МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

СТРЕЛЬБІЦЬКИЙ МИХАЙЛО АНАТОЛІЙОВИЧ

УДК 623.618:351.746.1

ТЕХНОЛОГІЯ ЗАБЕЗПЕЧЕННЯ ФУНКЦІОНАЛЬНОЇ БЕЗПЕКИ ІНТЕГРОВАНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ ДЕРЖПРИКОРДОНСЛУЖБИ НА СТАДІЇ МОДЕРНІЗАЦІЇ

Спеціальність 05.13.06 – інформаційні технології

Автореферат
дисертації на здобуття наукового ступеня
доктора технічних наук

Київ–2018

Дисертацією є рукопис
Робота виконана в Національній академії Державної прикордонної служби імені Б. Хмельницького

Науковий консультант: доктор технічних наук, професор
Юдін Олександр Костянтинович,
Національний авіаційний університет,
директор Навчально-наукового інституту комп'ютерних інформаційних технологій

Офіційні опоненти: доктор технічних наук, професор
Теслюк Василь Миколайович,
Національний університет "Львівська політехніка",
професор кафедри систем автоматизованого проектування

доктор технічних наук, професор
Барабаш Олег Володимирович,
Державний університет телекомунікацій,
завідувач кафедри вищої математики

доктор технічних наук, доцент
Субач Ігор Юрійович,
Інститут спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського»,
завідувач спеціальної кафедри № 5

Захист відбудеться "07" червня 2018 року о 13^{30} годині на засіданні спеціалізованої вченої ради Д 26.062.01, Національний авіаційний університет, 03680, Київ–680, пр. Космонавта Комарова, 1, ауд. 3/201

З дисертацією можна ознайомитись у бібліотеці Національного авіаційного університету, 03680, Київ–680, пр. Космонавта Комарова, 1.

Автореферат розісланий "03" травня 2018 року.

Учений секретар
спеціалізованої вченої ради, к.т.н. Ю. П. Бойко

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

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 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 висувають високі вимоги до оперативності управління та зумовлюють необхідність удосконалення системи забезпечення безпеки на державному кордоні України.

У зазначених 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 з основних завдань з реалізації інтегрованого управління кордонами є створення єдиного інформаційного простору. Його якісна реалізація потребує від Державної прикордонної служби України наявності сучасних систем збирання, обробки і аналізу даних про обстановку різного типу, великих об’ємів і з великої кількості джерел та їх здатність до ефективного отримання з них інформації, а також її висвітленням в інтерфейсах систем підтримки прийняття управлінських рішень.

Основними вимогами до систем такого класу є сучасність її елементів та архітектури, інтегрованість, відкритість до модернізації, забезпечення функціональної безпеки інформаційних систем (ІС) при великій їх територіальній розосередженості, наявність потужних аналітичних елементів та засобів швидкого та якісного висвітлення ситуаційної і загальної обстановки. Особливо важливим критерієм також є здатність таких систем ефективно функціонувати у гетерогенному інформаційному середовищі.

Бурхливий 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 та інформаційної підтримки правоохоронної, соціально-економічної, екологічної, науково-технічної, оборонної, національно-культурної та іншої діяльності у сферах загальнодержавного значення не має на сьогодні успіху.

Обмежена кількість досліджень з питань розробки підходів до функціонування відомчих ІС 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 властивостей 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, Г. Ф. Конахович, В. В. Ліпаєв, О. Є. Литвиненко, І. О. Мачалін, О. В. Потій, В. В. Скляр, В. С. Харченко, К. Шеннон, О. К. Юдін та інші.

Проведений аналіз сучасних підходів до забезпечення функціональної безпеки показав достатньо глибоке опрацювання досліджень окремо за кожною ІС. Однак залишаються невивченими особливості взаємодії зазначених систем, зокрема під час модернізації окремих інформаційних систем у складі інтегрованої інформаційної системи з точки зору забезпечення функціональної безпеки загалом.

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, причому навіть незначний збій, зупинка або порушення їх властивостей можуть призвести до серйозних збитків національного масштабу.

Аналіз такого типу систем показав, з одного боку, сталу тенденцію до зростання множини інформаційних дестабілізаційних факторів, які впливають на функціональну безпеку, з іншого – захист життєво важливих інтересів держави вимагає від таких систем забезпечення підвищених вимог до властивостей інформаційного ресурсу (ІнР), який міститься у них.

Інтегрована інформаційна система (ІІС) ДПСУ оперує критичним інформаційним ресурсом щодо прийняття рішень, від дотримання властивостей якого залежить функціональна безпека системи в цілому. Разом з цим, постійне вдосконалення засобів обчислювальної техніки, спеціального програмного забезпечення (СПЗ) передбачає якісні та кількісні їх зміни, що потребує постійної модернізації відомчих систем та приводить 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 ДПСУ імені Б. Хмельницького. Дисертаційне дослідження проводилось у межах науково–дослідних робіт № 216–0008І "Методичні

рекомендації підрозділам Державної прикордонної служби України щодо порядку визначення зон виявлення сигналу з метою визначення захищеного периметра використання об’єкта інформаційної діяльності", № 217-0012І "Системний захист інформації у інтегрованій інформаційно-телекомунікаційній системі "Гарт" на стадії модернізації", № 217-0015І "Інформаційні технології в діяльності військових формувань та правоохоронних органів України".

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

Для досягнення поставленої мети в роботі вирішувались такі ***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 дестабілізаційного 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.

Об’єктом дослідження є процеси забезпечення функціональної безпеки інтегрованої інформаційної системи Держприкордонслужби на стадії модернізації.

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

Методи дослідження. 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 методів у даній 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. У результаті проведених досліджень вирішено актуальну науково-прикладну проблему шляхом розробки технології забезпечення функціональної безпеки інтегрованої інформаційної системи Держприкордонслужби на стадії модернізації. При цьому отримані наступні нові наукові положення та результати.

1. Вперше 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. Вперше 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 наявних полягає у врахуванні дестабілізаційних факторів, викликаних стадією модернізації та визначенні ймовірності потреби у забезпеченні дотримання властивостей інформаційного ресурсу (ІнР) інформаційних систем, яка ґрунтується на функції розподілу Гомперца-Мейкгама.

4. Вперше 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 межах 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 завдань в умовах впливу як зовнішніх, так і внутрішніх дестабілізаційних факторів. Відмінність розробленого методу полягає в двоетапному формуванні переліку інформаційних дестабілізаційних впливів із визначення ступеня їх реалізації.

6. Вперше 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. Отримані в дисертаційній роботі наукові результати є практичною базою для розробки ефективних інструментальних засобів забезпечення функціональної безпеки інтегрованих інформаційних систем, а саме:

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 раз 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 урахувати фактори, які викликані процесом модернізації інформаційної системи та до двох раз підвищити точність порівняно з наявними методами.

4. Розроблений комплекс методів узгодження систем розмежування доступу в інформаційних системах на стадії модернізації гарантує безпечне функціонування ІС на спільному полі даних у разі дотримання базових методологічних засад. Разом із тим, у межах 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 14 науково-практичних конференціях, основні з яких: VII Всеукраїнська науково-практична конференція "Освітньо-наукове забезпечення діяльності правоохоронних органів і військових формувань України" (м. Хмельницький, 2014), Міжнародна науково-практична конференція "Історія, сучасність та перспективи розвитку ДПСУ та охорони державного кордону" (м. Київ, 2015), XI Міжнародна науково-практична конференція "Військова освіта і наука: сьогодення та майбутнє" (м. Київ, 2015), VIII Всеукраїнська науково-практична конференція "Освітньо-наукове забезпечення діяльності правоохоронних органів і військових формувань України" (м. Хмельницький, 2015), VII Науково-практична конференція “Наукове забезпечення службово-бойової діяльності Національної гвардії України” (м. Харків, 2015), Міжнародна науково-технічна конференція "Перспективи розвитку озброєння та військової техніки сухопутних військ" (м. Львів, 2016), Всеукраїнська науково-практична конференція

"Кібербезпека в Україні: правові та організаційні питання" (м. Одеса 2016), Міжнародна заочна науково-практична конференція Державного закладу освіти "Інститут прикордонної служби Республіки Білорусь" (м. Мінськ, 2017), X Всеукраїнська науково-практична конференція "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 й обсяг роботи. Дисертаційна робота складається з анотації, переліку умовних позначень, вступу, шести розділів, висновків, списку використаних джерел до кожного розділу (347 найменувань) на 44 сторінках та 15 додатків на 102 сторінках. Загальний обсяг дисертації складає 453 сторінок, у тому числі 283 сторінки основного тексту, ілюстрацій – 71 (з них 8 на окремих сторінках), таблиць – 41 (з них 1 – на окремих 4 сторінках).

ОСНОВНИЙ ЗМІСТ РОБОТИ

У вступі розкрито зміст і стан проблеми, обґрунтовано актуальність теми дисертаційної роботи, зазначено її зв’язок з науковими програмами, планами та темами, сформульовано мету, завдання досліджень, визначено об’єкт, предмет і методи дослідження, охарактеризовано наукову новизну та практичне значення отриманих наукових положень та результатів. Наведено відомості про впровадження результатів роботи, їх апробацію та публікації.

У першому розділі проведено аналіз потреб у забезпеченні функціональної безпеки на сучасному етапі еволюції відомчої інформаційної системи ДПСУ. Визначені особливості функціонування інтегрованої інформаційної системи ДПСУ. Проведений аналіз інформаційних дестабілізаційних факторів викликаних стадією модернізації. Проаналізовані та систематизовані причини виникнення збитків від реалізації дестабілізаційних чинників процесу модернізації. Проведений аналіз підходів до забезпечення функціональної безпеки в інтегрованих інформаційних системах на стадії модернізації. Визначений вплив процесів інформатизації прикордонного відомства на складові національної безпеки України. Наведені та проаналізовані сучасні підходи до проблеми забезпечення функціональної безпеки в інформаційних системах. Проведений аналіз моделей розмежування доступу в інформаційних системах.

Результати першого розділу дозволили сформувати задачі дослідження, комплексне розв’язання яких надає можливість вирішити зазначену у вступі проблему.

Другий розділ присвячено розробці концептуальних основ технології забезпечення функціональної безпеки в інтегрованих інформаційних системах на стадії модернізації. У результаті проведених досліджень сформульована стратегія функціональної безпеки на стадії модернізації як модель узагальнених дій, спрямованих на досягнення зазначеної мети, суть якої полягає у такій сукупності заходів по заміні складових інформаційної системи при якій рівень функціональної безпеки відповідав нормативному. Разом із тим, умови функціонування різних ІС, їх структура та вимоги до функціональної безпеки передбачають обґрунтування

стратегій модернізації за такими групами критеріїв: рівня функціональної безпеки, особливостей функціонування ІС.

Формуванню першої групи критеріїв присвячено велику кількість робіт, в яких дослідники у якості показника рівня функціональної безпеки пропонують використовувати ймовірність попередження шкоди, ураховуючи стохастичну природу ризиків та загроз. Разом із тим, значення ймовірності виникнення шкоди упродовж усього терміну модернізації буде різною. Отже, обирати стратегію модернізації за значенням імовірності в довільний момент часу є не коректним. Необхідно враховувати загальну тенденцію функції зміни зазначеної імовірності.

Найбільш доцільними є розподіл даної групи критеріїв на три складових критерії рівня забезпечення функціональної безпеки: нормативний – критерій, при якому поточне значення ймовірності порушення функціональної безпеки не перевищуватиме заданого; середній – при якому середнє значення ймовірності не перевищуватиме заданого; зважений – критерій, при якому середнє зважене значення ймовірності порушення функціональної безпеки не перевищуватиме заданого.

Друга група критеріїв, яка визначає особливості функціонування ІС на стадії модернізації, характеризує можливості щодо втручання в процес роботи системи. За даною групою критерії розподіляються на три види: системи реального часу, системи з можливістю часткової зупинки, системи з можливістю повної зупинки. Отже, декартовий добуток обох критеріїв реалізує узагальнену таблицю раціональних стратегій модернізації.

Вищенаведені дослідження дозволяють сформувати загальну концепцію забезпечення функціональної безпеки на стадії модернізації, як інструментально-методологічну базу, що забезпечує виконання розглянутих стратегій (рис. 1).

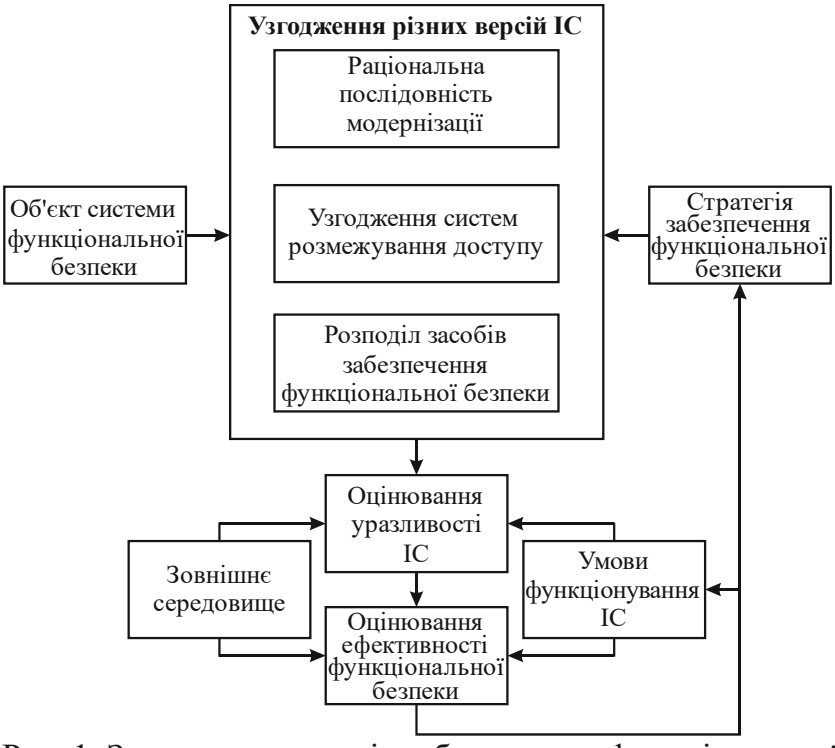


Рис. 1. Загальна концепція забезпечення функціональної безпеки на стадії модернізації

Проведена декомпозиція структури та інформаційних потоків ІІС прикордонного відомства стала основою для розробки вперше поданого ***методу визначення раціональної послідовності модернізації елементів ІС***.

У межах методу сформована структура інформаційних систем ІІС (рис. 2) і розроблена модель інформаційних потоків ІС на стадії модернізації (рис. 3). Визначено, що ймовірність порушення властивостей ІС на її окремому елементі під час здійснення однієї операції запит-відповідь від іншого елемента системи залежить від імовірностей модернізації взаємодіючих елементів $P_i^m(t)$, $P_j^m(t)$ та ймовірності порушення властивостей елемента ІС у разі невідповідності версій СПЗ $P_{i,j}$.

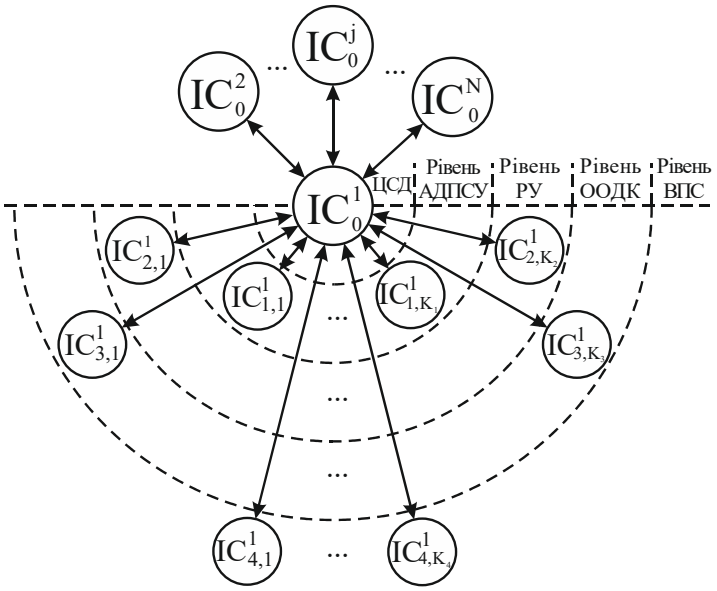


Рис. 2. Узагальнена структура інформаційних систем в ІІС

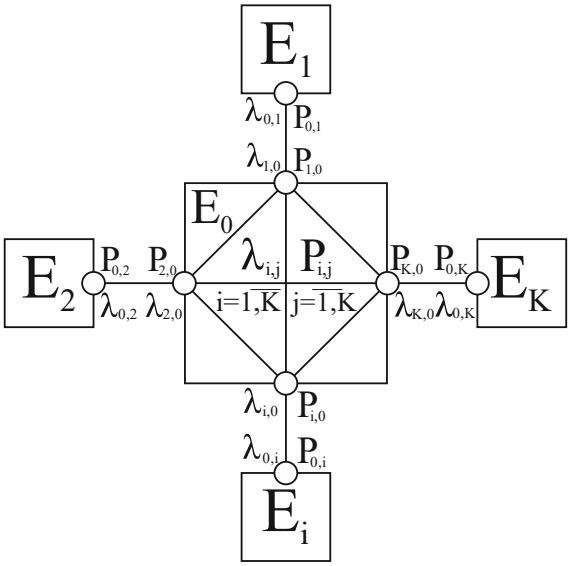


Рис. 3. Модель інформаційних потоків ІС на стадії модернізації

Отже, імовірність порушення властивостей елемента ІС під час отримання даних з іншого елемента становить:

$$P^*_{i,j}(t) = P^m_i(t) \cdot \left(1 - P^m_j(t)\right) \cdot P_{i,j}\,. \tag{1}$$

У моделі прийнято припущення, що порушення властивостей елемента ІС здійснюється тільки за умови наявності інформаційного потоку від нової версії СПЗ до старої. Отже, порушення властивостей елемента ІС у разі отримання хоча б одного блоку даних упродовж терміну t під час взаємодії з j-м елементом становить:

$$P^E_{i,j}(t) = 1 - \left(1 - P^*_{i,j}(t)\right)^{k_{i,j}(t)}, \tag{2}$$

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

Імовірність порушення властивостей елемента ІС упродовж терміну t під час модернізації ІС на її окремому елементі $P^E_i(t)$ у разі взаємодії із рештою складових є:

$$P^E_i(t) = 1 - \prod_{j=0}^{K} \left[1 - P^E_{j,i}(t)\right]. \tag{3}$$

Дана модель є основою для методу визначення раціональної послідовності модернізації елементів ІС, структура якого наведена на рис. 4.

Застосування розробленої математичної 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.

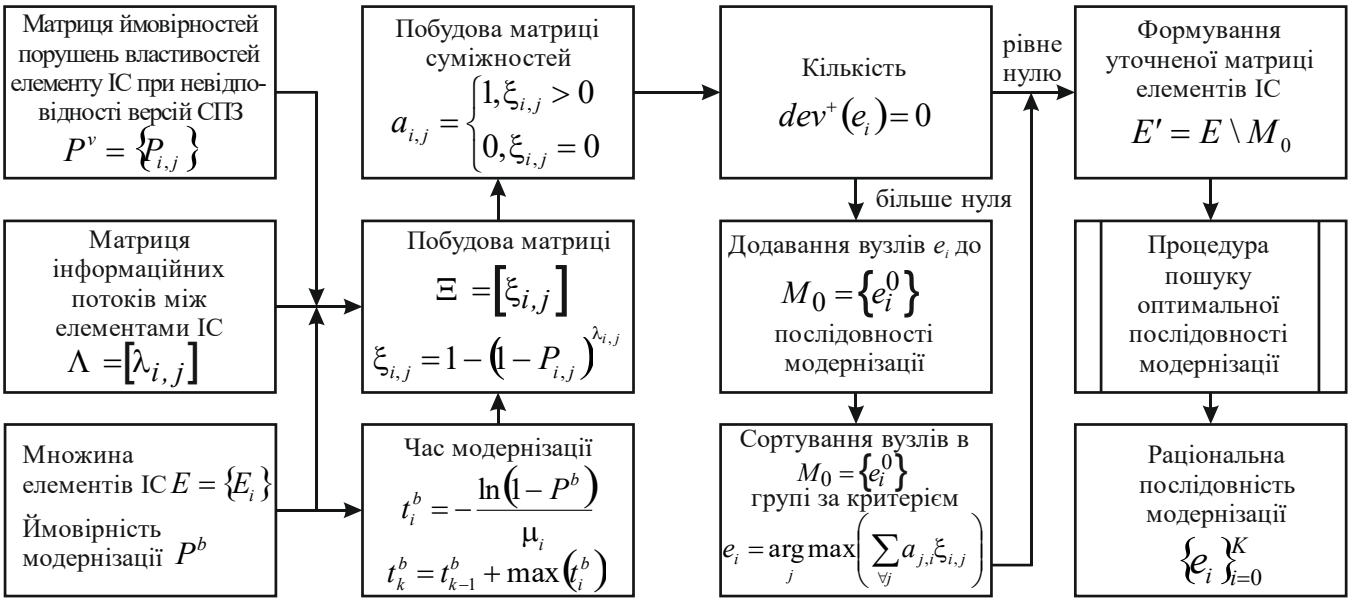


Рис. 4. Структура методу визначення послідовності модернізації елементів ІС

У третьому розділі розроблено метод розподілу засобів забезпечення функціональної безпеки в ІС на стадії модернізації та метод оцінювання уразливості ІС на стадії модернізації.

У межах вперше поданого ***методу розподілу засобів забезпечення функціональної безпеки в ІС на стадії модернізації*** розроблено: модель каналу інформаційного дестабілізаційного впливу (КІДВ), модель функціональної захищеності ІІС та метод розподілу засобів забезпечення функціональної безпеки (ЗЗФБ) відповідно до КІДВ.

Під час вибору кількісних характеристик можливих каналів інформаційного дестабілізаційного впливу використано загальновідомий емпіричний факт, який полягає в тому, що всі КІДВ не рівноцінні. Кожному КІДВ при цьому ставиться у відповідність безрозмірна позитивна величина C_i – вага КІДВ. Для визначення ваги КІДВ застосовано підхід, який полягає у використанні виміру або визначення кількості інформації, яка проходить через КІДВ, з урахуванням її рангу важливості. Отже, вага КІДВ становить:

$$C_i = \frac{\sum_{k=1}^{R} I_{ik} \cdot g_k}{\sum_{i=1}^{N} \sum_{k=1}^{R} I_{ik} \cdot g_k}, \tag{4}$$

де I_{ik} – кількість інформації, яка проходить через незахищений КІДВ з номером i та рангом важливості k; g_k – коефіцієнт важливості однієї одиниці інформації, з рангом k; N – кількість КІДВ; R – кількість рангів інформації.

Визначення захищеності КІДВ здійснюється за функціональною залежністю:

$$x_i = 1 - \prod_{j=1}^{S} (1 - q_{ij}), \tag{5}$$

де q_{ij} – коефіцієнт захисту i-го КІДФ j-м засобом; S – кількість засобів.

Модель КІДВ дозволила сформувати модель функціональної захищеності ІІС:

$$X = \sum_{i=1}^{N} C_i x_i \,. \tag{6}$$

Аналіз виразу (6) показав, що захищеність X об’єкта визначається через вагу C_i і захищеність x_i можливих каналів інформаційного дестабілізаційного впливу.

Наведені моделі дозволяють вирішити пряму задачу оцінювання функціональної захищеності ІІС (задача аналізу функціональної безпеки) за співвідношенням (6) і зворотну задачу оцінювання функціональної захищеності ІІС (задача синтезу функціональної безпеки), яка визначається таким чином:

$$\left.\begin{aligned} x_i &= 1 - \frac{C}{C_i}, i = \overline{M+1, N} \\ C &= \frac{1}{N-M}\left[(1-X) - \sum_{i=1}^{M}(1-x_i)C_i\right] \end{aligned}\right\}, \tag{7}$$

де M – кількість КІДВ до модернізації, N – кількість КІДВ після модернізації.

Для забезпечення нормативного рівня функціональної безпеки ІІС у межах методу розроблено метод раціонального розподілу ЗЗФБ відповідно до КІДВ, структурна схема якого наведена на рис. 5.

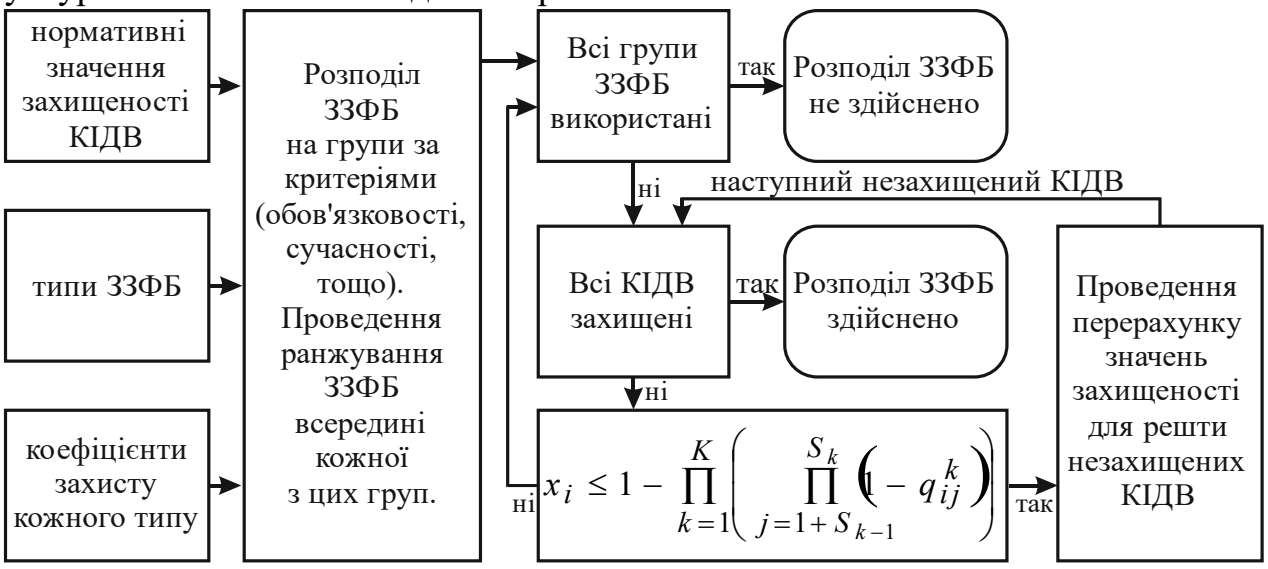


Рис. 5. Структурна схема методу розподілу засобів ЗЗФБ відповідно до КІДВ

Розроблені моделі та метод є складовою методу розподілу ЗЗФБ в ІІС на стадії модернізації, структурна схема якого наведена на рис. 6. Метод складається із окремих етапів.

Перший етап – премодернізація. На цьому етапі експертами здійснюється виявлення КІДВ і вибір ЗЗФБ, які можуть бути потенційно використані в ІІС. Ґрунтуючись на цих даних, аналітичними методами визначається кількість інформаційних дестабілізаційних впливів, яка проходить через кожний КІДВ і, 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.

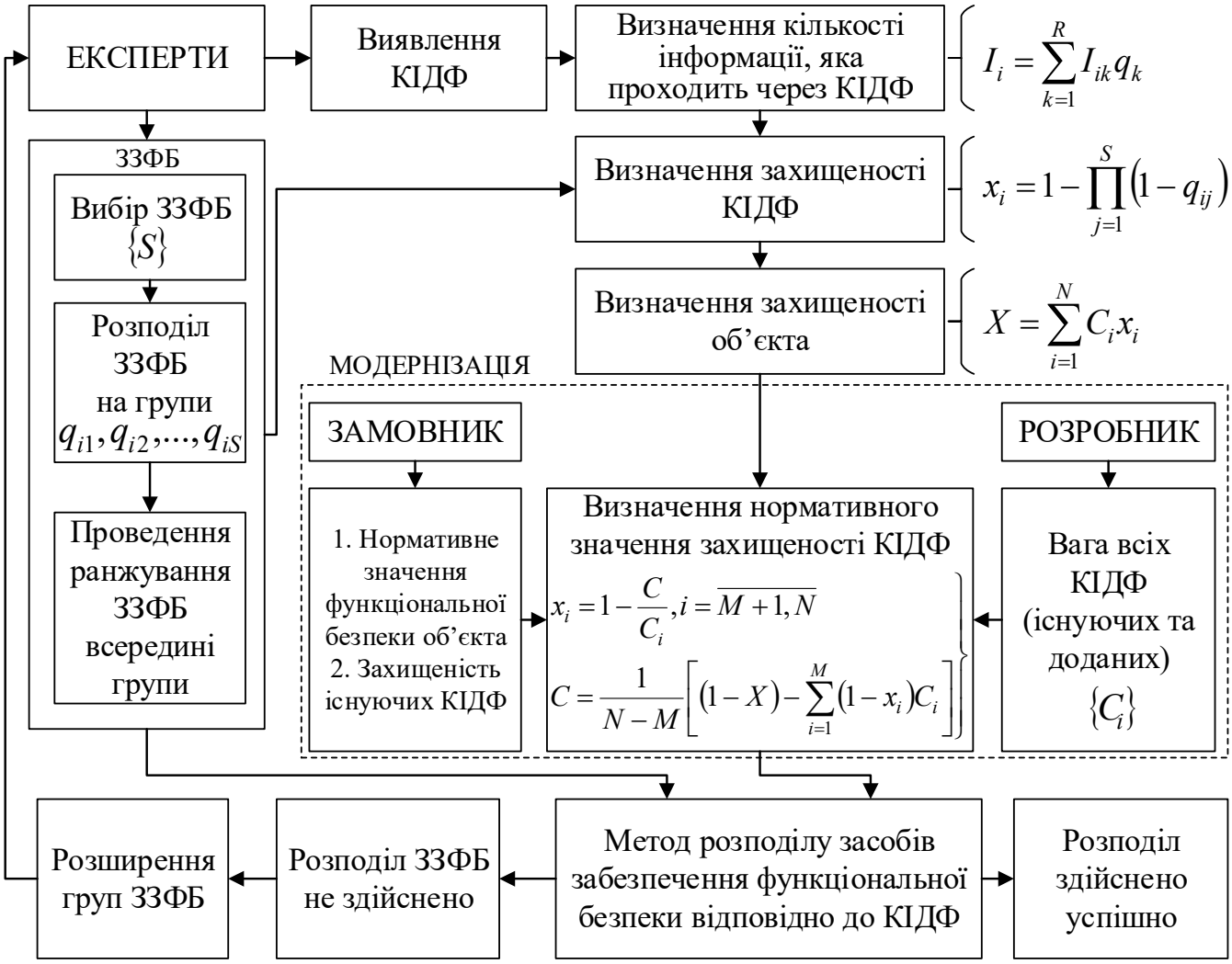


Рис. 6. Структурна схема методу розподілу ЗЗФБ в ІІС на стадії модернізації

Другий етап – модернізація. На цьому етапі замовник визначає нормативне значення функціональної безпеки об'єкта. Також надаються значення захищеності наявних КІДВ. З іншого боку, розробником визначаються ваги всіх КІДВ, які були визначені на попередньому етапі. На підставі цих даних визначається нормативне значення захищеності модернізованих і доданих КІДВ.

На третьому етапі – постмодернізації, здійснюється розподіл ЗЗФБ з визначеного експертами переліку та рангу. Результатом етапу є раціональний розподіл ЗЗФБ між КІДВ. У випадку неможливості забезпечити нормативне значення функціональної безпеки експертам визначається завдання щодо розширення переліку ЗЗФБ і здійснюється повторне використання методу.

Отже, застосування методу розподілу засобів забезпечення функціональної безпеки в ІІС на стадії модернізації дозволить підтримувати нормативне її значення у процесі модернізації як складових складної системи, так і під час впровадження нових елементів забезпечення функціональної безпеки.

У розділі наведено вдосконалений ***метод оцінювання уразливості ІС на стадії модернізації.*** У межах методу оцінювання уразливості ІС на стадії модернізації розроблені аналітичні моделі порушення властивостей ІС, а саме: цілісності, конфіденційності, доступності, спостереженості та визначений показник уразливості ІС (RI), загальний вираз якого є:

$$RI = 1-(1-P_i)\cdot(1-P_c)\cdot(1-P_a)\cdot(1-P_u), \tag{8}$$

де P_i, P_c, P_a, P_u – імовірності порушення цілісності, конфіденційності, доступності, спостереженості.

Розроблені математичні моделі порушення кожної із властивостей ІС:

$$P_i = P_{вх} + (1-P_{вх})P_н P_{нв}\left(1-\prod_{j=1}^{J}\left(1-P_j^i\right)\right), \tag{9}$$

$$P_c = P_д \cdot P_{кідф} \cdot P_{дост} \cdot P_{нд} \cdot P_{нв} \cdot P_н\left(1-\prod_{j=1}^{J}\left(1-P_j^c\right)\right), \tag{10}$$

$$P_a = P_д \cdot P_{кідф} \cdot P_{дост} \cdot P_{нд} \cdot P_{нв} \cdot P_н\left(1-\prod_{j=1}^{J}\left(1-P_j^a\right)\right), \tag{11}$$

$$P_u = P_н \cdot P_{нв} \cdot P_р \cdot P_{іа} \cdot P_{дк} \cdot P_{цкзз}, \tag{12}$$

де $P_{вх}$ – імовірність надходження даних у загальне поле елемента ІС зі старої або нової версій СПЗ з порушеною цілісністю; $P_н$ – імовірність надходження даних в елемент ІС іншої версії СПЗ; $P_{нв}$ – імовірності порушення властивості даних у результаті неузгодженості версій СПЗ; P_j – імовірності порушення властивостей даних під впливом *j*-го ДФ; $P_д$ – імовірність доступу порушника до елемента ІС; $P_{кідф}$ – імовірність наявності КІДФ в елементі ІС до даних певної категорії; $P_{дост}$ – імовірність доступу порушника до КІДФ в елементі ІС; $P_{нд}$ – імовірність наявності даних певної категорії на елементі ІС; $P_р$ – імовірність порушення реєстрації події щодо певної категорії даних; $P_{іа}$ – імовірність порушення ідентифікації і автентифікації порушника у складовій ІС; $P_{дк}$ – імовірність порушення достовірності каналу доступу порушником за умови доступу порушника до складової ІІС; $P_{цкзз}$ – імовірність порушення цілісності комплексу засобів забезпечення функціональної безпеки складової ІС.

Імовірність того, що дані надходять в елемент ІС з іншої версії СПЗ є відношення потоку даних λ_i старої версії СПЗ до загального потоку даних у наступний елемент ІС, а саме:

$$P_н = \sum_{i=1}^{k}\lambda_i \Big/ \sum_{i=1}^{K}\lambda_i . \tag{13}$$

Імовірність порушення ідентифікації і автентифікації залежить від імовірностей порушення цілісності та доступності:

$$P_{іа} = \left(1-(1-P_i)\cdot(1-P_c)\right)\cdot\prod_{m=1}^{M}P_m^{ia}, \tag{14}$$

де P_m^{ia} – імовірність порушення ідентифікації і автентифікації *m*-м типом.

Імовірність порушення цілісності комплексу ЗЗФБ виражається, як змога протистояти множині дестабілізаційних факторів, а саме:

$$P_{цкзз} = 1-\prod_{j=1}^{J}\left(1-P_j^{цкзз}\right). \tag{15}$$

Надалі модель розширена за рахунок введення, доданих функцій з метою компенсації потоку ДФ, обумовлених модернізацією ІІС. На стадії модернізації ІІС процес функціонування системи не є сталим, тому потік ДФ відповідає розподілу Вейбулла на ділянці періоду модернізації. Разом із врахуванням потоку ДФ, обумовлених стадією модернізації, модель враховує потребу у забезпеченні дотримання властивостей ІнР, яка виникає тільки у випадку знаходження його у загальному полі гетерогенної ІІС. Тривалість існування корисного ІнР або такого, який буде використовуватись і, відповідно, знаходитись у загальному полі ІІС, є випадковою величиною, залежить від певних факторів і може бути описана розподілом Гомперца-Мейкгама, в якому параметр інтенсивності експоненційного розподілу має часовий тренд, котрий може бути описаний рівнянням модифікованої експоненти $\lambda(t) = a + be^{\lambda_0 t}$, де λ, a, b – параметри життєвого циклу ІнР. Отже, функція розподілу ймовірності невикористання (старіння) ІнР прийме вигляд:

$$F_c(t) = \int_0^t \lambda(x) \cdot e^{\lambda(x)x} dx. \qquad (16)$$

Разом із тим, ІнР у процесі експлуатації ІІС постійно поповнюється новою інформацією з параметром потоку $\lambda_{вх}$ та функцією розподілу:

$$F_{вх}(t) = 1 - e^{-\lambda_{вх} t}. \qquad (17)$$

Під одиницею інформації, яка поступає в систему, будемо розуміти певний блок даних, який пов'язаний логікою функціонування системи (інформація про перетин кордону особою, транспортним засобом, доручення правоохоронних органів).

Отже, величина коефіцієнта використання інформації є випадковою та залежить від моменту появи інформації (рис. 7), імовірність якої розподілена за формулою (17).

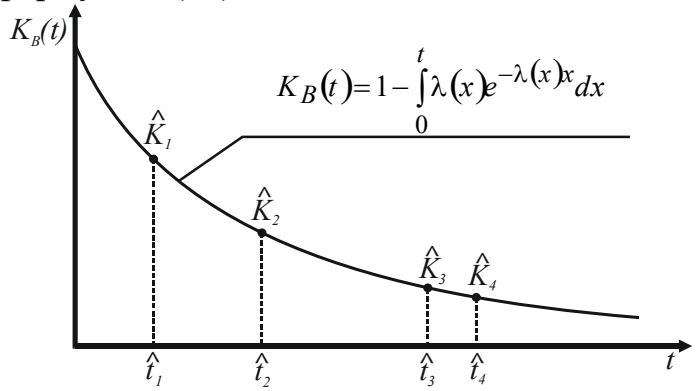


Рис. 7. Залежність коефіцієнту використання даних від часу їх перебування в ІІС

У результаті перетворень одновимірної випадкової величини, отримаємо:

$$F(K) = F_{вх}\left(K_в^{-1}(K)\right), \qquad (18)$$

де $K_в^{-1}(K)$ – обернена функція до $K_в(t)$

Фізичний сенс виразу (18) полягає у ймовірності появи інформації в загальному полі даних з величиною коефіцієнта використання не менше K.

Кількість інформації із рівнем коефіцієнта використання не менше K, яка поступила в систему в сталому режимі становить:

$$N = \lambda_{вх} K_в^{-1}(K). \qquad (19)$$

Як видно із (19), кількість інформації із заданим рівнем коефіцієнта використання не залежить від часу експлуатації ІІС, а залежить тільки від величини інтенсивності вхідного потоку.

На стадії модернізації, під впливом потоку дестабілізаційних факторів, спричинених спільним використанням загального поля даних як нової, так і старої версій СПЗ, ступінь дотримання властивостей ІнР знижується. Узагальнений показник уразливості описується моделями процесів порушення властивостей ІС. Вихідними даними для цих моделей, з одного боку, служать переважно висновки експертів, які визначають множину дестабілізаційних факторів. 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. Разом із тим, у методі враховані й організаційні заходи, які провадить замовник під час експлуатації ІІС, що можуть змінюватись залежно від вимог до модернізації системи.

Ураховуючи масштабність наявних ІІС, модернізація системи здійснюється поступово упродовж певного періоду часу, під час якого одночасно функціонують різні версії СПЗ, що вимагає врахування цього факту у зазначених моделях. Разом із тим, ступінь уразливості визначає потребу дотримання властивостей інформаційного ресурсу на стадії модернізації тільки у випадку сумісного використання спільних ресурсів системи користувачами з різними правами на дані, що розглядаються, і різними версіями СПЗ. Вищезазначене дозволяє сформувати структурну схему методу оцінювання уразливості ІС на стадії модернізації (рис. 8).

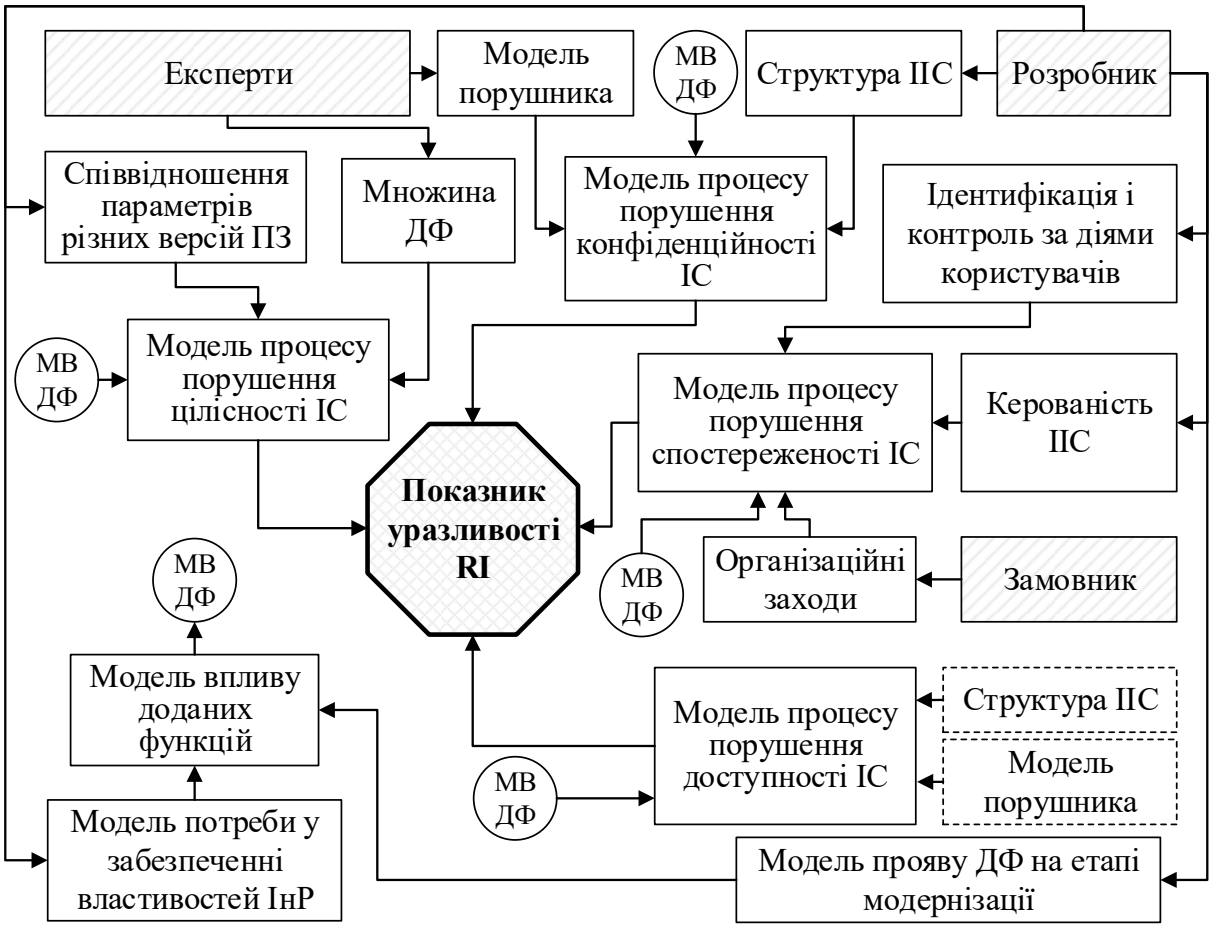


Рис. 8. Структурна схема методу оцінювання уразливості ІС на стадії модернізації

У результаті моделювання процесів порушення властивостей ІС визначається узагальнений показник уразливості ІС. Запровадження доданих функцій узгодження різних версій ІС впливає на загальний показник уразливості.

Четвертий розділ присвячено розробці теоретичних основ та сукупності методів і моделей узгодження різних версій систем розмежування доступу в інформаційних системах на стадії модернізації. Під час модернізації наявних складових ІІС або інтеграції нових виникає ситуація спільного функціонування систем розмежування доступу (СРД) на загальному полі даних. Для дослідження спільного функціонування різних версій моделей безпеки комп'ютерних системи обрано такі їх види: дискреційного, рольового, мандатного та тематичного моделей розмежування доступу; безпеки інформаційних потоків; суб'єктно-орієнтовану модель ізольованого програмного середовища. Показано, що спільне функціонування різних версій СРД, 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.

У розділі вперше розроблено ***метод узгодження решіток рівнів конфіденційності систем мандатного розмежування доступу ІС на стадії модернізації,*** структурна схема якого наведена на рис. 9.

Аналітично метод узгодження решіток рівнів конфіденційності різних версій систем розмежування доступу подається наступним 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; $f:\left(L,\leq\right)\to Q, Q\in\mathbb{R}$ – відображення меж решітки конфіденційності в підмножину дійсних чисел. Тоді спільна для обох версій СРД решітка конфіденційності є:

$$f^{-1}:\left(\left(L^{old},\leq\right)\xrightarrow{f}Q^{old}\cup\left(L^{new},\leq\right)\xrightarrow{f}Q^{new}\right)\to\left(L^{join},\leq\right), \qquad (20)$$

де $f^{-1}:Q\to L$ – обернене відображення множини дійсних чисел у межі решітки конфіденційності;

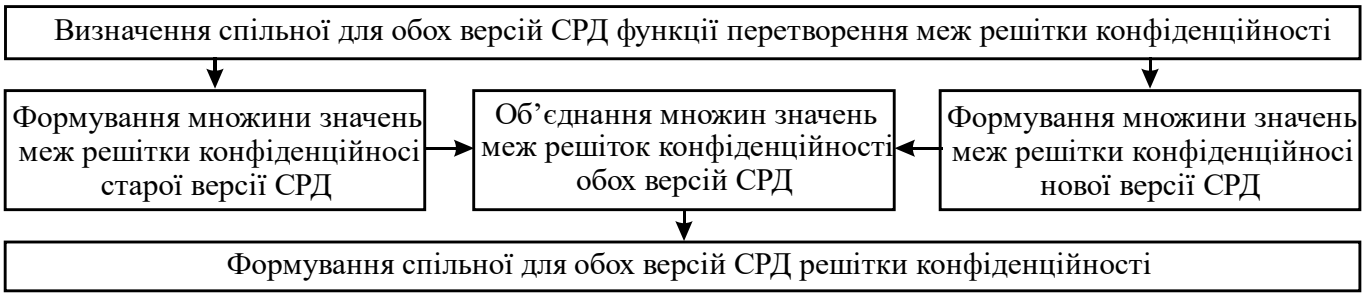


Рис. 9. Структурна схема методу узгодження решіток рівнів конфіденційності різних версій систем розмежування доступу

Вищенаведений метод вимагає формулювання та доказу того, що у запропонованій спільній решітці конфіденційності неможливо реалізувати заборонений інформаційний потік в одній версії СРД і дозволений в іншій.

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 в спільній решітці конфіденційності можливий такий потік, який в одній із версій СРД дозволений, а в іншій 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). Разом із тим, розбиття спільної решітки конфіденційності передбачає знаходження таких об’єктів у різних множинах спільної решітки конфіденційності (рис. 10). Отже, зазначений інформаційний потік буде забороненим, що суперечить припущенню про його існування.

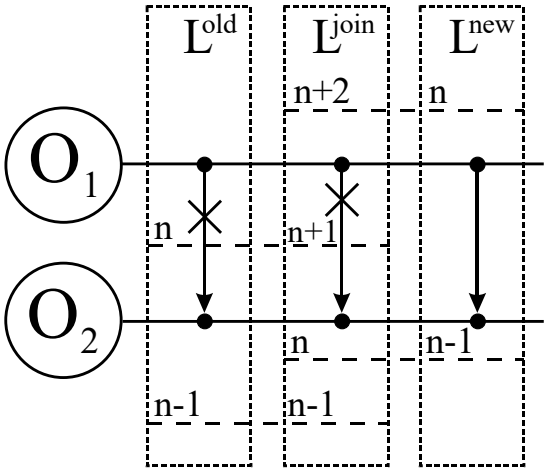


Рис. 10. До доказу теореми безпеки спільної решітки конфіденційності

Наступним в сукупності методів є вперше розроблений ***метод узгодження матриць доступу систем дискреційного розмежування доступу інформаційних систем на стадії модернізації,*** структурна схема якого наведена на рис. 11.

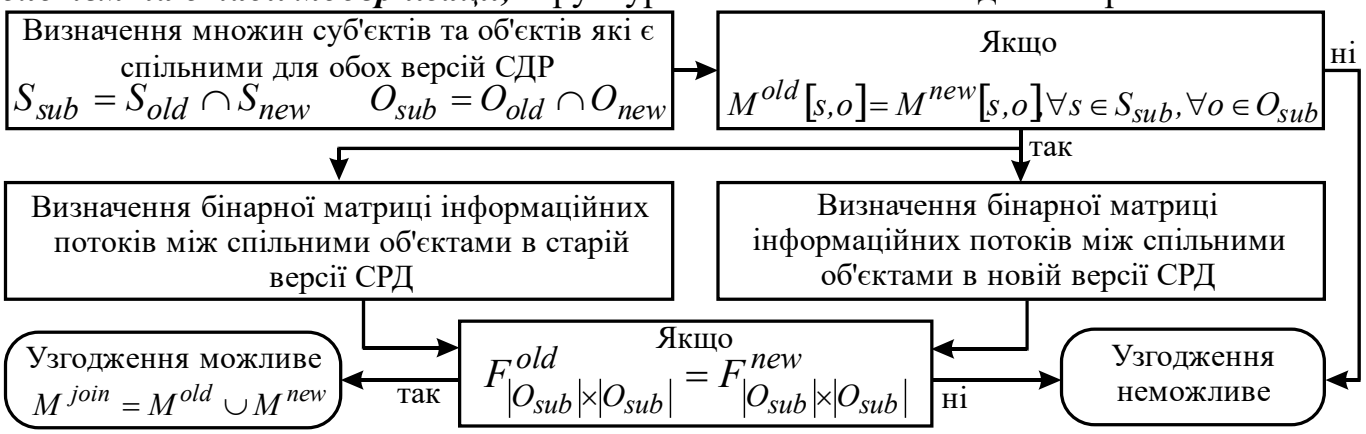


Рис. 11. Структурна схема методу узгодження матриць доступу різних версій систем дискреційного розмежування доступу

Вихідними даними методу є: $M^{old}_{|S_{old}|\times|O_{old}|} = M^{old}[s_{old}, o_{old}]$ – 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 $O_{join} = O_{old} \cup O_{new}$. Спільними для обох версій СДР множини суб’єктів та об’єктів є: $S_{sub} = S_{old} \cap S_{new}$ 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:

$$M^{old}[s,o] = M^{new}[s,o], \forall s \in S_{sub}, \forall o \in O_{sub}. \quad (21)$$

Наступним етапом методу є визначення можливості створення інформаційного потоку, який є легальним в одній версії СРД і забороненим 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 (21). Узгодженість різних версій СРД, а саме спільної матриці доступу $M^{join}[s_{join}, o_{join}]$, можлива тільки при 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 $M_{|S|\times|O|} = M[s, o]$ та 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, $\bar{R} \in R$ – підмножина прав доступу, яка формує інформаційний потік від об'єкта до суб'єкта, $\widetilde{R} \in R$ – підмножина прав доступу, яка не формує інформаційний потік. Елементи матриці суміжності $E_{|O|\times|O|} = \{e_{ij}\}$ формуються таким чином:

$$e_{ij} = \begin{cases} 1, \exists k\, M[s_k, o_i] \in \bar{R}, M[s_k, o_j] \in \vec{R} \\ 0, else \end{cases}. \qquad (22)$$

Надалі, ураховуючи властивості графу, визначається матриця досяжності як диз'юнкція степенів матриць суміжності: $E^* = E \vee E^2 \vee \ldots \vee E^{|O|}$.

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:

$$F = \{e^*_{ij}\}, \forall o_i, o_j \in O'. \qquad (23)$$

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.

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 і дозволений в іншій.

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 властивостей інформації, тобто виникнення недозволеного інформаційного потоку. Отже, у разі 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.

Наступним є вперше розроблений ***метод узгодження систем рольового розмежування доступу інформаційних систем на стадії модернізації,*** структурна схема якого наведена на рис. 12. Суть методу полягає у формуванні таких параметрів СРД, за яких неможливо реалізувати недозволений інформаційний потік у кожній з версій окремо.

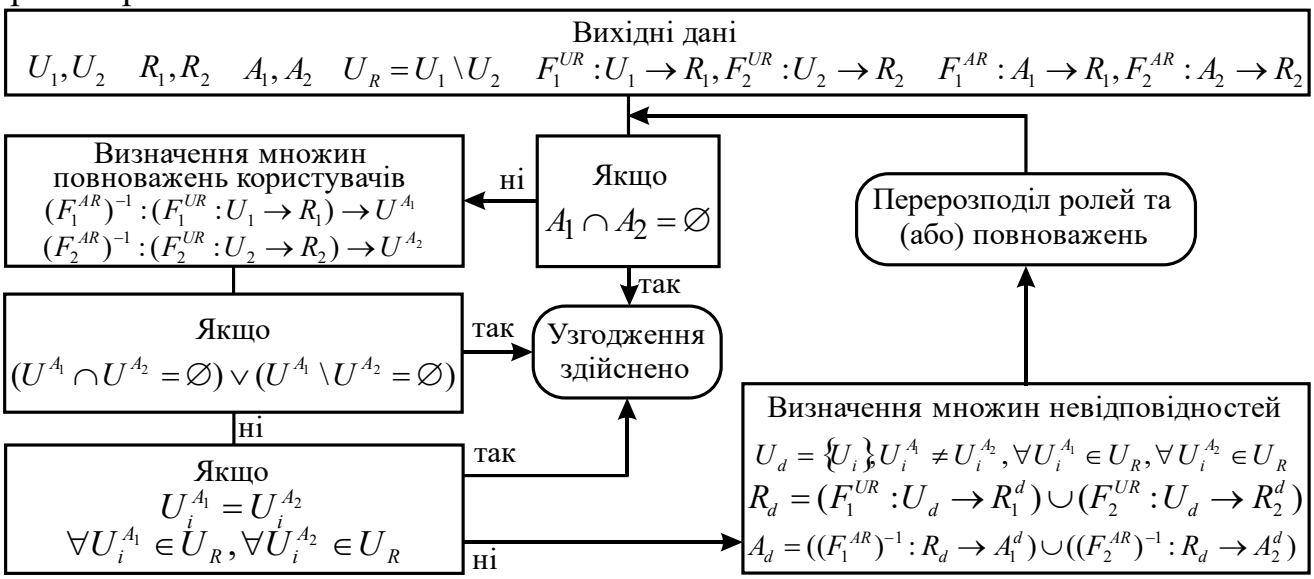


Рис. 12. Структурна схема методу узгодження різних версій систем рольового розмежування доступу

ІС, в якій спільно функціонують дві різні версії рольових СРД, 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:

$$a_i \cap a_j = \varnothing,\ \forall a_i \in A, \forall a_j \in A. \qquad (24)$$

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, це може

призвести до недозволених інформаційних потоків. Визначимо множину повноважень користувачів як:

$$\begin{matrix} \left(F_1^{AR}\right)^{-1} : \left(F_1^{UR} : U_1 \to R_1\right) \to U^{A_1} \\ \left(F_2^{AR}\right)^{-1} : \left(F_2^{UR} : U_2 \to R_2\right) \to U^{A_2} \end{matrix}, \quad (25)$$

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

$$\left(U^{A_1} \cap U^{A_2} = \varnothing\right) \vee \left(U^{A_1} \setminus U^{A_2} = \varnothing\right) \quad (26)$$

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 в межах повноваження $a \in A$, за умови, де $A \in f_{permission}(c)$. Це вимагає рівності повноважень для спільних в обох версіях СРД користувачів, тобто:

$$U_i^{A_1} = U_i^{A_2}, \forall U_i^{A_1} \in U_R, \forall U_i^{A_2} \in U_R. \quad (27)$$

У випадку невиконання умови (27) отримуємо множини користувачів, ролей і повноважень, які спричиняють порушення правила безпеки у разі спільного функціонування обох версій СРД і потребують зміни:

$$U_d = \{U_i\}, U_i^{A_1} \neq U_i^{A_2}, \forall U_i^{A_1} \in U_R, \forall U_i^{A_2} \in U_R, \quad (28)$$

$$R_d = \left(F_1^{UR} : U_d \to R_1^d\right) \cup \left(F_2^{UR} : U_d \to R_2^d\right), \quad (29)$$

$$A_d = \left(\left(F_1^{AR}\right)^{-1} : R_d \to A_1^d\right) \cup \left(\left(F_2^{AR}\right)^{-1} : R_d \to A_2^d\right). \quad (30)$$

Процес впровадження модернізованих складових у загальну систему здійснюється поетапно й 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 у межах політики безпеки, так і виходити за них.

Зазначимо, що порушення правил політики безпеки СРД можливо тільки за умови наявності недозволеного (заборони дозволеного) інформаційного потоку між об’єктом, який містить інформацію та суб’єктом. З цієї причини інформаційні потоки між суб’єктами в межах моделі не розглядаються.

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.

1. У випадку, коли СРД не мають спільних елементів та функціонують незалежно одна від одної. Недозволені інформаційні потоки відсутні.

2. У випадку, коли СРД мають тільки спільних користувачів. Необхідною умовою порушення властивостей інформації є наявність об'єкта, який містить інформацію, з якою не повинен ознайомитись користувач. Разом із тим, політика безпеки СРД не допустить наявності такої інформації в об'єкті, який належить користувачу (має доступ). Отже, у такому варіанті порушення властивостей інформації відсутнє.

3. У випадку, коли 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 призведе до недозволеного інформаційного потоку до певного суб'єкта.

4. У випадку, коли СРД мають спільні суб'єкти та об'єкти. Такий варіант об'єднує другий і третій випадки та передбачає можливість виникнення недозволеного інформаційного потоку між об'єктами.

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 у разі 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 наочний 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.

Розробка методів узгодження 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 оцінюється за допомогою імовірності виникнення недозволеного інформаційного потоку в різних версіях СРД:

$$P_{ITC}^{forb} = 1 - \prod_{\forall i} \prod_{\forall j} \left(1 - P_{ij}^{forb}\right), \tag{31}$$

де P_{ij}^{forb} – імовірність наявності недозволеного інформаційного потоку між двома об'єктами системи.

Значення ймовірності недозволеного інформаційного потоку між двома спільними об'єктами системи визначається так:

$$P_{ij}^{forb} = \begin{cases} 0, P_{ij}^1 > 0, P_{ij}^2 > 0 \\ 0, P_{ij}^1 = 0, P_{ij}^2 = 0 \\ P_{ij}^1, P_{ij}^1 > 0, P_{ij}^2 = 0 \\ P_{ij}^2, P_{ij}^1 = 0, P_{ij}^2 > 0 \end{cases}, \tag{32}$$

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 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).

Імовірність наявності інформаційного потоку P_{sd} між s-м та d -м об'єктом СРД описується матрицею величин інформаційних потоків $\Lambda = \{\lambda_{ij}\}$ навантаженого графу станів системи (рис. 13). Приймемо: $P_1(t),...,P_i(t),...,P_N(t)$ – як імовірності наявності інформації в певному об'єкті, який позначений індексом. Наочно, що для будь-якого моменту часу виконується умова $\sum_{i=1}^{N} P_i(t) = 1$.

Відповідно до графу станів опишемо систему диференційних рівнянь першого порядку (33) та початкові умови (34):

$$\begin{cases} \dfrac{dP_1(t)}{dt} = \sum\limits_{k=1}^{N} \lambda_{k1} P_k(t) - P_1(t) \sum\limits_{k=1}^{N} \lambda_{1k} \\ ... \\ \dfrac{dP_i(t)}{dt} = \sum\limits_{k=1}^{N} \lambda_{ki} P_k(t) - P_i(t) \sum\limits_{k=1}^{N} \lambda_{ik} \\ ... \\ \dfrac{dP_N(t)}{dt} = \sum\limits_{k=1}^{N} \lambda_{kN} P_k(t) - P_N(t) \sum\limits_{k=1}^{N} \lambda_{Nk} \end{cases} . \quad (33)$$

$$P_s(0) = 1, P_i(0) = 0, \forall i \neq s . \quad (34)$$

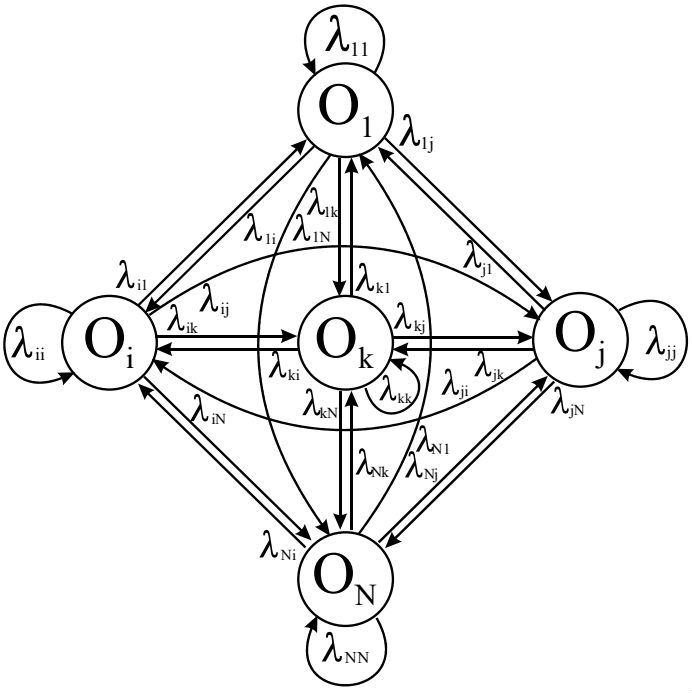


Рис. 13. Граф станів системи

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 у s-му об'єкті, знаходитимуться в d-му об'єкті в момент часу t.

У п'ятому розділі розроблений метод оцінювання ефективності функціональної безпеки ІС на стадії модернізації. Аналіз підходів до оцінювання ефективності систем функціональної безпеки показав, що найбільш коректним є підхід теорії ефективності цілеспрямованих процесів. Разом із тим, використання такого підходу обмежується наступними причинами: висока ступінь невизначеності вихідних даних, складність формалізації процесів функціонування. У межах методу сформульовані його семантичні аспекти, а саме: визначено поняття функціональної безпеки ІІС прикордонного відомства як цілеспрямований процес з єдиною (що є принциповим) метою – недопущення несанкціонованих дій стосовно інформації під час усього життєвого циклу ІІС та розширено поняття "несанкціонованих дій щодо інформації в системі" в рамках системи забезпечення функціональної безпеки.

Інформаційні системи ДПСУ є чутливими, насамперед, до таких властивостей інформації як доступність і достовірність. Саме якість виконання цих послуг суттєво впливає на функціональну безпеку ІС прикордонного відомства та на національну безпеку держави. Визначено поняття "навколишнє середовище" у межах терміну "функціональна безпека" як сукупність об'єктів, які не входять до СФБ та безпосередньо не беруть участь у процесі функціонування ІС, але здійснюють вплив на досягнення мети СФБ. Надалі під поняттям "навколишнє середовище" розуміється сукупність умов функціонування та застосування системи функціональної безпеки.

Під час оцінювання якості СФБ, яка описується *n*-вимірним векторним показником $Y_{\langle n\rangle}$ визначено сукупність критеріїв, які належать класу критеріїв придатності $\{G\}$, математичне формулювання якого має вигляд:

$$G:\left(Y_{\langle n\rangle}\in\left\{Y^{A}_{\langle n\rangle}\right\}\right), \tag{35}$$

де $Y_{\langle n\rangle}$ – показник якості СФБ; $\left\{Y^{A}_{\langle n\rangle}\right\}$ – множина допустимих значень.

Отже, СФБ, для якої виконується умова (35), придатна до використання за призначенням та виконує свої функції.

Серед множини властивостей системи функціональної безпеки істотними є ті, які визначають якість процесу функціональної безпеки. У керівних документах визначені функціональні критерії, що визначають множину типів показників якості СФБ ІІС прикордонного відомства.

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, ресурсоємністю та оперативністю.

Із зазначеного вище можна зробити висновок, що якість СФБ не може бути охарактеризована окремими властивостями, а визначається тільки їх сукупністю. У результаті згортання часткових показників, вектор показників якості функціонування СФБ прийме вигляд:

$$Y=\langle v_i, v_c, v_a, v_u\rangle, \tag{36}$$

де v_i – показник цілісності; v_c – показник конфіденційності; v_a – показник доступності; v_u – показник спостереженості;

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.

Кожна з компонент вектора Y залежить від характеристик СФБ та її організації, умов функціонування та застосування системи. Компоненти вектора Y^{A} допустимих значень також залежать від умов застосування системи і визначаються керуючою системою. Отже, характеристикою якості СФБ є імовірність випадкової події:

$$P_{ДМ}=P\left(\hat{Y}\in\left\{\hat{Y}^{A}\right\}\right). \tag{37}$$

Для опису умов функціонування та умов застосування системи в межах методу розроблена методика формування моделі інформаційних дестабілізаційних факторів (ІДФ) на стадії модернізації, мета якої полягає у визначенні уточнених характеристик ІДФ. На підставі сформованих уточнених характеристик ІДФ складовим ІнР в ІС формуються функціональні залежності залишкового ризику за його властивостями. У загальному випадку функція залежності залишкового ризику ІнР від часу експлуатації для кожної загрози має вигляд:

$$P_p^k(t)=\begin{cases} F_{p,k}^{ind}(t) - \textit{не залежить від модернізації} \\ F_{p,k}^{dep}(t) - \textit{залежить від модернізації} \end{cases}, \quad (38)$$

де $F_{p,k}^{ind}(t)$ – функція розподілу ймовірності реалізації p–ї властивості та k–го ІДФ, імовірність виникнення якого не залежить від модернізації ІС; $F_{p,k}^{dep}(t)$ – функція розподілу ймовірності реалізації p–ї властивості та k–го ІДФ, імовірність виникнення якого залежить від модернізації ІС.

Отже, імовірність порушення властивостей ІнР становить:

$$P_p = 1 - \prod_{k=1}^{N}\left(1 - P_p^k(t)\right), \quad (39)$$

де N – кількість складових ІДФ.

Імовірність виникнення ІДФ, яка не залежить від модернізації ІС та може бути описана законом розподілу:

$$F_{p,k}^{ind}(t)=\begin{cases} 0, t<0 \\ P_{p,k}^{ind} \\ 1, t>t_{експл} \end{cases}, \quad (40)$$

де $P_{p,k}^{ind}$ – значення імовірності виникнення ІДФ, яка не залежить від модернізації ІС; $t_{експл}$ – час експлуатації СФБ.

Імовірність виникнення ІДФ, який залежить від модернізації ІС, залежить від ймовірності безвідмовної роботи модернізованої ІС, описується розподілом Вейбула, що описує час безвідмовної роботи та застосовується для оцінки надійності програмних засобів.

Отримані функціональні залежності дозволили сформувати закони розподілу порушення властивостей ІнР:

$$P_p^A\left(v_p^A\right) = 1 - \prod_{\forall k \in \left\{T_{ind}^p\right\}}\left(1 - F_{p,k}^{ind}\left(v_p^A\right)\right) \prod_{\forall k \in \left\{T_{dep}^p\right\}} e^{-\left(\frac{v_p^A}{\beta_{p,k}}\right)^{\alpha_{p,k}}}. \quad (41)$$

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:

$$\left\{\hat{Y}^A\right\} = \left(\hat{v}_i^A, \infty\right) \times \left(\hat{v}_c^A, \infty\right) \times \left(\hat{v}_a^A, \infty\right) \times \left(\hat{v}_u^A, \infty\right), \quad (42)$$

з вершиною в точці $\hat{Z} = \left\langle \hat{v}_i^A, \hat{v}_c^A, \hat{v}_a^A, \hat{v}_u^A \right\rangle$.

У загальному випадку події, пов'язані з порушенням властивостей ІнР, є взаємозалежними. З метою оцінки ступеня залежності показників якості системи функціональної безпеки пропонується використати метод експертних оцінок або статистичне значення ймовірностей виникнення події порушення властивості ІнР за умови порушення іншої, для чого визначимо множину гіпотез:

$$\mathrm{H} = \{H_i, H_c, H_a, H_u, H_d\}, \tag{43}$$

де H_i – порушення цілісності; H_c – порушення конфіденційності; H_a – порушення доступності; H_u – порушення спостереженості; H_d – дотримання всіх властивостей.

Відповідно до відомих підходів теорії імовірностей, порушення цілісності ІнР за умови порушення конфіденційності становить:

$$P_{H_1}^c = P_i(v_i^A) + \left(1 - P_i(v_i^A)\right) \cdot \left(1 - \left[\left(1 - P_c(v_i^A)\right) + P_c(v_i^A) \cdot \left(1 - P_c(i)\right)\right]\right). \tag{44}$$

Використовуючи цей підхід, розширимо множину подій на решту властивостей. Отже, порушення цілісності ІнР є зворотною подією до події не порушення цілісності з урахуванням імовірностей порушень інших властивостей:

$$\begin{aligned} P_{H_i}\left(v_i^A\right) &= P_i(v_i^A) + (1 - P_i(v_i^A)) \times \\ &\times \left(1 - \left[\left(1 - P_c(v_i^A)\right) + P_c(v_i^A)\left(1 - P_c(i)\right)\right]\right) \times \\ &\times \left(1 - \left[\left(1 - P_a(v_i^A)\right) + P_a(v_i^A)\left(1 - P_a(i)\right)\right]\right) \times \\ &\times \left(1 - \left[\left(1 - P_u(v_i^A)\right) + P_u(v_i^A)\left(1 - P_u(i)\right)\right]\right) \end{aligned}. \tag{45}$$

Аналогічно для інших гіпотез:

$$\begin{aligned} P_{H_c}\left(v_c^A\right) &= P_c(v_c^A) + (1 - P_c(v_c^A)) \times \\ &\times \left(1 - \left[\left(1 - P_i(v_c^A)\right) + P_i(v_c^A)\left(1 - P_i(c)\right)\right]\right) \times \\ &\times \left(1 - \left[\left(1 - P_a(v_c^A)\right) + P_a(v_c^A)\left(1 - P_a(c)\right)\right]\right) \times \\ &\times \left(1 - \left[\left(1 - P_u(v_c^A)\right) + P_u(v_c^A)\left(1 - P_u(c)\right)\right]\right) \end{aligned}, \tag{46}$$

$$\begin{aligned} P_{H_a}\left(v_a^A\right) &= P_a(v_a^A) + (1 - P_a(v_a^A)) \times \\ &\times \left(1 - \left[\left(1 - P_i(v_a^A)\right) + P_i(v_a^A)\left(1 - P_i(a)\right)\right]\right) \times \\ &\times \left(1 - \left[\left(1 - P_c(v_a^A)\right) + P_c(v_a^A)\left(1 - P_c(a)\right)\right]\right) \times \\ &\times \left(1 - \left[\left(1 - P_u(v_a^A)\right) + P_u(v_a^A)\left(1 - P_u(a)\right)\right]\right) \end{aligned}, \tag{47}$$

$$\begin{aligned} P_{H_u}\left(v_u^A\right) &= P_u(v_u^A) + (1 - P_u(v_u^A)) \times \\ &\times \left(1 - \left[\left(1 - P_i(v_u^A)\right) + P_i(v_u^A)\left(1 - P_i(u)\right)\right]\right) \times \\ &\times \left(1 - \left[\left(1 - P_c(v_u^A)\right) + P_c(v_u^A)\left(1 - P_c(u)\right)\right]\right) \times \\ &\times \left(1 - \left[\left(1 - P_a(v_u^A)\right) + P_a(v_u^A)\left(1 - P_a(u)\right)\right]\right) \end{aligned}. \tag{48}$$

Враховуючи (42, 45–48) отримаємо аналітичну форму закону розподілу випадкового вектора $\hat{Z}$:

$$F_{\hat{Z}}\left(Y^{A}\right)=\left(1-P_{H_i}\left(v_i^{A}\right)\right)\cdot\left(1-P_{Hc}\left(v_c^{A}\right)\right)\cdot\left(1-P_{H_a}\left(v_a^{A}\right)\right)\cdot\left(1-P_{H_u}\left(v_u^{A}\right)\right). \tag{49}$$

Отже, отримані функціональні залежності дозволяють описати множину допустимих значень показника якості системи функціональної безпеки.

Семантичні аспекти методу описують компоненти вектора $V_{\langle n_1\rangle}$ як показники результативності СФБ, що є кількісними характеристиками тільки кількісних результатів системи. Зазначимо, що така інтерпретація допустима тільки за умови дотримання якісних характеристик складових результативності СФБ.

Враховуючи особливості опису показників якості СФБ, а саме складових вектора, фізичним сенсом яких є час, упродовж якого властивості ІнР не будуть порушені, більш інформативною є така форма інтегрального закону розподілу:

$$\Phi_{\hat{Y}}\left(Y\right)=P\left[\left(\hat{v}_i>v_i\right)\wedge\left(\hat{v}_c>v_c\right)\wedge\left(\hat{v}_a>v_a\right)\wedge\left(\hat{v}_u>v_u\right)\right]. \tag{50}$$

Проведені в попередніх розділах дослідження дозволили сформувати аналітичні залежності для визначення імовірності порушення властивостей ІнР, що дозволяє розкрити залежність (50), а саме:

$$\begin{aligned}\Phi_{\hat{Y}}\left(Y\right)=&\left(\begin{array}{l}1-P_{вх}+\left(1-P_{вх}\right)P_{н}\left(v_i\right)\times\\ \times P_{нв}\left(1-\prod_{j=1}^{J}\left(1-P_j^{i}\left(v_i\right)\right)\right)\end{array}\right)^{N}\times\\ &\times\left(1-\left(\prod_{k=1}^{m}\left(1-P_{д}^{k}\cdot P_{кнсд}^{k}\cdot P_{дост}^{k}\cdot P_{нд}^{k}\cdot P_{нв}^{k}\cdot P_{н}\left(v_c\right)\left(1-\prod_{j=1}^{J}\left(1-P_j^{c}\left(v_c\right)\right)\right)\right)\right)^{N}\right)\times\\ &\times\left(1-\left(\prod_{k=1}^{m}\left(1-P_{д}^{k}\cdot P_{кнсд}^{k}\cdot P_{дост}^{k}\cdot P_{нд}^{k}\cdot P_{нв}^{k}\cdot P_{н}\left(v_a\right)\left(1-\prod_{j=1}^{J}\left(1-P_j^{a}\left(v_a\right)\right)\right)\right)\right)^{N}\right)\times\\ &\times\left(1-\left(\begin{array}{l}1-P_{н}\left(v_u\right)\cdot P_{нв}\cdot P_{р}\cdot\left(1-\left(1-P_i\right)\cdot\left(1-P_c\right)\right)\times\\ \times\prod_{m=1}^{M}P_m^{ia}\cdot P_{дк}\cdot\left(1-\prod_{j=1}^{J}\left(1-P_j^{цкзз}\left(v_u\right)\right)\right)\end{array}\right)^{N}\right)\end{aligned}. \tag{51}$$

Вищезазначене дозволяє сформувати за формулою повної імовірності ймовірність досягнення мети СФБ, як:

$$P_{ДМ}=P\left(\hat{Y}\in\left\{\hat{Y}^{A}\right\}\right)=\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}\Phi_{\hat{Y}}\left(Z\right)dF_{\hat{Z}}\left(Z\right). \tag{52}$$

У шостому розділі вперше сформовано технологію забезпечення функціональної безпеки ІС на стадії модернізації, структура якої наведена на рис. 14.

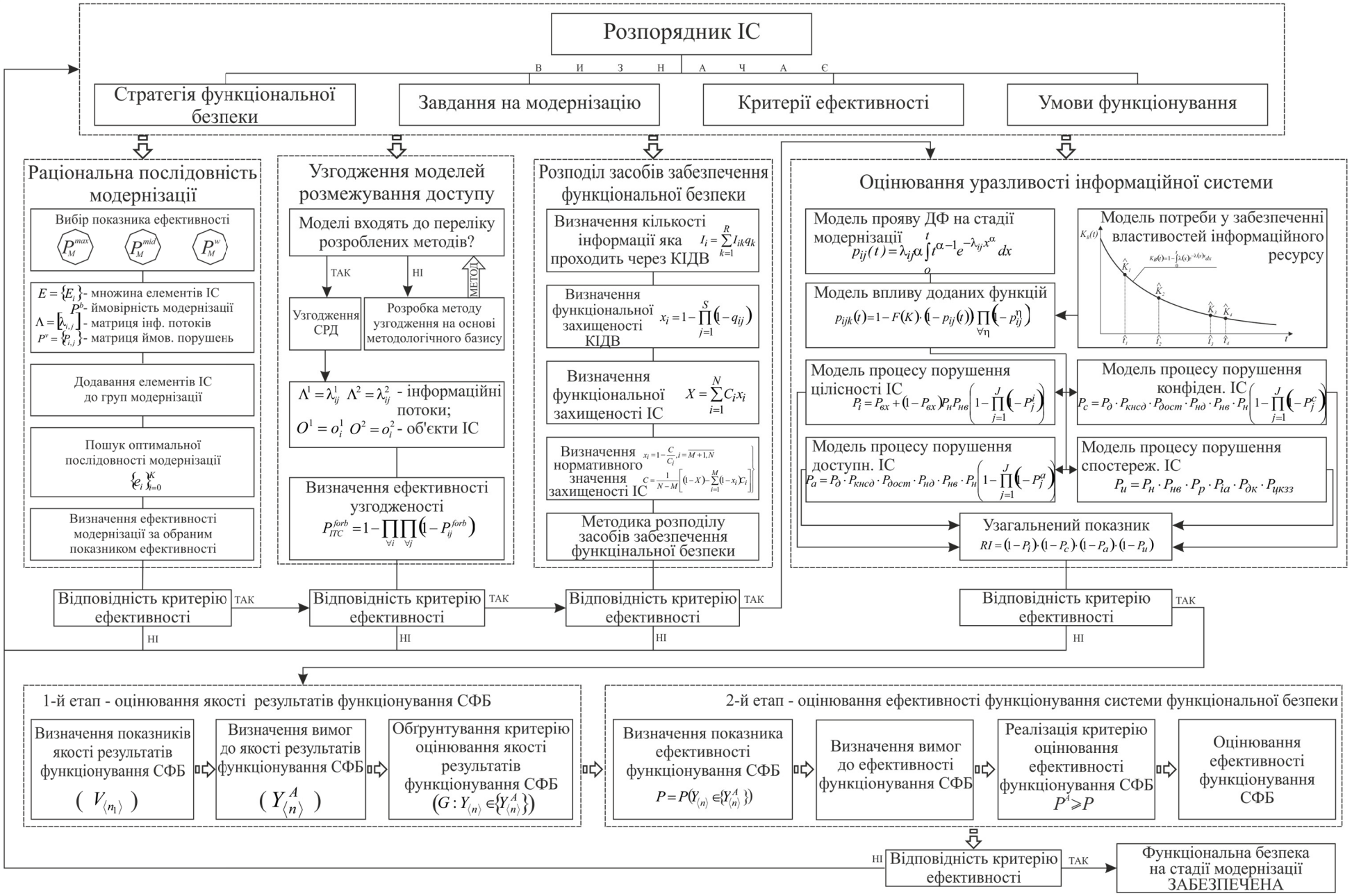


Рис. 14. Інформаційна технологія забезпечення функціональної безпеки ІС на стадії модернізації

Першим етапом технології забезпечення функціональної безпеки ІС на стадії модернізації є визначення розпорядником системи базових засад, а саме: стратегії функціональної безпеки; завдання на модернізацію конкретних ІС; критеріїв ефективності щодо кожної складової узгодження; умов функціонування модернізованих ІС.

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. Відповідно до розробленого методу визначається раціональна послідовність модернізації та здійснюється оцінювання її ефективності за обраним показником.

Разом із тим здійснюється узгодження моделей розмежування доступу модернізованих ІС і проводиться оцінювання ефективності цього процесу. У разі 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 ІС.

На третьому етапі визначається вплив дестабілізаційних факторів, які викликані стадією модернізації на властивості ІС. Моделювання зазначених процесів дозволяє провести оцінювання уразливості ІС, викликаних стадією модернізації. У разі відповідності узагальненого показника, визначеного розпорядником ІС, критерію здійснюється перехід до четвертого етапу технології – оцінювання ефективності СФБ.

На четверному етапі здійснюються оцінювання ефективності функціонування СФБ. Результатом зазначеного 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.

У межах технології проведено визначення раціональної послідовності модернізації елементів експериментального зразка програмно-технічного комплексу автоматизації прикордонної служби (ПТК АПС) "Гарт-3/П", структура якого наведена на рис. 15. Результат роботи методики показав, що раціональна послідовність модернізації така $\{e_4, e_0, e_3, e_5, e_2, e_1\}$, при якій максимальна ймовірність порушення властивостей ІС становить 0,052. На рис. 16 зображена динаміка зміни поточного значення ймовірності упродовж терміну модернізації при різних послідовностях модернізації, аналіз якої показав, що, незважаючи на загальне достатньо низьке значення ймовірності, пікові значення можуть бути достатньо високими. Крім того, при середньому значенні ймовірності меншим за визначене, максимальне значення є більшим за оптимальну послідовність. Отже, відповідно до обраних стратегії модернізації та режиму роботи ІС визначено раціональні послідовності модернізації елементів системи.

Рис. 15. Структура експериментального ПТК АПС "Гарт-3/П"

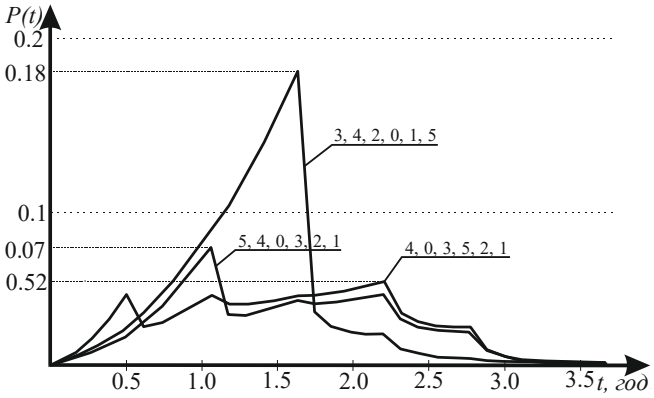


Рис. 16. Динаміка зміни поточного значення ймовірності при різних послідовностях модернізації

Практична реалізація завдання узгодження вимагає адаптації теоретичних положень до реалізації конкретних систем. З цією метою розглянемо розподіл засобів забезпечення функціональної безпеки під час 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 (рис. 17) та власного досвіду виявляють множину каналів інформаційних дестабілізаційних впливів.

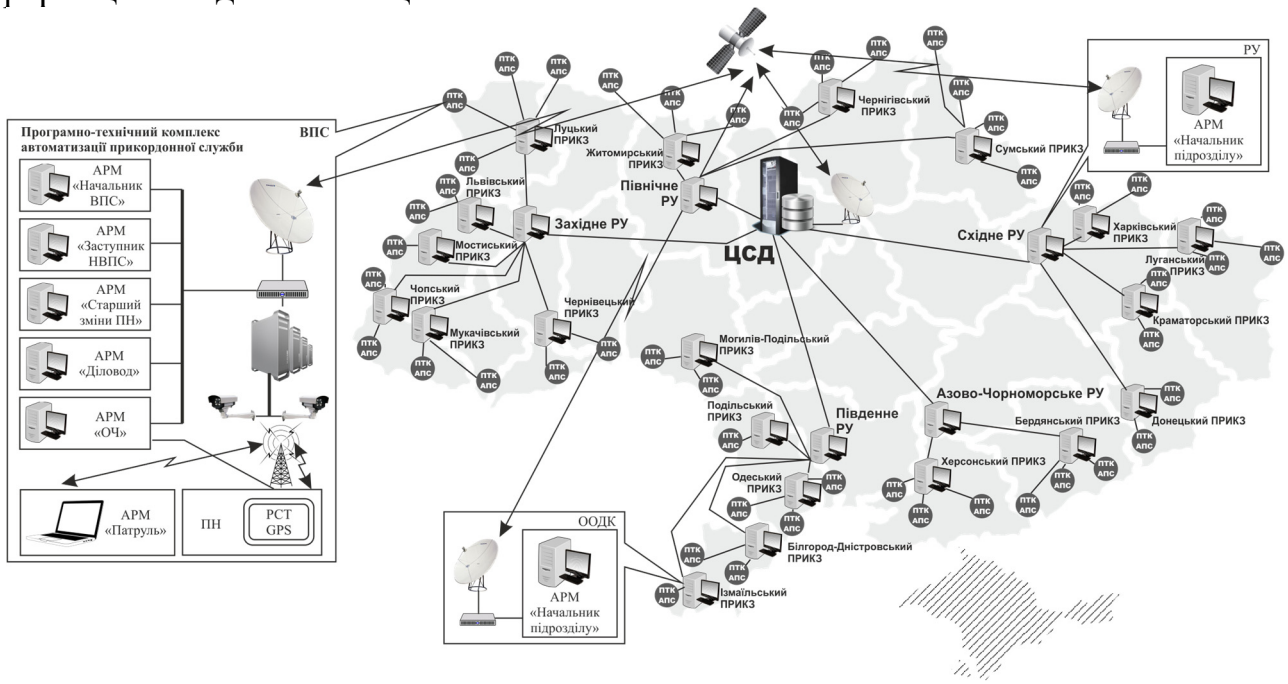
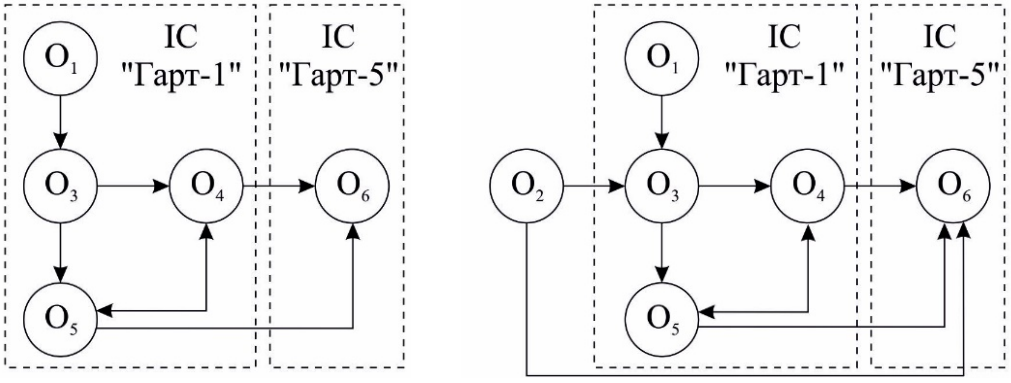


Рис. 17. Узагальнена схема розгортання ІС "Гарт-3"

Під час модернізації ІС "Гарт-3" ДПСУ прийнято рішення щодо розгортання додаткових двох ВПС на ділянці Білгород-Дністровського прикордонного загону із встановленням на них ПТК АПС "Гарт-3/П" та інтеграції в ІС "Гарт-3". Розробнику системи в технічному завданні на модернізацію вказано, що рівень функціональної безпеки системи в цілому повинен бути не менше 0,95. У роботі проведені розрахунки щодо розподілу КІДВ. Загалом кількість КІДВ після модернізації становить 113, разом із тим, модернізованими є елементи, додані ПТК АПС на двох ВПС і канали зв'язку. Отже, кількість модернізованих КІДВ становить 4 одиниці з рівнем захищеності $x_i = 0{,}95$.

У розділі проведено оцінювання ефективності узгодження систем розмежування доступу на прикладі взаємодії двох ІС у складі інтегрованої інформаційної системи "Гарт-1" та "Гарт-5". Для дослідження було розгорнуто дві експериментальних ІС з реалізацією їх взаємодії та обрано окремі елементи, які підлягали модернізації (рис. 18).

Результати розрахунків показали, що ефективність спільного функціонування обох версій СРД для одного елемента даних становитиме 0,9999883. В експериментальних зразках ІС вхідний потік передбачався 20 осіб на годину та часом модернізації систем 20 хв. Отже, імовірність порушення властивостей хоча б одного елемента даних становитиме 0,00024.



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

Рис. 18. Інформаційні потоки ІС "Гарт-1" та "Гарт-5"

Завершальним етапом технології є оцінювання ефективності функціональної безпеки в інформаційних системах на стадії модернізації. У якості зразка дослідження був обраний ПТК АПС. За результатами експертного оцінювання сформовані функції розподілу для ІДФ щодо складових ІнР, основу яких складало статистичне спостереження на експериментальному ПТК АПС "Гарт-3/П". Обчислення значень ефективності здійснено за допомогою ЕОМ. Аналіз результатів визначення ймовірності порушення властивостей ІнР за умови дотримання їх значень у допустимих межах проведемо поетапно за кожною із властивостей ІнР.

З метою порівняння значень імовірностей у різних умовах для якісного оцінювання ступеня впливу наведемо графік різниці двох імовірностей. Позитивне значення свідчить про перевагу першого параметра, негативне – другого (рис. 19).

Аналіз різниці ймовірностей порушення властивостей ІнР за параметрами цілісності та конфіденційності показав, що на початку модернізації більший вплив на $P_{ДМ}$ має показник цілісності, разом із тим, у разі збільшення нормативного часу кожного із них характерна різка зміна ступеня впливу конфіденційності (стрибок площини в межах 8 год модернізації). Така зміна властива незалежно від нормативного значення цілісності. Аналогічний аналіз за іншими властивостям, а саме цілісності та спостереженості показав аналогічну тенденцію (рис. 20). Варто зазначити певне зростання впливу цілісності на значення $P_{ДМ}$ порівняно з параметром конфіденційності.

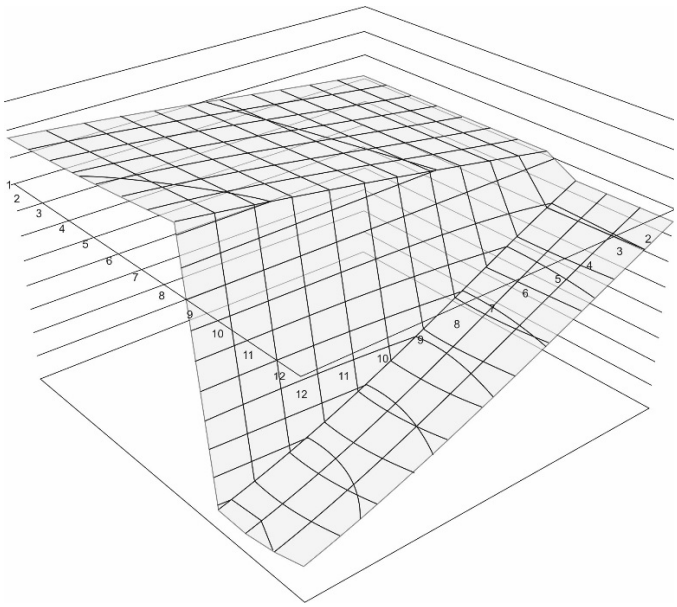


Рис. 19. Різниця імовірностей порушення властивостей ІнР за параметрами цілісності та конфіденційності

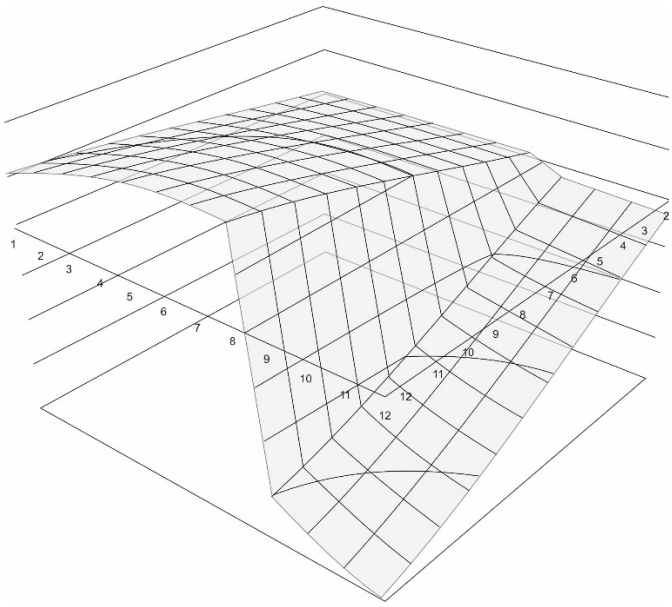


Рис. 20. Різниця імовірностей порушення властивостей ІнР за параметрами цілісності та доступності

Отже, аналіз впливу нормативних значень властивостей ІнР під час дослідження імовірності порушення властивостей ІнР 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 інформації.

Разом із тим, аналіз динаміки впливу окремих властивостей на результуючу функцію показав наявність стрибка зміни впливу окремих параметрів, при чому для різних параметрів в межах одного і того ж значення. Вищенаведене дозволить визначити спільне для всіх нормативних параметрів значення, за яких їх вплив на загальну ймовірність порушення властивостей ІнР буде однаковий.

ВИСНОВКИ

Результатом виконаної роботи є вирішення актуальної і важливої науково-прикладної 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.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ 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.

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. – Національний авіаційний університет, м. Київ, 2018.

В дисертаційній роботі вирішувалась науково-прикладна проблема забезпечення функціональної безпеки відомчої інтегрованої інформаційної системи на стадії модернізації. Сформована загальна концепція забезпечення функціональної безпеки на стадії модернізації, як інструментально-методологічна база, яка забезпечує виконання розглянутих стратегій.

Розроблена математична модель інформаційних потоків ІС на стадії модернізації та метод визначення раціональної послідовності модернізації елементів інформаційних систем. Розроблені моделі каналу інформаційного дестабілізуючого впливу і функціональної захищеності інформаційної системи та метод розподілу засобів забезпечення функціональної безпеки інформаційних систем на стадії модернізації. Сформований метод оцінювання уразливості ІС в інтегрованій інформаційній системі на стадії модернізації на базі розроблених аналітичних моделей порушення властивостей ІС. Розроблений комплекс методів узгодження систем розмежування доступу в інформаційних системах на стадії модернізації. Зазначена сукупність методів дозволила сформувати методологічний базис узгодження моделей розмежування доступу інформаційних систем на стадії модернізації. В рамках методів сформульовані та доказані базові теореми безпеки.

Розроблена модель інформаційних дестабілізуючих факторів на стадії модернізації і метод оцінювання ефективності забезпечення функціональної безпеки інформаційних систем на стадії модернізації та інформаційна технологія забезпечення функціональної безпеки інтегрованої інформаційної системи на стадії модернізації.

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

АННОТАЦИЯ

Стрельбицкий М.А. Технология обеспечения функциональной безопасности интегрированной информационной системы Госпогранслужбы на стадии модернизации – Квалификационный научный труд на правах рукописи.

Диссертация на соискание ученой степени доктора технических наук по специальности 05.13.06 – информационные технологии. – Национальный авиационный университет, г. Киев, 2018.

В диссертационной работе решалась научно-прикладная проблема обеспечения функциональной безопасности ведомственной интегрированной информационной системы на стадии модернизации.

Анализ существующих подходов к проблеме обеспечения функциональной безопасности информационных систем показал наличие циклического процесса ее совершенствования, требующей структурированного анализа и декомпозиции

факторов, влияющих на соблюдение свойств информационных систем на стадии модернизации.

Сформирована общая концепция обеспечения функциональной безопасности на стадии модернизации, как инструментально-методологическая база, обеспечивающая выполнение рассмотренных стратегий. Концепцией предусмотрено три задачи согласования совместного функционирования: специального программного обеспечения, программных и технических (аппаратных) средств обеспечения функциональной безопасности, а также определения величины уязвимости ИС при проведении мероприятий по модернизации и оценки эффективности системы обеспечения функциональной безопасности ИС на стадии модернизации. Результатом является получение оценки эффективности проведенных мероприятий используемой владельцем системы для принятия решения о проведении модернизации и определения организационных мероприятий по особенностям проведения самого процесса обновления составляющих ИС.

Разработана математическая модель информационных потоков ИС на стадии модернизации и метод определения рациональной последовательности модернизации элементов информационных систем, что позволило рационализировать процесс модернизации элементов информационных систем произвольной структуры с выбранной стратегией модернизации.

Разработаны модели канала информационного дестабилизирующего влияния и функциональной защищенности информационной системы и метод распределения средств обеспечения функциональной безопасности информационных систем на стадии модернизации, что позволило обеспечить нормативный уровень функциональной безопасности системы в целом.

Разработан метод оценки уязвимости ИС в интегрированной информационной системе на стадии модернизации на базе аналитических моделей нарушения свойств ИС, что позволило определить интегральную величину уязвимости ИС. Отличие приведенных моделей от существующих состоит в учете дестабилизирующих факторов, вызванных стадией модернизации и определении вероятности потребности в обеспечении соблюдения свойств информационного ресурса информационных систем, основанная на функции распределения Гомперца-Мейкгама.

Разработан комплекс методов согласования систем разграничения доступа в информационных системах на стадии модернизации, а именно: метод согласования решеток уровней конфиденциальности систем мандатного разграничения доступа, метод согласования матриц доступа систем дискреционного разграничения доступа, метод согласования систем ролевого разграничения доступа. Указанная совокупность методов позволила сформировать методологический базис согласования моделей разграничения доступа информационных систем на стадии модернизации. В рамках методов сформулированы и доказаны базовые теоремы безопасности. Разработан методологический базис и методы согласования систем разграничения доступа, позволяющие обеспечить функциональную безопасность информационных систем в рамках систем разграничения доступа.

Разработана модель информационных дестабилизирующих факторов на стадии модернизации и метод оценки эффективности обеспечения функциональной безопасности информационных систем на стадии модернизации, что позволило

определить вероятность выполнения системой функциональных задач в условиях влияния как внешних, так и внутренних дестабилизирующих факторов. Отличие разработанного метода заключается в двухэтапном формировании перечня информационных дестабилизирующих воздействий по определению степени их реализации.

Впервые разработана информационная технология обеспечения функциональной безопасности интегрированной информационной системы на стадии модернизации, что позволит осуществлять поэтапное совершенствование информационных систем реального времени критического применения.

Ключевые слова: информационная система, технология, модернизация, эффективность, разграничение доступа, функциональная безопасность.

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 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. 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 mathematical model of information streams and method for determining the rational sequence of modernization of elements of information systems were developed.

A 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.

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.

A set of methods for reconciling access systems in information systems at the stage of modernization has been developed. 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 model of information destabilizing influence and method for assessing the effectiveness of providing functional security of information systems at the stage of modernization have been further developed.

The information technology for ensuring the functional security of integrated information systems at the stage of modernization was developed.

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