній довірчій ймовірності. Кількість ступенів свободи становить 5. Так як табличне значення більше за обчислене $1.14 \chi^2_{0,95} > 1.05$, гіпотезу про правильність вибраного закону розподілу приймаємо.

Для визначення параметрів функції розподілу ймовірностей помилок при модернізації ПТК АПС "Гарт-1/П" проведемо аналогічну процедуру. Числові значення параметрів функції розподілу визначимо за допомогою відомих програмних математичних пакетів, результати яких зведено в таблицю К.5 при визначених параметрах $k = 2$ та $\lambda = 18$.

Таблиця К.5 – Розрахунок числових значень функції розподілу ймовірності здійснення помилок при введенні даних в ПТК АПС "Гарт-1/П"

№ інтервалу	Кількість елементів	Частота (x_i)	Теоретична ймовірність (p_i)	$(x_i - p_i)^2$
1	0	0	0,006154	3,79E-05
2	0	0	0,012194	0,000149
3	1	0,04	0,018011	0,000484
4	1	0,04	0,023502	0,000272
5	1	0,04	0,028572	0,000131
6	1	0,04	0,033142	4,7E-05
7	1	0,04	0,037145	8,15E-06
8	1	0,04	0,040531	2,82E-07
9	1	0,04	0,043267	1,07E-05
10	1	0,04	0,045336	2,85E-05
11	1	0,04	0,04674	4,54E-05
12	2	0,08	0,047495	0,001057
13	2	0,08	0,047632	0,001048
14	2	0,08	0,047195	0,001076
15	1	0,04	0,046236	3,89E-05
16	1	0,04	0,044819	2,32E-05
17	1	0,04	0,043008	9,05E-06
18	1	0,04	0,040875	7,66E-07
19	1	0,04	0,03849	2,28E-06
20	1	0,04	0,035921	1,66E-05
21	1	0,04	0,033234	4,58E-05
22	1	0,04	0,030489	9,05E-05
23	1	0,04	0,027742	0,00015
24	1	0,04	0,025039	0,000224
	Всього: 25			Сума: 0,0044

Перевіримо гіпотезу щодо відповідності статистичних даних зазначеній функції розподілу за критерієм χ^2 Пірсона. Результати обчислень зведені в таблицю К.6.

Таблиця К.6 – Згруповані дані для перевірки гіпотез про вид функції розподілу ймовірності здійснення помилок при модернізації ПТК АПС "Гарт-1/П"

№ інтервалу	Статистична частота	Теоретична частота	$\frac{\left(\nu_i^* - \nu_i\right)^2}{\nu_i}$
1	0,04	0,036359	0,000365
2	0,12	0,085216	0,014198
3	0,12	0,120943	7,35E-06
4	0,16	0,139571	0,00299
5	0,2	0,141063	0,024625
6	0,12	0,128703	0,000588
7	0,12	0,107645	0,001418
8	0,12	0,08327	0,016201
			Сума: 0,06
			$\chi^2 = 26 \cdot 0.06 = 1.5$

Обчислене значення χ^2 порівняємо з табличним значенням які відповідають вибраній довірчій ймовірності. Кількість ступенів свободи становить 5. Так як табличне значення більше за обчислене $1.61_{\chi^2_{0,90}} > 1.5$, гіпотезу про правильність вибраного закону розподілу приймаємо.

ДОДАТОК Л

Експертне оцінювання ступеня взаємного впливу ймовірностей порушення властивостей інформаційного ресурсу

Таблиця Л.1 – Структура анкети для проведення експертизи

Вкажіть кваліфікаційний індекс_____				
Властивість інформації	Умовна ймовірність порушення властивості інформації			
	цілісність	конфіденційність	доступність	спостереженість
цілісність	1			
конфіденційність		1		
доступність			1	
спостереженість				1

Таблиця Л.2 – Шкала оцінювання ступеня взаємного впливу ймовірностей порушення властивостей інформації

№	Ступінь впливу	Значення ймовірності	Кількість балів
1	постійна	1	10
2	занадто висока	0,95	9
3	дуже висока	0,8	8
4	висока	0,7	7
5	більше середнього	0,6	6
6	середня	0,5	5
7	менше середнього	0,4	4
8	низька	0,3	3
9	дуже низька	0,2	2
10	занадто низька	0,05	1
11	неможлива	0	0

Таблиця Л.3 – Зведені результати експертного оцінювання

Умовна	Експерт																					Сер.	$\tilde{\sigma}$	ε
ймов.	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	зважене		
$P_i(c)$	1	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1	1	1	0,95	0,22	0,10
$P_i(a)$	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	7	8	7,98	0,15	0,07
$P_i(u)$	6	6	6	6	5	6	6	6	6	6	6	6	6	6	6	6	5	6	6	6	6	5,91	0,29	0,13
$P_c(i)$	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1	1	1	1	0	0,92	0,27	0,11
$P_c(a)$	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1,00	0,00	0,00
$P_c(u)$	1	1	1	2	1	2	2	1	1	1	1	1	1	1	1	1	1	1	1	1	0	1,14	0,41	0,17
$P_a(i)$	3	2	2	2	2	1	2	2	2	2	2	2	3	2	2	2	2	2	2	2	2	2,06	0,40	0,17
$P_a(c)$	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	1	0,98	0,15	0,07
$P_a(u)$	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4,00	0,00	0,00
$P_u(i)$	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1	0,95	0,22	0,10
$P_u(c)$	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5,00	0,00	0,00
$P_u(a)$	2	2	2	2	2	2	2	2	2	2	2	3	2	2	2	2	2	2	2	2	2	2,05	0,22	0,09

Таблиця Л.4 – Результат експертизи оцінювання ступеня взаємного впливу ймовірностей порушення властивостей інформації на експериментальному ПТК АПС "Гарт-1П"

Властивість інформації	Умовна ймовірність порушення властивості інформації			
	цілісність	конфіденційність	доступність	спостереженість
цілісність	1	0,05	0,8	0,6
конфіденційність	0,05	1	0,05	0,05
доступність	0,2	0,05	1	0,4
спостереженість	0,05	0,5	0,2	1

ДОДАТОК М

Пошук щільності розподілу випадкового вектору множини допустимих значень показника якості функціонування системи функціональної безпеки

З метою скорочення запису введемо окремі константи:

$k_1 = 13;\ k_2 = 1.3;\ k_3 = 18;\ k_4 = 2;$

$a_1 = 0.83;\ a_2 = 0.0000109;$

$b_1 = 0.82;\ b_2 = 0.00028;\ b_3 = -0.000123;$

$c_1 = 0.908;\ c_2 = 0.00174;$

$d_1 = 0.838;\ d_2 = 0.00316;\ d_3 = -0.00137;$

Таким чином, (6.24) прийме вигляд:

$$F_{\hat{Z}}(v_i, v_c, v_a, v_u) = \left(a_1 f(v_i) + a_2 f^2(v_i)\right) \cdot \left(b_1 + b_2 f(v_c) + b_3 f^2(v_c)\right) \times \\ \times \left(c_1 f(v_a) + c_2 f^2(v_a)\right) \cdot \left(d_1 + d_2 f(v_u) + d_3 f^2(v_u)\right) \quad \text{(M.1)}$$

де: $f(x) = e^{-\left(\left(\frac{x}{k_1}\right)^{k_2} + \left(\frac{x}{k_3}\right)^{k_4}\right)}$

Розкриємо дужки в (М.1):

$$F_{\hat{Z}}(v_i, v_c, v_a, v_u) = a_1 b_1 c_1 d_1 f(v_i) f(v_a) + a_1 b_1 c_1 d_2 f(v_i) f(v_a) f(v_u) + \\ a_1 b_1 c_1 d_3 f(v_i) f(v_a) f^2(v_u) + a_1 b_1 c_2 d_1 f(v_i) f^2(v_a) + \\ a_1 b_1 c_2 d_2 f(v_i) f^2(v_a) f(v_u) + a_1 b_1 c_2 d_3 f(v_i) f^2(v_a) f^2(v_u) + \\ a_1 b_2 c_1 d_1 f(v_i) f(v_c) f(v_a) + a_1 b_2 c_1 d_2 f(v_i) f(v_c) f(v_a) f(v_u) + \\ a_1 b_2 c_1 d_3 f(v_i) f(v_c) f(v_a) f^2(v_u) + a_1 b_2 c_2 d_1 f(v_i) f(v_c) f^2(v_a) + \\ a_1 b_2 c_2 d_2 f(v_i) f(v_c) f^2(v_a) f(v_u) + a_1 b_2 c_2 d_3 f(v_i) f(v_c) f(v_a) f^2(v_u) + \\ a_1 b_3 c_1 d_1 f(v_i) f^2(v_c) f(v_a) + a_1 b_3 c_1 d_2 f(v_i) f^2(v_c) f(v_a) f(v_u) + \\ a_1 b_3 c_1 d_3 f(v_i) f^2(v_c) f(v_a) f^2(v_u) + a_1 b_3 c_2 d_1 f(v_i) f^2(v_c) f^2(v_a) + \\ a_1 b_3 c_2 d_2 f(v_i) f^2(v_c) f^2(v_a) f(v_u) + a_1 b_3 c_2 d_3 f(v_i) f^2(v_c) f^2(v_a) f^2(v_u) + \quad \text{(M.2)}$$

$$+a_2b_1c_1d_1f^2(v_i)f(v_c)f(v_a)+a_2b_1c_1d_2f^2(v_i)f(v_a)f(v_u)+$$
$$a_2b_1c_1d_3f^2(v_i)f(v_a)f^2(v_u)+a_2b_1c_2d_1f^2(v_i)f^2(v_a)+$$
$$a_2b_1c_2d_2f^2(v_i)f^2(v_a)f(v_u)+a_2b_1c_2d_3f^2(v_i)f^2(v_a)f^2(v_u)+$$
$$a_2b_2c_1d_1f^2(v_i)f(v_c)f(v_a)+a_2b2c_1d_2f^2(v_i)f(v_c)f(v_a)f(v_u)+$$
$$a_2b_2c_1d_3f^2(v_i)f(v_c)f(v_a)f^2(v_u)+a_2b_2c_2d_1f^2(v_i)f(v_c)f^2(v_a)+$$
$$a_2b_2c_2d_2f^2(v_i)f(v_c)f^2(v_a)f(v_u)+a_2b_2c_2d_3f^2(v_i)f(v_c)f^2(v_a)f^2(v_u)+$$
$$a_2b_3c_1d_1f^2(v_i)f^2(v_c)f(v_a)+a_2b_3c_1d_2f^2(v_i)f^2(v_c)f(v_a)f(v_u)+$$
$$a_2b_3c_1d_3f^2(v_i)f^2(v_c)f(v_a)f^2(v_u)+a_2b_3c_2d_1f^2(v_i)f^2(v_c)f^2(v_a)+$$
$$a_2b_3c_2d_2f^2(v_i)f^2(v_c)f^2(v_a)f(v_u)+a_2b_3c_2d_3f^2(v_i)f^2(v_c)f^2(v_a)f^2(v_u)$$

Наочно, що складові суми в яких відсутні змінні v_i, v_c, v_a, v_u при диференціюванні стануть рівними нулю, тому їх можна не враховувати.

Для проведення диференціювання використаємо пакет комп'ютерної алгебри Maxima та наведемо результати обчислень у вигляді рисунків.

$$F(v_i,v_c,v_a,v_u)=(a_2\,b_3\,c_2\,d_3\,f(v_a)^2\,f(v_c)^2\,f(v_i)^2\,f(v_u)^2-a_2\,b_3\,c_1\,d_3\,f(v_a)\,f(v_c)^2\,f(v_i)^2\,f(v_u)^2+a_2\,b_2\,c_2\,d_3\,f(v_a)^2\,f(v_c)\,f(v_i)^2\,f(v_u)^2-a_2\,b_2\,c_1\,d_3\,f(v_a)\,f(v_c)\,f(v_i)^2\,f(v_u)^2+a_1\,b_3\,c_2\,d_3\,f(v_a)^2\,f(v_c)^2\,f(v_i)\,f(v_u)^2-a_1\,b_3\,c_1\,d_3\,f(v_a)\,f(v_c)^2\,f(v_i)\,f(v_u)^2+a_1\,b_2\,c_2\,d_3\,f(v_a)^2\,f(v_c)\,f(v_i)\,f(v_u)^2-a_1\,b_2\,c_1\,d_3\,f(v_a)\,f(v_c)\,f(v_i)\,f(v_u)^2-a_2\,b_3\,c_2\,d_2\,f(v_a)^2\,f(v_c)^2\,f(v_i)^2\,f(v_u)+a_2\,b_3\,c_1\,d_2\,f(v_a)\,f(v_c)^2\,f(v_i)^2\,f(v_u)-a_2\,b_2\,c_2\,d_2\,f(v_a)^2\,f(v_c)\,f(v_i)^2\,f(v_u)+a_2\,b_2\,c_1\,d_2\,f(v_a)\,f(v_c)\,f(v_i)^2\,f(v_u)-a_1\,b_3\,c_2\,d_2\,f(v_a)^2\,f(v_c)^2\,f(v_i)\,f(v_u)+a_1\,b_3\,c_1\,d_2\,f(v_a)\,f(v_c)^2\,f(v_i)\,f(v_u)-a_1\,b_2\,c_2\,d_2\,f(v_a)^2\,f(v_c)\,f(v_i)\,f(v_u)+a_1\,b_2\,c_1\,d_2\,f(v_a)\,f(v_c)\,f(v_i)^2\,f(v_u)-a_1\,b_3\,c_2\,d_2\,f(v_a)^2\,f(v_c)^2\,f(v_i)\,f(v_u)+a_1\,b_3\,c_1\,d_2\,f(v_a)\,f(v_c)^2\,f(v_i)\,f(v_u)-a_1\,b_2\,c_2\,d_2\,f(v_a)^2\,f(v_c)\,f(v_i)\,f(v_u)+a_1\,b_2\,c_1\,d_2\,f(v_a)\,f(v_c)\,f(v_i)^2\,f(v_u)-a_1\,b_3\,c_2\,d_2\,f(v_a)^2\,f(v_c)^2\,f(v_i)\,f(v_u)+a_1\,b_3\,c_1\,d_2\,f(v_a)\,f(v_c)^2\,f(v_i)\,f(v_u)-a_1\,b_2\,c_2\,d_2\,f(v_a)^2\,f(v_c)\,f(v_i)\,f(v_u)+a_1\,b_2\,c_1\,d_2\,f(v_a)\,f(v_c)\,f(v_i)\,f(v_u)=a_1\,b_2\,c_1\,d_2\,\%e^{-\left(\frac{v_u}{k_3}\right)^{k_4}-\left(\frac{v_u}{k_1}\right)^{k_2}-\left(\frac{v_i}{k_3}\right)^{k_4}-\left(\frac{v_i}{k_1}\right)^{k_2}-\left(\frac{v_c}{k_3}\right)^{k_4}-\left(\frac{v_c}{k_1}\right)^{k_2}-\left(\frac{v_a}{k_3}\right)^{k_4}-\left(\frac{v_a}{k_1}\right)^{k_2}}-a_1\,b_2\,c_2\,d_2\,\%e^{-\left(\frac{v_u}{k_3}\right)^{k_4}-\left(\frac{v_u}{k_1}\right)^{k_2}-\left(\frac{v_i}{k_3}\right)^{k_4}-\left(\frac{v_i}{k_1}\right)^{k_2}-\left(\frac{v_c}{k_3}\right)^{k_4}-\left(\frac{v_c}{k_1}\right)^{k_2}-2\left(\frac{v_a}{k_3}\right)^{k_4}-2\left(\frac{v_a}{k_1}\right)^{k_2}}+a_1\,b_3\,c_1\,d_2\,\%e^{-\left(\frac{v_u}{k_3}\right)^{k_4}-\left(\frac{v_u}{k_1}\right)^{k_2}-\left(\frac{v_i}{k_3}\right)^{k_4}-\left(\frac{v_i}{k_1}\right)^{k_2}-2\left(\frac{v_c}{k_3}\right)^{k_4}-2\left(\frac{v_c}{k_1}\right)^{k_2}-\left(\frac{v_a}{k_3}\right)^{k_4}-\left(\frac{v_a}{k_1}\right)^{k_2}}-a_1\,b_3\,c_2\,d_2\,\%e^{-\left(\frac{v_u}{k_3}\right)^{k_4}-\left(\frac{v_u}{k_1}\right)^{k_2}-\left(\frac{v_i}{k_3}\right)^{k_4}-\left(\frac{v_i}{k_1}\right)^{k_2}-2\left(\frac{v_c}{k_3}\right)^{k_4}-2\left(\frac{v_c}{k_1}\right)^{k_2}-2\left(\frac{v_a}{k_3}\right)^{k_4}-2\left(\frac{v_a}{k_1}\right)^{k_2}}+a_2\,b_2\,c_1\,d_2\,\%e^{-\left(\frac{v_u}{k_3}\right)^{k_4}-\left(\frac{v_u}{k_1}\right)^{k_2}-2\left(\frac{v_i}{k_3}\right)^{k_4}-2\left(\frac{v_i}{k_1}\right)^{k_2}-\left(\frac{v_c}{k_3}\right)^{k_4}-\left(\frac{v_c}{k_1}\right)^{k_2}-\left(\frac{v_a}{k_3}\right)^{k_4}-\left(\frac{v_a}{k_1}\right)^{k_2}}-a_2\,b_2\,c_2\,d_2\,\%e^{-\left(\frac{v_u}{k_3}\right)^{k_4}-\left(\frac{v_u}{k_1}\right)^{k_2}-2\left(\frac{v_i}{k_3}\right)^{k_4}-2\left(\frac{v_i}{k_1}\right)^{k_2}-\left(\frac{v_c}{k_3}\right)^{k_4}-\left(\frac{v_c}{k_1}\right)^{k_2}-2\left(\frac{v_a}{k_3}\right)^{k_4}-2\left(\frac{v_a}{k_1}\right)^{k_2}}+a_2\,b_3\,c_1\,d_2\,\%e^{-\left(\frac{v_u}{k_3}\right)^{k_4}-\left(\frac{v_u}{k_1}\right)^{k_2}-2\left(\frac{v_i}{k_3}\right)^{k_4}-2\left(\frac{v_i}{k_1}\right)^{k_2}-2\left(\frac{v_c}{k_3}\right)^{k_4}-2\left(\frac{v_c}{k_1}\right)^{k_2}-\left(\frac{v_a}{k_3}\right)^{k_4}-\left(\frac{v_a}{k_1}\right)^{k_2}}-a_2\,b_3\,c_2\,d_2\,\%e^{-\left(\frac{v_u}{k_3}\right)^{k_4}-\left(\frac{v_u}{k_1}\right)^{k_2}-2\left(\frac{v_i}{k_3}\right)^{k_4}-2\left(\frac{v_i}{k_1}\right)^{k_2}-2\left(\frac{v_c}{k_3}\right)^{k_4}-2\left(\frac{v_c}{k_1}\right)^{k_2}-\left(\frac{v_a}{k_3}\right)^{k_4}-\left(\frac{v_a}{k_1}\right)^{k_2}}-a_1\,b_2\,c_1\,d_3\,\%e^{-2\left(\frac{v_u}{k_3}\right)^{k_4}-2\left(\frac{v_u}{k_1}\right)^{k_2}-\left(\frac{v_i}{k_3}\right)^{k_4}-\left(\frac{v_i}{k_1}\right)^{k_2}-\left(\frac{v_c}{k_3}\right)^{k_4}-\left(\frac{v_c}{k_1}\right)^{k_2}-\left(\frac{v_a}{k_3}\right)^{k_4}-\left(\frac{v_a}{k_1}\right)^{k_2}}+a_1\,b_2\,c_2\,d_3\,\%e^{-2\left(\frac{v_u}{k_3}\right)^{k_4}-2\left(\frac{v_u}{k_1}\right)^{k_2}-\left(\frac{v_i}{k_3}\right)^{k_4}-\left(\frac{v_i}{k_1}\right)^{k_2}-2\left(\frac{v_c}{k_3}\right)^{k_4}-2\left(\frac{v_c}{k_1}\right)^{k_2}-\left(\frac{v_a}{k_3}\right)^{k_4}-\left(\frac{v_a}{k_1}\right)^{k_2}}-a_1\,b_3\,c_1\,d_3\,\%e^{-2\left(\frac{v_u}{k_3}\right)^{k_4}-2\left(\frac{v_u}{k_1}\right)^{k_2}-\left(\frac{v_i}{k_3}\right)^{k_4}-\left(\frac{v_i}{k_1}\right)^{k_2}-2\left(\frac{v_c}{k_3}\right)^{k_4}-2\left(\frac{v_c}{k_1}\right)^{k_2}-\left(\frac{v_a}{k_3}\right)^{k_4}-\left(\frac{v_a}{k_1}\right)^{k_2}}+a_1\,b_3\,c_2\,d_3\,\%e^{-2\left(\frac{v_u}{k_3}\right)^{k_4}-2\left(\frac{v_u}{k_1}\right)^{k_2}-\left(\frac{v_i}{k_3}\right)^{k_4}-\left(\frac{v_i}{k_1}\right)^{k_2}-2\left(\frac{v_c}{k_3}\right)^{k_4}-2\left(\frac{v_c}{k_1}\right)^{k_2}-2\left(\frac{v_a}{k_3}\right)^{k_4}-2\left(\frac{v_a}{k_1}\right)^{k_2}}-a_2\,b_2\,c_1\,d_3\,\%e^{-2\left(\frac{v_u}{k_3}\right)^{k_4}-2\left(\frac{v_u}{k_1}\right)^{k_2}-2\left(\frac{v_i}{k_3}\right)^{k_4}-2\left(\frac{v_i}{k_1}\right)^{k_2}-\left(\frac{v_c}{k_3}\right)^{k_4}-\left(\frac{v_c}{k_1}\right)^{k_2}-\left(\frac{v_a}{k_3}\right)^{k_4}-\left(\frac{v_a}{k_1}\right)^{k_2}}+a_2\,b_2\,c_2\,d_3\,\%e^{-2\left(\frac{v_u}{k_3}\right)^{k_4}-2\left(\frac{v_u}{k_1}\right)^{k_2}-2\left(\frac{v_i}{k_3}\right)^{k_4}-2\left(\frac{v_i}{k_1}\right)^{k_2}-\left(\frac{v_c}{k_3}\right)^{k_4}-\left(\frac{v_c}{k_1}\right)^{k_2}-2\left(\frac{v_a}{k_3}\right)^{k_4}-2\left(\frac{v_a}{k_1}\right)^{k_2}}-a_2\,b_3\,c_1\,d_3\,\%e^{-2\left(\frac{v_u}{k_3}\right)^{k_4}-2\left(\frac{v_u}{k_1}\right)^{k_2}-2\left(\frac{v_i}{k_3}\right)^{k_4}-2\left(\frac{v_i}{k_1}\right)^{k_2}-2\left(\frac{v_c}{k_3}\right)^{k_4}-2\left(\frac{v_c}{k_1}\right)^{k_2}-\left(\frac{v_a}{k_3}\right)^{k_4}-\left(\frac{v_a}{k_1}\right)^{k_2}}+a_2\,b_3\,c_2\,d_3\,\%e^{-2\left(\frac{v_u}{k_3}\right)^{k_4}-2\left(\frac{v_u}{k_1}\right)^{k_2}-2\left(\frac{v_i}{k_3}\right)^{k_4}-2\left(\frac{v_i}{k_1}\right)^{k_2}-2\left(\frac{v_c}{k_3}\right)^{k_4}-2\left(\frac{v_c}{k_1}\right)^{k_2}-2\left(\frac{v_a}{k_3}\right)^{k_4}-2\left(\frac{v_a}{k_1}\right)^{k_2}})$$

Рисунок М.1 – Запис вихідної функції в пакеті Maxima

$$\frac{d}{dv_i}F(v_i,v_c,v_a,v_u)=(2a_2b_3c_2d_3f(v_a)^2f(v_c)^2f(v_i)\left(\frac{d}{dv_i}f(v_i)\right)f(v_u)^2-2a_2b_3c_1d_3f(v_a)f(v_c)^2f(v_i)\left(\frac{d}{dv_i}f(v_i)\right)f(v_u)^2+2a_2b_2c_2d_3$$
$$f(v_a)^2f(v_c)f(v_i)\left(\frac{d}{dv_i}f(v_i)\right)f(v_u)^2-2a_2b_2c_1d_3f(v_a)f(v_c)f(v_i)\left(\frac{d}{dv_i}f(v_i)\right)f(v_u)^2+a_1b_3c_2d_3f(v_a)^2f(v_c)^2\left(\frac{d}{dv_i}f(v_i)\right)f(v_u)^2-a_1b_3c_1$$
$$d_3f(v_a)f(v_c)^2\left(\frac{d}{dv_i}f(v_i)\right)f(v_u)^2+a_1b_2c_2d_3f(v_a)^2f(v_c)\left(\frac{d}{dv_i}f(v_i)\right)f(v_u)^2-a_1b_2c_1d_3f(v_a)f(v_c)\left(\frac{d}{dv_i}f(v_i)\right)f(v_u)^2-2a_2b_3c_2d_2f(v_a)^2$$
$$f(v_c)^2f(v_i)\left(\frac{d}{dv_i}f(v_i)\right)f(v_u)+2a_2b_3c_1d_2f(v_a)f(v_c)^2f(v_i)\left(\frac{d}{dv_i}f(v_i)\right)f(v_u)-2a_2b_2c_2d_2f(v_a)^2f(v_c)f(v_i)\left(\frac{d}{dv_i}f(v_i)\right)f(v_u)+2a_2b_2c_1d_2$$
$$f(v_a)f(v_c)f(v_i)\left(\frac{d}{dv_i}f(v_i)\right)f(v_u)-a_1b_3c_2d_2f(v_a)^2f(v_c)^2\left(\frac{d}{dv_i}f(v_i)\right)f(v_u)+a_1b_3c_1d_2f(v_a)f(v_c)^2\left(\frac{d}{dv_i}f(v_i)\right)f(v_u)-a_1b_2c_2d_2f(v_a)^2$$
$$f(v_c)\left(\frac{d}{dv_i}f(v_i)\right)f(v_u)+a_1b_2c_1d_2f(v_a)f(v_c)\left(\frac{d}{dv_i}f(v_i)\right)f(v_u)=a_1b_2c_1d_2\left(-\frac{k_4\left(\frac{v_i}{k_3}\right)^{k_4}}{v_i}-\frac{k_2\left(\frac{v_i}{k_1}\right)^{k_2}}{v_i}\right)$$
$$\%e^{-\left(\frac{v_u}{k_3}\right)^{k_4}-\left(\frac{v_u}{k_1}\right)^{k_2}-\left(\frac{v_i}{k_3}\right)^{k_4}-\left(\frac{v_i}{k_1}\right)^{k_2}-\left(\frac{v_c}{k_3}\right)^{k_4}-\left(\frac{v_c}{k_1}\right)^{k_2}-\left(\frac{v_a}{k_3}\right)^{k_4}-\left(\frac{v_a}{k_1}\right)^{k_2}}-a_1b_2c_2d_2\left(-\frac{k_4\left(\frac{v_i}{k_3}\right)^{k_4}}{v_i}-\frac{k_2\left(\frac{v_i}{k_1}\right)^{k_2}}{v_i}\right)$$
$$\%e^{-\left(\frac{v_u}{k_3}\right)^{k_4}-\left(\frac{v_u}{k_1}\right)^{k_2}-\left(\frac{v_i}{k_3}\right)^{k_4}-\left(\frac{v_i}{k_1}\right)^{k_2}-\left(\frac{v_c}{k_3}\right)^{k_4}-\left(\frac{v_c}{k_1}\right)^{k_2}-2\left(\frac{v_a}{k_3}\right)^{k_4}-2\left(\frac{v_a}{k_1}\right)^{k_2}}+a_1b_3c_1d_2\left(-\frac{k_4\left(\frac{v_i}{k_3}\right)^{k_4}}{v_i}-\frac{k_2\left(\frac{v_i}{k_1}\right)^{k_2}}{v_i}\right)$$
$$\%e^{-\left(\frac{v_u}{k_3}\right)^{k_4}-\left(\frac{v_u}{k_1}\right)^{k_2}-\left(\frac{v_i}{k_3}\right)^{k_4}-\left(\frac{v_i}{k_1}\right)^{k_2}-2\left(\frac{v_c}{k_3}\right)^{k_4}-2\left(\frac{v_c}{k_1}\right)^{k_2}-\left(\frac{v_a}{k_3}\right)^{k_4}-\left(\frac{v_a}{k_1}\right)^{k_2}}-a_1b_3c_2d_2\left(-\frac{k_4\left(\frac{v_i}{k_3}\right)^{k_4}}{v_i}-\frac{k_2\left(\frac{v_i}{k_1}\right)^{k_2}}{v_i}\right)$$
$$\%e^{-\left(\frac{v_u}{k_3}\right)^{k_4}-\left(\frac{v_u}{k_1}\right)^{k_2}-\left(\frac{v_i}{k_3}\right)^{k_4}-\left(\frac{v_i}{k_1}\right)^{k_2}-2\left(\frac{v_c}{k_3}\right)^{k_4}-2\left(\frac{v_c}{k_1}\right)^{k_2}-2\left(\frac{v_a}{k_3}\right)^{k_4}-2\left(\frac{v_a}{k_1}\right)^{k_2}}+a_2b_2c_1d_2\left(-\frac{2k_4\left(\frac{v_i}{k_3}\right)^{k_4}}{v_i}-\frac{2k_2\left(\frac{v_i}{k_1}\right)^{k_2}}{v_i}\right)$$
$$\%e^{-\left(\frac{v_u}{k_3}\right)^{k_4}-\left(\frac{v_u}{k_1}\right)^{k_2}-2\left(\frac{v_i}{k_3}\right)^{k_4}-2\left(\frac{v_i}{k_1}\right)^{k_2}-\left(\frac{v_c}{k_3}\right)^{k_4}-\left(\frac{v_c}{k_1}\right)^{k_2}-\left(\frac{v_a}{k_3}\right)^{k_4}-\left(\frac{v_a}{k_1}\right)^{k_2}}-a_2b_2c_2d_2\left(-\frac{2k_4\left(\frac{v_i}{k_3}\right)^{k_4}}{v_i}-\frac{2k_2\left(\frac{v_i}{k_1}\right)^{k_2}}{v_i}\right)$$
$$\%e^{-\left(\frac{v_u}{k_3}\right)^{k_4}-\left(\frac{v_u}{k_1}\right)^{k_2}-2\left(\frac{v_i}{k_3}\right)^{k_4}-2\left(\frac{v_i}{k_1}\right)^{k_2}-\left(\frac{v_c}{k_3}\right)^{k_4}-\left(\frac{v_c}{k_1}\right)^{k_2}-2\left(\frac{v_a}{k_3}\right)^{k_4}-2\left(\frac{v_a}{k_1}\right)^{k_2}}+a_2b_3c_1d_2\left(-\frac{2k_4\left(\frac{v_i}{k_3}\right)^{k_4}}{v_i}-\frac{2k_2\left(\frac{v_i}{k_1}\right)^{k_2}}{v_i}\right)$$
$$\%e^{-\left(\frac{v_u}{k_3}\right)^{k_4}-\left(\frac{v_u}{k_1}\right)^{k_2}-2\left(\frac{v_i}{k_3}\right)^{k_4}-2\left(\frac{v_i}{k_1}\right)^{k_2}-2\left(\frac{v_c}{k_3}\right)^{k_4}-2\left(\frac{v_c}{k_1}\right)^{k_2}-\left(\frac{v_a}{k_3}\right)^{k_4}-\left(\frac{v_a}{k_1}\right)^{k_2}}-a_2b_3c_2d_2\left(-\frac{2k_4\left(\frac{v_i}{k_3}\right)^{k_4}}{v_i}-\frac{2k_2\left(\frac{v_i}{k_1}\right)^{k_2}}{v_i}\right)$$
$$\%e^{-\left(\frac{v_u}{k_3}\right)^{k_4}-\left(\frac{v_u}{k_1}\right)^{k_2}-2\left(\frac{v_i}{k_3}\right)^{k_4}-2\left(\frac{v_i}{k_1}\right)^{k_2}-2\left(\frac{v_c}{k_3}\right)^{k_4}-2\left(\frac{v_c}{k_1}\right)^{k_2}-2\left(\frac{v_a}{k_3}\right)^{k_4}-2\left(\frac{v_a}{k_1}\right)^{k_2}}-a_1b_2c_1d_3\left(-\frac{k_4\left(\frac{v_i}{k_3}\right)^{k_4}}{v_i}-\frac{k_2\left(\frac{v_i}{k_1}\right)^{k_2}}{v_i}\right)$$
$$\%e^{-2\left(\frac{v_u}{k_3}\right)^{k_4}-2\left(\frac{v_u}{k_1}\right)^{k_2}-\left(\frac{v_i}{k_3}\right)^{k_4}-\left(\frac{v_i}{k_1}\right)^{k_2}-\left(\frac{v_c}{k_3}\right)^{k_4}-\left(\frac{v_c}{k_1}\right)^{k_2}-\left(\frac{v_a}{k_3}\right)^{k_4}-\left(\frac{v_a}{k_1}\right)^{k_2}}+a_1b_2c_2d_3\left(-\frac{k_4\left(\frac{v_i}{k_3}\right)^{k_4}}{v_i}-\frac{k_2\left(\frac{v_i}{k_1}\right)^{k_2}}{v_i}\right)$$
$$\%e^{-2\left(\frac{v_u}{k_3}\right)^{k_4}-2\left(\frac{v_u}{k_1}\right)^{k_2}-\left(\frac{v_i}{k_3}\right)^{k_4}-\left(\frac{v_i}{k_1}\right)^{k_2}-\left(\frac{v_c}{k_3}\right)^{k_4}-\left(\frac{v_c}{k_1}\right)^{k_2}-2\left(\frac{v_a}{k_3}\right)^{k_4}-2\left(\frac{v_a}{k_1}\right)^{k_2}}-a_1b_3c_1d_3\left(-\frac{k_4\left(\frac{v_i}{k_3}\right)^{k_4}}{v_i}-\frac{k_2\left(\frac{v_i}{k_1}\right)^{k_2}}{v_i}\right)$$
$$\%e^{-2\left(\frac{v_u}{k_3}\right)^{k_4}-2\left(\frac{v_u}{k_1}\right)^{k_2}-\left(\frac{v_i}{k_3}\right)^{k_4}-\left(\frac{v_i}{k_1}\right)^{k_2}-2\left(\frac{v_c}{k_3}\right)^{k_4}-2\left(\frac{v_c}{k_1}\right)^{k_2}-\left(\frac{v_a}{k_3}\right)^{k_4}-\left(\frac{v_a}{k_1}\right)^{k_2}}+a_1b_3c_2d_3\left(-\frac{k_4\left(\frac{v_i}{k_3}\right)^{k_4}}{v_i}-\frac{k_2\left(\frac{v_i}{k_1}\right)^{k_2}}{v_i}\right)$$
$$\%e^{-2\left(\frac{v_u}{k_3}\right)^{k_4}-2\left(\frac{v_u}{k_1}\right)^{k_2}-\left(\frac{v_i}{k_3}\right)^{k_4}-\left(\frac{v_i}{k_1}\right)^{k_2}-2\left(\frac{v_c}{k_3}\right)^{k_4}-2\left(\frac{v_c}{k_1}\right)^{k_2}-2\left(\frac{v_a}{k_3}\right)^{k_4}-2\left(\frac{v_a}{k_1}\right)^{k_2}}-a_2b_2c_1d_3\left(-\frac{2k_4\left(\frac{v_i}{k_3}\right)^{k_4}}{v_i}-\frac{2k_2\left(\frac{v_i}{k_1}\right)^{k_2}}{v_i}\right)$$
$$\%e^{-2\left(\frac{v_u}{k_3}\right)^{k_4}-2\left(\frac{v_u}{k_1}\right)^{k_2}-2\left(\frac{v_i}{k_3}\right)^{k_4}-2\left(\frac{v_i}{k_1}\right)^{k_2}-\left(\frac{v_c}{k_3}\right)^{k_4}-\left(\frac{v_c}{k_1}\right)^{k_2}-\left(\frac{v_a}{k_3}\right)^{k_4}-\left(\frac{v_a}{k_1}\right)^{k_2}}+a_2b_2c_2d_3\left(-\frac{2k_4\left(\frac{v_i}{k_3}\right)^{k_4}}{v_i}-\frac{2k_2\left(\frac{v_i}{k_1}\right)^{k_2}}{v_i}\right)$$
$$\%e^{-2\left(\frac{v_u}{k_3}\right)^{k_4}-2\left(\frac{v_u}{k_1}\right)^{k_2}-2\left(\frac{v_i}{k_3}\right)^{k_4}-2\left(\frac{v_i}{k_1}\right)^{k_2}-\left(\frac{v_c}{k_3}\right)^{k_4}-\left(\frac{v_c}{k_1}\right)^{k_2}-2\left(\frac{v_a}{k_3}\right)^{k_4}-2\left(\frac{v_a}{k_1}\right)^{k_2}}-a_2b_3c_1d_3\left(-\frac{2k_4\left(\frac{v_i}{k_3}\right)^{k_4}}{v_i}-\frac{2k_2\left(\frac{v_i}{k_1}\right)^{k_2}}{v_i}\right)$$
$$\%e^{-2\left(\frac{v_u}{k_3}\right)^{k_4}-2\left(\frac{v_u}{k_1}\right)^{k_2}-2\left(\frac{v_i}{k_3}\right)^{k_4}-2\left(\frac{v_i}{k_1}\right)^{k_2}-2\left(\frac{v_c}{k_3}\right)^{k_4}-2\left(\frac{v_c}{k_1}\right)^{k_2}-\left(\frac{v_a}{k_3}\right)^{k_4}-\left(\frac{v_a}{k_1}\right)^{k_2}}+a_2b_3c_2d_3\left(-\frac{2k_4\left(\frac{v_i}{k_3}\right)^{k_4}}{v_i}-\frac{2k_2\left(\frac{v_i}{k_1}\right)^{k_2}}{v_i}\right)$$
$$\%e^{-2\left(\frac{v_u}{k_3}\right)^{k_4}-2\left(\frac{v_u}{k_1}\right)^{k_2}-2\left(\frac{v_i}{k_3}\right)^{k_4}-2\left(\frac{v_i}{k_1}\right)^{k_2}-2\left(\frac{v_c}{k_3}\right)^{k_4}-2\left(\frac{v_c}{k_1}\right)^{k_2}-2\left(\frac{v_a}{k_3}\right)^{k_4}-2\left(\frac{v_a}{k_1}\right)^{k_2}})$$

Рисунок М.2 – Часткова похідна за параметром v_i

$$\frac{d^2}{d v_c\, d v_i} F(v_i, v_c, v_a, v_u) = (4\, a_2\, b_3\, c_2\, d_3\, f(v_a)^2\, f(v_c) \left(\frac{d}{d v_c} f(v_c)\right) f(v_i) \left(\frac{d}{d v_i} f(v_i)\right) f(v_u)^2 - 4\, a_2\, b_3\, c_1\, d_3\, f(v_a)\, f(v_c) \left(\frac{d}{d v_c} f(v_c)\right) f(v_i)$$
$$\left(\frac{d}{d v_i} f(v_i)\right) f(v_u)^2 + 2\, a_2\, b_2\, c_2\, d_3\, f(v_a)^2 \left(\frac{d}{d v_c} f(v_c)\right) f(v_i) \left(\frac{d}{d v_i} f(v_i)\right) f(v_u)^2 - 2\, a_2\, b_2\, c_1\, d_3\, f(v_a) \left(\frac{d}{d v_c} f(v_c)\right) f(v_i) \left(\frac{d}{d v_i} f(v_i)\right) f(v_u)^2 + 2\, a_1\, b_3\, c_2$$
$$d_3\, f(v_a)^2\, f(v_c) \left(\frac{d}{d v_c} f(v_c)\right)\left(\frac{d}{d v_i} f(v_i)\right) f(v_u)^2 - 2\, a_1\, b_3\, c_1\, d_3\, f(v_a)\, f(v_c) \left(\frac{d}{d v_c} f(v_c)\right)\left(\frac{d}{d v_i} f(v_i)\right) f(v_u)^2 + a_1\, b_2\, c_2\, d_3\, f(v_a)^2 \left(\frac{d}{d v_c} f(v_c)\right)$$
$$\left(\frac{d}{d v_i} f(v_i)\right) f(v_u)^2 - a_1\, b_2\, c_1\, d_3\, f(v_a) \left(\frac{d}{d v_c} f(v_c)\right)\left(\frac{d}{d v_i} f(v_i)\right) f(v_u)^2 - 4\, a_2\, b_3\, c_2\, d_2\, f(v_a)^2\, f(v_c) \left(\frac{d}{d v_c} f(v_c)\right) f(v_i) \left(\frac{d}{d v_i} f(v_i)\right) f(v_u) + 4\, a_2\, b_3\, c_1$$
$$d_2\, f(v_a)\, f(v_c) \left(\frac{d}{d v_c} f(v_c)\right) f(v_i) \left(\frac{d}{d v_i} f(v_i)\right) f(v_u) - 2\, a_2\, b_2\, c_2\, d_2\, f(v_a)^2 \left(\frac{d}{d v_c} f(v_c)\right) f(v_i) \left(\frac{d}{d v_i} f(v_i)\right) f(v_u) + 2\, a_2\, b_2\, c_1\, d_2\, f(v_a) \left(\frac{d}{d v_c} f(v_c)\right) f(v_i)$$
$$\left(\frac{d}{d v_i} f(v_i)\right) f(v_u) - 2\, a_1\, b_3\, c_2\, d_2\, f(v_a)^2\, f(v_c) \left(\frac{d}{d v_c} f(v_c)\right)\left(\frac{d}{d v_i} f(v_i)\right) f(v_u) + 2\, a_1\, b_3\, c_1\, d_2\, f(v_a)\, f(v_c) \left(\frac{d}{d v_c} f(v_c)\right)\left(\frac{d}{d v_i} f(v_i)\right) f(v_u) - a_1\, b_2\, c_2\, d_2$$
$$f(v_a)^2 \left(\frac{d}{d v_c} f(v_c)\right)\left(\frac{d}{d v_i} f(v_i)\right) f(v_u) + a_1\, b_2\, c_1\, d_2\, f(v_a) \left(\frac{d}{d v_c} f(v_c)\right)\left(\frac{d}{d v_i} f(v_i)\right) f(v_u) = a_1\, b_2\, c_1\, d_2 \left(-\frac{k_4 \left(\frac{v_c}{k_3}\right)^{k_4}}{v_c} - \frac{k_2 \left(\frac{v_c}{k_1}\right)^{k_2}}{v_c}\right)$$
$$\left(-\frac{k_4 \left(\frac{v_i}{k_3}\right)^{k_4}}{v_i} - \frac{k_2 \left(\frac{v_i}{k_1}\right)^{k_2}}{v_i}\right) \%e^{-\left(\frac{v_u}{k_3}\right)^{k_4} - \left(\frac{v_u}{k_1}\right)^{k_2} - \left(\frac{v_i}{k_3}\right)^{k_4} - \left(\frac{v_i}{k_1}\right)^{k_2} - \left(\frac{v_c}{k_3}\right)^{k_4} - \left(\frac{v_c}{k_1}\right)^{k_2} - \left(\frac{v_a}{k_3}\right)^{k_4} - \left(\frac{v_a}{k_1}\right)^{k_2}} - a_1\, b_2\, c_2\, d_2 \left(-\frac{k_4 \left(\frac{v_c}{k_3}\right)^{k_4}}{v_c} - \frac{k_2 \left(\frac{v_c}{k_1}\right)^{k_2}}{v_c}\right)$$
$$\left(-\frac{k_4 \left(\frac{v_i}{k_3}\right)^{k_4}}{v_i} - \frac{k_2 \left(\frac{v_i}{k_1}\right)^{k_2}}{v_i}\right) \%e^{-\left(\frac{v_u}{k_3}\right)^{k_4} - \left(\frac{v_u}{k_1}\right)^{k_2} - \left(\frac{v_i}{k_3}\right)^{k_4} - \left(\frac{v_i}{k_1}\right)^{k_2} - \left(\frac{v_c}{k_3}\right)^{k_4} - \left(\frac{v_c}{k_1}\right)^{k_2} - 2\left(\frac{v_a}{k_3}\right)^{k_4} - 2\left(\frac{v_a}{k_1}\right)^{k_2}} + a_1\, b_3\, c_1\, d_2 \left(-\frac{2\, k_4 \left(\frac{v_c}{k_3}\right)^{k_4}}{v_c} - \frac{2\, k_2 \left(\frac{v_c}{k_1}\right)^{k_2}}{v_c}\right)$$
$$\left(-\frac{k_4 \left(\frac{v_i}{k_3}\right)^{k_4}}{v_i} - \frac{k_2 \left(\frac{v_i}{k_1}\right)^{k_2}}{v_i}\right) \%e^{-\left(\frac{v_u}{k_3}\right)^{k_4} - \left(\frac{v_u}{k_1}\right)^{k_2} - \left(\frac{v_i}{k_3}\right)^{k_4} - \left(\frac{v_i}{k_1}\right)^{k_2} - 2\left(\frac{v_c}{k_3}\right)^{k_4} - 2\left(\frac{v_c}{k_1}\right)^{k_2} - \left(\frac{v_a}{k_3}\right)^{k_4} - \left(\frac{v_a}{k_1}\right)^{k_2}} - a_1\, b_3\, c_2\, d_2 \left(-\frac{2\, k_4 \left(\frac{v_c}{k_3}\right)^{k_4}}{v_c} - \frac{2\, k_2 \left(\frac{v_c}{k_1}\right)^{k_2}}{v_c}\right)$$
$$\left(-\frac{k_4 \left(\frac{v_i}{k_3}\right)^{k_4}}{v_i} - \frac{k_2 \left(\frac{v_i}{k_1}\right)^{k_2}}{v_i}\right) \%e^{-\left(\frac{v_u}{k_3}\right)^{k_4} - \left(\frac{v_u}{k_1}\right)^{k_2} - \left(\frac{v_i}{k_3}\right)^{k_4} - \left(\frac{v_i}{k_1}\right)^{k_2} - 2\left(\frac{v_c}{k_3}\right)^{k_4} - 2\left(\frac{v_c}{k_1}\right)^{k_2} - \left(\frac{v_a}{k_3}\right)^{k_4} - \left(\frac{v_a}{k_1}\right)^{k_2}} + a_2\, b_2\, c_1\, d_2 \left(-\frac{k_4 \left(\frac{v_c}{k_3}\right)^{k_4}}{v_c} - \frac{k_2 \left(\frac{v_c}{k_1}\right)^{k_2}}{v_c}\right)$$
$$\left(-\frac{2\, k_4 \left(\frac{v_i}{k_3}\right)^{k_4}}{v_i} - \frac{2\, k_2 \left(\frac{v_i}{k_1}\right)^{k_2}}{v_i}\right) \%e^{-\left(\frac{v_u}{k_3}\right)^{k_4} - \left(\frac{v_u}{k_1}\right)^{k_2} - 2\left(\frac{v_i}{k_3}\right)^{k_4} - 2\left(\frac{v_i}{k_1}\right)^{k_2} - \left(\frac{v_c}{k_3}\right)^{k_4} - \left(\frac{v_c}{k_1}\right)^{k_2} - \left(\frac{v_a}{k_3}\right)^{k_4} - \left(\frac{v_a}{k_1}\right)^{k_2}} - a_2\, b_2\, c_2\, d_2 \left(-\frac{k_4 \left(\frac{v_c}{k_3}\right)^{k_4}}{v_c} - \frac{k_2 \left(\frac{v_c}{k_1}\right)^{k_2}}{v_c}\right)$$
$$\left(-\frac{2\, k_4 \left(\frac{v_i}{k_3}\right)^{k_4}}{v_i} - \frac{2\, k_2 \left(\frac{v_i}{k_1}\right)^{k_2}}{v_i}\right) \%e^{-\left(\frac{v_u}{k_3}\right)^{k_4} - \left(\frac{v_u}{k_1}\right)^{k_2} - 2\left(\frac{v_i}{k_3}\right)^{k_4} - 2\left(\frac{v_i}{k_1}\right)^{k_2} - \left(\frac{v_c}{k_3}\right)^{k_4} - \left(\frac{v_c}{k_1}\right)^{k_2} - 2\left(\frac{v_a}{k_3}\right)^{k_4} - 2\left(\frac{v_a}{k_1}\right)^{k_2}} + a_2\, b_3\, c_1\, d_2 \left(-\frac{2\, k_4 \left(\frac{v_c}{k_3}\right)^{k_4}}{v_c} - \frac{2\, k_2 \left(\frac{v_c}{k_1}\right)^{k_2}}{v_c}\right)$$
$$\left(-\frac{2\, k_4 \left(\frac{v_i}{k_3}\right)^{k_4}}{v_i} - \frac{2\, k_2 \left(\frac{v_i}{k_1}\right)^{k_2}}{v_i}\right) \%e^{-\left(\frac{v_u}{k_3}\right)^{k_4} - \left(\frac{v_u}{k_1}\right)^{k_2} - 2\left(\frac{v_i}{k_3}\right)^{k_4} - 2\left(\frac{v_i}{k_1}\right)^{k_2} - 2\left(\frac{v_c}{k_3}\right)^{k_4} - 2\left(\frac{v_c}{k_1}\right)^{k_2} - \left(\frac{v_a}{k_3}\right)^{k_4} - \left(\frac{v_a}{k_1}\right)^{k_2}} - a_2\, b_3\, c_2\, d_2 \left(-\frac{2\, k_4 \left(\frac{v_c}{k_3}\right)^{k_4}}{v_c} - \frac{2\, k_2 \left(\frac{v_c}{k_1}\right)^{k_2}}{v_c}\right)$$
$$\left(-\frac{2\, k_4 \left(\frac{v_i}{k_3}\right)^{k_4}}{v_i} - \frac{2\, k_2 \left(\frac{v_i}{k_1}\right)^{k_2}}{v_i}\right) \%e^{-\left(\frac{v_u}{k_3}\right)^{k_4} - \left(\frac{v_u}{k_1}\right)^{k_2} - 2\left(\frac{v_i}{k_3}\right)^{k_4} - 2\left(\frac{v_i}{k_1}\right)^{k_2} - 2\left(\frac{v_c}{k_3}\right)^{k_4} - 2\left(\frac{v_c}{k_1}\right)^{k_2} - 2\left(\frac{v_a}{k_3}\right)^{k_4} - 2\left(\frac{v_a}{k_1}\right)^{k_2}} - a_1\, b_2\, c_1\, d_3 \left(-\frac{k_4 \left(\frac{v_c}{k_3}\right)^{k_4}}{v_c} - \frac{k_2 \left(\frac{v_c}{k_1}\right)^{k_2}}{v_c}\right)$$
$$\left(-\frac{k_4 \left(\frac{v_i}{k_3}\right)^{k_4}}{v_i} - \frac{k_2 \left(\frac{v_i}{k_1}\right)^{k_2}}{v_i}\right) \%e^{-2\left(\frac{v_u}{k_3}\right)^{k_4} - 2\left(\frac{v_u}{k_1}\right)^{k_2} - \left(\frac{v_i}{k_3}\right)^{k_4} - \left(\frac{v_i}{k_1}\right)^{k_2} - \left(\frac{v_c}{k_3}\right)^{k_4} - \left(\frac{v_c}{k_1}\right)^{k_2} - \left(\frac{v_a}{k_3}\right)^{k_4} - \left(\frac{v_a}{k_1}\right)^{k_2}} + a_1\, b_2\, c_2\, d_3 \left(-\frac{k_4 \left(\frac{v_c}{k_3}\right)^{k_4}}{v_c} - \frac{k_2 \left(\frac{v_c}{k_1}\right)^{k_2}}{v_c}\right)$$
$$\left(-\frac{k_4 \left(\frac{v_i}{k_3}\right)^{k_4}}{v_i} - \frac{k_2 \left(\frac{v_i}{k_1}\right)^{k_2}}{v_i}\right) \%e^{-2\left(\frac{v_u}{k_3}\right)^{k_4} - 2\left(\frac{v_u}{k_1}\right)^{k_2} - \left(\frac{v_i}{k_3}\right)^{k_4} - \left(\frac{v_i}{k_1}\right)^{k_2} - 2\left(\frac{v_c}{k_3}\right)^{k_4} - 2\left(\frac{v_c}{k_1}\right)^{k_2} - \left(\frac{v_a}{k_3}\right)^{k_4} - \left(\frac{v_a}{k_1}\right)^{k_2}} - a_1\, b_3\, c_1\, d_3 \left(-\frac{2\, k_4 \left(\frac{v_c}{k_3}\right)^{k_4}}{v_c} - \frac{2\, k_2 \left(\frac{v_c}{k_1}\right)^{k_2}}{v_c}\right)$$
$$\left(-\frac{k_4 \left(\frac{v_i}{k_3}\right)^{k_4}}{v_i} - \frac{k_2 \left(\frac{v_i}{k_1}\right)^{k_2}}{v_i}\right) \%e^{-2\left(\frac{v_u}{k_3}\right)^{k_4} - 2\left(\frac{v_u}{k_1}\right)^{k_2} - \left(\frac{v_i}{k_3}\right)^{k_4} - \left(\frac{v_i}{k_1}\right)^{k_2} - \left(\frac{v_c}{k_3}\right)^{k_4} - \left(\frac{v_c}{k_1}\right)^{k_2} - \left(\frac{v_a}{k_3}\right)^{k_4} - \left(\frac{v_a}{k_1}\right)^{k_2}} + a_1\, b_3\, c_2\, d_3 \left(-\frac{2\, k_4 \left(\frac{v_c}{k_3}\right)^{k_4}}{v_c} - \frac{2\, k_2 \left(\frac{v_c}{k_1}\right)^{k_2}}{v_c}\right)$$
$$\left(-\frac{k_4 \left(\frac{v_i}{k_3}\right)^{k_4}}{v_i} - \frac{k_2 \left(\frac{v_i}{k_1}\right)^{k_2}}{v_i}\right) \%e^{-2\left(\frac{v_u}{k_3}\right)^{k_4} - 2\left(\frac{v_u}{k_1}\right)^{k_2} - \left(\frac{v_i}{k_3}\right)^{k_4} - \left(\frac{v_i}{k_1}\right)^{k_2} - \left(\frac{v_c}{k_3}\right)^{k_4} - \left(\frac{v_c}{k_1}\right)^{k_2} - 2\left(\frac{v_a}{k_3}\right)^{k_4} - 2\left(\frac{v_a}{k_1}\right)^{k_2}} - a_2\, b_2\, c_1\, d_3 \left(-\frac{k_4 \left(\frac{v_c}{k_3}\right)^{k_4}}{v_c} - \frac{k_2 \left(\frac{v_c}{k_1}\right)^{k_2}}{v_c}\right)$$
$$\left(-\frac{2\, k_4 \left(\frac{v_i}{k_3}\right)^{k_4}}{v_i} - \frac{2\, k_2 \left(\frac{v_i}{k_1}\right)^{k_2}}{v_i}\right) \%e^{-2\left(\frac{v_u}{k_3}\right)^{k_4} - 2\left(\frac{v_u}{k_1}\right)^{k_2} - 2\left(\frac{v_i}{k_3}\right)^{k_4} - 2\left(\frac{v_i}{k_1}\right)^{k_2} - \left(\frac{v_c}{k_3}\right)^{k_4} - \left(\frac{v_c}{k_1}\right)^{k_2} - \left(\frac{v_a}{k_3}\right)^{k_4} - \left(\frac{v_a}{k_1}\right)^{k_2}} + a_2\, b_2\, c_2\, d_3 \left(-\frac{k_4 \left(\frac{v_c}{k_3}\right)^{k_4}}{v_c} - \frac{k_2 \left(\frac{v_c}{k_1}\right)^{k_2}}{v_c}\right)$$
$$\left(-\frac{2\, k_4 \left(\frac{v_i}{k_3}\right)^{k_4}}{v_i} - \frac{2\, k_2 \left(\frac{v_i}{k_1}\right)^{k_2}}{v_i}\right) \%e^{-2\left(\frac{v_u}{k_3}\right)^{k_4} - 2\left(\frac{v_u}{k_1}\right)^{k_2} - 2\left(\frac{v_i}{k_3}\right)^{k_4} - 2\left(\frac{v_i}{k_1}\right)^{k_2} - \left(\frac{v_c}{k_3}\right)^{k_4} - \left(\frac{v_c}{k_1}\right)^{k_2} - 2\left(\frac{v_a}{k_3}\right)^{k_4} - 2\left(\frac{v_a}{k_1}\right)^{k_2}} - a_2\, b_3\, c_1\, d_3 \left(-\frac{2\, k_4 \left(\frac{v_c}{k_3}\right)^{k_4}}{v_c} - \frac{2\, k_2 \left(\frac{v_c}{k_1}\right)^{k_2}}{v_c}\right)$$
$$\left(-\frac{2\, k_4 \left(\frac{v_i}{k_3}\right)^{k_4}}{v_i} - \frac{2\, k_2 \left(\frac{v_i}{k_1}\right)^{k_2}}{v_i}\right) \%e^{-2\left(\frac{v_u}{k_3}\right)^{k_4} - 2\left(\frac{v_u}{k_1}\right)^{k_2} - 2\left(\frac{v_i}{k_3}\right)^{k_4} - 2\left(\frac{v_i}{k_1}\right)^{k_2} - 2\left(\frac{v_c}{k_3}\right)^{k_4} - 2\left(\frac{v_c}{k_1}\right)^{k_2} - \left(\frac{v_a}{k_3}\right)^{k_4} - \left(\frac{v_a}{k_1}\right)^{k_2}} + a_2\, b_3\, c_2\, d_3 \left(-\frac{2\, k_4 \left(\frac{v_c}{k_3}\right)^{k_4}}{v_c} - \frac{2\, k_2 \left(\frac{v_c}{k_1}\right)^{k_2}}{v_c}\right)$$
$$\left(-\frac{2\, k_4 \left(\frac{v_i}{k_3}\right)^{k_4}}{v_i} - \frac{2\, k_2 \left(\frac{v_i}{k_1}\right)^{k_2}}{v_i}\right) \%e^{-2\left(\frac{v_u}{k_3}\right)^{k_4} - 2\left(\frac{v_u}{k_1}\right)^{k_2} - 2\left(\frac{v_i}{k_3}\right)^{k_4} - 2\left(\frac{v_i}{k_1}\right)^{k_2} - 2\left(\frac{v_c}{k_3}\right)^{k_4} - 2\left(\frac{v_c}{k_1}\right)^{k_2} - 2\left(\frac{v_a}{k_3}\right)^{k_4} - 2\left(\frac{v_a}{k_1}\right)^{k_2}}\Bigg)$$

Рисунок М.3 – Часткова похідна за параметрами v_i та v_c

$$\frac{d^3}{d\,v_a\,d\,v_c\,d\,v_i}F(v_i,v_c,v_a,v_u)=(8\,a_2\,b_3\,c_2\,d_3\,f(v_a)\left(\frac{d}{d\,v_a}f(v_a)\right)f(v_c)\left(\frac{d}{d\,v_c}f(v_c)\right)f(v_i)\left(\frac{d}{d\,v_i}f(v_i)\right)f(v_u)^2-4\,a_2\,b_3\,c_1\,d_3\left(\frac{d}{d\,v_a}f(v_a)\right)f(v_c)$$
$$\left(\frac{d}{d\,v_c}f(v_c)\right)f(v_i)\left(\frac{d}{d\,v_i}f(v_i)\right)f(v_u)^2+4\,a_2\,b_2\,c_2\,d_3\,f(v_a)\left(\frac{d}{d\,v_a}f(v_a)\right)\left(\frac{d}{d\,v_c}f(v_c)\right)f(v_i)\left(\frac{d}{d\,v_i}f(v_i)\right)f(v_u)^2-2\,a_2\,b_2\,c_1\,d_3\left(\frac{d}{d\,v_a}f(v_a)\right)\left(\frac{d}{d\,v_c}f(v_c)\right)$$
$$f(v_i)\left(\frac{d}{d\,v_i}f(v_i)\right)f(v_u)^2+4\,a_1\,b_3\,c_2\,d_3\,f(v_a)\left(\frac{d}{d\,v_a}f(v_a)\right)f(v_c)\left(\frac{d}{d\,v_c}f(v_c)\right)\left(\frac{d}{d\,v_i}f(v_i)\right)f(v_u)^2-2\,a_1\,b_3\,c_1\,d_3\left(\frac{d}{d\,v_a}f(v_a)\right)f(v_c)\left(\frac{d}{d\,v_c}f(v_c)\right)$$
$$\left(\frac{d}{d\,v_i}f(v_i)\right)f(v_u)^2+2\,a_1\,b_2\,c_2\,d_3\,f(v_a)\left(\frac{d}{d\,v_a}f(v_a)\right)\left(\frac{d}{d\,v_c}f(v_c)\right)\left(\frac{d}{d\,v_i}f(v_i)\right)f(v_u)^2-a_1\,b_2\,c_1\,d_3\left(\frac{d}{d\,v_a}f(v_a)\right)\left(\frac{d}{d\,v_c}f(v_c)\right)\left(\frac{d}{d\,v_i}f(v_i)\right)f(v_u)^2-8\,a_2$$
$$b_3\,c_2\,d_2\,f(v_a)\left(\frac{d}{d\,v_a}f(v_a)\right)f(v_c)\left(\frac{d}{d\,v_c}f(v_c)\right)f(v_i)\left(\frac{d}{d\,v_i}f(v_i)\right)f(v_u)+4\,a_2\,b_3\,c_1\,d_2\left(\frac{d}{d\,v_a}f(v_a)\right)f(v_c)\left(\frac{d}{d\,v_c}f(v_c)\right)f(v_i)\left(\frac{d}{d\,v_i}f(v_i)\right)f(v_u)-4\,a_2\,b_2$$
$$c_2\,d_2\,f(v_a)\left(\frac{d}{d\,v_a}f(v_a)\right)\left(\frac{d}{d\,v_c}f(v_c)\right)f(v_i)\left(\frac{d}{d\,v_i}f(v_i)\right)f(v_u)+2\,a_2\,b_2\,c_1\,d_2\left(\frac{d}{d\,v_a}f(v_a)\right)\left(\frac{d}{d\,v_c}f(v_c)\right)f(v_i)\left(\frac{d}{d\,v_i}f(v_i)\right)f(v_u)-4\,a_1\,b_3\,c_2\,d_2\,f(v_a)$$
$$\left(\frac{d}{d\,v_a}f(v_a)\right)f(v_c)\left(\frac{d}{d\,v_c}f(v_c)\right)\left(\frac{d}{d\,v_i}f(v_i)\right)f(v_u)+2\,a_1\,b_3\,c_1\,d_2\left(\frac{d}{d\,v_a}f(v_a)\right)f(v_c)\left(\frac{d}{d\,v_c}f(v_c)\right)\left(\frac{d}{d\,v_i}f(v_i)\right)f(v_u)-2\,a_1\,b_2\,c_2\,d_2\,f(v_a)\left(\frac{d}{d\,v_a}f(v_a)\right)$$
$$\left(\frac{d}{d\,v_c}f(v_c)\right)\left(\frac{d}{d\,v_i}f(v_i)\right)f(v_u)+a_1\,b_2\,c_1\,d_2\left(\frac{d}{d\,v_a}f(v_a)\right)\left(\frac{d}{d\,v_c}f(v_c)\right)\left(\frac{d}{d\,v_i}f(v_i)\right)f(v_u)=a_1\,b_2\,c_1\,d_2\left(-\frac{k_4\left(\frac{v_a}{k_3}\right)^{k_4}}{v_a}-\frac{k_2\left(\frac{v_a}{k_1}\right)^{k_2}}{v_a}\right)$$
$$\left(-\frac{k_4\left(\frac{v_c}{k_3}\right)^{k_4}}{v_c}-\frac{k_2\left(\frac{v_c}{k_1}\right)^{k_2}}{v_c}\right)\left(-\frac{k_4\left(\frac{v_i}{k_3}\right)^{k_4}}{v_i}-\frac{k_2\left(\frac{v_i}{k_1}\right)^{k_2}}{v_i}\right)\%e^{-\left(\frac{v_u}{k_3}\right)^{k_4}-\left(\frac{v_u}{k_1}\right)^{k_2}-\left(\frac{v_i}{k_3}\right)^{k_4}-\left(\frac{v_i}{k_1}\right)^{k_2}-\left(\frac{v_c}{k_3}\right)^{k_4}-\left(\frac{v_c}{k_1}\right)^{k_2}-\left(\frac{v_a}{k_3}\right)^{k_4}-\left(\frac{v_a}{k_1}\right)^{k_2}}-a_1\,b_2\,c_2\,d_2$$
$$\left(-\frac{2\,k_4\left(\frac{v_a}{k_3}\right)^{k_4}}{v_a}-\frac{2\,k_2\left(\frac{v_a}{k_1}\right)^{k_2}}{v_a}\right)\left(-\frac{k_4\left(\frac{v_c}{k_3}\right)^{k_4}}{v_c}-\frac{k_2\left(\frac{v_c}{k_1}\right)^{k_2}}{v_c}\right)\left(-\frac{k_4\left(\frac{v_i}{k_3}\right)^{k_4}}{v_i}-\frac{k_2\left(\frac{v_i}{k_1}\right)^{k_2}}{v_i}\right)$$
$$\%e^{-\left(\frac{v_u}{k_3}\right)^{k_4}-\left(\frac{v_u}{k_1}\right)^{k_2}-\left(\frac{v_i}{k_3}\right)^{k_4}-\left(\frac{v_i}{k_1}\right)^{k_2}-\left(\frac{v_c}{k_3}\right)^{k_4}-\left(\frac{v_c}{k_1}\right)^{k_2}-2\left(\frac{v_a}{k_3}\right)^{k_4}-2\left(\frac{v_a}{k_1}\right)^{k_2}}+a_1\,b_3\,c_1\,d_2\left(-\frac{k_4\left(\frac{v_a}{k_3}\right)^{k_4}}{v_a}-\frac{k_2\left(\frac{v_a}{k_1}\right)^{k_2}}{v_a}\right)\left(-\frac{2\,k_4\left(\frac{v_c}{k_3}\right)^{k_4}}{v_c}-\frac{2\,k_2\left(\frac{v_c}{k_1}\right)^{k_2}}{v_c}\right)$$
$$\left(-\frac{k_4\left(\frac{v_i}{k_3}\right)^{k_4}}{v_i}-\frac{k_2\left(\frac{v_i}{k_1}\right)^{k_2}}{v_i}\right)\%e^{-\left(\frac{v_u}{k_3}\right)^{k_4}-\left(\frac{v_u}{k_1}\right)^{k_2}-\left(\frac{v_i}{k_3}\right)^{k_4}-\left(\frac{v_i}{k_1}\right)^{k_2}-2\left(\frac{v_c}{k_3}\right)^{k_4}-2\left(\frac{v_c}{k_1}\right)^{k_2}-\left(\frac{v_a}{k_3}\right)^{k_4}-\left(\frac{v_a}{k_1}\right)^{k_2}}-a_1\,b_3\,c_2\,d_2\left(-\frac{2\,k_4\left(\frac{v_a}{k_3}\right)^{k_4}}{v_a}-\frac{2\,k_2\left(\frac{v_a}{k_1}\right)^{k_2}}{v_a}\right)$$
$$\left(-\frac{2\,k_4\left(\frac{v_c}{k_3}\right)^{k_4}}{v_c}-\frac{2\,k_2\left(\frac{v_c}{k_1}\right)^{k_2}}{v_c}\right)\left(-\frac{k_4\left(\frac{v_i}{k_3}\right)^{k_4}}{v_i}-\frac{k_2\left(\frac{v_i}{k_1}\right)^{k_2}}{v_i}\right)\%e^{-\left(\frac{v_u}{k_3}\right)^{k_4}-\left(\frac{v_u}{k_1}\right)^{k_2}-\left(\frac{v_i}{k_3}\right)^{k_4}-\left(\frac{v_i}{k_1}\right)^{k_2}-2\left(\frac{v_c}{k_3}\right)^{k_4}-2\left(\frac{v_c}{k_1}\right)^{k_2}-2\left(\frac{v_a}{k_3}\right)^{k_4}-2\left(\frac{v_a}{k_1}\right)^{k_2}}+a_2\,b_2\,c_1\,d_2$$
$$\left(-\frac{k_4\left(\frac{v_a}{k_3}\right)^{k_4}}{v_a}-\frac{k_2\left(\frac{v_a}{k_1}\right)^{k_2}}{v_a}\right)\left(-\frac{k_4\left(\frac{v_c}{k_3}\right)^{k_4}}{v_c}-\frac{k_2\left(\frac{v_c}{k_1}\right)^{k_2}}{v_c}\right)\left(-\frac{2\,k_4\left(\frac{v_i}{k_3}\right)^{k_4}}{v_i}-\frac{2\,k_2\left(\frac{v_i}{k_1}\right)^{k_2}}{v_i}\right)$$
$$\%e^{-\left(\frac{v_u}{k_3}\right)^{k_4}-\left(\frac{v_u}{k_1}\right)^{k_2}-2\left(\frac{v_i}{k_3}\right)^{k_4}-2\left(\frac{v_i}{k_1}\right)^{k_2}-\left(\frac{v_c}{k_3}\right)^{k_4}-\left(\frac{v_c}{k_1}\right)^{k_2}-\left(\frac{v_a}{k_3}\right)^{k_4}-\left(\frac{v_a}{k_1}\right)^{k_2}}-a_2\,b_2\,c_2\,d_2\left(-\frac{2\,k_4\left(\frac{v_a}{k_3}\right)^{k_4}}{v_a}-\frac{2\,k_2\left(\frac{v_a}{k_1}\right)^{k_2}}{v_a}\right)\left(-\frac{k_4\left(\frac{v_c}{k_3}\right)^{k_4}}{v_c}-\frac{k_2\left(\frac{v_c}{k_1}\right)^{k_2}}{v_c}\right)$$
$$\left(-\frac{2\,k_4\left(\frac{v_i}{k_3}\right)^{k_4}}{v_i}-\frac{2\,k_2\left(\frac{v_i}{k_1}\right)^{k_2}}{v_i}\right)\%e^{-\left(\frac{v_u}{k_3}\right)^{k_4}-\left(\frac{v_u}{k_1}\right)^{k_2}-2\left(\frac{v_i}{k_3}\right)^{k_4}-2\left(\frac{v_i}{k_1}\right)^{k_2}-\left(\frac{v_c}{k_3}\right)^{k_4}-\left(\frac{v_c}{k_1}\right)^{k_2}-2\left(\frac{v_a}{k_3}\right)^{k_4}-2\left(\frac{v_a}{k_1}\right)^{k_2}}+a_2\,b_3\,c_1\,d_2\left(-\frac{k_4\left(\frac{v_a}{k_3}\right)^{k_4}}{v_a}-\frac{k_2\left(\frac{v_a}{k_1}\right)^{k_2}}{v_a}\right)$$
$$\left(-\frac{2\,k_4\left(\frac{v_c}{k_3}\right)^{k_4}}{v_c}-\frac{2\,k_2\left(\frac{v_c}{k_1}\right)^{k_2}}{v_c}\right)\left(-\frac{2\,k_4\left(\frac{v_i}{k_3}\right)^{k_4}}{v_i}-\frac{2\,k_2\left(\frac{v_i}{k_1}\right)^{k_2}}{v_i}\right)\%e^{-\left(\frac{v_u}{k_3}\right)^{k_4}-\left(\frac{v_u}{k_1}\right)^{k_2}-2\left(\frac{v_i}{k_3}\right)^{k_4}-2\left(\frac{v_i}{k_1}\right)^{k_2}-2\left(\frac{v_c}{k_3}\right)^{k_4}-2\left(\frac{v_c}{k_1}\right)^{k_2}-\left(\frac{v_a}{k_3}\right)^{k_4}-\left(\frac{v_a}{k_1}\right)^{k_2}}-a_2\,b_3\,c_2\,d_2$$
$$\left(-\frac{2\,k_4\left(\frac{v_a}{k_3}\right)^{k_4}}{v_a}-\frac{2\,k_2\left(\frac{v_a}{k_1}\right)^{k_2}}{v_a}\right)\left(-\frac{2\,k_4\left(\frac{v_c}{k_3}\right)^{k_4}}{v_c}-\frac{2\,k_2\left(\frac{v_c}{k_1}\right)^{k_2}}{v_c}\right)\left(-\frac{2\,k_4\left(\frac{v_i}{k_3}\right)^{k_4}}{v_i}-\frac{2\,k_2\left(\frac{v_i}{k_1}\right)^{k_2}}{v_i}\right)$$
$$\%e^{-2\left(\frac{v_u}{k_3}\right)^{k_4}-2\left(\frac{v_u}{k_1}\right)^{k_2}-\left(\frac{v_i}{k_3}\right)^{k_4}-\left(\frac{v_i}{k_1}\right)^{k_2}-2\left(\frac{v_c}{k_3}\right)^{k_4}-2\left(\frac{v_c}{k_1}\right)^{k_2}-\left(\frac{v_a}{k_3}\right)^{k_4}-\left(\frac{v_a}{k_1}\right)^{k_2}}-a_1\,b_2\,c_1\,d_3\left(-\frac{k_4\left(\frac{v_a}{k_3}\right)^{k_4}}{v_a}-\frac{k_2\left(\frac{v_a}{k_1}\right)^{k_2}}{v_a}\right)\left(-\frac{k_4\left(\frac{v_c}{k_3}\right)^{k_4}}{v_c}-\frac{k_2\left(\frac{v_c}{k_1}\right)^{k_2}}{v_c}\right)$$
$$\left(-\frac{k_4\left(\frac{v_i}{k_3}\right)^{k_4}}{v_i}-\frac{k_2\left(\frac{v_i}{k_1}\right)^{k_2}}{v_i}\right)\%e^{-2\left(\frac{v_u}{k_3}\right)^{k_4}-2\left(\frac{v_u}{k_1}\right)^{k_2}-\left(\frac{v_i}{k_3}\right)^{k_4}-\left(\frac{v_i}{k_1}\right)^{k_2}-\left(\frac{v_c}{k_3}\right)^{k_4}-\left(\frac{v_c}{k_1}\right)^{k_2}-\left(\frac{v_a}{k_3}\right)^{k_4}-\left(\frac{v_a}{k_1}\right)^{k_2}}+a_1\,b_2\,c_2\,d_3\left(-\frac{2\,k_4\left(\frac{v_a}{k_3}\right)^{k_4}}{v_a}-\frac{2\,k_2\left(\frac{v_a}{k_1}\right)^{k_2}}{v_a}\right)$$
$$\left(-\frac{k_4\left(\frac{v_c}{k_3}\right)^{k_4}}{v_c}-\frac{k_2\left(\frac{v_c}{k_1}\right)^{k_2}}{v_c}\right)\left(-\frac{k_4\left(\frac{v_i}{k_3}\right)^{k_4}}{v_i}-\frac{k_2\left(\frac{v_i}{k_1}\right)^{k_2}}{v_i}\right)\%e^{-2\left(\frac{v_u}{k_3}\right)^{k_4}-2\left(\frac{v_u}{k_1}\right)^{k_2}-2\left(\frac{v_i}{k_3}\right)^{k_4}-2\left(\frac{v_i}{k_1}\right)^{k_2}-\left(\frac{v_c}{k_3}\right)^{k_4}-\left(\frac{v_c}{k_1}\right)^{k_2}-\left(\frac{v_a}{k_3}\right)^{k_4}-\left(\frac{v_a}{k_1}\right)^{k_2}}-a_1\,b_3\,c_1\,d_3$$
$$\left(-\frac{k_4\left(\frac{v_a}{k_3}\right)^{k_4}}{v_a}-\frac{k_2\left(\frac{v_a}{k_1}\right)^{k_2}}{v_a}\right)\left(-\frac{2\,k_4\left(\frac{v_c}{k_3}\right)^{k_4}}{v_c}-\frac{2\,k_2\left(\frac{v_c}{k_1}\right)^{k_2}}{v_c}\right)\left(-\frac{k_4\left(\frac{v_i}{k_3}\right)^{k_4}}{v_i}-\frac{k_2\left(\frac{v_i}{k_1}\right)^{k_2}}{v_i}\right)$$
$$\%e^{-2\left(\frac{v_u}{k_3}\right)^{k_4}-2\left(\frac{v_u}{k_1}\right)^{k_2}-\left(\frac{v_i}{k_3}\right)^{k_4}-\left(\frac{v_i}{k_1}\right)^{k_2}-2\left(\frac{v_c}{k_3}\right)^{k_4}-2\left(\frac{v_c}{k_1}\right)^{k_2}-\left(\frac{v_a}{k_3}\right)^{k_4}-\left(\frac{v_a}{k_1}\right)^{k_2}}+a_1\,b_3\,c_2\,d_3\left(-\frac{2\,k_4\left(\frac{v_a}{k_3}\right)^{k_4}}{v_a}-\frac{2\,k_2\left(\frac{v_a}{k_1}\right)^{k_2}}{v_a}\right)\left(-\frac{2\,k_4\left(\frac{v_c}{k_3}\right)^{k_4}}{v_c}-\frac{2\,k_2\left(\frac{v_c}{k_1}\right)^{k_2}}{v_c}\right)$$
$$\left(-\frac{k_4\left(\frac{v_i}{k_3}\right)^{k_4}}{v_i}-\frac{k_2\left(\frac{v_i}{k_1}\right)^{k_2}}{v_i}\right)\%e^{-2\left(\frac{v_u}{k_3}\right)^{k_4}-2\left(\frac{v_u}{k_1}\right)^{k_2}-2\left(\frac{v_i}{k_3}\right)^{k_4}-2\left(\frac{v_i}{k_1}\right)^{k_2}-\left(\frac{v_c}{k_3}\right)^{k_4}-\left(\frac{v_c}{k_1}\right)^{k_2}-2\left(\frac{v_a}{k_3}\right)^{k_4}-2\left(\frac{v_a}{k_1}\right)^{k_2}}-a_2\,b_2\,c_1\,d_3\left(-\frac{k_4\left(\frac{v_a}{k_3}\right)^{k_4}}{v_a}-\frac{k_2\left(\frac{v_a}{k_1}\right)^{k_2}}{v_a}\right)$$
$$\left(-\frac{k_4\left(\frac{v_c}{k_3}\right)^{k_4}}{v_c}-\frac{k_2\left(\frac{v_c}{k_1}\right)^{k_2}}{v_c}\right)\left(-\frac{2\,k_4\left(\frac{v_i}{k_3}\right)^{k_4}}{v_i}-\frac{2\,k_2\left(\frac{v_i}{k_1}\right)^{k_2}}{v_i}\right)\%e^{-2\left(\frac{v_u}{k_3}\right)^{k_4}-2\left(\frac{v_u}{k_1}\right)^{k_2}-2\left(\frac{v_i}{k_3}\right)^{k_4}-2\left(\frac{v_i}{k_1}\right)^{k_2}-2\left(\frac{v_c}{k_3}\right)^{k_4}-2\left(\frac{v_c}{k_1}\right)^{k_2}-2\left(\frac{v_a}{k_3}\right)^{k_4}-2\left(\frac{v_a}{k_1}\right)^{k_2}}+a_2\,b_2\,c_2\,d_3$$
$$\left(-\frac{2\,k_4\left(\frac{v_a}{k_3}\right)^{k_4}}{v_a}-\frac{2\,k_2\left(\frac{v_a}{k_1}\right)^{k_2}}{v_a}\right)\left(-\frac{k_4\left(\frac{v_c}{k_3}\right)^{k_4}}{v_c}-\frac{k_2\left(\frac{v_c}{k_1}\right)^{k_2}}{v_c}\right)\left(-\frac{2\,k_4\left(\frac{v_i}{k_3}\right)^{k_4}}{v_i}-\frac{2\,k_2\left(\frac{v_i}{k_1}\right)^{k_2}}{v_i}\right)$$
$$\%e^{-2\left(\frac{v_u}{k_3}\right)^{k_4}-2\left(\frac{v_u}{k_1}\right)^{k_2}-2\left(\frac{v_i}{k_3}\right)^{k_4}-2\left(\frac{v_i}{k_1}\right)^{k_2}-\left(\frac{v_c}{k_3}\right)^{k_4}-\left(\frac{v_c}{k_1}\right)^{k_2}-2\left(\frac{v_a}{k_3}\right)^{k_4}-2\left(\frac{v_a}{k_1}\right)^{k_2}}-a_2\,b_3\,c_1\,d_3\left(-\frac{k_4\left(\frac{v_a}{k_3}\right)^{k_4}}{v_a}-\frac{k_2\left(\frac{v_a}{k_1}\right)^{k_2}}{v_a}\right)\left(-\frac{2\,k_4\left(\frac{v_c}{k_3}\right)^{k_4}}{v_c}-\frac{2\,k_2\left(\frac{v_c}{k_1}\right)^{k_2}}{v_c}\right)$$
$$\left(-\frac{2\,k_4\left(\frac{v_i}{k_3}\right)^{k_4}}{v_i}-\frac{2\,k_2\left(\frac{v_i}{k_1}\right)^{k_2}}{v_i}\right)\%e^{-2\left(\frac{v_u}{k_3}\right)^{k_4}-2\left(\frac{v_u}{k_1}\right)^{k_2}-2\left(\frac{v_i}{k_3}\right)^{k_4}-2\left(\frac{v_i}{k_1}\right)^{k_2}-2\left(\frac{v_c}{k_3}\right)^{k_4}-2\left(\frac{v_c}{k_1}\right)^{k_2}-\left(\frac{v_a}{k_3}\right)^{k_4}-\left(\frac{v_a}{k_1}\right)^{k_2}}+a_2\,b_3\,c_2\,d_3\left(-\frac{2\,k_4\left(\frac{v_a}{k_3}\right)^{k_4}}{v_a}-\frac{2\,k_2\left(\frac{v_a}{k_1}\right)^{k_2}}{v_a}\right)$$
$$\left(-\frac{2\,k_4\left(\frac{v_c}{k_3}\right)^{k_4}}{v_c}-\frac{2\,k_2\left(\frac{v_c}{k_1}\right)^{k_2}}{v_c}\right)\left(-\frac{2\,k_4\left(\frac{v_i}{k_3}\right)^{k_4}}{v_i}-\frac{2\,k_2\left(\frac{v_i}{k_1}\right)^{k_2}}{v_i}\right)\%e^{-2\left(\frac{v_u}{k_3}\right)^{k_4}-2\left(\frac{v_u}{k_1}\right)^{k_2}-2\left(\frac{v_i}{k_3}\right)^{k_4}-2\left(\frac{v_i}{k_1}\right)^{k_2}-2\left(\frac{v_c}{k_3}\right)^{k_4}-2\left(\frac{v_c}{k_1}\right)^{k_2}-2\left(\frac{v_a}{k_3}\right)^{k_4}-2\left(\frac{v_a}{k_1}\right)^{k_2}}\Bigg)$$

Рисунок М.4 – Часткова похідна за параметрами v_i, v_c, v_a

$$\frac{d^4}{d\,v_a\,d\,v_c\,d\,v_i\,d\,v_u}F(v_i,v_c,v_a,v_u)=(\,16\,a_2\,b_3\,c_2\,d_3\,f(v_a)\left(\frac{d}{d\,v_a}f(v_a)\right)f(v_c)\left(\frac{d}{d\,v_c}f(v_c)\right)f(v_i)\left(\frac{d}{d\,v_i}f(v_i)\right)f(v_u)\left(\frac{d}{d\,v_u}f(v_u)\right)-8\,a_2\,b_3\,c_1\,d_3$$
$$\left(\frac{d}{d\,v_a}f(v_a)\right)f(v_c)\left(\frac{d}{d\,v_c}f(v_c)\right)f(v_i)\left(\frac{d}{d\,v_i}f(v_i)\right)f(v_u)\left(\frac{d}{d\,v_u}f(v_u)\right)+8\,a_2\,b_2\,c_2\,d_3\,f(v_a)\left(\frac{d}{d\,v_a}f(v_a)\right)\left(\frac{d}{d\,v_c}f(v_c)\right)f(v_i)\left(\frac{d}{d\,v_i}f(v_i)\right)f(v_u)$$
$$\left(\frac{d}{d\,v_u}f(v_u)\right)-4\,a_2\,b_2\,c_1\,d_3\left(\frac{d}{d\,v_a}f(v_a)\right)\left(\frac{d}{d\,v_c}f(v_c)\right)f(v_i)\left(\frac{d}{d\,v_i}f(v_i)\right)f(v_u)\left(\frac{d}{d\,v_u}f(v_u)\right)+8\,a_1\,b_3\,c_2\,d_3\,f(v_a)\left(\frac{d}{d\,v_a}f(v_a)\right)f(v_c)\left(\frac{d}{d\,v_c}f(v_c)\right)$$
$$\left(\frac{d}{d\,v_i}f(v_i)\right)f(v_u)\left(\frac{d}{d\,v_u}f(v_u)\right)-4\,a_1\,b_3\,c_1\,d_3\left(\frac{d}{d\,v_a}f(v_a)\right)f(v_c)\left(\frac{d}{d\,v_c}f(v_c)\right)\left(\frac{d}{d\,v_i}f(v_i)\right)f(v_u)\left(\frac{d}{d\,v_u}f(v_u)\right)+4\,a_1\,b_2\,c_2\,d_3\,f(v_a)\left(\frac{d}{d\,v_a}f(v_a)\right)$$
$$\left(\frac{d}{d\,v_c}f(v_c)\right)\left(\frac{d}{d\,v_i}f(v_i)\right)f(v_u)\left(\frac{d}{d\,v_u}f(v_u)\right)-2\,a_1\,b_2\,c_1\,d_3\left(\frac{d}{d\,v_a}f(v_a)\right)\left(\frac{d}{d\,v_c}f(v_c)\right)\left(\frac{d}{d\,v_i}f(v_i)\right)f(v_u)\left(\frac{d}{d\,v_u}f(v_u)\right)-8\,a_2\,b_3\,c_2\,d_2\,f(v_a)\left(\frac{d}{d\,v_a}f(v_a)\right)$$
$$f(v_c)\left(\frac{d}{d\,v_c}f(v_c)\right)f(v_i)\left(\frac{d}{d\,v_i}f(v_i)\right)\left(\frac{d}{d\,v_u}f(v_u)\right)+4\,a_2\,b_3\,c_1\,d_2\left(\frac{d}{d\,v_a}f(v_a)\right)f(v_c)\left(\frac{d}{d\,v_c}f(v_c)\right)f(v_i)\left(\frac{d}{d\,v_i}f(v_i)\right)\left(\frac{d}{d\,v_u}f(v_u)\right)-4\,a_2\,b_2\,c_2\,d_2\,f(v_a)$$
$$\left(\frac{d}{d\,v_a}f(v_a)\right)\left(\frac{d}{d\,v_c}f(v_c)\right)f(v_i)\left(\frac{d}{d\,v_i}f(v_i)\right)\left(\frac{d}{d\,v_u}f(v_u)\right)+2\,a_2\,b_2\,c_1\,d_2\left(\frac{d}{d\,v_a}f(v_a)\right)\left(\frac{d}{d\,v_c}f(v_c)\right)f(v_i)\left(\frac{d}{d\,v_i}f(v_i)\right)\left(\frac{d}{d\,v_u}f(v_u)\right)-4\,a_1\,b_3\,c_2\,d_2\,f(v_a)$$
$$\left(\frac{d}{d\,v_a}f(v_a)\right)f(v_c)\left(\frac{d}{d\,v_c}f(v_c)\right)\left(\frac{d}{d\,v_i}f(v_i)\right)\left(\frac{d}{d\,v_u}f(v_u)\right)+2\,a_1\,b_3\,c_1\,d_2\left(\frac{d}{d\,v_a}f(v_a)\right)f(v_c)\left(\frac{d}{d\,v_c}f(v_c)\right)\left(\frac{d}{d\,v_i}f(v_i)\right)\left(\frac{d}{d\,v_u}f(v_u)\right)-2\,a_1\,b_2\,c_2\,d_2\,f(v_a)$$
$$\left(\frac{d}{d\,v_a}f(v_a)\right)\left(\frac{d}{d\,v_c}f(v_c)\right)\left(\frac{d}{d\,v_i}f(v_i)\right)\left(\frac{d}{d\,v_u}f(v_u)\right)+a_1\,b_2\,c_1\,d_2\left(\frac{d}{d\,v_a}f(v_a)\right)\left(\frac{d}{d\,v_c}f(v_c)\right)\left(\frac{d}{d\,v_i}f(v_i)\right)\left(\frac{d}{d\,v_u}f(v_u)\right)=a_1\,b_2\,c_1\,d_2$$

$$\left(-\frac{k_4\left(\frac{v_a}{k_3}\right)^{k_4}}{v_a}-\frac{k_2\left(\frac{v_a}{k_1}\right)^{k_2}}{v_a}\right)\left(-\frac{k_4\left(\frac{v_c}{k_3}\right)^{k_4}}{v_c}-\frac{k_2\left(\frac{v_c}{k_1}\right)^{k_2}}{v_c}\right)\left(-\frac{k_4\left(\frac{v_i}{k_3}\right)^{k_4}}{v_i}-\frac{k_2\left(\frac{v_i}{k_1}\right)^{k_2}}{v_i}\right)\left(-\frac{k_4\left(\frac{v_u}{k_3}\right)^{k_4}}{v_u}-\frac{k_2\left(\frac{v_u}{k_1}\right)^{k_2}}{v_u}\right)$$
$$\%e^{-\left(\frac{v_u}{k_3}\right)^{k_4}-\left(\frac{v_u}{k_1}\right)^{k_2}-\left(\frac{v_i}{k_3}\right)^{k_4}-\left(\frac{v_i}{k_1}\right)^{k_2}-\left(\frac{v_c}{k_3}\right)^{k_4}-\left(\frac{v_c}{k_1}\right)^{k_2}-\left(\frac{v_a}{k_3}\right)^{k_4}-\left(\frac{v_a}{k_1}\right)^{k_2}}-a_1\,b_2\,c_2\,d_2\left(-\frac{2\,k_4\left(\frac{v_a}{k_3}\right)^{k_4}}{v_a}-\frac{2\,k_2\left(\frac{v_a}{k_1}\right)^{k_2}}{v_a}\right)\left(-\frac{k_4\left(\frac{v_c}{k_3}\right)^{k_4}}{v_c}-\frac{k_2\left(\frac{v_c}{k_1}\right)^{k_2}}{v_c}\right)$$
$$\left(-\frac{k_4\left(\frac{v_i}{k_3}\right)^{k_4}}{v_i}-\frac{k_2\left(\frac{v_i}{k_1}\right)^{k_2}}{v_i}\right)\left(-\frac{k_4\left(\frac{v_u}{k_3}\right)^{k_4}}{v_u}-\frac{k_2\left(\frac{v_u}{k_1}\right)^{k_2}}{v_u}\right)\%e^{-\left(\frac{v_u}{k_3}\right)^{k_4}-\left(\frac{v_u}{k_1}\right)^{k_2}-\left(\frac{v_i}{k_3}\right)^{k_4}-\left(\frac{v_i}{k_1}\right)^{k_2}-\left(\frac{v_c}{k_3}\right)^{k_4}-\left(\frac{v_c}{k_1}\right)^{k_2}-2\left(\frac{v_a}{k_3}\right)^{k_4}-2\left(\frac{v_a}{k_1}\right)^{k_2}}+a_1\,b_3\,c_1\,d_2$$
$$\left(-\frac{k_4\left(\frac{v_a}{k_3}\right)^{k_4}}{v_a}-\frac{k_2\left(\frac{v_a}{k_1}\right)^{k_2}}{v_a}\right)\left(-\frac{2\,k_4\left(\frac{v_c}{k_3}\right)^{k_4}}{v_c}-\frac{2\,k_2\left(\frac{v_c}{k_1}\right)^{k_2}}{v_c}\right)\left(-\frac{k_4\left(\frac{v_i}{k_3}\right)^{k_4}}{v_i}-\frac{k_2\left(\frac{v_i}{k_1}\right)^{k_2}}{v_i}\right)\left(-\frac{k_4\left(\frac{v_u}{k_3}\right)^{k_4}}{v_u}-\frac{k_2\left(\frac{v_u}{k_1}\right)^{k_2}}{v_u}\right)$$
$$\%e^{-\left(\frac{v_u}{k_3}\right)^{k_4}-\left(\frac{v_u}{k_1}\right)^{k_2}-\left(\frac{v_i}{k_3}\right)^{k_4}-\left(\frac{v_i}{k_1}\right)^{k_2}-2\left(\frac{v_c}{k_3}\right)^{k_4}-2\left(\frac{v_c}{k_1}\right)^{k_2}-\left(\frac{v_a}{k_3}\right)^{k_4}-\left(\frac{v_a}{k_1}\right)^{k_2}}-a_1\,b_3\,c_2\,d_2\left(-\frac{2\,k_4\left(\frac{v_a}{k_3}\right)^{k_4}}{v_a}-\frac{2\,k_2\left(\frac{v_a}{k_1}\right)^{k_2}}{v_a}\right)\left(-\frac{2\,k_4\left(\frac{v_c}{k_3}\right)^{k_4}}{v_c}-\frac{2\,k_2\left(\frac{v_c}{k_1}\right)^{k_2}}{v_c}\right)$$
$$\left(-\frac{k_4\left(\frac{v_i}{k_3}\right)^{k_4}}{v_i}-\frac{k_2\left(\frac{v_i}{k_1}\right)^{k_2}}{v_i}\right)\left(-\frac{k_4\left(\frac{v_u}{k_3}\right)^{k_4}}{v_u}-\frac{k_2\left(\frac{v_u}{k_1}\right)^{k_2}}{v_u}\right)\%e^{-\left(\frac{v_u}{k_3}\right)^{k_4}-\left(\frac{v_u}{k_1}\right)^{k_2}-\left(\frac{v_i}{k_3}\right)^{k_4}-\left(\frac{v_i}{k_1}\right)^{k_2}-2\left(\frac{v_c}{k_3}\right)^{k_4}-2\left(\frac{v_c}{k_1}\right)^{k_2}-2\left(\frac{v_a}{k_3}\right)^{k_4}-2\left(\frac{v_a}{k_1}\right)^{k_2}}+a_2\,b_2\,c_1\,d_2$$
$$\left(-\frac{k_4\left(\frac{v_a}{k_3}\right)^{k_4}}{v_a}-\frac{k_2\left(\frac{v_a}{k_1}\right)^{k_2}}{v_a}\right)\left(-\frac{k_4\left(\frac{v_c}{k_3}\right)^{k_4}}{v_c}-\frac{k_2\left(\frac{v_c}{k_1}\right)^{k_2}}{v_c}\right)\left(-\frac{2\,k_4\left(\frac{v_i}{k_3}\right)^{k_4}}{v_i}-\frac{2\,k_2\left(\frac{v_i}{k_1}\right)^{k_2}}{v_i}\right)\left(-\frac{k_4\left(\frac{v_u}{k_3}\right)^{k_4}}{v_u}-\frac{k_2\left(\frac{v_u}{k_1}\right)^{k_2}}{v_u}\right)$$
$$\%e^{-\left(\frac{v_u}{k_3}\right)^{k_4}-\left(\frac{v_u}{k_1}\right)^{k_2}-2\left(\frac{v_i}{k_3}\right)^{k_4}-2\left(\frac{v_i}{k_1}\right)^{k_2}-\left(\frac{v_c}{k_3}\right)^{k_4}-\left(\frac{v_c}{k_1}\right)^{k_2}-\left(\frac{v_a}{k_3}\right)^{k_4}-\left(\frac{v_a}{k_1}\right)^{k_2}}-a_2\,b_2\,c_2\,d_2\left(-\frac{2\,k_4\left(\frac{v_a}{k_3}\right)^{k_4}}{v_a}-\frac{2\,k_2\left(\frac{v_a}{k_1}\right)^{k_2}}{v_a}\right)\left(-\frac{k_4\left(\frac{v_c}{k_3}\right)^{k_4}}{v_c}-\frac{k_2\left(\frac{v_c}{k_1}\right)^{k_2}}{v_c}\right)$$
$$\left(-\frac{2\,k_4\left(\frac{v_i}{k_3}\right)^{k_4}}{v_i}-\frac{2\,k_2\left(\frac{v_i}{k_1}\right)^{k_2}}{v_i}\right)\left(-\frac{k_4\left(\frac{v_u}{k_3}\right)^{k_4}}{v_u}-\frac{k_2\left(\frac{v_u}{k_1}\right)^{k_2}}{v_u}\right)\%e^{-\left(\frac{v_u}{k_3}\right)^{k_4}-2\left(\frac{v_u}{k_1}\right)^{k_2}-\left(\frac{v_i}{k_3}\right)^{k_4}-2\left(\frac{v_i}{k_1}\right)^{k_2}-\left(\frac{v_c}{k_3}\right)^{k_4}-\left(\frac{v_c}{k_1}\right)^{k_2}-\left(\frac{v_a}{k_3}\right)^{k_4}-2\left(\frac{v_a}{k_1}\right)^{k_2}}+a_2\,b_3\,c_1\,d_2$$
$$\left(-\frac{k_4\left(\frac{v_a}{k_3}\right)^{k_4}}{v_a}-\frac{k_2\left(\frac{v_a}{k_1}\right)^{k_2}}{v_a}\right)\left(-\frac{k_4\left(\frac{v_c}{k_3}\right)^{k_4}}{v_c}-\frac{k_2\left(\frac{v_c}{k_1}\right)^{k_2}}{v_c}\right)\left(-\frac{2\,k_4\left(\frac{v_i}{k_3}\right)^{k_4}}{v_i}-\frac{2\,k_2\left(\frac{v_i}{k_1}\right)^{k_2}}{v_i}\right)\left(-\frac{k_4\left(\frac{v_u}{k_3}\right)^{k_4}}{v_u}-\frac{k_2\left(\frac{v_u}{k_1}\right)^{k_2}}{v_u}\right)$$
$$\%e^{-\left(\frac{v_u}{k_3}\right)^{k_4}-2\left(\frac{v_u}{k_1}\right)^{k_2}-\left(\frac{v_i}{k_3}\right)^{k_4}-2\left(\frac{v_i}{k_1}\right)^{k_2}-2\left(\frac{v_c}{k_3}\right)^{k_4}-\left(\frac{v_c}{k_1}\right)^{k_2}-\left(\frac{v_a}{k_3}\right)^{k_4}-\left(\frac{v_a}{k_1}\right)^{k_2}}-a_2\,b_3\,c_2\,d_2\left(-\frac{2\,k_4\left(\frac{v_a}{k_3}\right)^{k_4}}{v_a}-\frac{2\,k_2\left(\frac{v_a}{k_1}\right)^{k_2}}{v_a}\right)\left(-\frac{2\,k_4\left(\frac{v_c}{k_3}\right)^{k_4}}{v_c}-\frac{2\,k_2\left(\frac{v_c}{k_1}\right)^{k_2}}{v_c}\right)$$
$$\left(-\frac{2\,k_4\left(\frac{v_i}{k_3}\right)^{k_4}}{v_i}-\frac{2\,k_2\left(\frac{v_i}{k_1}\right)^{k_2}}{v_i}\right)\left(-\frac{k_4\left(\frac{v_u}{k_3}\right)^{k_4}}{v_u}-\frac{k_2\left(\frac{v_u}{k_1}\right)^{k_2}}{v_u}\right)\%e^{-\left(\frac{v_u}{k_3}\right)^{k_4}-\left(\frac{v_u}{k_1}\right)^{k_2}-2\left(\frac{v_i}{k_3}\right)^{k_4}-2\left(\frac{v_i}{k_1}\right)^{k_2}-2\left(\frac{v_c}{k_3}\right)^{k_4}-2\left(\frac{v_c}{k_1}\right)^{k_2}-\left(\frac{v_a}{k_3}\right)^{k_4}-\left(\frac{v_a}{k_1}\right)^{k_2}}-a_2\,b_3\,c_1\,d_2$$
$$\left(-\frac{k_4\left(\frac{v_a}{k_3}\right)^{k_4}}{v_a}-\frac{k_2\left(\frac{v_a}{k_1}\right)^{k_2}}{v_a}\right)\left(-\frac{k_4\left(\frac{v_c}{k_3}\right)^{k_4}}{v_c}-\frac{k_2\left(\frac{v_c}{k_1}\right)^{k_2}}{v_c}\right)\left(-\frac{k_4\left(\frac{v_i}{k_3}\right)^{k_4}}{v_i}-\frac{k_2\left(\frac{v_i}{k_1}\right)^{k_2}}{v_i}\right)\left(-\frac{2\,k_4\left(\frac{v_u}{k_3}\right)^{k_4}}{v_u}-\frac{2\,k_2\left(\frac{v_u}{k_1}\right)^{k_2}}{v_u}\right)$$
$$\%e^{-2\left(\frac{v_u}{k_3}\right)^{k_4}-2\left(\frac{v_u}{k_1}\right)^{k_2}-\left(\frac{v_i}{k_3}\right)^{k_4}-\left(\frac{v_i}{k_1}\right)^{k_2}-\left(\frac{v_c}{k_3}\right)^{k_4}-\left(\frac{v_c}{k_1}\right)^{k_2}-\left(\frac{v_a}{k_3}\right)^{k_4}-\left(\frac{v_a}{k_1}\right)^{k_2}}+a_1\,b_2\,c_2\,d_3\left(-\frac{2\,k_4\left(\frac{v_a}{k_3}\right)^{k_4}}{v_a}-\frac{2\,k_2\left(\frac{v_a}{k_1}\right)^{k_2}}{v_a}\right)\left(-\frac{k_4\left(\frac{v_c}{k_3}\right)^{k_4}}{v_c}-\frac{k_2\left(\frac{v_c}{k_1}\right)^{k_2}}{v_c}\right)$$
$$\left(-\frac{k_4\left(\frac{v_i}{k_3}\right)^{k_4}}{v_i}-\frac{k_2\left(\frac{v_i}{k_1}\right)^{k_2}}{v_i}\right)\left(-\frac{2\,k_4\left(\frac{v_u}{k_3}\right)^{k_4}}{v_u}-\frac{2\,k_2\left(\frac{v_u}{k_1}\right)^{k_2}}{v_u}\right)\%e^{-2\left(\frac{v_u}{k_3}\right)^{k_4}-2\left(\frac{v_u}{k_1}\right)^{k_2}-\left(\frac{v_i}{k_3}\right)^{k_4}-\left(\frac{v_i}{k_1}\right)^{k_2}-\left(\frac{v_c}{k_3}\right)^{k_4}-\left(\frac{v_c}{k_1}\right)^{k_2}-2\left(\frac{v_a}{k_3}\right)^{k_4}-2\left(\frac{v_a}{k_1}\right)^{k_2}}-a_1\,b_3\,c_1\,d_3$$
$$\left(-\frac{k_4\left(\frac{v_a}{k_3}\right)^{k_4}}{v_a}-\frac{k_2\left(\frac{v_a}{k_1}\right)^{k_2}}{v_a}\right)\left(-\frac{2\,k_4\left(\frac{v_c}{k_3}\right)^{k_4}}{v_c}-\frac{2\,k_2\left(\frac{v_c}{k_1}\right)^{k_2}}{v_c}\right)\left(-\frac{k_4\left(\frac{v_i}{k_3}\right)^{k_4}}{v_i}-\frac{k_2\left(\frac{v_i}{k_1}\right)^{k_2}}{v_i}\right)\left(-\frac{2\,k_4\left(\frac{v_u}{k_3}\right)^{k_4}}{v_u}-\frac{2\,k_2\left(\frac{v_u}{k_1}\right)^{k_2}}{v_u}\right)$$
$$\%e^{-2\left(\frac{v_u}{k_3}\right)^{k_4}-2\left(\frac{v_u}{k_1}\right)^{k_2}-\left(\frac{v_i}{k_3}\right)^{k_4}-\left(\frac{v_i}{k_1}\right)^{k_2}-2\left(\frac{v_c}{k_3}\right)^{k_4}-2\left(\frac{v_c}{k_1}\right)^{k_2}-\left(\frac{v_a}{k_3}\right)^{k_4}-\left(\frac{v_a}{k_1}\right)^{k_2}}+a_1\,b_3\,c_2\,d_3\left(-\frac{2\,k_4\left(\frac{v_a}{k_3}\right)^{k_4}}{v_a}-\frac{2\,k_2\left(\frac{v_a}{k_1}\right)^{k_2}}{v_a}\right)\left(-\frac{2\,k_4\left(\frac{v_c}{k_3}\right)^{k_4}}{v_c}-\frac{2\,k_2\left(\frac{v_c}{k_1}\right)^{k_2}}{v_c}\right)$$
$$\left(-\frac{k_4\left(\frac{v_i}{k_3}\right)^{k_4}}{v_i}-\frac{k_2\left(\frac{v_i}{k_1}\right)^{k_2}}{v_i}\right)\left(-\frac{2\,k_4\left(\frac{v_u}{k_3}\right)^{k_4}}{v_u}-\frac{2\,k_2\left(\frac{v_u}{k_1}\right)^{k_2}}{v_u}\right)\%e^{-2\left(\frac{v_u}{k_3}\right)^{k_4}-2\left(\frac{v_u}{k_1}\right)^{k_2}-2\left(\frac{v_i}{k_3}\right)^{k_4}-\left(\frac{v_i}{k_1}\right)^{k_2}-\left(\frac{v_c}{k_3}\right)^{k_4}-\left(\frac{v_c}{k_1}\right)^{k_2}-2\left(\frac{v_a}{k_3}\right)^{k_4}-2\left(\frac{v_a}{k_1}\right)^{k_2}}-a_2\,b_2\,c_1\,d_3$$
$$\left(-\frac{k_4\left(\frac{v_a}{k_3}\right)^{k_4}}{v_a}-\frac{k_2\left(\frac{v_a}{k_1}\right)^{k_2}}{v_a}\right)\left(-\frac{2\,k_4\left(\frac{v_c}{k_3}\right)^{k_4}}{v_c}-\frac{2\,k_2\left(\frac{v_c}{k_1}\right)^{k_2}}{v_c}\right)\left(-\frac{2\,k_4\left(\frac{v_i}{k_3}\right)^{k_4}}{v_i}-\frac{2\,k_2\left(\frac{v_i}{k_1}\right)^{k_2}}{v_i}\right)\left(-\frac{2\,k_4\left(\frac{v_u}{k_3}\right)^{k_4}}{v_u}-\frac{2\,k_2\left(\frac{v_u}{k_1}\right)^{k_2}}{v_u}\right)$$
$$\%e^{-2\left(\frac{v_u}{k_3}\right)^{k_4}-2\left(\frac{v_u}{k_1}\right)^{k_2}-2\left(\frac{v_i}{k_3}\right)^{k_4}-2\left(\frac{v_i}{k_1}\right)^{k_2}-2\left(\frac{v_c}{k_3}\right)^{k_4}-2\left(\frac{v_c}{k_1}\right)^{k_2}-2\left(\frac{v_a}{k_3}\right)^{k_4}-2\left(\frac{v_a}{k_1}\right)^{k_2}}-a_2\,b_3\,c_1\,d_3$$

Рисунок М.5 – Часткова похідна за параметрами v_i, v_c, v_a, v_u

ДОДАТОК Н

Код програми визначення значень ймовірності порушення властивостей інформаційного ресурсу на експериментальному програмно-технічному комплексі автоматизації прикордонного контролю "Гарт-3/П"

```
<?php
const k1 = 13;
const k2 = 1.3;
const k3 = 18;
const k4 = 2;
const a1 = 0.83;
const a2 = 0.0000109;
const b1 = 0.82;
const b2 = 0.00028;
const b3 = -0.000123;
const c1 = 0.908;
const c2 = 0.00174;
const d1 = 0.838;
const d2 = 0.00316;
const d3 = -0.00137;
const w = -0.23;
const c = 0.08;
function f($x) {
   return exp(-1*(pow($x/k1, k2) + pow($x/k3, k4)));
}
function p($x) {
   return exp(w*$x) / (c*(1-exp(w*$x))+exp(w*$x));
}
function FM($i, $c, $a, $u) {
   return (1-0.05*p($i)*pow(1-0.83*f($i), 6))*
```

```
        (1-pow(0.0243*p($c), 6))*
        (1-p($a)*pow(1-0.91*f($a), 6))*
        (1-pow((0.0455*p($u)*(1-(1-0.83*f($u))*(1-0.1494*f($u)))*f($u)), 6));
}
function h1($x, $koef = 1) {
    return (-($koef*k4*pow($x/k3, k4)/$x) - ($koef*k2*pow($x/k1, k2)/$x));
}
function e1($x, $koef = 1){
    return $koef*pow($x/k1, k2);
}
function e2($x, $koef = 1){
    return $koef*pow($x/k3, k4);
}
function h($i, $c, $a, $u, $k_1, $k_2, $k_3, $k_4) {
    return h1($a, $k_1)*h1($c, $k_2)*h1($i, $k_3)*h1($u, $k_4)*exp(-e2($u, $k_4)-
e1($u, $k_4)-e2($i, $k_3)-e1($i, $k_3)-e2($c, $k_2)-e1($c, $k_2)-e2($a, $k_1)-e1($a,
$k_1));
}
function fpr($i, $c, $a, $u) {
    $res = 0;
    $res += a1*b2*c1*d2*h($i, $c, $a, $u, 1, 1, 1, 1);
    $res += a1*b2*c2*d2*h($i, $c, $a, $u, 2, 1, 1, 1);
    $res += a1*b3*c1*d2*h($i, $c, $a, $u, 1, 2, 1, 1);
    $res += a1*b3*c2*d2*h($i, $c, $a, $u, 2, 2, 1, 1);
    $res += a2*b2*c1*d2*h($i, $c, $a, $u, 1, 1, 2, 1);
    $res += a2*b2*c2*d2*h($i, $c, $a, $u, 2, 1, 2, 1);
    $res += a2*b3*c1*d2*h($i, $c, $a, $u, 1, 2, 2, 1);
    $res += a2*b3*c2*d2*h($i, $c, $a, $u, 2, 2, 2, 1);
```

```
    $res += a1*b2*c1*d3*h($i, $c, $a, $u, 1, 1, 1, 2);
    $res += a1*b2*c2*d3*h($i, $c, $a, $u, 2, 1, 1, 2);
    $res += a1*b3*c1*d3*h($i, $c, $a, $u, 1, 2, 1, 2);
    $res += a1*b3*c2*d3*h($i, $c, $a, $u, 2, 2, 1, 2);
    $res += a2*b2*c1*d3*h($i, $c, $a, $u, 1, 1, 2, 2);
    $res += a2*b2*c2*d3*h($i, $c, $a, $u, 2, 1, 2, 2);
    $res += a2*b3*c1*d3*h($i, $c, $a, $u, 1, 2, 2, 2);
    $res += a2*b3*c2*d3*h($i, $c, $a, $u, 2, 2, 2, 2);
    return $res;
}
$V_i = 1;
$V_c = 12;
$V_a = 12;
$V_u = 12;
$res = array();
for($V_i = 1; $V_i <= 12; $V_i++) {
    for ($V_c = 1; $V_c <= 12; $V_c++) {
        $sum = 0;
        for ($i = 1; $i <= $V_i; $i++) {
            for ($c = 1; $c <= $V_c; $c++) {
                for ($a = 1; $a <= $V_a; $a++) {
                    for ($u = 1; $u <= $V_u; $u++) {
                        $sum += FM($i, $c, $a, $u) * fpr($i, $c, $a, $u);
                    }
                }
            }
        }
        $res[$V_i][$V_c] = $sum;
```

```
    }
}
echo "<table border='1'>";
echo "<tr><td colspan='13'>i</td></tr>";
echo "<tr>";
for ($i = 0; $i <= 12; $i++) {
    echo "<td>".$i."</td>";
}
echo "</tr>";
for ($j = 1; $j <= 12; $j++) {
    echo "<tr>";
    echo "<td>".$j."</td>";
    for ($i = 1; $i <= 12; $i++) {
        echo "<td>";
        echo sprintf('%.12f', $res[$i][$j]);
        echo "</td>";
    }
    echo "</tr>";
}
echo "</table>";
```

ДОДАТОК П

Результати обчислень значень ймовірності порушення властивостей інформаційного ресурсу на експериментальному програмно-технічному комплексі автоматизації прикордонного контролю "Гарт-3/П"

Таблиця П.1 – Ймовірності порушення властивостей інформаційного ресурсу при фіксованих нормативних значеннях доступності та спостережності

Норм. знач. конф. (год)	Нормативне значення цілісності (год)											
	1	2	3	4	5	6	7	8	9	10	11	12
1	0,000007	0,000015	0,000025	0,000034	0,000044	0,000054	0,000063	0,000072	0,000080	0,000087	0,000094	0,000100
2	0,000018	0,000040	0,000065	0,000091	0,000117	0,000142	0,000167	0,000190	0,000212	0,000231	0,000249	0,000265
3	0,000034	0,000076	0,000122	0,000171	0,000220	0,000268	0,000315	0,000359	0,000399	0,000436	0,000470	0,000499
4	0,000054	0,000122	0,000197	0,000275	0,000354	0,000432	0,000506	0,000577	0,000642	0,000702	0,000756	0,000803
5	0,000079	0,000178	0,000287	0,000401	0,000516	0,000629	0,000738	0,000841	0,000936	0,001020	0,001100	0,001170
6	0,000108	0,000242	0,000390	0,000545	0,000701	0,000855	0,001000	0,001140	0,001270	0,001390	0,001500	0,001590
7	0,000139	0,000311	0,000502	0,000702	0,000904	0,001100	0,001290	0,001470	0,001640	0,001790	0,001930	0,002050
8	0,000171	0,000385	0,000621	0,000868	0,001120	0,001360	0,001600	0,001820	0,002030	0,002210	0,002380	0,002530
9	0,000205	0,000459	0,000741	0,001040	0,001330	0,001630	0,001910	0,002170	0,002420	0,002640	0,002850	0,003030
10	0,000238	0,000533	0,000860	0,001200	0,001550	0,001890	0,002210	0,002520	0,002810	0,003070	0,003300	0,003510
11	0,000269	0,000604	0,000975	0,001360	0,001750	0,002140	0,002510	0,002860	0,003180	0,003480	0,003740	0,003980
12	0,000299	0,000671	0,001080	0,001510	0,001950	0,002380	0,002790	0,003170	0,003530	0,003860	0,004160	0,004420

Таблиця П.2 – Ймовірності порушення властивостей інформаційного ресурсу при фіксованих нормативних значеннях конфіденційності та спостережності

Норм. знач. дост. (год)	Нормативне значення цілісності (год)											
	1	2	3	4	5	6	7	8	9	10	11	12
1	0,000021	0,000046	0,000075	0,000105	0,000135	0,000164	0,000193	0,000219	0,000244	0,000267	0,000287	0,000306
2	0,000046	0,000104	0,000168	0,000235	0,000302	0,000368	0,000432	0,000492	0,000548	0,000599	0,000645	0,000685
3	0,000075	0,000168	0,000271	0,000379	0,000487	0,000594	0,000697	0,000794	0,000884	0,000966	0,001040	0,001110
4	0,000105	0,000235	0,000379	0,000529	0,000681	0,000831	0,000974	0,001110	0,001240	0,001350	0,001450	0,001550
5	0,000135	0,000302	0,000487	0,000681	0,000877	0,001070	0,001250	0,001430	0,001590	0,001740	0,001870	0,001990
6	0,000164	0,000368	0,000593	0,000830	0,001070	0,001300	0,001530	0,001740	0,001940	0,002120	0,002280	0,002420
7	0,000192	0,000431	0,000695	0,000971	0,001250	0,001520	0,001790	0,002040	0,002270	0,002480	0,002670	0,002840
8	0,000218	0,000489	0,000790	0,001100	0,001420	0,001730	0,002030	0,002310	0,002580	0,002820	0,003030	0,003220
9	0,000242	0,000543	0,000876	0,001230	0,001580	0,001920	0,002260	0,002570	0,002860	0,003130	0,003360	0,003580
10	0,000264	0,000591	0,000954	0,001330	0,001720	0,002090	0,002460	0,002800	0,003110	0,003400	0,003660	0,003900
11	0,000283	0,000634	0,001020	0,001430	0,001840	0,002240	0,002630	0,003000	0,003340	0,003650	0,003930	0,004180
12	0,000299	0,000671	0,001080	0,001510	0,001950	0,002380	0,002790	0,003170	0,003530	0,003860	0,004160	0,004420

Таблиця П.3 – Ймовірності порушення властивостей інформаційного ресурсу при фіксованих нормативних значеннях конфіденційності та доступності

Норм. знач. спост. (год)	Нормативне значення цілісності (год)											
	1	2	3	4	5	6	7	8	9	10	11	12
1	0,000007	0,000016	0,000026	0,000036	0,000047	0,000057	0,000067	0,000076	0,000084	0,000092	0,000099	0,000106
2	0,000019	0,000042	0,000068	0,000095	0,000122	0,000148	0,000174	0,000198	0,000221	0,000241	0,000260	0,000276
3	0,000035	0,000078	0,000126	0,000177	0,000227	0,000277	0,000325	0,000370	0,000412	0,000450	0,000485	0,000516
4	0,000056	0,000125	0,000202	0,000282	0,000363	0,000442	0,000519	0,000591	0,000658	0,000719	0,000774	0,000823
5	0,000081	0,000181	0,000292	0,000408	0,000526	0,000641	0,000752	0,000856	0,000953	0,001040	0,001120	0,001190
6	0,000109	0,000245	0,000395	0,000552	0,000711	0,000867	0,001020	0,001160	0,001290	0,001410	0,001520	0,001610
7	0,000140	0,000314	0,000507	0,000709	0,000913	0,001110	0,001310	0,001490	0,001660	0,001810	0,001950	0,002070
8	0,000173	0,000387	0,000625	0,000874	0,001120	0,001370	0,001610	0,001830	0,002040	0,002230	0,002400	0,002550
9	0,000206	0,000461	0,000744	0,001040	0,001340	0,001630	0,001920	0,002180	0,002430	0,002660	0,002860	0,003040
10	0,000238	0,000534	0,000862	0,001210	0,001550	0,001890	0,002220	0,002530	0,002810	0,003080	0,003310	0,003520
11	0,000270	0,000605	0,000976	0,001360	0,001760	0,002140	0,002510	0,002860	0,003190	0,003480	0,003750	0,003990
12	0,000299	0,000671	0,001080	0,001510	0,001950	0,002380	0,002790	0,003170	0,003530	0,003860	0,004160	0,004420

Таблиця П.4 – Ймовірності порушення властивостей інформаційного ресурсу при фіксованих нормативних значеннях цілісності та спостереженості

Норм. знач. дост. (год)	Нормативне значення конфіденційності (год)											
	1	2	3	4	5	6	7	8	9	10	11	12
1	0,000007	0,000018	0,000035	0,000056	0,000081	0,000110	0,000142	0,000175	0,000209	0,000243	0,000275	0,000306
2	0,000016	0,000041	0,000077	0,000125	0,000182	0,000247	0,000318	0,000393	0,000469	0,000544	0,000617	0,000685
3	0,000025	0,000066	0,000125	0,000201	0,000293	0,000398	0,000513	0,000634	0,000757	0,000878	0,000995	0,001110
4	0,000035	0,000093	0,000175	0,000281	0,000409	0,000556	0,000717	0,000886	0,001060	0,001230	0,001390	0,001550
5	0,000045	0,000119	0,000225	0,000361	0,000527	0,000716	0,000922	0,001140	0,001360	0,001580	0,001790	0,001990
6	0,000055	0,000145	0,000274	0,000440	0,000641	0,000872	0,001120	0,001390	0,001660	0,001920	0,002180	0,002420
7	0,000064	0,000170	0,000320	0,000515	0,000751	0,001020	0,001320	0,001630	0,001940	0,002250	0,002550	0,002840
8	0,000073	0,000193	0,000364	0,000586	0,000854	0,001160	0,001490	0,001850	0,002210	0,002560	0,002900	0,003220
9	0,000081	0,000214	0,000404	0,000650	0,000947	0,001290	0,001660	0,002050	0,002450	0,002840	0,003220	0,003580
10	0,000088	0,000233	0,000440	0,000708	0,001030	0,001400	0,001810	0,002230	0,002670	0,003090	0,003510	0,003900
11	0,000095	0,000250	0,000472	0,000759	0,001110	0,001500	0,001940	0,002390	0,002860	0,003320	0,003760	0,004180
12	0,000100	0,000265	0,000499	0,000803	0,001170	0,001590	0,002050	0,002530	0,003030	0,003510	0,003980	0,004420

Таблиця П.5 – Ймовірності порушення властивостей інформаційного ресурсу при фіксованих нормативних значеннях цілісності та доступності

Норм. знач. спост. (год)	Нормативне значення конфіденційності (год)											
	1	2	3	4	5	6	7	8	9	10	11	12
1	0,000002	0,000006	0,000012	0,000019	0,000028	0,000038	0,000049	0,000061	0,000072	0,000084	0,000095	0,000106
2	0,000006	0,000017	0,000031	0,000050	0,000073	0,000099	0,000128	0,000158	0,000189	0,000219	0,000249	0,000276
3	0,000012	0,000031	0,000058	0,000094	0,000137	0,000186	0,000239	0,000295	0,000353	0,000410	0,000464	0,000516
4	0,000019	0,000049	0,000093	0,000150	0,000218	0,000296	0,000382	0,000472	0,000563	0,000654	0,000741	0,000823
5	0,000027	0,000071	0,000135	0,000217	0,000316	0,000429	0,000553	0,000683	0,000816	0,000947	0,001070	0,001190
6	0,000037	0,000097	0,000182	0,000293	0,000427	0,000580	0,000748	0,000924	0,001100	0,001280	0,001450	0,001610
7	0,000047	0,000124	0,000234	0,000376	0,000548	0,000745	0,000960	0,001190	0,001420	0,001640	0,001860	0,002070
8	0,000058	0,000153	0,000288	0,000464	0,000676	0,000918	0,001180	0,001460	0,001750	0,002030	0,002300	0,002550
9	0,000069	0,000182	0,000343	0,000552	0,000805	0,001090	0,001410	0,001740	0,002080	0,002410	0,002740	0,003040
10	0,000080	0,000211	0,000398	0,000640	0,000932	0,001270	0,001630	0,002020	0,002410	0,002800	0,003170	0,003520
11	0,000090	0,000239	0,000450	0,000724	0,001060	0,001430	0,001850	0,002280	0,002730	0,003170	0,003590	0,003990
12	0,000100	0,000265	0,000499	0,000803	0,001170	0,001590	0,002050	0,002530	0,003030	0,003510	0,003980	0,004420

Таблиця П.6 – Ймовірності порушення властивостей інформаційного ресурсу при фіксованих нормативних значеннях цілісності та конфіденційності

Норм. знач. спостереж. (год)	Нормативне значення доступність (год)											
	1	2	3	4	5	6	7	8	9	10	11	12
1	0,000007	0,000016	0,000026	0,000037	0,000048	0,000058	0,000068	0,000077	0,000086	0,000093	0,000100	0,000106
2	0,000019	0,000043	0,000069	0,000097	0,000124	0,000151	0,000177	0,000201	0,000224	0,000243	0,000261	0,000276
3	0,000036	0,000080	0,000129	0,000180	0,000232	0,000283	0,000331	0,000376	0,000417	0,000454	0,000487	0,000516
4	0,000057	0,000128	0,000206	0,000288	0,000370	0,000451	0,000528	0,000600	0,000666	0,000725	0,000777	0,000823
5	0,000082	0,000185	0,000298	0,000417	0,000536	0,000653	0,000765	0,000869	0,000965	0,001050	0,001130	0,001190
6	0,000112	0,000250	0,000403	0,000564	0,000725	0,000884	0,001030	0,001180	0,001310	0,001420	0,001520	0,001610
7	0,000143	0,000321	0,000518	0,000724	0,000931	0,001130	0,001330	0,001510	0,001680	0,001820	0,001960	0,002070
8	0,000176	0,000396	0,000638	0,000892	0,001150	0,001400	0,001640	0,001860	0,002060	0,002250	0,002410	0,002550
9	0,000210	0,000471	0,000760	0,001060	0,001370	0,001670	0,001950	0,002220	0,002460	0,002680	0,002870	0,003040
10	0,000243	0,000546	0,000881	0,001230	0,001580	0,001930	0,002260	0,002570	0,002850	0,003100	0,003330	0,003520
11	0,000275	0,000618	0,000997	0,001390	0,001790	0,002180	0,002560	0,002910	0,003220	0,003510	0,003760	0,003990
12	0,000306	0,000685	0,001110	0,001550	0,001990	0,002420	0,002840	0,003220	0,003580	0,003900	0,004180	0,004420

ДОДАТОК Р

Список публікацій за темою дисертації та відомості про апробацію результатів дисертації

1. Підходи до оцінювання ефективності захисту інформації в інформаційно-телекомунікаційних системах на стадії модернізації / О. К. Юдін, М. А. Стрельбіцький // Наукоємні технології в інфокомунікаціях: обробка інформації, кібербезпека, інформаційна боротьба : Монографія / під заг. ред. В. М. Безрука, В. В. Баранника. – Х. : Вид. "Лидер", 2017. – С. 582–599.

2. Технологія забезпечення функціональної безпеки інтегрованої інформаційної системи Держприкордонслужби на стадії модернізації : Монографія / О. К. Юдін, М. А. Стрельбіцький – К. : ТОВ «СІК ГРУП Україна», 2017. – 312 с.

3. Стрельбіцький М. А. Прикордонний інформаційний ресурс: визначення поняття / М. А. Стрельбіцький // Сучасні інформаційні технології у сфері безпеки та оборони: наук. збірник. – К.: НУОУ, 2016. – № 1(25). – С. 205–208.

4. Barannik V. Method of Ciphergrams Coding for Increasing the Effectiveness of Selective Cyber-Protection Technologies / Barannik V., Barannik D., Hahanova A., Medvedev D., Strelbtskiy M. // Radioelectronics & Informatics. – Kharkiv: 2016. – № 4 (75) – P. 34–40.

5. Юдін О.К. Ієрархічний класифікатор автоматизованих систем прикордонного відомства / О. К. Юдін, М. А. Стрельбіцький // Радіоелектроніка і інформатика. –Харків: 2017. – № 1 (76). – С. 57–60.

6. Юдін О.К. Спосіб визначення кількості інформації з урахуванням фактору її старіння / О. К. Юдін, М. А. Стрельбіцький // Наукоємні технології. – К.: 2017. – № 1 (33). – С. 8–12.

7. Стрельбіцький М. А. Метод узгодження матриць доступу систем дискреційного розмежування доступу інформаційно-телекомунікаційних систем на стадії модернізації / М. А. Стрельбіцький // Сучасні інформаційні технології у сфері безпеки та оборони. – К.: НУОУ, 2017. – № 1 (28). – С. 58–62.

8. Юдін О.К. Технологія забезпечення функціональної безпеки інформаційних систем на стадії модернізації / О. К. Юдін, М. А. Стрельбіцький // Наукоємні технології. – К.: 2017. – № 4 (36). – С. 323–328.

9. Стрельбіцький М. А. Обґрунтування та вибір цільової функції системного захисту інформації в інтегрованій інформаційно-телекомунікаційній системі Державної прикордонної служби України / М. А. Стрельбіцький // Збірник наукових праць Національної академії Державної прикордонної служби України: зб. наук. праць. – Хмельницький: НАДПСУ, 2011. – № 56. – С. 63–64.

10. Стрельбіцький М. А. Аналіз і систематизація причин виникнення збитків від реалізації загроз в інтегрованій інформаційно-телекомунікаційній системі Державної прикордонної служби України / М. А. Стрельбіцький // Збірник наукових праць Національної академії Державної прикордонної служби України: зб. наук. праць. –Хмельницький: НАДПСУ, 2012. – № 58. – С. 151–153.

11. Стрельбіцький М. А. Декомпозиція технології захисту інформації в корпоративих системах / М. А. Стрельбіцький // Збірник наукових праць Національної академії Державної прикордонної служби України: зб. наук. праць. –Хмельницький: НАДПСУ, 2013. – № 1(59). – С. 296–301.

12. Стрельбіцький М. А. Окремі питання синтезу системного захисту інформації в інтегрованій інформаційно-телекомунікаційній системі прикордонного відомства на стадії модернізації / М. А. Стрельбіцький // Збірник наукових праць Національної академії Державної прикордонної служби України: зб. наук. праць. –Хмельницький: НАДПСУ, 2014. – № 3 (65). – С. 353–361.

13. Стрельбіцький М. А. Класифікація загроз інформації в інтегрованій інформаційно-телекомунікаційній системі прикордонного відомства на етапі модернізації / М. А. Стрельбіцький // Збірник наукових праць Військового інституту Київського національного університету ім. Т. Шевченка: зб. наук. праць. –К.: ВІКНУ, 2015. – № 50. – С. 248–252.

14. Стрельбіцький М. А. Визначення показника уразливості даних в інформаційно-телекомунікаційних системах на стадії модернізації / М. А. Стрельбіцький // Збірник наукових праць Військового інституту Київського національного університету ім. Т. Шевченка. – К. : ВІКНУ. 2016. – № 51. – С. 208 –213.

15. Юдін О.К. Класифікація загроз інформаційному ресурсу ДПСУ на стадії модернізації / О. К. Юдін, М. А. Стрельбіцький // Вісник інженерної академії України. – К. 2016. – вип 4. – С.166–170.

16. Стрельбіцький М. А. Визначення залишкового ризику загроз інформації на стадії модернізації інформаційно-телекомунікаційних систем / М. А. Стрельбіцький // Збірник наукових праць Національної академії Державної прикордонної служби України: зб. наук. праць. –Хмельницький: НАДПСУ, 2016. – № 3 (69). – С.308–321.

17. Стрельбіцький М. А. Аналіз спільного функціонування моделей розмежування доступу на стадії модернізації інформаційно-телекомунікаційних систем на стадії модернізації / М. А. Стрельбіцький // Збірник наукових праць Національної академії Державної прикордонної служби України: зб. наук. праць. –Хмельницький: НАДПСУ, 2016. – № 4 (70). – С. 276–287.

18. Стрельбіцький М. А. Формування множини допустимих значень показника якості системи захисту інформації інформаційно-телекомунікаційних систем на стадії модернізації / М. А. Стрельбіцький // Збірник наукових праць Національної академії Державної прикордонної служби України: зб. наук. праць. –Хмельницький: НАДПСУ, 2017. – Вип. 1 (29). – С. 27–32.

19. Кузавков В.В. Метод узгодження решіток рівнів конфіденційності систем мандатного розмежування доступу інформаційно-телекомунікаційних систем на стадії модернізації / В. В. Кузавков, М. А. Стрельбіцький, В. О. Данько // Збірник наукових праць Військового інституту телекомунікацій та інформатизації: зб. наук. праць. – К.: ВІТІ, 2017. – № 1. – С. 56–60.

20. Стрельбіцький М. А. Аналіз загроз інформаційної безпеки при використанні у Державній прикордонній службі України геоінформаційних систем/ М. А. Стрельбіцький, Р. В. Рачок, Д. А. Мул, Є. В. Прокопенко // Збірник наукових праць Національної академії Державної прикордонної служби України: зб. наук. праць. –Хмельницький: НАДПСУ, 2017. – № 1 (71). – С 394–403.

21. Стрельбіцький М. А. Обґрунтування показника ефективності функціонування системи захисту інформації на стадії модернізації / М. А. Стрельбіцький // Збірник наукових праць Військового інституту Київського національного університету ім. Т. Шевченка: зб. наук. праць. – К.: 2017. – № 56. – С. 166–177.

22. Стрельбіцький М. А. Метод узгодження систем рольового розмежування доступу інформаційно-телекомунікаційних систем на стадії модернізації / М. А. Стрельбіцький, Д. А. Мул, Є. В. Прокопенко // Збірник наукових праць Національної академії Державної прикордонної служби України: зб. наук. праць. –Хмельницький: НАДПСУ, 2017. – №2 (72). – С 330–339.

23. Стрельбіцький М. А. Методологічний базис узгодження моделей розмежування доступу інформаційно-телекомунікаційних систем на стадії модернізації / М. А. Стрельбіцький // Збірник наукових праць Національної академії Державної прикордонної служби України: зб. наук. праць. – Хмельницький: НАДПСУ, 2017. – № 3 (73). – С 370–379.

24. Стрельбіцький М. А. Перспективні напрямки розвитку системи висвітлення надводної обстановки в Азово-Чорноморському басейні на сучасному етапі / М. А. Стрельбіцький, В. І. Кривий // Збірник наукових праць Військового інституту Київського національного університету ім. Т. Шевченка: зб. наук. праць. – К.: ВІКНУ, 2006. – № 4. – С 130 –133.

25. Шевченко В.Л. Перспективи застосування волоконно-оптичних системи у системі інформаційного забезпечення Державної прикордонної служби України / В. Л. Шевченко, М. А. Стрельбіцький, М. І. Лисий // Збірник

наукових праць Національної академії Державної прикордонної служби України: зб. наук. праць. –Хмельницький: НАДПСУ, 2008. – № 42. – С. 70–72.

26. Стрельбіцький М. А. Оцінка ефективності методів отримання та обробки діагностичної інформації / М. А. Стрельбіцький, В. В. Кузавков // Збірник наукових праць Національної академії Державної прикордонної служби України: зб. наук. праць. –Хмельницький: НАДПСУ, 2014. – № 2 (62). – С. 277–289.

27. Юдін О.К. Зміст та ієрархія реєстру інформаційних ресурсів Держприкордонслужби України / О. К. Юдін, М. А. Стрельбіцький // Проблеми інформатизації та управління. – К.: НАУ, 2016. – № 4 (56). – С. 85–91

28. Стрельбіцький М. А. Шляхи захисту інформації в корпоративній мережі Державної прикордонної служби України на стадії модернізації / М. А. Стрельбіцький, Д. А. Купрієнко // Пріоритетні напрямки розвитку телекомунікаційних систем спеціального призначення: Труди III науково-практичної конференції. – К. : ВІНІ НТУУ "КПІ", 2006 – С. 247–249

29. Стрельбіцький М. А. Конструктивні елементи моделі системного захисту інформації в інтегрованій інформаційно-телекомунікаційній системі Державної прикордонної служби України / М. А. Стрельбіцький, Д. А. Мул // Освітньо-наукове забезпечення діяльності правоохоронних органів і військових формувань України: II Всеукраїнська науково-практична конф. 20 листопала 2009 р.: тези доп. – Хмельницький. – 2009. – С. 111.

30. Стрельбіцький М. А. Декомпозиція технології захисту сенсорної інформації в корпоративних системах. / М. А. Стрельбіцький, Т. О. Прищепа // Проблеми телекомунікацій : 7-ма міжнародна науково–технічна конф. 16-19 квітня 2013 р.: тези доп. – К. – 2013. – С 278–280

31. Стрельбіцький М. А. Конструктивні елементи моделі системного захисту інформації в рамках сучасних концепцій / М. А. Стрельбіцький, О. А. Ваврічен // Освітньо-наукове забезпечення діяльності правоохоронних

органів і військових формувань України: Матеріали V всеукраїнської науково-практичної конф. 7 грудня 2012 р.: тези доп. – Хмельницький. – 2012. – С. 115–116.

32. Стрельбіцький М. А. Системний захист інформації як складова забезпечення національної безпеки в інформаційній сфері / М. А. Стрельбіцький, В. А. Кириленко // Освітньо-наукове забезпечення діяльності правоохоронних органів і військових формувань України: Матеріали VI всеукраїнської науково-практичної конф. 15 листопада 2013 р.: тези доп. – Хмельницький. – 2013. – С. 240 – 241.

33. Стрельбіцький М. А. Нечіткий пошук інформації у базі даних програмно–технічного комплексу "Гарт–1/П" / М. А. Стрельбіцький, Р. В. Рачок, Д. А. Мул // Освітньо-наукове забезпечення діяльності правоохоронних органів і військових формувань України: Матеріали VII всеукраїнської науково-практичної конф. 21 листопада 2014 р.: тези доп. – Хмельницький. – 2014. – С. 139.

34. Стрельбіцький М. А. Прикордонний інформаційний ресурс: визначення поняття / М. А. Стрельбіцький // Історія, сучасність та перспективи розвитку ДПСУ та охорони державного кордону: Матеріали міжнародної науково-практичної конф. 26 травня 2015 р.: тези доп. – К. – 2015. – С. 297–299.

35. Стрельбіцький М. А. Класифікація загроз інформації в інтегрованій інформаційно-телекомунікаційній системі прикордонного відомства на етапі модернізації / М. А. Стрельбіцький // Військова освіта і наука: сьогодення та майбутнє: Матеріали XI міжнародної науково-практичної конф. 27 листопада 2015 р.: тези доп. – К. – 2015. – С. 78.

36. Стрельбіцький М. А. Окремі питання синтезу системного захисту інформації в інформаційно-телекомунікаційній системі прикордонного відомства на стадії модернізації / М. А. Стрельбіцький // Освітньо–наукове забезпечення діяльності правоохоронних органів і військових формувань

України: Матеріали VIII всеукраїнської науково-практичної конф. 10 грудня 2015 р.: тези доп. – Хмельницький. – 2015. – С. 524–525.

37. Стрельбіцький М. А. Аналіз і систематизація причин виникнення збитків від реалізації загроз у відомчих інформаційно-телекомунікаційних системах / М. А. Стрельбіцький // Перспективи розвитку озброєння та військової техніки сухопутних військ: Матеріали міжнародної науково-технічної конф. 18-20 травня 2016 р.: тези доп. – Львів. –2016. – С. 227.

38. Стрельбіцький М. А. Приховані канали витоку інформації в інформаційно-телекомунікаційних системах Державної прикордонної служби України та шляхи їх ліквідації / М. А. Стрельбіцький, О. А. Ваврічен // Кібербезпека в Україні: правові та організаційні питання: Матеріали всеукраїнської науково-практичної конф. 21 жовтня 2016 р.: тези доп. – Одеса. – 2016. – С. 140–142.

39. Стрельбицкий М. А. Информационный ресурс пограничной службы– составляющая национальной безопасности Украины / М. А. Стрельбицкий // Материалы международной заочной научно-практической конф. Государственного учреждения образования "Институт пограничной службы Республики Беларусь". – Минск. – 2017. – С. 452–454.

40. Стрельбіцький М. А. Методологія узгодження моделей розмежування доступу інформаційно–телекомунікаційних систем на стадії модернізації / М. А. Стрельбіцький // Освітньо–наукове забезпечення діяльності правоохоронних органів і військових формувань України: Матеріали X всеукраїнської науково-практичної конф. 2 листопада 2017 р.: тези доп. – Хмельницький. – 2017. – С. 620–621.

41. Стрельбіцький М. А. Вплив процесів інформатизації прикордонного відомства на складові національної безпеки України / М. А. Стрельбіцький // Наукове забезпечення службово-бойової діяльності Національної гвардії України: VII науково-практична конф. 31 березня 2016 р.: тези доп. – Харків. – 2016. – С. 137–138.

ДОДАТОК С

Акти реалізації дисертаційних досліджень

ЗАТВЕРДЖУЮ
Начальник Головного центру зв'язку, автоматизації та захисту інформації
полковник
О. В. Сєткін
«26» 12 2017 року

АКТ
про реалізацію результатів дисертаційного дослідження на здобуття наукового ступеня доктора технічних наук
Стрельбіцького Михайла Анатолійовича

Комісія у складі: голови комісії – заступника начальника Головного центру зі зв'язку та автоматизації – головного інженера полковника Ворончука В.Л. та членів комісії: начальника центру технічного захисту інформації підполковника Процюка А.А. та заступника начальника центру - начальника відділу досліджень новітніх засобів (систем) зв'язку та захисту інформації підполковника Шинкаренка В.В. підтверджує цим актом те, що теоретичні розробки та практичні напрацювання дисертаційного дослідження за темою: «Технологія забезпечення функціональної безпеки інтегрованої інформаційної системи Держприкордонслужби на стадії модернізації» кандидата технічних наук, доцента, полковника Стрельбіцького Михайла Анатолійовича використані під час модернізації інтегрованої інформаційно–телекомунікаційної системи Державної прикордонної служби України, а саме:

застосування методів узгодження систем розмежування доступу при підключенні до інтегрованої інформаційної системи Державної прикордонної служби до баз даних Інтерполу дозволило забезпечити дотримання властивостей інформаційної системи автоматизації прикордонного контролю. Аналіз ефективності узгодження систем розмежування доступу при взаємодії різних ІС у складі інтегрованої інформаційної системи показало підвищення ймовірності дотримання властивостей інформаційної системи до 6% від існуючого значення;

враховані основні положення методу визначення раціональної послідовності модернізації елементів інформаційних систем при розробці рекомендацій органам та підрозділам охорони державного кордону з модернізації інформаційних систем;

проведено оцінювання ефективності забезпечення функціональної безпеки інтегрованої інформаційно-телекомунікаційної системи прикордонного відомства та застосований метод розподілу засобів

забезпечення функціональної безпеки інформаційних систем на стадії модернізації, що дозволило забезпечити нормативний рівень функціональної безпеки інформаційної системи в цілому;

при формуванні технічного завдання на модернізацію інформаційно-телекомунікаційних систем Державної прикордонної служби України використана інформаційна технологія забезпечення функціональної безпеки, застосування якої показало зменшення до 2-х разів кількості інформаційних повідомлень про порушення властивостей інформаційних систем при їх модернізації;

використання розробленого програмного комплексу підвищило до 3-х разів оперативність формування проектів розпоряджень на модернізацію спеціального програмного забезпечення.

Голова комісії:

Заступник начальника Головного центру зі зв'язку та автоматизації-головний інженер

полковник В.Л. Ворончук

Члени комісії:

Начальник центру технічного захисту інформації

підполковник А.А. Процюк

Заступник начальника центру - начальник відділу досліджень новітніх засобів (систем) зв'язку та захисту інформації

підполковник В.В. Шинкаренко

УКРАЇНА
Державна прикордонна служба України
НАЦІОНАЛЬНА АКАДЕМІЯ ДЕРЖАВНОЇ ПРИКОРДОННОЇ СЛУЖБИ УКРАЇНИ
імені БОГДАНА ХМЕЛЬНИЦЬКОГО
Код № 14321481
«___» _____20___р. № _____
на №_____ від «___» _____20___р.

ЗАТВЕРДЖУЮ
Начальник Східного регіонального управління Державної прикордонної служби України
генерал-майор _____ С. В. Бідило
«26» 12 2017 року

АКТ
про реалізацію результатів дисертаційного дослідження на здобуття наукового ступеня доктора технічних наук
Стрельбіцького Михайла Анатолійовича

Комісія у складі: голови комісії – першого заступника начальника регіонального управління – начальника штабу генерал-майора, кандидата педагогічних наук, доцента Луцького О.Л. та членів комісії: начальника відділу зв'язку штабу регіонального управління полковника Бєляцького І.А., старшого офіцера відділу зв'язку штабу регіонального управління підполковника Токара О.В. підтверджує цим актом те, що теоретичні розробки та практичні напрацювання дисертаційного дослідження за темою: «Технологія забезпечення функціональної безпеки інтегрованої інформаційної системи Держприкордонслужби на стадії модернізації» кандидата технічних наук, доцента, полковника Стрельбіцького Михайла Анатолійовича використані під час проведення модернізації інформаційно-телекомунікаційних систем у підрозділах Східного регіонального управління Державної прикордонної служби України, зокрема:

застосування методів узгодження систем рольового та дискреційного розмежування доступу при інтеграції інформаційних систем, які розгорнуті на контрольних пунктах в'їзду-виїзду до ІТС автоматизації прикордонного контролю дозволило забезпечити функціональну безпеку програмно-технічних комплексів автоматизації прикордонного контролю підрозділів регіонального управління в умовах особливого режиму антитерористичної операції;

застосування методу розподілу засобів забезпечення функціональної безпеки інформаційно-телекомунікаційної системи автоматизації прикордонного контролю дозволило підвищити рівень функціональної безпеки програмно-технічних комплексів на 7 % за рахунок раціонального їх перерозподілу;

застосування методу визначення раціональної послідовності модернізації елементів інформаційних систем дозволило зменшити до 3-х

разів кількість відмов інформаційно-телекомунікаційних систем викликаних процесом модернізації;

застосування методу оцінювання ефективності забезпечення функціональної безпеки інформаційних систем на стадії модернізації дозволило врахувати особливості функціонування інформаційних систем, які розгорнуті на лінії розмежування з тимчасово окупованими територіями Донецької та Луганської областей в зоні відповідальності підрозділів Східного регіонального управління та визначити шляхи підвищення рівня функціональної безпеки ІС;

застосування розробленого в рамках дисертаційної роботи програмного комплексу дозволив до 4 разів зменшити час формування рекомендацій з модернізації ІС підрозділам охорони кордону з питань раціоналізації процесу модернізації програмно-технічних комплексів автоматизації прикордонного контролю.

Голова комісії:
кандидата педагогічних наук, доцент
генерал-майор О.Л. Луцький

Члени комісії:
полковник І.А. Бєляцький

підполковник О.В. Токар

УКРАЇНА
Державна прикордонна служба України
НАЦІОНАЛЬНА АКАДЕМІЯ ДЕРЖАВНОЇ
ПРИКОРДОННОЇ СЛУЖБИ УКРАЇНИ
імені БОГДАНА ХМЕЛЬНИЦЬКОГО
Код № 14321481
«12» 12 2017 р. № 2611/796
на №____ від «___» _____ 20__ р.

ЗАТВЕРДЖУЮ
Ректор Національної академії
Державної прикордонної служби України
імені Богдана Хмельницького
доктор технічних наук, професор
генерал-майор _____
О. М. Шинкарук
«12» 12 2017 року

АКТ
про реалізацію результатів дисертаційного дослідження на здобуття наукового ступеня доктора технічних наук Стрельбіцького Михайла Анатолійовича

Комісія у складі: голови комісії – заступника ректора академії з наукової роботи, доктора військових наук, професора, полковника Кириленка В.А. та членів комісії: начальника докторантури – головного наукового співробітника, доктора технічних наук, професора полковника Андрощука О.С., начальника кафедри транспортних засобів та спеціальної техніки, доктора технічних наук, доцента полковника Осташевського С.А., начальника кафедри інженерного забезпечення та технічних засобів охорони кордону доктора технічних наук, доцента полковника Сівака В.А. підтверджує цим актом те, що теоретичні розробки та практичні напрацювання дисертаційного дослідження за темою: "Технологія забезпечення функціональної безпеки інтегрованої інформаційної системи Держприкордонслужби на стадії модернізації" кандидата технічних наук, доцента, полковника Стрельбіцького Михайла Анатолійовича використані під час підготовки та проведення з 18 по 19 грудня 2017 року ділової гри з персоналом академії та впроваджені в навчальний процес Національної академії Державної прикордонної служби України при викладанні навчальних дисциплін, а саме:

1. За спеціальністю 252 "Безпека державного кордону", дисципліна "Зв'язок в Державній прикордонній службі":

а) тема 2 "Рухомі засоби зв'язку та автоматизації":

– заняття 1 "Спеціальні комплексні інформаційно-телекомунікаційні апаратні тактичного рівня («СКІТА-04»)";

– заняття 4 "Рухомі програмно-технічні комплекси автоматизації".

б) тема 5 "Інформаційно-телекомунікаційні системи":

– заняття 1 "ІТС забезпечення виконання основних завдань з оперативно-службової діяльності";

– заняття 2 "ІТС забезпечення реєстрації подій з оперативно-службової діяльності";

– заняття 3 "Застосування складових інтегрованої ІТС «Гарт» в плануванні оперативно-службової діяльності";

– заняття 4 "Розробка моделі інформаційно-телекомунікаційної системи органу охорони державного кордону";

– заняття 5 "Висвітлення обстановки та обмін документальною інформацією".

в) тема 7 "Інформаційна безпека":

– заняття 1 " Основи забезпечення державної інформаційної політики";

– заняття 2 "Захист інформації в інформаційно-телекомунікаційних системах";

2. За спеціальністю 172 "Телекомунікації та радіотехніка", дисципліна "Системи та комплекси зв'язку":

а) тема 1 "Введення в навчальну дисципліну":

– заняття 1 "Загальні відомості про системи та комплекси зв'язку ДПСУ".

б) тема 4 "Рухомі апаратні зв'язку":

– заняття 5 "Спеціальні комплексні інформаційно-телекомунікаційні апаратні тактичного та оперативно-тактичного рівнів управління";

– заняття 7 "Спеціальні комплексні інформаційно-телекомунікаційні апаратні оперативного та стратегічного рівнів управління";

III. За спеціальностями 081–Право, 262–Правоохоронна діяльність, 035–Філологія, 053–Психологія, дисципліна "Інформаційно-телекомунікаційні системи прикордонних підрозділів":

а) тема 1 "Сучасний стан та перспективи розвитку засобів зв'язку та автоматизації в Державній прикордонній службі України":

– заняття 1 "Сучасний стан та перспективи розвитку засобів зв'язку та автоматизації в Державній прикордонній службі України";

б) тема 5 "Складові інформаційно-телекомунікаційних систем забезпечення центру управління службою прикордонного підрозділу":

– заняття 1 "Інформаційно-телекомунікаційні системи забезпечення центру управління службою прикордонного підрозділу";

– заняття 4 "Структура та склад ІТС "Гарт-5";

– заняття 6 "Комплексне використання ІТС забезпечення центру управління службою прикордонного підрозділу";

в) тема 7 "Структура та порядок застосування складових інформаційно-телекомунікаційної системи "Гарт-1" та "Гарт-3":

– заняття 1 "Інформаційно-телекомунікаційна система "Гарт – 3";

– заняття 4 "Структура та склад ІТС "Гарт-1".

г) тема 8 "Основи інформаційної безпеки":

– заняття 1 "Основи забезпечення державної інформаційної політики".

Під час проведення з 18 по 19 грудня 2017 року ділової гри з персоналом академії були впроваджені наступні результати:

метод визначення раціональної послідовності модернізації елементів інформаційних систем, що дозволило зменшити ймовірність порушення

властивостей інформаційних системи за обраною стратегією модернізації до 8 разів від максимального та до 3-х разів від середнього значення;

метод розподілу засобів забезпечення функціональної безпеки інформаційних систем на стадії модернізації, що дозволило забезпечити нормативний рівень функціональної безпеки інформаційної системи в цілому;

методи узгодження систем розмежування доступу в інформаційних системах на стадії модернізації. Проведене оцінювання ефективності узгодження систем розмежування доступу при взаємодії двох ІС у складі інтегрованої інформаційної системи "Гарт-1" та "Гарт-5" показало ймовірність порушення властивостей хоча б одного елементу інформаційного ресурсу під час модернізації на рівні до 0,0003.

інформаційна технологія забезпечення функціональної безпеки інтегрованої інформаційної системи на стадії модернізації, застосування якої дозволило забезпечити нормативний рівень порушення функціональної безпеки при модернізації ІС "Гарт-1/П" на рівні до 0,005.

Розроблений в рамках дисертаційної роботи програмний комплекс, що базується на створених технології, методах та моделях, дозволив до трьох разів підвищити оперативність формування практичних рекомендацій із адаптації засобів забезпечення функціональної безпеки інформаційних систем на стадії модернізації.

Результати дисертаційного дослідження впроваджені в науково-дослідні роботи Національної академії Державної прикордонної служби України імені Б. Хмельницького, а саме:

216-0008 І "Методичні рекомендації підрозділам Державної прикордонної служби України щодо порядку визначення зон виявлення сигналу з метою визначення захищеного периметра використання об'єкта інформаційної діяльності".

217-0012 І "Системний захист інформації у інтегрованій інформаційно-телекомунікаційній системі "Гарт" на стадії модернізації".

217-0015І "Інформаційні технології в діяльності військових формувань та правоохоронних органів України".

Голова комісії:
доктор військових наук, професор
полковник В.А. Кириленко

Члени комісії:
доктор технічних наук, професор
полковник О.С. Андрощук

доктор технічних наук, доцент
полковник С.А. Осташевський

доктор технічних наук, доцент
полковник В.А. Сівак

ЗАТВЕРДЖУЮ
Директор АТ "БАНКОМЗВ'ЯЗОК"
_____ Поносов С.М.
_____ 2018 року

АКТ
про реалізацію результатів дисертаційного дослідження на здобуття наукового ступеня доктора технічних наук Стрельбіцького Михайла Анатолійовича

Комісія у складі: голова комісії Директор Департаменту систем прикордонного контролю Грянка О.В., та членів комісії: керівник проектів та програм в сфері нематеріального виробництва Диндар В.В., інженер проектів Бурман О.М., провідний інженер з техпідтримки Кравчук С.В. підтверджує цим актом те, що теоретичні розробки та практичні напрацювання дисертаційного дослідження за темою: "Технологія забезпечення функціональної безпеки інтегрованої інформаційної системи Держприкордонслужби на стадії модернізації" кандидата технічних наук, доцента, полковника Стрельбіцького Михайла Анатолійовича використані під час модернізації інтегрованої інформаційно–телекомунікаційної системи Державної прикордонної служби України. З наукових результатів, які отримані у межах дисертаційної роботи і належать особисто автору, впроваджені наступні результати:

інформаційна технологія забезпечення функціональної безпеки інтегрованих інформаційних систем на стадії модернізації, застосування якої дозволило забезпечити дотримання значення ймовірності порушення функціональної безпеки при модернізації інформаційної системи до 0,005;

метод визначення раціональної послідовності модернізації елементів інформаційних систем, що дозволило зменшити ймовірність порушення властивостей інформаційних системи за обраною стратегією модернізації до 8 разів від максимального та до 3-х разів від середнього значення;

метод узгодження систем дискреційного розмежування доступу в інформаційних системах на стадії модернізації, що дозволило адаптувати різні версії систем розмежування доступу та не допустити порушення властивостей інформаційної системи. З метою оцінювання ефективності узгодження систем розмежування доступу при взаємодії різних версій інформаційних систем застосовувалась розроблена в дисертаційній роботі методика. Результати оцінювання показали ймовірність порушення властивостей інформаційної системи під час модернізації на рівні до 0,0002;

метод розподілу засобів забезпечення функціональної безпеки інформаційних систем на стадії модернізації, що дозволило визначити

необхідну сукупність додаткових засобів за умови дотримання нормативного рівня функціональної безпеки системи в цілому;

метод оцінювання уразливості інформаційних систем в інтегрованій інформаційній системі на стадії модернізації дозволив врахувати фактори, які викликані процесом модернізації інформаційної системи та до 2-х разів підвищити точність у порівнянні з існуючими методами.

Голова комісії: **Грянка О.В.**

Члени комісії: **Диндар В.В.**
Бурман О.М.
Кравчук С.В.