НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

На правах рукопису

Хохлачова Юлія Євгеніївна

УДК 004.056.53

МЕТОДИ ОЦІНЮВАННЯ УРАЗЛИВОСТЕЙ ТА ОПТИМІЗАЦІЇ ІНФОРМАЦІЙНИХ СИСТЕМ В УМОВАХ ІНФОРМАЦІЙНИХ ВПЛИВІВ

05.13.21 – системи захисту інформації

Дисертація на здобуття наукового ступеня
кандидата технічних наук

Науковий керівник:
Хорошко Володимир Олексійович
доктор технічних наук, професор

Київ – 2015

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

АС	автоматизована система
ЕОМ	електронно-обчислювальна машина
ЕОТ	електронно-обчислювальна техніка
ЗІ	захист інформації
ЗМІ	засоби масової інформації
ЗОТ	засоби обчислювальної техніки
ЗП	запам’ятовуючий пристрій
ІБ	інформаційна безпека
ІзОД	інформація з обмеженим доступом
ІС	інформаційна система
ІТС	інформаційно-телекомунікаційна система
КСЗІ	комплексна система захисту інформації
ОС	операційна система
ОТ	обчислювальна техніка
ПЗ	програмне забезпечення
ПЦС	пульт центрального спостереження
ПЗЗУ	пам’ять на зовнішніх запам’ятовуючих пристроях
РЕБ	радіоелектронна боротьба
РКД	рольове керування доступом
СУБД	системи управління базами даних
СБ	система безпеки
СЗІ	система захситу інформації
СОТ	системи обчислювальної техніки
СПТВ	спеціальний програмно-технічний вплив

ТСЗІ технічна система захисту інформації

ВСТУП

Актуальність. Розвиток сучасних інформаційних і комунікаційних технологій впливає на усі на сфери людської життєдіяльності, підвищуючи їх ефективність і, одночасно, породжуючи множину неконтрольованих загроз, у тому числі і в інформаційній сфері. З огляду на це, постійно підвищуються вимоги щодо захисту критично важливих інформаційних ресурсів. На сьогодні ключовими і визначальними міжнародними нормативно-правовими актами у галузі управління інформаційною безпекою (ІБ) і захисту інформації є серія стандартів ISO 27k. Згідно останньої основними процедурами для організації ефективної системи менеджменту ІБ є управління ресурсами, комунікаціями та операціями, ризиками, безперервністю роботи, інцидентами ІБ тощо. Менеджмент інцидентів, згідно міжнародного стандарту ISO/IEC 27035:2011, дозволяє своєчасно та ефективно виявляти, аналізувати й розслідувати інциденти ІБ для мінімізації негативних наслідків для інформаційних систем (ІС) і організацій взагалі. Крім зазначеного міжнародного стандарту, сьогодні є багато галузевих нормативних документів, а також практичних рекомендацій та керівництв, що базуються на кращих світових практиках щодо інцидент-менеджменту. Згідно цих документів виконання процедури управління інцидентами покладається на спеціалізовані групи швидкого реагування, які, відповідно до своїх організаційних і функціональних особливостей, надають своїм клієнтам певні сервіси. Серед базових сервісів варто виділити ідентифікацію та аналіз інцидентів, реагування на інциденти та їх розслідування, аналіз уразливостей ІС, а також випробування їх стійкості шляхом моделювання атак і впливів. З огляду на те, що успішність реалізації інформаційного впливу на систему залежить від її уразливостей і в гіршому випадку перетворюється на інцидент, дослідження поведінки системи (оптимізації її ключових параметрів та показників захищеності) під дією інформаційних

впливів з точки зору захисту інформації є актуальним напрямком наукових досліджень.

Значний внесок у розвиток теорії і практики у цьому напрямку внесли такі вітчизняні і закордонні вчені як Баранов В.Л., Браіловський М.М., Гордон Л.А., Грищук Р.В., Дудикевич В.Б., Кобозєва А.А., Козловський В.В., Корченко О.Г., Лоеб М.П., Пархуць Л.Т., Самохвалов Ю.Я., Скурихін В.І., Стасюк О.І., Хорошко В.О., Юдін О.К. та ін.

Однак, у зазначеній галузі залишається низка завдань, вирішення яких має важливе наукове та практичне значення. З цих позицій, побудова і дослідження методів моделювання впливів на ІС, оцінювання уразливостей та оптимізація показників систем захисту в умовах впливів, є *актуальним науковим завданням.*

Зв'язок роботи з науковими програмами, планами, темами. Одержані результати дисертаційної роботи відображені у звітах держбюджетних науково-дослідних робіт Національного авіаційного університету («Організація систем захисту інформації від кібератак», № 0111U000171), Кіровоградського національного технічного університету («Розробка методів підвищення оперативності передачі та захисту інформації у телекомунікаційних системах», № 0113U003086) та Державного університету інформаційно-комунікаційних технологій («Безпека – 01П», що виконувалась відповідно до постанови КМУ №01086 від 25.12.2005).

Мета і задачі дослідження. Метою дисертаційної роботи є розробка методів оцінювання уразливостей та оптимізації інформаційних систем в умовах інформаційних впливів.

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

– проаналізувати існуючі методи і засоби оцінки уразливостей інформаційних систем для виявлення їх недоліків, а також провести аналіз сучасних методів моделювання впливів на інформаційні системи для їх подальшого використання в процесах оптимізації параметрів цих систем;

– розробити метод знаходження оптимальної конфігурації інформаційної системи на базі теорії графів;

– запропонувати систему правил щодо моделювання критеріїв оптимальності та обмеження загроз інформації для їх використання з метою оптимізації параметрів інформаційних систем в умовах інформаційних впливів;

– розробити метод оптимізації інформаційних систем на основі диференціальних ігор для визначення у реальному часі оптимальної стратегії поведінки сторони захисту в умовах інформаційних впливів;

– розробити метод оптимізації систем захисту інформації з метою визначення оптимальної поведінки у системі «вплив-безпека» і підвищення рівня захищеності інформації в інформаційній системі;

– розробити алгоритми та програмне забезпечення для реалізації розроблених методів і проведення експериментального дослідження з метою верифікації отриманих у роботі результатів.

Об'єктом дослідження є процеси оцінювання уразливостей та моделювання інформаційних впливів на інформаційні системи.

Предметом дослідження є моделі та методи моделювання впливів на інформаційні системи та оцінювання їх уразливостей.

Методи дослідження. Проведені у дисертаційній роботі дослідження базуються на методах теорії ймовірності (розробка та дослідження методики оцінювання уразливостей та розрахунки кількісних показників рівня ІБ), теорії диференціальних ігор (розробка методів оптимізації систем захисту інформації та параметрів ІС в умовах впливів), теорії графів (розробка методу знаходження оптимальної конфігурації ІС), моделювання інформаційних процесів та структур (дослідження антагоністичних відносин у системі «інформаційний вплив – система безпеки») та ін.

Наукова новизна одержаних результатів полягає в наступному:

– *вперше* запропоновано диференціально-ігровий метод оптимізації параметрів інформаційних систем, що, за рахунок врахування стратегії

гравця впливу, критерію оптимізації ресурсів гравців у процесі оптимізації і енергетичної складової у заданий період часу, дозволяє визначати у реальному часі оптимальну стратегію безпеки інформації в інформаційних системах;

– *вперше* запропонована система правил щодо моделювання визначених критеріїв оптимальності для систем захисту інформації, яка, за рахунок синтезу морфологічним методом сепарабельних адитивних критеріїв та обмежень, дозволяє розв'язувати задачі аналізу, синтезу та оптимізації систем за обраними критеріями та виділеними обмеженнями, а також оцінювати рівень захищеності інформаційних систем з урахуванням дозволених границь гарантованого рівня захисту інформації;

– *отримав* подальший розвиток метод оптимізації систем захисту інформації, що, за рахунок врахування параметрів системи безпеки (кількість засобів безпеки, тип підсистеми безпеки, сумарний ресурс безпеки та цінність інформації), дозволяє визначати оптимальну поведінку в системі «вплив-безпека»;

– *удосконалено* метод знаходження оптимальної конфігурації інформаційної системи, який, за рахунок використання теоретико-графового моделювання зворотного ходу побудови оптимального вихідного дерева, дозволяє визначати оптимальну архітектуру інформаційної системи в умовах інформаційних впливів.

Практичне значення одержаних результатів

Отримані в дисертаційній роботі результати можуть бути використані для розширення інструментарію груп швидкого реагування на інциденти ІБ, підрозділів ІБ організацій, оцінювання уразливостей ІС, а також для підвищення ефективності розробки методів і систем захисту інформації. Практична цінність роботи полягає у такому:

– використання запропонованих методів при розробці спеціального програмного забезпечення дозволило підвищити захищеність інформаційних ресурсів, що підтверджується актом впровадження у діяльність військової

частини К-1410 (акт від 14.06.2012 р.) та ТОВ «Конзьюмер Експрес» (акт від 17.11.2014 р.);

– розроблена комп'ютерна програма, яка використовується для моделювання атакуючих дій і оцінки уразливостей в ІКС та у навчальному процесі підготовки фахівців у галузі ІБ. Практичне використання результатів дисертаційного дослідження підтверджується актами впровадження у навчальний процес Національного авіаційного університету (акт від 10.02.2015 р.), Державного університету інформаційно-комунікаційних технологій (акт від 26.06.2012 р.) та Кіровоградського національного технічного університету (акт від 17.09.2014 р.);

– запропоновано методику оцінки уразливостей та інформаційних впливів, які, за рахунок використання логіко-ймовірнісних пар зв'язок «параметри → уразливості», дозволяють ідентифікувати уразливості інформаційних систем в умовах впливів;

– розроблено методику проведення експерименту, що дозволила дослідити запропоновані у роботі методи.

Особистий внесок здобувача. Основні положення і результати дисертаційної роботи, що виносяться до захисту, отримані автором самостійно. У роботах, написаних у співавторстві, автору належать: [1] – дослідження існуючих методів теорії диференціальних ігор та визначення оптимальних стратегій; [2, 22, 23] – розробка моделі ІБ, на базі якої можна вибрати систему контрзаходів, що зменшують ризики з найбільшою ціновою ефективністю; [3, 20] – дослідження та аналіз функціональних особливостей систем управління інцидентами ІБ; [5, 13, 14, 16] – аналіз та дослідження існуючих методів і засобів оцінки уразливостей ІС та сучасних методів моделювання впливів на ІС; [6, 9, 21] – розробка методики оцінки захищеності ІС на основі застосування принципів системотехніки; [11] – розробка методики оцінки рівня захищеності системи зв'язку; [12] – аналіз та дослідження існуючих методик оцінювання рівня безпеки; [15] – розробка алгоритму визначення показників для оцінки надійності систем спеціального

призначення; [17] – розробка та дослідження методик оцінки уразливостей та інформаційних впливів; [18, 19] – удосконалення методу знаходження оптимальної конфігурації інформаційної системи; [21, 30] – розробка методу оптимізації параметрів ІС.

Апробація результатів дисертації. Основні положення дисертаційної роботи доповідалися та обговорювалися на наукових конференціях та семінарах, серед яких: НПК «Захист інформації з обмеженим доступом та автоматизація її обробки» (Київ 2010 р.); X міжнародна НТК «АВІА-2011» (Київ 2011 р.); IX міжнародна НПК «ПОЛІТ-2011» (Київ 2011 р.); IV міжнародна НПК «Інтегровані інтелектуальні робототехнічні комплекси (ІІРТК-2011)» (Київ 2011 р.); II НТК «Безпека інформаційних технологій («Information Technology Security», ITSEC-2012)» (Київ 2012 р.); НТК «Захист інформації і безпека інформаційних систем» (Львів 2013 р., 2014 р.); XVI міжнародна НПК «Безопасность информации в информационно-телекоммуникационных системах» (Київ 2013 р.); НПК «Інформаційні управляючі системи та технології» (Одеса 2013 р., 2014 р.); VI міжнародна НПК «Проблеми і перспективи розвитку ІТ-індустрії» (Харків 2014 р.); XV міжнародна НПК «Современные информационные и электронные технологии (СИЭТ-2014)» (Одеса 2014 р.); IV міжнародна НПК «Фізико-технологічні проблеми радіотехнічних пристроїв, засобів телекомунікацій, нано- та мікроелектроніки» (Чернівці 2014 р.), НПК «Актуальні питання забезпечення кібернетичної безпеки та захисту інформації» (Київ 2015 р.).

Публікації. Основні положення дисертації опубліковано у 29 наукових працях, у тому числі 20 статей у наукових журналах та збірниках наукових праць, які входять до переліку фахових наукових видань МОН України (серед них 4 статті у виданнях, що входять до міжнародних наукометричних баз даних), а також 9 тез доповідей і матеріалів конференцій.

РОЗДІЛ 1. СУЧАСНІ ПІДХОДИ ДО ОЦІНКИ УРАЗЛИВОСТЕЙ ТА МОДЕЛЮВАННЯ ВПЛИВІВ НА ІНФОРМАЦІЙНІ СИСТЕМИ

1.1. Поняття та види впливів на ІС

Досліджуючи проблему інформаційних впливів проаналізуємо класифікацію вхідних даних, виходячи з класифікації алгоритмів їх обробки (див. рис. 1.1).

Вся множина алгоритмів, які в принципі здатна виконувати ІС, умовно можна розбити на наступні класи:

1. Алгоритми, що реалізують способи інформаційного захисту. Ними можуть бути алгоритми, відповідальні за:

а) обробку помилок;

б) блокування вхідних даних, куди може входити: установка захисних екранів, видалення (знищення) джерела небезпечної інформації;

в) верифікація виконуваного коду або «психоаналіз», як виявлення прихованих програм і(або) причин їх виникнення.

2. Алгоритми, відповідальні за самомодифікацію, за зміну тих, що існують і генерацію додаткових програм, призначених для обробки вхідних послідовностей.

3. Алгоритми, здатні порушити звичний режим функціонування, тобто здійснити виведення системи за межі допустимого стану, що в більшості випадків рівносильне спричиненню збитку аж до знищення. У цей клас разом з алгоритмами, виконання яких системою заподіє їй же самій шкоду, входять так звані «несертифіковані», тобто ті, що не пройшли якісного тестування алгоритми (програми). Подібні програми постійно з'являються в складних

самонавчальних системах, в яких можливе виконання алгоритмів другого класу.

4. Решта всіх алгоритмів.

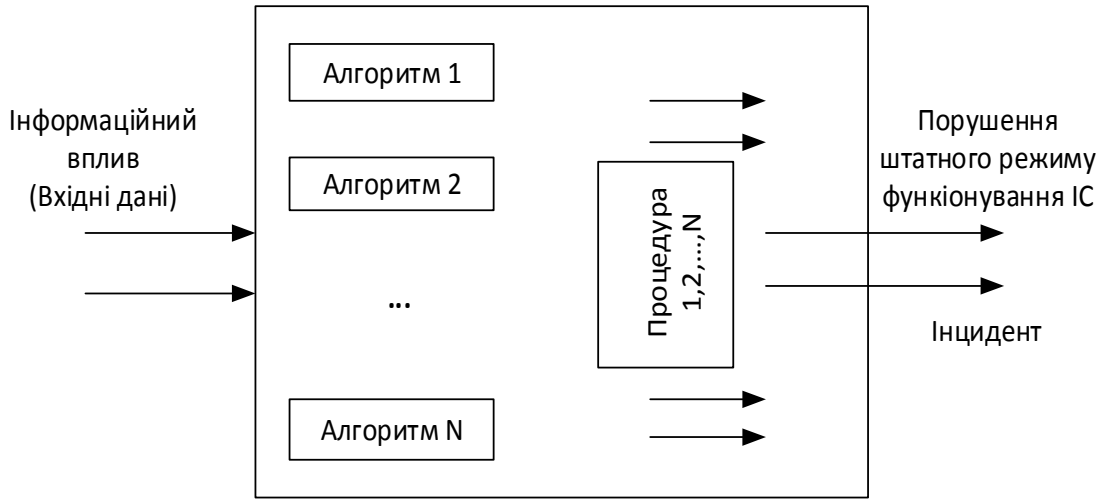


Рис.1.1. Множина алгоритмів, які здатна виконувати ІС

Тепер можна перейти до визначення мети і причин інформаційних впливів.

Метою інформаційного впливу є активізація алгоритмів, відповідальних за порушення звичного режиму функціонування, тобто за виведення ІС за межі допустимого стану.

Джерело впливу може бути як зовнішнім по відношенню до системи, так і внутрішнім (див. рис. 1.2).

Причини зовнішніх впливів у разі цілеспрямованої інформаційної дії (у разі інформаційної війни) приховані в боротьбі конкуруючих ІС за загальні ресурси, що забезпечують системі допустимий режим для існування.

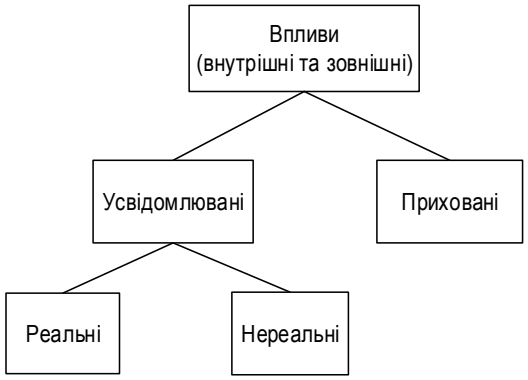
Причини внутрішніх впливів зобов'язані своїм існуванням появі усередині системи множини елементів, підструктур, для яких звичний режим функціонування став з огляду на ряд обставин неприпустимим.

Тут і далі під допустимим режимом функціонування розуміється таке функціонування ІС, яке, з погляду даної системи, забезпечене необхідними матеріальними ресурсами. Відповідно, неприпустимим режимом будемо

називати режим, знаходячись в якому система не забезпечена повною мірою необхідними для нормального функціонування матеріальними ресурсами.

Таким чином, інформаційний вплив є вхідними даними, призначеними для активізації в ІС алгоритмів, відповідальних за порушення штатного режиму функціонування.

Проведемо класифікацію впливів. Зовнішні і внутрішні впливи поділяються на усвідомлювальні системою (явні) і не усвідомлювальні (приховані) (див. рис. 1.2).



Р

ис. 1.2. Класифікація впливів

Явний вплив, як правило, направлений на порушення штатного режиму функціонування системи. Крім того, явний вплив може бути реальним, а може бути нереальним. Проте, незалежно від того, як система сприймає вплив (або реальність), важливо, що якщо ІС здатна сприймати вхідні дані як вплив, то цей факт однозначно говорить про те, що даний вплив є явним.

Етапи обробки явного впливу.

1. Система приймає вхідні дані.

2. Система оцінює вхідні дані. Вхідні дані є впливом? Якщо так, то перехід до п.3, інакше до п.1.

3. Система оцінює реальність впливу. Якщо вплив реальний, то перехід до п.4, інакше повернення до п.1.

4. Система оцінює свої можливості по організації захисту і величину власного збитку у разі програшу. Якщо втрати у разі організації захисту оцінені меншою величиною (моральний, матеріальний збиток тощо), чим збиток від приведеного в дію впливу, то перехід до п.5, інакше до п.7.

5. Активізація алгоритмів, що реалізують способи інформаційного захисту. Якщо цього недостатньо, то активізація алгоритмів, відповідальних за пошук нових, нестандартних способів вирішення задачі.

6. Система оцінює результати інформаційного протиборства. У разі успіху перехід до п.1, інакше до п.7.

7. Виконання дій, відповідно до вимог інформаційного агресора. Якщо система залишається «функціонуючою», то перехід до п.1, отже, до тих пір, поки система «функціонує».

Як було показано вище, явний вплив залишає системі шанс, дозволяє робити ходи у відповідь та припускає, що за ним прослідують певні дії, які завдають інформаційній системі збитку. Прихований вплив тому і називається прихованим, що він не фіксується системою захисту інформації об'єкту в режимі реального часу та не надає шансу.

Виходячи з аналізу впливів для захисту від агресора доцільно виконати наступні операції:

- поставити бар'єр між собою і джерелом небезпеки;
- сховатися від небезпеки за недосяжні межі;
- знищити джерело небезпеки;
- сховатися або видозмінитися до невпізнання, стати іншим.

В даний час різним аспектам інформаційної боротьби (протиборства, дій, загрози війни) приділяється велика увага в засобах масової інформації і в наукових виданнях. Проведений аналіз дозволяє зробити висновок, що при спільності поглядів на інформаційну боротьбу існують різні підходи до визначення цілей, об'єктів дії, способів дії і засобів інформаційної боротьби [10, 36].

З погляду України джерелом інформаційних впливів, за їх походженнями і внутрішній природі можна розділити на три категорії [10, 21, 30, 50].

До *першої категорії* відносяться джерела зовнішніх впливів:

- наявність інформаційних атак із зовні;
- зацікавленість у зміні інформаційних потоків як із зовні, так і внутрішніх;
- зацікавленість в ослабленні політичної, економічної і військової ролі України в регіоні, на континенті і в світі;
- підтримка і позитивне відношення до дій дестабілізуючих сил в Україні;
- зацікавленість в інформаційних ресурсах України, у встановленні контролю над її інформаційними ресурсами.

Друга категорія складає такі джерела:

- джерела, які утворюються об'єктивними зовнішніми умовами: діють або існують за межами України і не мають прямих ознак інформаційних впливів для України;
- стійке збільшення витрат на інформаційну боротьбу;
- внутрішня соціально-політична нестабільність.

До *третьої категорії* відносяться джерела внутрішнього походження, які так або інакше, впливають на рівень інформаційної небезпеки для України:

- незадовільний стан інформаційної безпеки;
- недостатнє фінансування з державного бюджету України на потреби інформаційної безпеки;
- прояв соціально-політичної і морально-психологічної кризи у відношенні до інформаційної боротьби.

Всі ці категорії впливу більшою чи меншою мірою діють на безпеку інформації в державі, а, отже, посилюють умови інформаційної боротьби.

Процес розробки теоретичних основ інформаційної боротьби і дій ускладнений тим, що до сьогоднішнього дня не існує однозначного визначення і всіма прийнятого поняття – «інформація». Закон України «Про інформацію» [14] визначає інформацію як документовані або такі, що публічно оповістили, відомості про події і явища, що відбуваються в суспільстві, державі і навколишньому середовищі. У той же час філософське визначення поняття «інформація» звучить, як система ідеальних (суб'єктивних) образів об'єктів, процесів і явищ навколишнього світу в свідомості людини, а так само сукупність ознак, властивих матерії і формуючих ідеальних образів. Виходячи з наведених понять, можна зробити висновок, що вони не дозволяють розглядати «інформацію» як об'єкт впливу, що звужує сферу інформаційної боротьби і впливу.

Враховуючи реальне різноманіття знань про інформацію, обумовлене як складністю і різноманіттям самого об'єкту пізнання, так формами і методами його теоретичного освоєння, ми вибираємо такий аспект дослідження, що не зводиться до всіх інших, а саме - філософський.

Філософський аспект проблеми, розглядаючи суб'єктно-об'єктні відносини, дозволяє визначити інформацію як об'єкт інформаційної боротьби, виділити області, в яких вона ведеться. Такий підхід забезпечує побудову системи загальних і приватних категорій інформаційної боротьби як виду боротьби, який характеризується властивими нею об'єктами і засобами дії, способами і формами їх застосування. Урахування загальних і окремих категорій інформаційної боротьби може бути подано у вигляді наступного підходу (див. рис. 1.3).

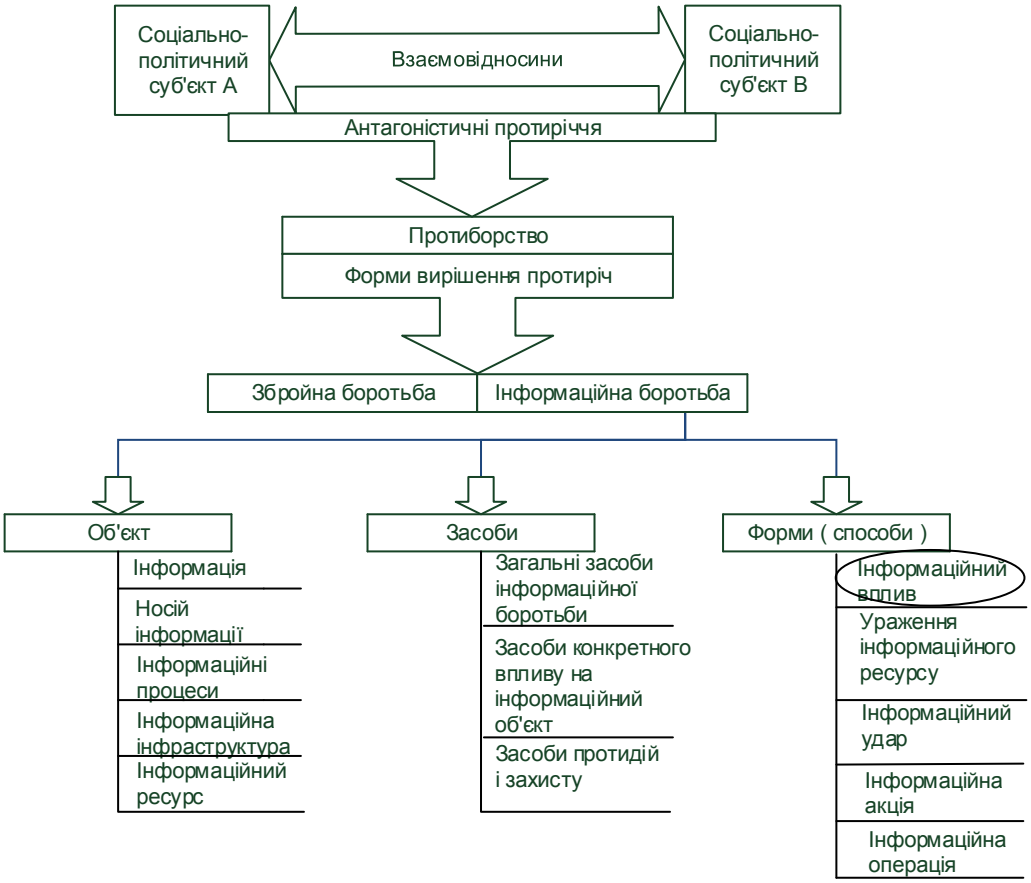


Рис. 1.3. Підхід до побудови загальних і окремих категорій інформаційної боротьби

Розглянемо суть і зміст таких основних категорій інформаційної боротьби як інформація, інформаційні процеси, інформаційний ресурс. Детально зміст інформаційного впливу як основоположній категорії інформаційної боротьби було розглянуто в [36].

Поняття «інформація» є базовим для розуміння процесів, що протікають у ході інформаційної боротьби.

Обговорення проблеми інформації в сучасній науці ведеться в різних аспектах. З єдиного об'єкту пізнання - інформація - фахівці в різних областях знань вибирають «свій» аспект, який і є для них предметом пізнання. Так, фахівець в області теорії передачі інформації основну увагу приділяє кількісним характеристикам інформації, кодуванню, впливу шумів, перешкод тощо.

Об'єкт дослідження тут один – інформація. Але оскільки інформація вивчається різними галузями науки, що мають різні предмети, то і сама інформація представляється в різному «світлі», в ракурсі предмету тієї або іншої науки.

Поняття інформації спочатку було пов'язане виключно з соціальною сферою, з комунікативною діяльністю людей. Цей висновок спирається на результат дослідження значень слова «інформація», яке вперше зародилося в латинській мові. У Російській імперії це слово вперше з'явилося в петровську епоху. Так, Н.А. Смірнов, вважає, що це слово перейшло у російську мову з польської «informacia», яка запозичила його у латинської. У той час слово інформація уживалося в сенсі «ідея, наука» [46].

Необхідно відзначити, що зараз поняття «інформація» трактується достатньо широко. Наприклад, як вид даних до сукупності знань. Проте, для того, щоб зрозуміти суть інформації, побудуємо систему понять терміну «інформація».

Таким чином, можна припустити, що «інформація» в прямому розумінні - це сукупність образів і зв'язків між ними в рамках певної системи.

На підставі цього можна сформулювати друге непряме поняття терміну «інформація», яке свідчить, що інформація є множиною ознак, властивих об'єктам, процесам і явищам матеріального світу, які формують ідеальні (суб'єктивні) образи [36].

На підставі першого і другого непрямих понять інформації сформулюємо наступне визначення. Інформація є системою ідеальних (суб'єктивних) образів, об'єктів, процесів і явищ навколишнього світу в свідомості людини, а також множини ознак, властивих матерії і які формують ідеальні образи.

Запропоноване визначення в деякій мірі пояснюють ідеалістичний і матеріалістичний підходи до поняття «інформація», яка як множина

образоутворюючих ознак є властивістю матерії і за своєю природою матеріальна, але як система ідеальних образів і зв'язків між ними - ідеальна за своїм змістом.

Саме таке розуміння інформації дозволяє нам визначити її джерела і носії, тобто виділити ті об'єкти, на які здійснюється дія в ході інформаційної війни (боротьби).

Носіями інформації є енергетичні поля, потоки заряджених частинок, а також біохімічні процеси, комплекс яких об'єднаний загальною назвою «механізм електричної збудливості».

Джерелами інформації є самі об'єкти, процеси і (або) явища, що генерують (відображають, випромінюють) коливання і хвилі, а також випускають потоки заряджених частинок, і, звичайно, центральна нервова система (мозок) людини.

Визначення суті і природи інформації дозволяє зрозуміти природу і зміст інформаційних процесів, що є носіями інформації в часі і просторі. Зупинимося в першу чергу на елементарних інформаційних процесах, таких як отримання (сприйняття), переробка, передача і зберігання (накопичення) інформації, під якою розуміють [36,]:

- отримання (сприйняття) - виокремлення розпізнаної інформації зі всієї різноманітності навколишнього світу;
- переробка - зміна інформації, відповідно до раніше визначеного алгоритму. Мета переробки інформації - отримання суб'єктивно нової інформації;
- передача - рух незмінної інформації в просторі і в часі. При передачі інформації ознаки образів можуть змінюватися із збереженням смислового змісту;
- зберігання - передача інформації не в просторі, а в часі, тобто відтворення образу (ознак) об'єкту в необхідний момент часу.

Сукупність елементарних інформаційних процесів утворюють такі їх види, як інформаційні ланцюги і інформаційні мережі.

У об'єктів природної неживої природи відображення здійснюється у вигляді віддзеркалення, а інформаційні процеси - зберігання внутрішньої різноманітності структури речовини.

Вищий рівень розвитку живих систем зумовив наявність у них усіх форм елементарних процесів: сприйняття, переробку, передачу і зберігання, а також деяких видів інформаційних процесів.

Високоорганізованій системі, якою є суспільство і сама людина, властиві всі форми і види інформаційних процесів.

В ієрархічній структурі матеріального світу техніка займає проміжне положення між неживою натуральною природою і суспільством і є частиною неживої штучної природи. Таке розташування обумовлене тим, що, розробляючи і створюючи різні технічні пристрої, людина перш за все прагнула удосконалювати свої технічні здібності і можливості по взаємодії з навколишнім світом.

Розглянемо зміст інформаційних процесів і сформулюємо поняття «інформаційний ресурс».

Таким чином, з урахуванням вище викладеного дамо наступне визначення. *Інформаційним ресурсом* є сукупність інформації та її носіїв, інформаційних технологій та інформаційної інфраструктури.

Отже, інформація має нерозривний зв'язок з джерелами інформації, які є початком відліку в реалізації інформаційних процесів.

Зміст інформаційної боротьби полягає у впливі цілеспрямованих інформаційних впливів на інформаційні ресурси. При цьому під інформаційним впливом слід розуміти процес або дію направлену на поразку

або зменшення (нарощування) інформаційного ресурсу протиборчої сторони [10, 46].

На підставі сформульованого підходу до побудови загальних і приватних категорій інформаційної боротьби можна виділити напрями інформаційних впливів і визначити їх суть. Встановлено [18, 73], що інформаційні впливи можуть бути навмисними і ненавмисними.

У ході інформаційної боротьби на інформаційний ресурс здійснюються навмисні інформаційні впливи, які по своєму характеру можуть бути активними і пасивними [18].

До активних відноситься такі інформаційні впливи, які призводять до зміни складу ознак, що визначають конкретний смисловий зміст, або порушення стійкості інформаційних процесів, а також до поразки зв'язків у системах образів.

При пасивних інформаційних впливах зміна складу ознак і порушення зв'язків у системі образів не відбуваються.

Для реалізації дій в рамках виділених напрямів у ході інформаційної боротьби можна відзначити наступні види інформаційних впливів (див. рис. 1.4).

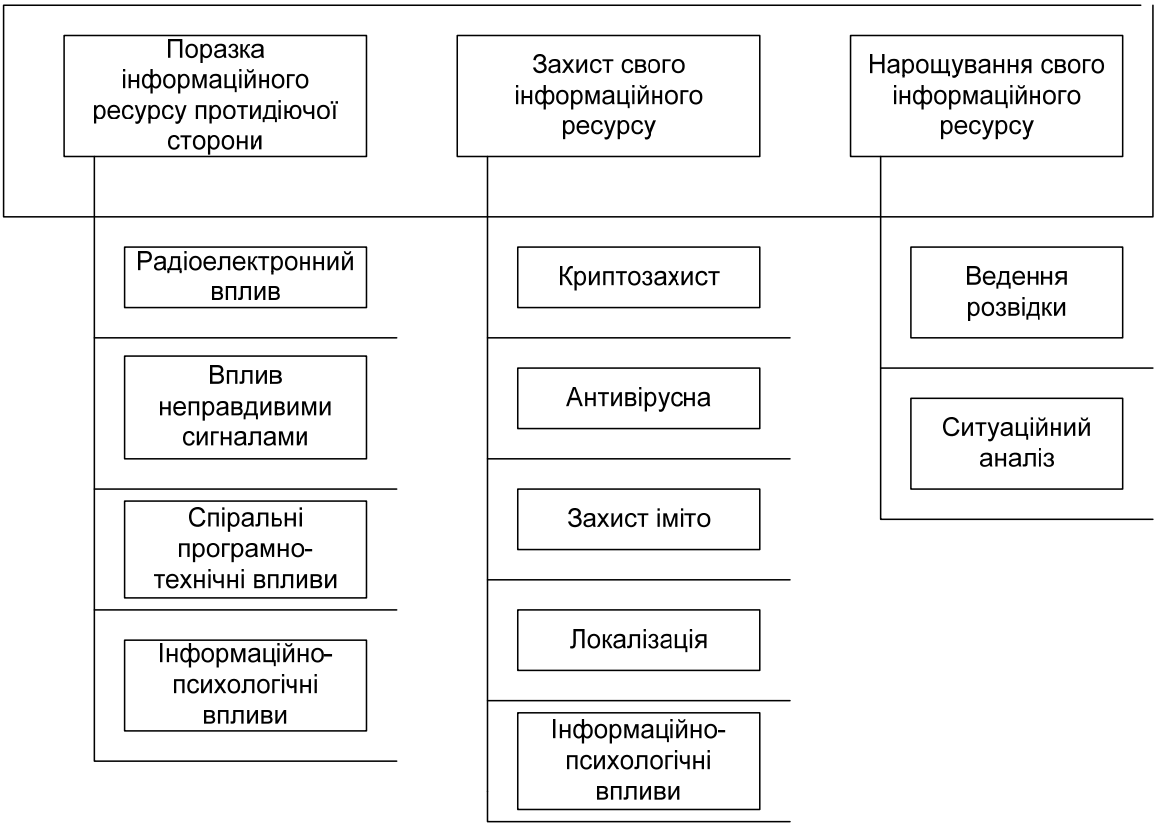


Рис. 1.4. Види інформаційних впливів

1.2. Аналіз методів і засобів оцінки уразливостей ІС

Захищеність є одним з найважливіших показників ефективності функціонування ІС. Під захищеністю ІС будемо розуміти ступінь адекватності реалізованих в ній механізмів захисту інформації існуючим в даному середовищі функціонування ризикам, пов'язаним із здійсненням загроз безпеки інформації. Під загрозами безпеці інформації [5] традиційно розуміється можливість порушення таких властивостей інформації як конфіденційність, цілісність і доступність. Арсенал програмних засобів, які використовують для аналізу захищеності ІС є досить широким. Одним із найбільш поширених інструментів для аналізу захищеності є сканер безпеки – програмний чи апаратно-програмний засіб, що дозволяє шляхом здійснення певних перевірок виявити схильність досліджуваного об'єкта до різноманітних уразливостей [5]. Під останніми, як правило, розуміють слабкі місця в ІС, які може привести до порушення безпеки шляхом реалізації

певної загрози [5]. Сканери безпеки є зручним і простим інструментом, що допомагає своєчасно виявляти уразливості в ІС. Спочатку сканери безпеки зародилися як інструментальні засоби, що використовувалися зловмисниками для організації атак, а потім цей інструментарій взяли на озброєння фахівці в галузі захисту інформації. Більш того, найбільш вдалі інструменти для аналізу захищеності переросли в комерційні продукти.

Сьогоднішній ринок інформаційної безпеки представлений різними сканерами безпеки, більшість з яких є орієнтованими на пошук уразливостей у певній технологічній області, наприклад: безпека Web-застосунків (HP WebInspect, Acunetix Web Vulerability Scanner, Open Source w3af та ін.); безпека систем управління базами даних (СУБД) (AppSecInc AppDetective, NGSS, Safety-Lab Shadow Database Scanner); безпека операційних систем і мережевих застосунків (GFI LANguard Network Security Scanner, Microsoft Baseline Security Analyzer тощо). Також існують комплексні продукти, що поєднують в собі можливості аналізу захищеності всіх перерахованих вище технологічних областей (Positive Technologies XSpider / MaxPatrol, TENABLE Nessus, IBM Internet Scanner).

Різноманітність інструментарію для аналізу уразливостей в ІС ускладнює їх вибір при побудові систем захисту інформації. З огляду на це, аналіз таких засобів за певним набором критеріїв є актуальним науковим завданням. Крім того, методів впливу (вхідних даних, призначених для активізації в ІС алгоритмів третього класу, тобто алгоритмів, відповідальних за порушення звичного режиму функціонування [28]) на ІС також відомо досить багато – систематизація та аналіз таких методів дозволить оцінити їх ефективність і підвищити рівень захисту ІС. Таким чином, метою цієї статті є проведення багатокритеріального аналізу інструментів для оцінки уразливостей і систематизація методів впливу на ІС.

Виклад основного матеріалу дослідження.

Відомий сканер вразливостей Nessus 2.2.4, побудований за технологією клієнт-сервер. Має багато переваг, а саме: зручний інтерфейс,

кросплатформеність, відкритий код, тощо. Для опису виявленої уразливості і включення її в базу даних у вигляді окремого модуля застосовується мова програмування Сі або спеціально розроблена мова сценаріїв NASL.

XSpider особливо зручний при пошуку вразливостей в Windows і Solaris. Але при видачі списку вразливостей виводиться дуже мало пояснювальної інформації, що передбачає високий рівень знань і професіоналізму у фахівця, який використовує цю програму. Ймовірно, це пояснюється тим, що розробник програми - російська компанія Positive Technologies, професійно спеціалізується на послугах з забезпечення безпеки комп'ютерних мереж, робила продукт, виходячи зі своїх внутрішніх потреб, і не особливо дбала про масового користувача. Але не зважаючи на відмінну якість роботи ця програма є безкоштовною.

LanGuard з натяжкою можна назвати сканером безпеки. Він дуже добре працює з NetBios, видаючи список ресурсів, сервісів і користувачів. Ця здатність сильно відрізняє сканер від інших, однак на цьому переваги LanGuard закінчуються.

У ShadowSecurityScanner простий інтерфейс і доступна ціна. Докладні поради та рекомендації щодо усунення вразливостей легко дозволяють впоратися з проблемами. Однак є й мінуси: невелика кількість розпізнаваних вразливостей, набагато більше споживання системних ресурсів при роботі в порівнянні з іншими сканерами, тощо.

Багато відомих продуктів або не дозволяють проводити повноцінну оцінку ризиків (Cobra), а скоріше є засобами для аналізу невідповідностей вимогам стандарту ISO 27001 (14 Day Trial), або включають в себе слабкі засоби оцінки ризиків, які не повністю відповідають вимогам ISO 27001, хоча в них багато іншого функціоналу (Callio Secura), або є занадто складними у використанні, дорогими (CRAMM).

Можна було б виділити з цього списку RA2 the art of risk. Як інструмент він повністю відповідає вимогам ISO 27001 (його розробники є авторами цього міжнародного стандарту), однак він не дозволяє порівнювати

між собою результати оцінок, що було б необхідно для великої організації, містить вкрай примітивні засоби побудови моделі активів і редагування текстової інформації, що ускладнює його використання, а також невірно відображає букви в звітах.

Також в цілому влаштовує RiskWatch, однак він, як і багато інших продуктів, не був спеціально розроблений для ISO 27001, а його ціна досить висока.

Звертаючи увагу на новий продукт vsRisk британської компанії IT Governance можно зробити висновок, що він дозволяє отримувати за результатами оцінки ризиків повноцінну Декларацію про застосовність в повній відповідності вимогам ISO 27001. Однак vsRisk також невірно відображає букви і містить ряд інших суттєвих недоліків, які ускладнюють його практичне застосування і які розробники обіцяли усунути коли-небудь в наступних версіях продукту.

X-Scan - безкоштовний сканер, але має не дуже читабельний інтерфейс програми і відсутність будь-яких коментарів про знайдені вразливості.

Крім того існує ряд продуктів, а саме AccessDiver 4.172, Nikto 1.32, Windows Vulnerability Scanner, Microsoft Baseline Security, Octave, Proteus enterprise, які не є досить популярними у зв'язку з наявністю ряду суттєвих недоліків.

Таблиця 1.1

Багатокритеріальний аналіз методів та засобів оцінки уразливостей ІС

№ з/п	Назва	Критерії						
		Оцінка ризиків	Оцінка захищеності	Кросплатформеність	Зручність у користуванні	Відкритий код	Низька вартість	Відповідність міжнародним стандартам у галузі ІБ
1	Nessus	+	+	+	+	+	+	+
2	AccessDiver	-	-	-	+	-	-	+
3	xSpider	-	+	-	+	-	-	-

4	LANguard Network Security Scanner	-	+	-	+	-	-	-
5	Shadow Security Scanner	-	+	-	+	-	+	-
6	Nikto	-	-	+	+	+	-	+
7	14 Day Trial	-	-	+	+	-	+	-
8	Windows Vulnerability Scanner	-	+	-	+	-	+	+
9	Microsoft Baseline Security	-	+	-	+	-	+	+
10	Cobra	+	+	-	+	-	-	+
11	Cramm	+	+	-	+	-	-	+
12	Calio Secura	+	+	-	+	-	-	-
13	Octave	+	+	-	+	-	-	+
14	Proteus enterprise	+	-	-	+	-	-	+
15	Ra2 the art of risk	+	+	-	-	-	-	+
16	Risk watch	+	+	-	+	-	-	+
17	VsRisk	+	+	-	-	+	-	+

Недоліки властиві багатьом програмним продуктам і обмежують їх практичне застосування. До числа найбільш поширених недоліків слід віднести:

- неповну сумісність з міжнародними стандартами. Наприклад, дуже мало продуктів було розроблено спеціально для ISO 27001;
- неповне охоплення активів. Більшість продуктів зосереджуються тільки на IT-активах, ігноруючи інші види активів, які, проте, є не менш важливими для інформаційної безпеки;
- складність використання. Багато продуктів мають занадто складний та незручний у використанні інтерфейс;
- ускладнення процесу оцінки ризиків, тому що розрахунок ризиків виконується автоматично і прихований від користувача;
- відсутність процесу оцінки захищеності;
- відсутність виконання функцій захисту;
- наявність проблем з відображенням вітчизняної мови, які є характерними для більшості імпортних програмних продуктів.

Виявити продукт, позбавлений всіх перерахованих недоліків і який в той же час повністю відповідає вимогам міжнародних стандартів, досить

складно. Не кажучи вже про те, що багато продуктів, що позиціонуються розробниками як засобу для оцінки або управління ризиками, насправді такими не є, тому що не реалізують ні методологію оцінки ризиків, ні алгоритм їх обчислення, а надають лише засоби представлення і збереження даних про ризики, залишаючи аналіз та оцінювання ризиків, по суті, на відкуп користувачеві.

В даний час питання аналізу захищеності ІС є добре опрацьованими. Існує багатий арсенал засобів і методів для проведення подібних робіт. Є відпрацьовані методики з проведення обстеження (аудиту) безпеки ІС відповідно перевіреним критеріям (затвердженим в якості міжнародних стандартів), які роблять можливим отримання вичерпної інформації про властивості ІС, що мають відношення до безпеки. На практиці аналіз захищеності ІС проводиться за допомогою потужного програмного інструментарію, в достатньому обсязі представленого на ринку засобів захисту інформації.

1.3. Аналіз сучасних методів моделювання впливів на ІС

Розглянемо сучасні підходи до моделювання впливів на ІС – виділимо вхідні та вихідні дані кожного з критеріїв, основні операції, а також їх переваги і недоліки (табл.1.2).

Таблиця 1.2

Аналіз методів моделювання впливів на ІС

№	Назва	Вхідні дані	Вихідні дані	Основні операції (матапарат)	Переваги	Недоліки
1.	Модель Мухіна-Волокіти [43]	Статистична вибірка даних	Лічильник загроз впливу на інформацію	Експертні оцінки, теорія графів	Висока точність виявлення впливу	Потреба у статистичних даних, залежність від компетенції експертів

2.	Модель Бела-Лападули та модель Біба [43]	Множини об'єктів і суб'єктів, а сторонніхт акож їх стани, запити	Рівень порушення цілісності	Теорія множин, булева алгебра	Простота реалізації, контроль цілісності	Врахування лише цілісності; можливість створення двосторонніх потоків інформації і як наслідок необхідне створення довірених потоків.
3.	Модель Хартсона (п'ятивимірна статична модель) [28]	Ресурси системи та їх стани; користувачі та їх повноваження	Область безпеки системи	Декартів добуток множин	Можливість отримання кількісних оцінок	Абстрактна формалізація процесу нападу
4.	Модель на основі нейронних оперет та ланцюгів Маркова [65]	Статистичні дані для навчання нейромережж та задавання матриць ймовірностей переходів СЗІ	Виявлення вірусів, спаму та атак на Web-сервери	Теорія нейронних мереж; теорія ланцюгів Маркова	Адаптивні виявлення нападу та захист інформації	Потреба у статистичному наборі даних для динамічного функціонування
5.	Модель на основі мереж Петрі-Маркова [11]	Інформаційні стани системи (більше 3-х)	Можливість реалізації загрози впливу на інформацію	Теорія мереж Петрі та теорія ланцюгів Маркова	Кількість оцінки з урахуванням часових параметрів	Складність розрахунків для практичної реалізації
6.	Диференціально-ігрова однокритеріальна графова модель [23]	Множина станів ІС	Оптимальна стратегія захисту інформації	Теорія графів, диференціально-ігрове моделювання	Дозволяє здійснити розподіл інформаційних ресурсів, що виділяютьс	Не відображає загальну динаміку впливу на інформацію

					я на захист інформації	
7.	Диференціально-ігрові спектральні однокритеріальні моделі [23]	Множина станів ІС	Оптимальна стратегія та ціна гри (гарантований рівень захищеності)	Диференціально-ігрове моделювання	Низька обчислювальна складність, врахування нестаціонарності	Не точний покроковий процес впливу на інформацію
8.	Диференціально-ігрова нетейлорівська модель [23]	Інтенсивність потоку захисних і атакуючих дій	Траєкторія та ціна гри	Диференціальні перетворення нетейлорівського типу	Точний опис процесу нападу на інформапцію	Висока обчислювальна складність, низький рівень науково-технічних досліджень
9.	Гібридна диференціально-ігрова модель [23]	Показники надійності та захищеності, ймовірності загроз, часові параметри	Оптимальний розподіл ресурсів захисту	Диференціально ігрове моделювання	Врахування показника якісного функціонування СЗІ; висока точність навіть в умовах невизначеності	Точність досягається лише при певному застосуванні (послідовно) математичних методів
10.	Неперервна дискретна диференціально-ігрова модель [23]	Скінченна множина станів системи	Оптимальний розподіл ресурсів захисту у режимі реального часу	Числово-аналітичне моделювання, диференціальні перетворення	Розширення діапазону моделювання впливу на інформацію; низька обчислювальна складність	Не враховує усіх критеріїв (порівняно з багатокритеріальним и моделями)
11.	Багатокритеріальна диференціально-ігрова	Стратегії протиборчих сторін, часові	Оптимальні стратегії гравців, ціна гри	Диференціально-ігрове моделювання; теорія	Можливість захисту інформації в умовах	Обмеження на частинні критерії якості

	модель на основі інтегральної оптимальності [23]	параметри	(гарантований рівень захищеності)	підтримки прийняття рішень	конфлікту частинних критеріїв та несанкціонованого розподілу інформаційних ресурсів атакуючої сторони	
12.	Багатокритеріальна диференціально-ігрова модель на основі нелінійної схеми компромісів [23, 16]	Інтенсивності потоків розподілу ресурсів протиборчих сторін, часові характеристики	Оптимальні стратегії протиборчих сторін	Диференціальні перетворення, теорія підтримки прийняття рішень	Простота реалізації, адаптивність до різних ситуацій	Значних недоліків не виявлено

1.4. Формалізація проблеми оптимізації систем захисту в умовах впливів на ІС

Приймаючи до уваги узагальнену модель процесу захисту інформації та її цільову функцію, можливо здійснити спробу знаходження оптимальних параметрів систем захисту - характеристик системи ТЗІ, наприклад, в розумінні максимальної шкоди, яка попереджається, завдяки застосуванню системи захисту.

На рис. 1.5 умовно представлені інформаційні ресурси систем спеціального призначення (ССП), які потрібно захистити від природних та штучних впливів. Під природними впливами розуміються потоки будь-яких подій, які здатні тимчасово вивести ССП зі строю (збій, для якого характерно самоусунення) або на тривалий термін (збій, усунення якого потребує вторгнення персоналу), тобто потоки відмов. Причинами таких впливів

можуть бути недостатня здатність вже згаданих первинних технічних засобів попередити дію таких впливів; недостатня надійність засобів ССП; виходи за межі допустимих значень температури, вологості, радіаційного або електромагнітного випромінювання, яке діє на елементи ССП. Такі події впливають як безпосередньо на інформаційні ресурси ССП, так і на засоби технічного захисту цієї системи. При цьому стійкість ССП до природних впливів визначається такою її властивістю як надійність та забезпечується відповідними заходами (резервування - гаряче та холодне, застосування елементів підвищеної надійності та ін.). Для боротьби зі збоями, котрі призводять до порушення цілісності програмних засобів та інформації, що обробляється, можливо застосовувати засоби контролю й відновлення цілісності чи інші засоби відновлення ССП після збоїв.

Під штучними впливами розуміються ті події, котрі є результатом діяльності користувачів, як авторизованих, так і неавторизованих по відношенню до ресурсів ССП, що є, по якимось причинам, забороненим для даних користувачів. Такі впливи прийнято називати спробами несанкціонованого доступу (НСД), та вони можуть бути випадковими (в результаті помилки користувача) чи зловмисними, тобто спеціальними, з метою використання чи то ресурсів, чи то інформації ССП [61,92].

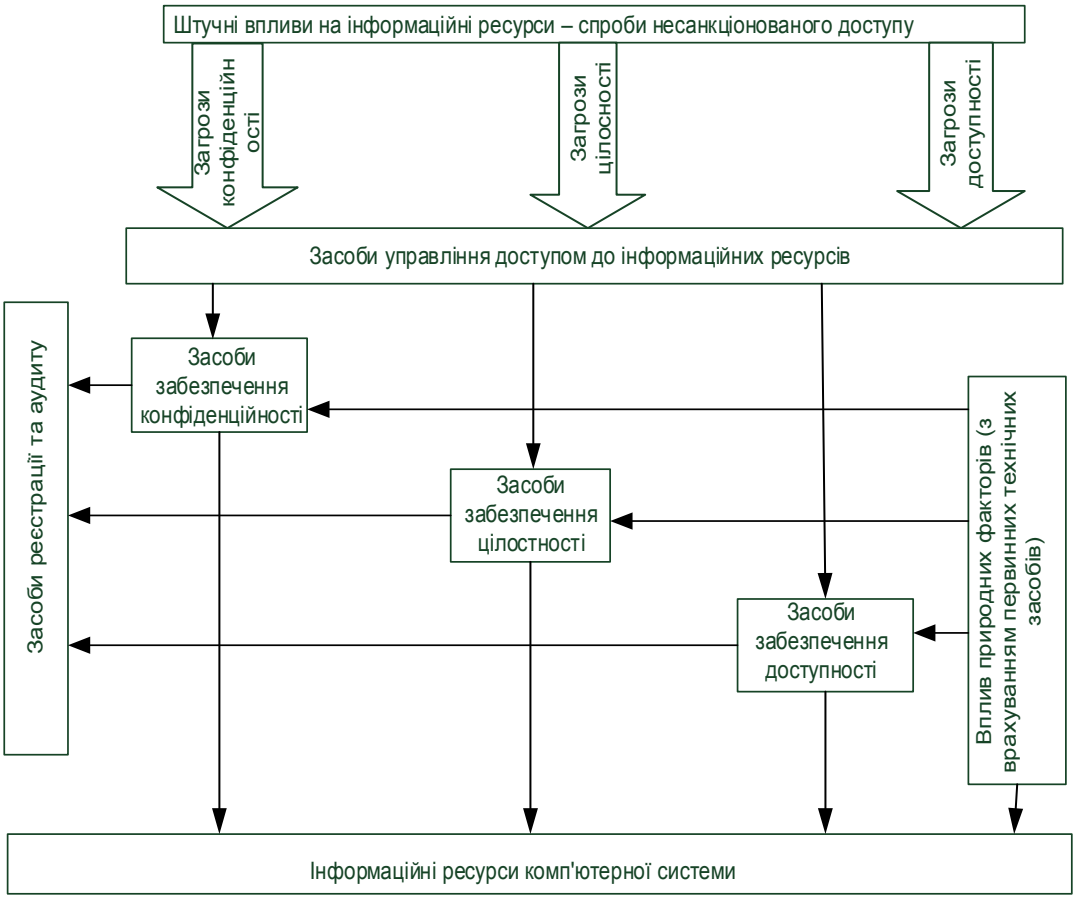


Рис. 1.5. Модель взаємодії засобів в процесі технічного захисту інформації

Спроби НСД можуть подіяти на ССП лише після подолання засобів управління доступом та відповідних засобів забезпечення тієї чи іншої функціональної послуги.

Таким чином, на інформаційні ресурси ССП можуть впивати як спроби несанкціонованого доступу, за умови подолання системи управління доступом, так і безпосередньо природні впливи [64,68].

Нехай потоки кожного з типів впливів є простішими з інтенсивностями $\lambda_{зі}$. Зрозуміло, що ця інтенсивність дорівнює сумі інтенсивностей впливів штучних $\lambda_{ші}$ та природних λ_i, так що

$$\lambda_{зі}=\lambda_{ші}+\lambda_i. \qquad (1.1)$$

Звернемо увагу на те, що під величиною λ_i потрібно розглядати ту частину потоку відмов ССП з загальною інтенсивністю λ, яка створює лише вплив *i*-го типу, так що

$$\lambda = \sum_{i=1}^{i=n} \lambda_i .$$

Потрібно враховувати те, що $p_{вi}$ - імовірність виявлення та подальшої протидії впливу (імовірність захисту ССН від впливів) *i*-го типу є імовірністю складної події, яка полягає у тому, що система ТЗІ запобігла (не допустила) дії цього впливу, або встановила факт дії та ліквідувала відповідні наслідки.

Перша з цих задач вирішується, як правило, шляхом управління доступом до інформаційних ресурсів ССП (ідентифікація, аутентифікація, надання певних повноважень або привілей, з наступною їх перевіркою під час кожної зі спроб доступу до ресурсів). Помітимо, що оскільки адміністратор безпеки має, як правило, найширші права відносно управління доступом до ресурсів ССП, то захопивши його повноваження можливо порушити процес надання цій ССП будь-якої функціональної послуги. Тому потрібно рахувати, що стійкість (в розумінні імовірності неподолання) $p_{Д}$ системи управління доступом визначається стійкістю процесів ідентифікації та аутентифікації самого адміністратора безпеки, як користувача з найширшими повноваженнями. Останнє визначається можливостями системи ідентифікації та кількістю можливих варіантів паролів і надійністю їх конфіденційного зберігання [61].

Оскільки штучні впливи можуть діяти тільки у випадку їх не виявлення засобами управління доступом, то інтенсивність цих впливів, які діють на засоби забезпечення відповідної функціональної послуги ССН, зменшується (за рахунок проріджування, фільтрації штучних впливів засобами управління доступом) до $\lambda_{шi}(1 - p_{Д})$.

Друга задача (встановлення факту дії впливу, якщо система управління доступом виявилась нездатною не допустити такого впливу, та ліквідації відповідних наслідків) вирішується шляхом перевірки цілісності й доступності інформації та її відновлення, у випадку виявлення такого порушення. Тому з урахуванням застосування відповідних засобів захисту - засобів забезпечення відповідної функціональної послуги ССН, підсумкова інтенсивність впливів λ_{pi} може бути розрахована як

$$\lambda_{pi} = (\lambda_{ші}(1 - p_{\partial i}) \cdot (1 - p_{ві}), \quad (1.2)$$

де $p_{ві}$ - вже згадана вище імовірність виявлення (і, зрозуміло, усунення) засобами забезпечення відповідної функціональної послуги ССН впливу відповідного типу.

Будемо рахувати закон розподілу імовірності впливу на ресурси пуасоновським. Тоді імовірність дії на *i*-тий ресурс хоча б одного впливу відповідного типу $p_{зі}$ на інтервалі $(T_{кі} - \Delta T_{кі})$ при умові застосування системи ТЗІ, тобто коли система захисту не проявила і, зрозуміло, протидіяла цьому впливу, дорівнює

$$p_{зі} = 1 - p_{\partial i} = 1 - exp\{-(T_{кі} - \Delta T_{кі}) \cdot [(\lambda_{ші}(1 - p_{\partial i}) + \lambda_i)\,(1 - p_{ві})]\}, \quad (1.3)$$

де $p_{\partial i}$ - імовірність відсутності впливів, або наявність рівно нуля впливів.

Виходячи з (1.3) величину втрат можливо записати у вигляді:

$$L_i = G_i \cdot (T_{ki} - \Delta T_{ki}) \cdot [1 - \exp\{-(T_{ki} - \Delta T_{ki}) \cdot [(\lambda_{ші}(1 - p_{\partial i}) + \lambda_i) \cdot (1 - p_{ві})]\}] +$$

$$+ C_i \Delta T_{ki} \exp\{-(T_{ki} - \Delta T_{ki}) \cdot [(\lambda_{ші}(1 - p_{\partial i}) + \lambda_i) \cdot (1 - p_{вуі})]\}. \quad (1.4)$$

Як випливає з останнього виразу, величина шкоди є функцією достатньо великого числа змінних. Серед цих змінних величини G_i, C_i, $\lambda_{ші}$ і λ_i є незалежними не тільки від дій адміністратора безпеки, але й від характеристик підсистеми захисту ССН у цілому, тобто принципово не

можуть розглядатися як параметри управління. Величини $p_{\hat{c}\hat{i}}$, $p_{ві}$, і ΔT_{ki} є залежними від якості розроблених та використаних засобів управління доступом й засобів забезпечення відповідної функціональної послуги ССН і не можуть бути зміненими оперативно, наприклад, за бажанням адміністратора безпеки, але під час розробки системи ТЗІ їх значення принципово можливо змінювати, тому ці параметри треба розглядати як параметри неоперативного управління. Після цих зауважень стає зрозумілим, що параметром оперативного управління треба рахувати лише величину періоду контролю T_{ki}.

Нескладно показати, що ця функція має мінімум в точці:

$$T_{ki}=\Delta T_{ki}+d, \qquad (1.5)$$

де величина ΔT_{ki} визначається з виразу

$$d=\frac{1}{z}+0.5\sqrt{s}\ , \quad s=\square T_{ki}^2\left(1+4\cdot\frac{C_i}{G_i}\right)+4\left(\frac{1}{z^2}+\frac{C_i\square T_{ki}}{G_i\cdot z}\right),$$

а величина

$$z=[(\lambda_{шi}(1-p_{\hat{c}\hat{i}})+\lambda_i)\cdot(1-p_{ві})],$$

є не що інше, як раніше введена підсумкова інтенсивність впливів $z = \lambda_{pi}$.

Отриманий результат має чіткі та зрозумілі тлумачення. Величина шкоди при зміні періоду контролю $T_{кі}$ є мінімальною при такому його значенні, яке перевищує середнє значення його тривалості ΔT_{ki} на величину d, яка, у свою чергу, визначається інтенсивністю потоку впливів, величинами завад G_i і C_i характеристиками системи ТЗІ та тривалостями процедур контролю наявності порушення відповідної функціональної властивості Δt_{ki} і його усунення Δt_{ni}, а також ймовірностями не подолання впливом системи управління доступом $p_{\hat{c}i}$ і поновлення порушеної функціональної властивості $p_{ві}$).

Вираз для розрахунку мінімального значення втрат при цьому має вигляд

$$\min L_i = G_i d\left[1 - \exp\{-dz\}\right] + C_i \Delta T_{ki} \exp\{-dz\},$$

з якого її легко розрахувати при відомих значеннях згаданих вище величин.

Цікавим є результат пошуку оптимального значення (в розумінні мінімуму втрат) тривалості контролю ΔT_{ki}. Нескладно показати, що точка

$$\Delta T_{ki} = \frac{2G_i T_{ki} z + C_i - C_i T_{ki} z}{2z(G_i - C_i)} = \Delta T_{kiopt},$$

є точкой максимуму шкоди. При цьому оптимальне значення тривалості контролю перевищує значення тривалості його періоду $\Delta T_{kiopt} > T_{ki}$. Таке значення тривалості контролю є неможливим, але цей факт дозволяє зробити наступний, важливий для тактики висновок: на інтервалі від $\Delta T_{ki} = 0$ до $\Delta T_{ki} = \Delta T_{kiopt}$ значенню шкоди із збільшенням ΔT_{ki} зростає, або чим менше значення тривалості контролю ΔT_{ki}, тим меншим є значення шкоди у вигляді (1.3). Іншими словами, при побудові, проектуванні, або виборі засобів ТЗІ перевагу треба віддавати таким засобам, котрі мають найменший час виконання операції контролю [61,64].

Пошук екстремуму цільової функції (1.4) за підсумковою інтенсивністю загроз z призводить до висновку, що при надійних (високоефективних) системах управління доступом та виявлення і усунення впливів, коли на інтервал роботи ССН довжиною $(T_{ki} - \Delta T_{ki})$ попадає менше, ніж один вплив, який є пропущеним системою управління доступом й не виявленим та не усуненим системою контролю, тобто при

$$(T_{ki} - \Delta T_{ki})\left[(\lambda_{ші}(1 - p_{ді}) + \lambda_i)(1 - p_{ві})\right] < 1, \qquad (1.6)$$

величина шкоди залежить лише від параметрів T_{ki} і ΔT_{ki} та має екстремуми в точках, які є близькими до

$\Delta T_{kiopt} = T_{ki}$, і $\Delta T_{kiopt} = T_{ki} / C$.

Останній результат лише підтверджує вже отримані висновки і, при цьому його цінність полягає в підтвердженні адекватності запропонованої моделі реальним процесам, пов'язаним з ТЗІ.

Примітка. Звернемо увагу, що отримані результати функцій в попередніх дослідженнях, не рахуючи їх цінність, отримані внаслідок оптимізації (1.3) при обмеженнях у вигляді (1.6), коли для знаходження екстремуму цільової функції використовувалось розкладання в ряд експонентної функції $\exp\{-(T_{ki} - \Delta T_{ki})[(\lambda_{ші}(1 - p_{ді}) + \lambda_i)(1 - p_{ві})]\}$ (коли можна рахувати $\exp\{-x\} \approx 1 - x$).

Але, якщо розглядати вираз (1.6) як таке обмеження при (1.4), що при визначених умовах перетворюється в окрему цільову функцію, тоді отримаємо важливі для практики вимоги відносно допустимих значень:

1. Тривалості періоду контролю (з урахуванням раніше отриманого результату відносно величини $\Delta T_{ki} << T_{ki}$)

$$T_{ki} < 1/[(\lambda_{ші}(1 - p_{ді}) + \lambda_i)(1 - p_{ві})]. \qquad (1.7)$$

2. Або відносно підсумкової інтенсивності дії впливів

$$\lambda_{ші}(1 - p_{ді}) + \lambda_i)(1 - p_{ві}) < 1/\mathrm{T_{ki}}. \qquad (1.8)$$

Умова (1.7) дозволяє визначити вимоги відносно тривалості періоду контролю T_{ki}, при відомих інтенсивностях впливів $\lambda_i, \lambda_{ші}$ та реалізованих в системі ТЗІ ймовірностей $p_{ді}, p_{ві}$.

В свою чергу, умова (1.8) при заданій тривалості періоду контролю T_{ki} дозволяє визначити вимоги відповідно таких параметрів системи ТЗІ як імовірності $p_{ді}, p_{ві}$ при відомих інтенсивностях впливів $\lambda_i, \lambda_{ші}$.

З виразу (1.4) можна отримати значення екстремумів цієї ж функції та по будь-яким іншим параметрам неоперативного управління.

Таким чином, розглянуті узагальнені моделі дозволяють сформулювати або отримати цілий ряд дуже важливих для вирішення задачі захисту ресурсів інформаційних систем умов, обмежень і оптимальних значень найбільш загальних параметрів системи захисту, але не дають можливості сформулювати більш конкретні вимоги відносно складу та параметрів системи захисту.

Розгляду цих питань присвячені наступні розділи даної роботи.

1.5. Висновки до першого розділу

Проведений аналіз існуючих методів і засобів оцінки уразливостей інформаційних систем дозволив виявити їх недоліки і формалізувати завдання щодо розробки більш ефективного засобу. У результаті багатокритеріального аналізу встановлено, що усі ці засоби не є досконалими і мають певні обмеження щодо практичного застосування для розв’язання різного роду завдань ІБ.

Аналіз сучасних методів моделювання впливів на інформаційні системи дав можливість визначити найбільш ефективний підхід і використати його з метою оптимізації параметрів систем захисту.

РОЗДІЛ 2. МЕТОДИ ОЦІНКИ УРАЗЛИВОСТЕЙ ІНФОРМАЦІЙНИХ СИСТЕМ ТА ВПЛИВІВ НА НИХ

2.1. Метод оцінки уразливості ІС

Низка питань виникає при спільному розгляді понять небезпеки та безпеки інформації, а саме: яке з цих двох явищ є первинним; якими є їх взаємний вплив і взаємний зв'язок; якими можуть бути критерії їх оцінки?

Зрозуміло, що первинним є поняття небезпеки інформації. Шляхи, способи та засоби забезпечення безпеки інформації визначаються саме на противагу небезпеці інформації.

Багато спільного можна знайти незважаючи на смислову протилежність понять небезпеки інформації і безпеки інформації. По-перше, обидва явища цілеспрямовано виникають в однакових сферах людської діяльності - політиці, економіки, ідеології, військовому будівництві тощо. По-друге, небезпека інформації і безпека інформації створюються однаковими суб'єктами - державою, соціальними верствами, організаціями, підприємствами, людьми. По-третє, і небезпека інформації, і безпека інформації можуть створюватися однаковими засобами.

Відмінностей між небезпекою інформації і безпекою інформації лежать у різних площинах.

У першу чергу, це відмінність предметів небезпеки інформації та безпеки інформації стосовно об'єктів діяльності. Предметом небезпеки інформації є оволодіння, опанування, загарблення, отримання. В свою чергу, предметом безпеки інформації є захист, збереження, забезпечення умов для безперешкодного існування, зберігання, використання.

Між небезпекою інформації і безпекою інформації у їх взаємовідносинах з об'єктами діяльності існує інша принципова різниця. Для своїх об'єктів небезпека інформації є зовнішнім, ворожим фактором. Безпека інформації об'єднана зі своїми об'єктами спільністю державної, комерційної,

особистої єдністю цілей та інтересів особливо в екстремальних ситуаціях. Об'єкти безпеки інформації у просторовому уявленні оточені захисною оболонкою, а небезпека інформації спрямована на несанкціоноване її отримання та руйнування як самого цього захисту, так і самої інформації (об'єкту).

Також, небезпека інформації і безпека інформації відрізняються ще й тими арсеналами засобів, за допомогою яких ці явища створюються у сфері життєвого циклу інформації. Якщо для небезпеки інформації це, насамперед, засоби впливу та впливу на неї, то безпека інформації, яка теж спирається на активні протидії, має досягатися, перш за все, шляхами запобігання несанкціонованим діям впливу на інформацію.

Взаємозалежність небезпеки інформації і безпеки інформації є беззаперечною та має кілька важливих рис, які значною мірою впливають на ситуацію навколо інформації.

По-перше, це стримуючий вплив безпеки інформації на небезпеку інформації. Імовірність несанкціонованих дій та впливів зменшують заходи, що вживаються державними та приватними організаціями в напрямі забезпечення інформаційної безпеки. Якщо той самий стримуючий вплив безпеки інформації здійснюється одним типом захисту, часто виявляється тимчасовим, якщо не усунені первинні причини конфліктної ситуації або не застосувати комплексну систему захисту.

По-друге, має місце стимулюючий вплив небезпеки інформації на безпеку інформації. Іншу реакцію, яка виражається у зростанні зусиль та зміцненні комплексної системи захисту інформації, викликає у суспільстві будь-яке зростання небезпеки інформації.

При цьому питання методичних основ оцінки рівня безпеки інформації є дуже актуальним. І досить ефективними є логічні методи аналізу проблем безпеки інформації, однак, вони не дають змоги встановити чіткі функціональні зв'язки між дією окремих чинників та їх сукупним

результатом. Тому розробка методу кількісно-якісного аналізу та об'єктивного визначення рівня безпеки інформації є нагальною потребою.

Під час розгляду поняття небезпеки інформації можна дійти висновку про те, що небезпеку інформації можна оцінювати за допомогою інтегральною показника (рівня небезпеки інформації), пов'язаного у певний спосіб зі ступенем застосування ситуації та очікуваним масштабом потенційного впливу . Перш за все необхідно з'ясувати сутність оцінки рівня безпеки інформації.

По-перше, слід з'ясувати чи можна за умови відсутності небезпеки інформації говорити про безпеку інформації. Можна, оскільки безпека інформації полягає у відсутності небезпеки інформації. Тобто, повна відсутність небезпеки інформації означає повну безпеку інформації.

По-друге, слід з'ясувати чи можна за умови наявності небезпеки інформації говорити про безпеку інформації. Можна, але з застереженням: чим вищий рівень небезпеки інформації, тим, менше підстав стверджувати про безпеку інформації.

Сама по собі небезпека інформації достатньою мірою характеризує безпеку інформації. Цей висновок може бути твердо доведений.

Як відзначалось [76], безпека інформації досягається двома основними шляхами:

- відвернення впливу, пов'язаного з застосуванням пасивних та активних дій щодо можливого зловмисника, тобто використання для впливу на нього економічних, ідеологічних та інших дій з метою відвернення спроб вирішення конфліктної ситуації;
- протидія впливу, тобто стримуванням (або відбиттям) впливу, шляхом застосування певних методів та засобів.

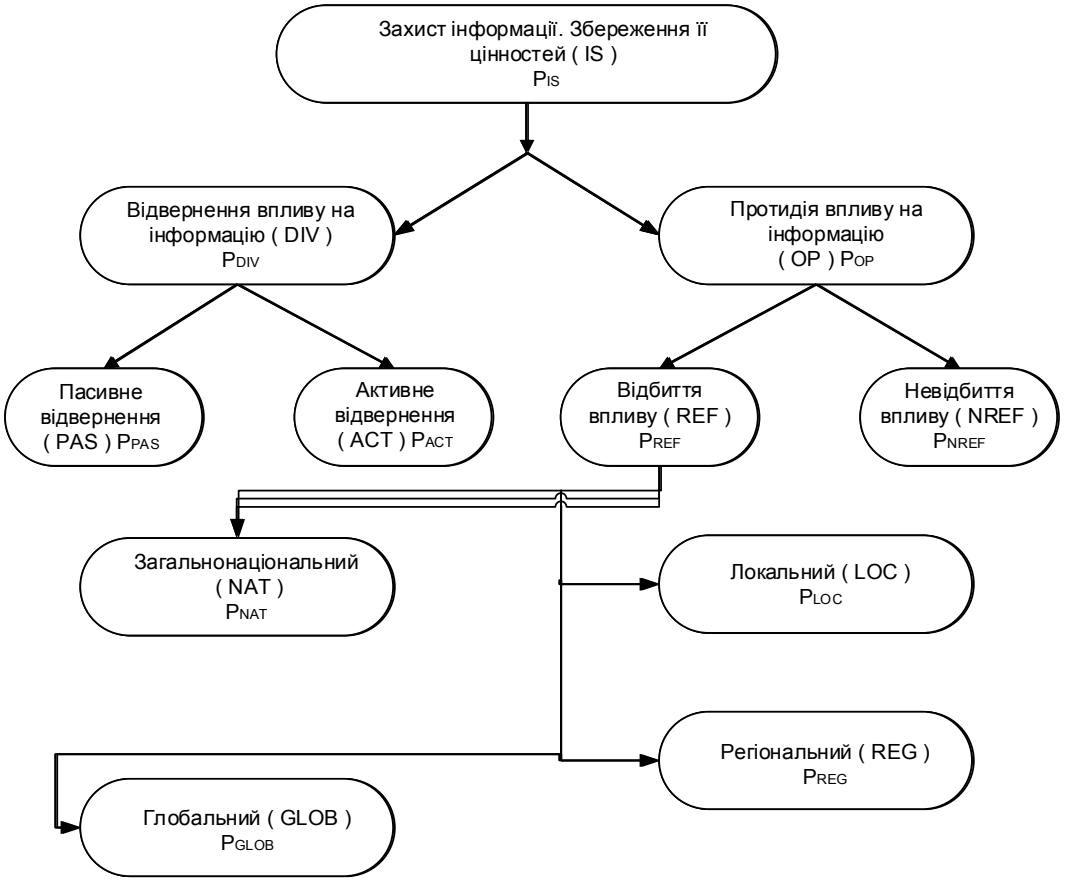


Рис.2.1. Схема подій, які пов'язані із забезпеченням безпеки інформації

У центрі є потенційний вплив на інформацію як деяка подія, що може відбутися або не відбутися, залежно від ступеня зацікавленості в ній потенційного зловмисника та від ефективності системи забезпечення безпеки інформації (об'єкта потенційного впливу). Безпеку інформації забезпечено, якщо вплив на інформацію вдалося відвернути. Якщо атака все ж таки розпочалася, то можливість забезпечення безпеки інформації зберігається через можливість успішної протидії впливу. В залежності від рівня впливу при цьому подія може набути локального, регіонального, загальнонаціонального або глобального масштабу.

Відповідну схему подій, пов'язану з реалізацією небезпеки інформації та із забезпеченням безпеки інформації, можна побудувати ототожнюючи небезпеку інформації з потенційним впливом та його наслідками, а безпеку інформації - з успішним захистом (у будь-який спосіб) інформації та збереження її цінності. (див. рис. 2.1).

Головними є такі пари протилежних подій:

- відвернення впливу та протидія йому;
- пасивне та активне відвернення впливу;
- відбиття впливу та його успіх.

Для аналізу взаємозв'язку цих подій може бути використано математичний апарат теорії ймовірностей тому, що саме вона оперує, як правило, подіями та явищами, які мають таку властивість як статистична стійкість. Існує тисячі прикладів конфліктів, але умови їх виникнення, розвитку і завершення є настільки різноманітними, що виділити стійкі статистичні ознаки дуже складно. Є чимало аргументів на користь того, що в цій сфері має право на застосування імовірнісний підхід.

Але існує інший більш реальний шлях для об'єктивного визначення імовірності виникнення інформаційного впливу. Для цього необхідно знати залежність цієї імовірності від таких факторів обстановки, як ступень захищеності інформаційної системи, співвідношення сил сторін (ступінь захищеності інформації та можливості нападника) тощо. Досить складна проблема може виникнути за відсутності статистичних даних вивчення такої залежності.

Теорія ймовірностей має багато способів, що дають змогу визначати імовірності подій побічно, через імовірності інших подій, пов'язаних з першими [69].

Вирішити зазначену проблему можливо при використанні широко відомого принципу невизначеності Лапласа, суть якого полягає в тому, що за наявності кількох гіпотез, жодній з яких не можна віддати перевагу, слід вважати імовірності настання відповідних подій однаковими або рівноймовірними. Оскільки в нашому випадку розглядаються пари протилежних подій, то вихідною точкою може служити та аксіома, що для таких подій сума ймовірностей їх настання дорівнює одиниці.

Такими є принципові основи для застосування теорії ймовірностей в інтересах дослідження механізмів виникнення та припинення конфліктів і впливів в інформаційному колі [29].

На рис. 2.1 подія, яка полягає у забезпеченні безпеки інформації, позначена через *IS*, а її імовірність - через P_{IS}. Ця подія може відбутися одночасно з однією із двох інших несумісних подій: з відверненням впливу (*DIV*) з імовірністю P_{DIV} або з протидії впливу (*OP*) з імовірністю P_{OP}. Оскільки події (*DIV*) та (*OP*) утворюють повну групу, то:

$$P_{OP} = 1 - P_{DIV}. \tag{2.1}$$

Розглядаючи настання подій *DIV* і *OP* за умов конкретного рівня небезпеки інформації як лише дві можливі гіпотези, у зв'язку з якими з імовірністю P_{IS} може стати подія *IS*, відповідно до формули повної імовірності [69] можна записати:

$$P_{IS} = P_{DIV} * P_{(IS/DIV)} + P_{OP} * P_{(IS/OP)}, \tag{2.2}$$

або з урахуванням (2.1):

$$P_{IS} = P_{DIV} * P_{(IS/DIV)} + (1 - P_{DIV}) * P_{(IS/OP)}, \tag{2.3}$$

$P_{IS/OP}$ - умовна імовірність настання події *IS* у разі настання події *OP*;

$P_{IS/DIV}$ - умовна імовірність настання події *IS* у разі настання події *DIV*.

Настання події *DIV* означає, що вплив відвернено, небезпека інформації нейтралізована. У такому випадку подія *IS* є достовірною, тобто:

$$P_{(IS/DIV)} = 1. \tag{2.4}$$

Якщо настала подія *OP*, то імовірність події *IS* визначається, по суті, імовірністю успішного відбиття впливу на інформацію P_{DIV}, тобто

$$P_{(IS/DIV)} = P_{DIV}. \tag{2.5}$$

Тоді, з урахуванням (2.4) і (2.5)

$$P_{IS} = P_{DIV} + (1 - P_{DIV}) * P_{DIV}. \tag{2.6}$$

Важливо визначитися з фізичним змістом величини P_{DIV}. Якщо позначити максимальний прогнозований збиток для організації внаслідок

зовнішнього впливу на інформацію як $G_{\max}$, то будемо вважати, що за певної імовірності відбиття впливу P_{DIV} збиток складе величину $G_{\max}(1-P_{DIV})$, а при P_{DIV}=1 (гіпотетичний випадок) величина збитку буде близькою до нуля.

Далі розглянемо взаємозв'язок подій наступним чином. Імовірність відвернення впливу шляхом пасивних дій (*PAS*) або активного стримування впливу (*ACT*) визначається таким рівнянням:

$$P_{DIV} = P_{PAS} + (1-P_{PAS}) * P_{ACT}. \quad (2.7)$$

При цьому імовірність стримування або відвернення впливу можна порівняти з імовірністю її успішного відбиття, оскільки потенційний нападник, приймаючи рішення про несанкціоноване отримання інформації, виходить з можливостей сторони, яка захищає інформацію. Враховуючи це рівняння (2.7) буде мати наступний вигляд:

$$P_{DIV} = P_{PAS} + (1-P_{PAS}) * P_{DIV}. \quad (2.8)$$

Стосовно відбиття впливу на інформацію, яку потрібно захистити, то вона може відбуватися за умов її локального, регіонального, загальнонаціонального або глобального характеру. При цьому імовірності відповідних гіпотез утворюють повну групу:

$$P_{LOC} + P_{REG} + P_{NAT} + P_{GLOB} = 1. \quad (2.9)$$

Тоді:

$$P_{DIV} = P_{LOC} * P_{DIV(LOC)} + P_{REG} * P_{DIV(REG)} + P_{NAT} * P_{DIV(NAT)} + P_{GLOB} * P_{DIV(GLOB)}, \quad (2.10)$$

де $P_{DIV(LOC)}, P_{DIV(REG)}, P_{DIV(NAT)}, P_{DIV(GLOB)}$ - імовірності відбиття впливу відповідного характеру.

З урахуванням (2.8) і (2.10) рівняння (2.6) є математичною моделлю, яка відображає ступінь загострення конфліктної ситуації та можливість щодо її вирішення шляхом відвернення або протидії впливу.

Проведені дослідження дають змогу визначити показники, які дозволяють зробити кількісну оцінку рівня безпеки інформації:

1. Імовірність успішного захисту інформації, може бути прийнята як основний кількісний показник рівня безпеки інформації, збереження її

цілісності за умов прогнозованої небезпеки інформації. Цей показник можна назвати індексом безпеки інформації, кількісне значення якого дає змогу робити певні висновки щодо рівня безпеки інформації.

2. Методика розрахунку індексу безпеки інформації має спиратися на результати оцінки небезпеки інформації, оскільки схеми подій, пов'язаних із забезпеченням безпеки інформації та з реалізацією небезпеки інформації, є аналогічними і характеризуються ймовірностями однакових подій. Основні вихідні данні для обчислення індексу безпеки інформації можуть бути віднесені до показників, що характеризують небезпеку інформації, а їх кількісні значення можуть визначатися під час оцінки останньої.

Отже, можна вважати доведеним припущення про те, що рівень небезпеки інформації одночасно характеризує й рівень безпеки інформації.

3. Виходячи із взаємозалежності небезпеки інформації і безпеки інформації основним кількісним показником небезпеки інформації можна вважати імовірність заподіяння суттєвої шкоди цілісності та цінності інформації внаслідок впливу ззовні. Цей показник доцільно назвати індексом небезпеки інформації, який у співставленні з масштабом небезпеки інформації дає змогу за наявності певного критерію, визначати рівень небезпеки інформації.

4. Індекси небезпеки інформації і безпеки інформації є ймовірностями протилежних подій, які, за визначенням, є несумісними і утворюють повну групу, тобто:

$$P_{НБІ} = 1 - P_{БІ} . \qquad (2.11)$$

Рівняння (2.11) дає змогу стверджувати про можливість застосувань єдиного методичного підходу до оцінки індексів небезпеки інформації і безпеки інформації.

5. Зважаючи на неминучі похибки, внаслідок неточності вихідних даних, кількісна оцінка індексу безпеки інформації сама по собі не може мати переважного значення. Більш важливим є інше: математичне моделювання індексу безпеки інформації має не тільки практичну, але й прогностичну

цінність. Оперуючи значеннями змінних величин, що входять до математичних залежностей для обчислення індексу безпеки інформації, можна оцінювати ефективність впровадження тих чи інших заходів, спрямованих на його зниження. Тому функціональна залежність між індексом безпеки інформації і значеннями часткових показників обставин навколо інформації може бути інструментом поглибленого дослідження проблеми безпеки інформаційної сфери.

Розглянута модель дозволяє ввести узагальнені кількісні характеристики захищеності інформаційних об'єктів. В якості таких узагальнених кількісних характеристик захищеності пропонується розглядати:

1. Імовірність порушення функціональних властивостей захищеного ресурсу через необхідні для їх забезпечення імовірнісні характеристики складових засобів захисту;

2. Час затримки у використанні ресурсів автоматизованої системи авторизованими користувачами з використанням засобів захисту в порівнянні з випадком, коли такі засоби відсутні.

Першу з цих кількісних характеристик - імовірність порушення функціональних властивостей захищеного ресурсу - можна ввести наступним чином.

З розглянутих моделей випливає, що порушення функціональних властивостей захищеної системи можливе, якщо порушено хоча б одну з них (або конфіденційність з імовірністю Q_C, або цілісність з імовірністю Q_I, або доступність з імовірністю Q_A). При цьому для оцінки імовірності порушення функціональних властивостей захищеної системи P_{VF} можна використовувати вираз:

$$P_{VF} = 1-(1-Q_C)(1-Q_I)(1-Q_A) \qquad (2.12)$$

Однак, нескладно отримати точніший, на погляд автора, вираз для розрахунку оцінки імовірності порушення функціональних властивостей захищеної системи P_{VF}, ніж вираз (4.12)

$$P_{VF} = 1-(1-P_2)(1-\mathrm{P}_3)(1-P_4)(1-Q_A) \qquad (2.13)$$

змінні P_2, P_3, P_4 визначені у попередніх підрозділах.

Друга з кількісних характеристик - час затримки у використанні ресурсів автоматизованої системи авторизованими користувачами при використанні засобів захисту, у порівнянні з випадком, коли такі засоби відсутні, потребує оцінок витрат часового ресурсу на підтримку функціонування власне засобів захисту та оцінок можливих затрат часового ресурсу при завантаженні системи обробкою інформації в умовах впливу завад та генерації порушниками безперервних запитів, спроб підбору паролів тощо. Тобто таку величину можна визначити як різницю між витратами часового ресурсу на підтримку функціонування власне засобів захисту t_{mp} та затратами часового ресурсу t_{cq} на обробку впливу завад, безперервних запитів, спроб підбору паролей тощо.

Система захисту буде ефективною, а її використання доцільним, якщо їх різниця – це час затримки у використання ресурсів, а саме:

$$\Delta t = t_{mp} - t_{cq} \le 0\,,$$

є не позитивною, тобто не перевищує нуль.

Витрати часового ресурсу на підтримку функціонування власне засобів захисту t_{mp} визначаються кількісним складом цих засобів, та часом виконання кожного з них під час реалізації своїх функцій та можуть бути визначеними або шляхом розрахунків, або фактичними випробовуваннями.

Витрати часового ресурсу t_{cq} на обробку впливу завад, безперервних запитів, спроб підбору паролів тощо можна оцінити, якщо відома середня

сумарна інтенсивність S_Σ потоку цих впливів (завад, безперервних запитів, спроб підбору паролів тощо) та часові витрати на обробку кожного з таких впливів. У більшості випадків можливим є перехід від часових характеристик, в цьому випадку від часу затримки у використанні ресурсу (або у доставці інформації) $\Delta t = t_{mp} - t_{cq}$, до імовірності, наприклад до імовірності P_T того, що математичне очікування часу функціонування власне засобів захисту t_{mp} не перевищить час обробки впливу завад, безперервних запитів, спроб підбору паролів тощо t_{cq}, тобто до імовірності $P_T = P(t_{mp} \le t_{cq})$.

Отже, узагальненою кількісною характеристикою захищеності може бути лише імовірність порушення функціональних властивостей захищеного ресурсу або зворотна до неї - імовірність її забезпечення. Зрозуміло, що подія, яка полягає у тому, що ресурс є захищеним, складається з подій, котрі полягають у тому, що, по-перше, функціональні властивості захищеності системи не порушені з імовірністю ($1-P_{VF}$), та, по-друге, математичне очікування часу затримки у доступі до ресурсу не перевищує допустимого (завідомо визначеного) значення з імовірністю цієї події P_T.

Тоді загальну імовірність P_{GA} порушення функціональних властивостей захищеного ресурсу можна визначити з виразу

$$P_{GA} = 1 - P_{VF}(1 - P_T).$$

Умови економічної доцільності застосування системи технічного захисту або окремих її компонентів, або, по можливості, економічні втрати на впровадження та використання засобів захисту або окремих її компонентів розглянуто раніше.

Таким чином, небезпечний характер інформаційних впливів і загроз інформаційній безпеці робить визначення рівня її принциповим аспектом зміцнення національної, регіональної, особистої та міжнародної безпеки і стратегічної стабільності, а в наслідок цього – окремим напрямом у середині і зовнішньополітичній діяльності всіх держав, які прагнуть інтегруватися в

глобальне інформаційне суспільство та сферу, роль яких у міру розвитку буде мабуть, тільки зростати.

Загальна схема оцінки рівня інформаційної безпеки відображена на рис. 2.2. Кожний з етапів оцінки має конкретний зміст, який у сукупності визначає порядок дій та визначення рівня інформаційної безпеки.

I. Загальна оцінка стану стабільності у суспільстві

1. Вихідні дані:

- наявність, характер і кількісний вимір спонукального мотиву формаційного впливу *(Q)*;
- можливі втрати нападаючої сторони *(D);*
- коефіцієнт експансії з боку потенційного нападника *(K_{ex});*
- величини інформаційних потенціалів протидії сторін;
- співвідношення сторін *(Z).*

2. Можливі висновки:

щодо рівня стабільності у суспільстві:

- баланс сил та інтересів ($K_{ex}\approx 0, Z\approx 1$);
- стабільність на основі балансу інтересів ($K_{ex}\approx 0, 0<Z\neq 1$);
- стабільність на основі балансу сил ($0<K_{ex}<1, Z\approx 1$);
- відносна стабільність на основі врегулювання ($K_{ex}<1, Z>1$);
- відносна стабільність на основі стимулювання ($K_{ex}>1, Z<1$);
- нестабільність на основі дисбалансу сил та інтересів ($K_{ex}>1{,}5, Z\geq 1{,}5$);

щодо наявності і характеру небезпеки інформації:

- відсутність вираженої небезпеки інформації (баланс сил та інтересів, стабільність на основі балансу інтересів);
- потенційна небезпека інформації;
- реальна небезпека інформації;

- загроза інформації, безпосередня загроза інформації; оцінка потенційного нападника як супротивника:

- евентуальний супротивник (відсутність вираженої і інформаційної небезпеки);

- потенційний інформаційний супротивник (потенційна інформаційна небезпека);

- імовірний інформаційний супротивник;

- конкретний інформаційний супротивник.

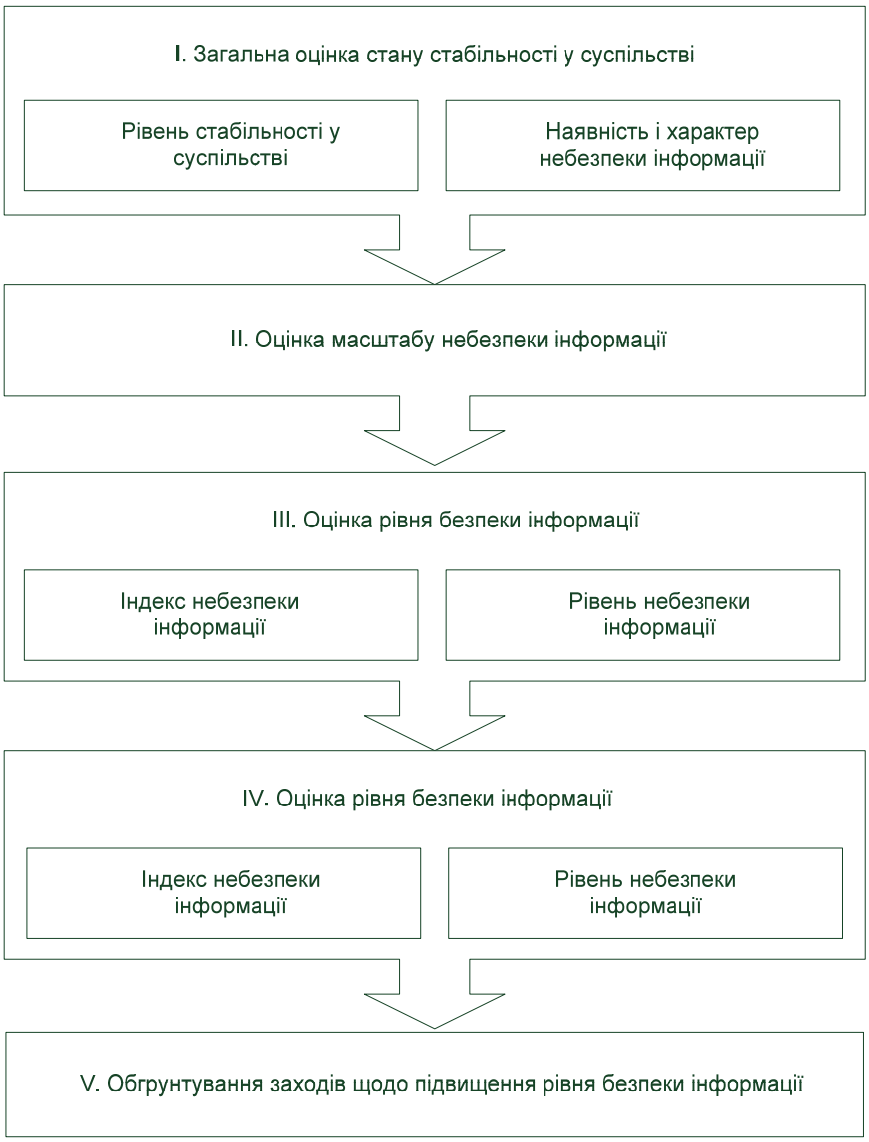


Рис. 2.2. Загальна схема оцінки рівня безпеки інформації

II. Оцінка масштабу небезпеки інформації

1. Вихідні дані:

- висновки за етапом I;
- просторовий розмах можливого впливу на інформацію (S_a).

2. Можливі висновки:

щодо масштабу небезпеки інформації (M_{ID});

- локальні;
- регіональні;
- глобальні;

щодо масштабу інформаційної безпеки:

- локальні *(M_{IS}<1%);*
- регіональні *(1%<M_{IS}<10%);*
- глобальні *(M_{IS}>10%).*

III. Оцінка рівня безпеки інформації

1. Вихідні дані - висновки за етапами I та II.
2. Можливі висновки:

- щодо імовірності інформаційної безпеки *(P_{IS}=0….1,0);*
- щодо імовірності не відбиття інформаційного впливу *(P_{NREF}=0....1,0);*
- щодо чисельного значення індексу інформаційної небезпеки *(P_{ID}=0….1,0);*

щодо рівня інформаційної небезпеки:

- низький;
- підвищений;
- критичний.

IV. Оцінка рівня безпеки інформації

1. Вихідні дані - висновки за етапами I - III.
2. Можливі висновки:

- щодо імовірності відвертання інформаційного впливу *(P_{DIV}=0....1,0);*
- щодо імовірності відбиття інформаційної атаки *(P_{REF}=0....1,0);*
- щодо чисельного значення індексу інформаційної безпеки *($P_{IS}=1-P_{ID}$);*

щодо рівня інформаційної безпеки:

- задовільний;
- нестійкий;
- критичний.

V. Обґрунтування заходів, спрямованих на підвищення рівня безпеки інформації.

1. Вихідні дані - висновки за етапами I - IV.
2. Основні напрямки:

- стабілізація рівня в суспільстві;
- підвищення ефективності стримування потенційного нападника;
- підвищення можливості щодо відбиття інформаційного впливу, який передбачається.

Викладений підхід стосується ситуації, коли розглядається лише один можливий напрям інформаційної небезпеки.

Якщо інформаційна небезпека походить від декількох зловмисників, то залежно від конкретних обставин можуть бути використані способи визначення рівня інформаційної небезпеки.

Варіант 1: інформаційна небезпека походить одночасно від двох або більше зловмисників, які утворюють коаліцію або злочинне угрупування.

Цей варіант припускає одночасний інформаційний вплив декількох зловмисників. Така група має розглядатися як єдина ворожа сила з єдиними інтересами. Тому підхід до визначення всієї сукупності характеристик інформаційної небезпеки в цій ситуації відрізняється від підходу, що використовується для оцінки двосторонніх відносин, лише тим, що інтереси і

можливості зловмисників необхідно належним чином узагальнювати та підсумовувати.

Варіант 2: інформаційна небезпека походить від двох або більше зловмисників, які не є союзниками. Якщо одночасно інформаційний вплив цих зловмисників виключена або малоймовірна, то слід оцінювати рівень інформаційної небезпеки за найбільш небезпечним напрямком; якщо одночасна інформаційна атака не виключається, то рівень інформаційної небезпеки слід оцінювати за варіантом 3.

Варіант 3: інформаційна небезпека походить від декількох зловмисників, інтереси та дії яких можуть збігатися за часом, тобто не виключена одночасний вплив цих зловмисників.

За такої ситуації оцінка інформаційної небезпеки з боку кожного із цих зловмисників здійснюється з урахуванням можливості їх одночасного впливу, внаслідок чого можна очікувати зменшення величини програшу та збільшення величини співвідношення сил за рахунок роздроблення сил захисту інформації - об'єкта впливу за декількома напрямками. Одержані в результаті такої оцінки значення індексів інформаційної небезпеки та масштабу інформаційної небезпеки узагальнюються таким чином:

а) для двох напрямів інформаційної небезпеки (позначимо їх цифрами 1 і 2) загальний індекс інформаційної небезпеки визначається за формулою:

$$P_{ID\Sigma} = P_{ID1} + P_{ID2} - P_{ID1} \times P_{ID2} \tag{2.14}$$

а загальний масштаб очікуваної інформаційної атаки за формулою

$$M_{ID\Sigma} = M_{ID1} + M_{ID2} \tag{2.15}$$

б) для трьох напрямів інформаційної небезпеки

$$\begin{aligned} P_{ID\Sigma} = {} & P_{ID1} + P_{ID2} + P_{ID3} - P_{ID1} \times P_{ID2} - P_{ID3} \times \\ & \times P_{ID1} - P_{ID1} \times P_{ID3} + P_{ID1} \times P_{ID2} \times P_{ID3} \end{aligned} \tag{2.16}$$

$$M_{ID\Sigma} = M_{ID1} + M_{ID2} + M_{ID3} \qquad (2.17)$$

Очевидно, що величина M_{ID} за своїм фізичним змістом не може перевищувати одиницю і тому, якщо одержане за формулами (2.15) або (2.17) значення $M_{ID\Sigma}$ внаслідок похибок більше за одиницю, слід вважати його таким, що дорівнює одиниці.

На основі розрахованих індексів і масштабу інформаційної небезпеки визначення рівня інформаційної безпеки в разі багатосторонніх відносин здійснюється за такою ж методикою, як і в разі двосторонніх відносин.

Вибір та обґрунтування заходів, спрямованих на підвищення рівня інформаційної безпеки, здійснюється з урахуванням накопиченого досвіду відтворення та припинення інформаційних атак.

При цьому заходи, спрямовані на підвищення рівня захищеності інформаційних систем, як правило, мають комплексний характер, оскільки охоплюють одночасно багато сфер діяльності як самої системи, так і навколо неї. При цьому кожна конкретна ситуація потребує своїх пріоритетів у формуванні політики безпеки. Визначення цих пріоритетів є складним і відповідальним завданням політики забезпечення інформаційної безпеки, оскільки можливі помилки здатні призвести до безрезультативності зусиль, що докладаються, та (або) до нераціональних витрат, які при цьому здійснюються. Вихідні аксіометричні положення, на основі яких доцільно вирішувати це завдання, можна сформулювати так:

- визначення основних напрямів забезпечення інформаційної безпеки має здійснюватися в інтересах найбільшої ефективності заходів, що вживаються при мінімальних витратах часових, фінансових, матеріальних і людських ресурсів;
- головним стратегічним напрямом запобігання масованого впливу (атаці) в будь-якій ситуації є запобігання або передбачення її, яке, в свою чергу, є найбільш ефективним шляхом врегулювання;
- заходи, спрямовані на активне відбиття або відбиття впливу та на

підготовку до цього відбиття, є найбільш витратними і можуть у деяких випадках форсувати загострення впливів.

Як вже було визначено у [29], цільовою функцією уразливості ІС може бути індекс інформаційної безпеки (ІІБ). Способи визначення величин, які визначені у [69] для обчислення індексу інформаційної безпеки, можуть бути різними.

Першим кроком до розвитку ІІБ має бути визначення індексу інформаційної небезпеки (ІІН) як імовірність заподіяння суттєвої шкоди інформації. Важливу роль у визначенні ІІН відіграє врахування можливостей носія інформації та самої інформації – об'єкта потенційного впливу щодо його отримування та відбуття.

Таким чином, спираючись на міркування, наведені у [21], розрахунок ІІН у взаємовідносинах двох суб'єктів (визначимо їх як сторони *A* і *B*) можна звести до визначення імовірності прийняття потенційного зловмисника (визначимо його як сторона *A*) рішення про здійснення впливу того чи іншого масштабу проти сторони *B* та імовірності успіху атаки за умов конкретних можливостей сторони *B* щодо її відбиття або відвернення.

З урахуванням досліджень, проведених у [39] та підходу до оцінки ситуації наявного об'єкту, головними показниками такої оцінки можуть бути:

- співвідношення "виграш-програш" для сторони *A*, тобто величина $K_{вх}^{AB}$;
- співвідношення сил сторін, тобто величина Θ^{AB}.

На підставі цих висновків, а також з урахуванням об'єктивних та суб'єктивних факторів, рішення сторони *A* про початок атаки на інформацію сторони *B* може бути прийняте або не прийняте. Певний вплив на це рішення буде чинним, зокрема рівень підготовки та готовність сторони *A* до позитивного сприйняття такого кроку стосовно сторони *B*.

Таким чином, рішення про вплив слід вважати подією, імовірність настання якого на прогнозований час визначається, головним чином, переліченими раніше факторами і умовами. Цю імовірність можна

ототожнити з імовірністю впливу, який в [21] позначимо через P_{AT}. Оскільки здійснення впливу такого відвернення згідно з [21] випливає, що

$$P_{AT} = 1 - P_{DIV} = (1 - P_{PAS})(1 - P_{ACT}), \quad (2.18)$$

де P_{AT} - імовірність протидії впливу на інформацію;

P_{DIV} - імовірність відвернення впливу на інформацію;

P_{PAS} - імовірність пасивного відвернення;

P_{ACT} - імовірність активного відвернення впливу на інформацію.

Розгляд виразу (2.18) з точки зору залежності співмножників, що входять до його правої частини, дозволяє зробити такі висновки:

по-перше, відвернення впливу зводиться по суті до зменшення величини, тобто до наближення, наскільки це можливо до балансу інтересів сторін *A* і *B*;

по-друге, активне відвернення можливого впливу, так само як і його відбиття, досягається головним чином, шляхом забезпечення відповідного співвідношення сил з урахуванням очікуваного впливу.

Відповідно до [21,69], у разі вирішення задач з ризиком особа, яка приймає рішення (ОПР), створює власне евристичне уявлення про задачу як список факторів (вимірів), що включає величину виграшу, величину програшу, імовірність програшу та рівень ризику. Рішення, відповідно до [69,76], є функцією двох основних змінних величин: величини виграшу (ВВ) та ризику (R). У результаті проведених досліджень встановлено, що під час оцінювання ризику беруть до уваги, головним чином, величину програшу (ВП) та суб'єктивну імовірність програшу (СІП). Для умов визначених в [69,76] досліджень емпірична залежність для оцінки величин ризику визначається рівнянням

$$R=3,12(СІП)+\lg(ВП). \quad (2.19)$$

Відповідно до [29,69], рівняння (2.19) має велику прогнозуючу цінність. Коефіцієнт кореляції між оцінками, отриманими за допомогою (2.19), та оцінки автора складає біля 0,98, що свідчить про високу точність прогнозу. Відповідь на запитання про те, як сполучення величин виграшу ВВ та ризику R впливає на відсоток, який приймає запропоновані умови виграшу та ступінь ризику, дає рівняння регресії за [21,69,76]

$$D(\%)=1{,}45(BB)-49{,}1(R)+140, \qquad (2.20)$$

яке отримано за підсумками проведених досліджень. При цьому коефіцієнт кореляції між оцінками, одержаними за допомогою рівняння (2.20) та даними досліджень, склав 0,9, що також є доказом високої збіжності.

На рис. 2.3 та 2.4 наведені розраховані за виразами (2.19) та (2.20) графіки.

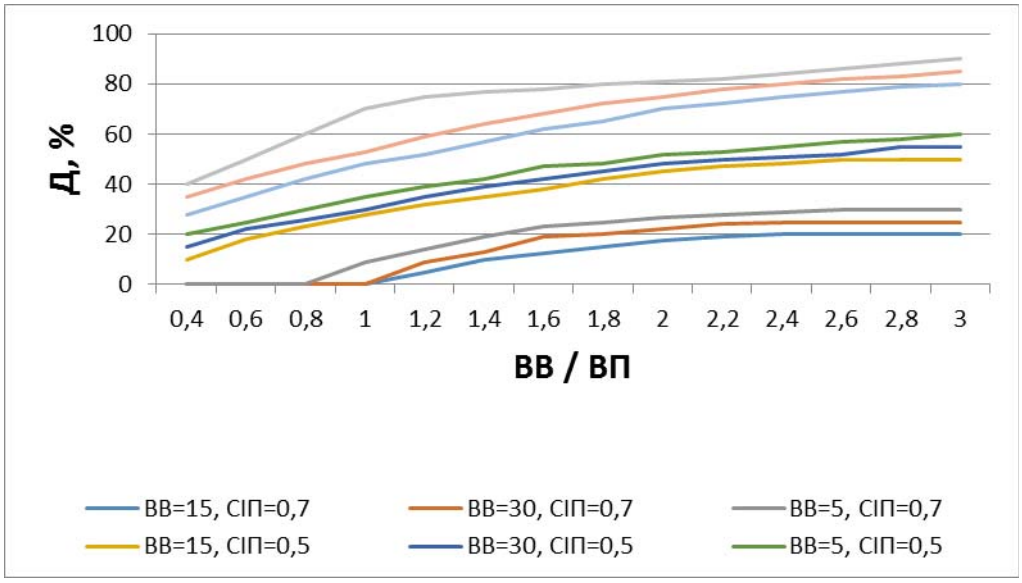


Рис. 2.3. Залежність прийняття альтернатив від абсолютних значень виграшу та програшу для різних значень суб'єктивної імовірності виграшу

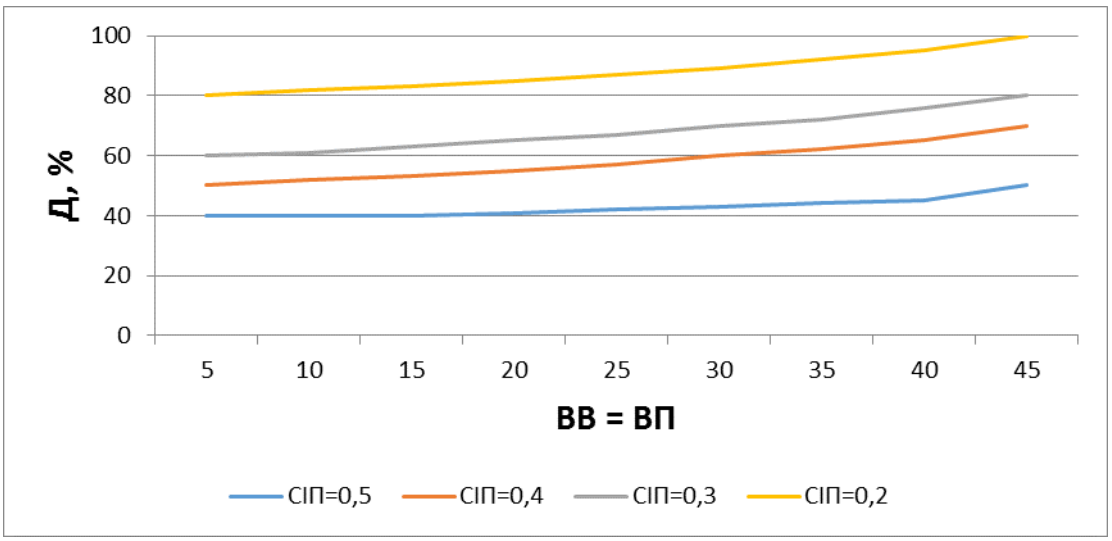


Рис. 2.4. Залежність прийняття альтернатив від абсолютних значень виграшу та програшу для різних значень суб'єктивної імовірності виграшу

2.2. Метод оцінки впливів на ресурси ІС

Розробка політики інформаційної безпеки (ПІБ) – це питання не тривіальне. Від ретельності її опрацювання залежатиме дієвість решти всіх рівнів забезпечення ІБ – процедурного і програмно-технічного. Складність розробки ПІБ визначається проблематичністю використання чужого досвіду, оскільки ПІБ ґрунтується на виробничих ресурсах і функціональних залежностях усередині об’єкта [21].

Необхідність розробки ПІБ пояснюється необхідністю формування основ планування і управління ІБ. Мета розробки ПІБ – мінімізація ризиків бізнесу шляхом захисту інтересів об’єктів в інформаційній сфері, планування і підтримка безперервності функціонування, зниження витрат і підвищення ефективності інвестицій в захист інформації.

ПІБ містить вимоги до персоналу та технічних служб. Основні напрями розробки політики безпеки [21]:

- визначення, які данні і наскільки серйозно необхідно захищати;
- визначення, хто і який збиток може завдати об’єкту в інформаційному аспекті;

- оцінки ризиків і визначення схеми зменшення їх до прийнятної величини.

Для досягнення цієї мети, варто відштовхуватися від стандартних канонів розробки ПІБ, але й, звичайно ж, враховувати специфіку конкретного об’єкта [39].

По-перше, необхідно прийняти до уваги цілі й основні напрямки діяльності об’єкта (на різних об’єктах установлюються різні вимоги до конфіденційності).

По-друге, політика, яка розробляється, повинна узгоджуватися з існуючими законами, ДСТУ, НД ТЗІ і внутрішньооб’єктовими правилами (тому що, найчастіше, локальна мережа об’єкта не є ізольованою, а має вихід у Internet). ПІБ повинна висвітлювати проблеми, що виникають на локальному комп’ютері через дії віддаленої сторони, а також віддалені проблеми, причиною яких є користувач або зловмисник.

Сукупність керівних принципів, правил, процедури фактичних прийомів, якими об’єкт керується в своїй діяльності складає ПІБ об’єкта.

Сукупність правил, які регулюють керування ресурсами, їх захист та розподіл всередині об’єкту, що захищається, та які виражаються за допомогою функціональних вимог безпеки, складає політику безпеки об’єкту.

ПІБ потенційно впливає на роботу всіх користувачів комп’ютерів на об’єкті, причому по декількох аспектах. Якщо ж такий документ (політика інформаційної безпеки об’єкта) передбачається розробляти і втілювати в життя не власними силами, а за допомогою фахівців ззовні, то потрібно, щоб були враховані наступні п’ять критеріїв оцінки політики [21,39]:

- чи узгоджується ПІБ з існуючим законодавством і обов’язками по відношенню до третіх сторін;
- чи не обмежуються без потреби інтереси працівників, роботодавців чи третіх сторін;
- чи реалістична політика й чи ймовірне її втілення в життя;

- чи зачіпає політика всі види передачі і збереження інформації, які використовуються в об’єкті;

- чи оголошена політика заздалегідь і чи одержала вона схвалення всіх зацікавлених сторін.

Одним з головних спонукальних мотивів розробки ПІБ об’єкта полягає в одержанні впевненості, що діяльність по захисту інформації побудована економічно і технічно виправданим образом. Дане положення здається очевидним, але, взагалі, можливі ситуації, коли зусилля прикладаються не там, де потрібно. Наприклад, основною задачею систем захисту інформації припускають захист від зовнішнього зловмисника, а напади в більшості випадків створюються внутрішніми порушеннями.

Політика звичайно складається з двох частин [63]: загальних принципів і конкретних правил роботи.

Загальні принципи визначають підхід до безпеки в Internet, правила регламентують – що дозволено і що заборонено (правила можуть доповнюватися конкретними процедурами і посібниками).

Звичайна політика безпеки регламентує використання основних сервісів мережі і доводить до відома користувачів мережі про їхні права доступу, що і є процедурою аутентифікації користувачів.

ІС об’єкта захисту можна вважати захищеною, якщо всі операції виконуються у відповідності зі строго визначеними правилами (див. рис.2.5), що забезпечують безпосередній захист об’єктів, ресурсів і операцій.

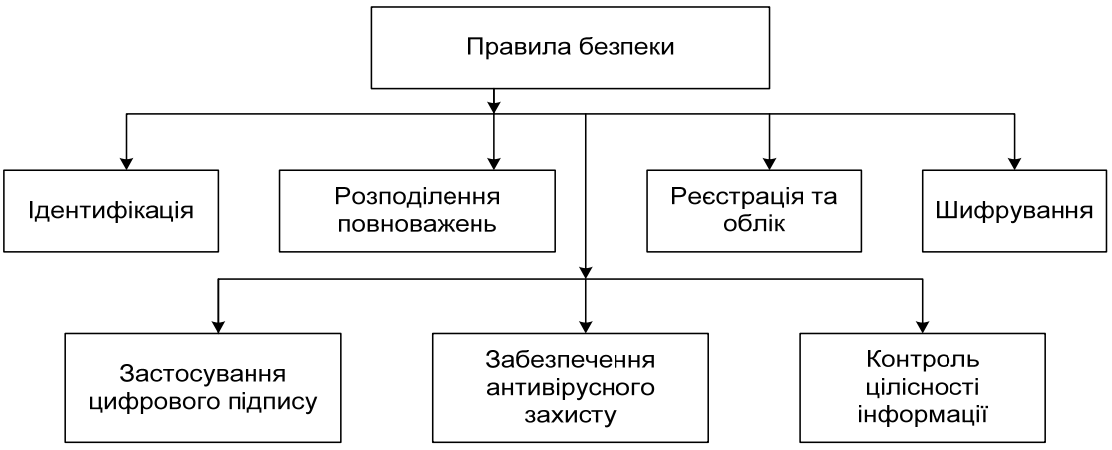


Рис.2.5. Основні правила забезпечення політики безпеки в ІС

Основу для формування вимог до захисту складає список загроз. Коли такі вимоги відомі, можуть бути визначені відповідні правила забезпечення захисту, що визначають необхідні функції і засоби захисту. Чим суворіші вимоги до захисту і більше відповідних правил, тим ефективніші її механізми і тим більше захищеною виявляється інформаційна система.

Таким чином, визначаємо, що захист інформації на інформаційному об'єкті – комп'ютерній мережі, буде ефективною в тому випадку, коли проектування та реалізація системи захисту інформаційного об'єкта відбувається по наступних етапа

1) аналіз ризиків; х [21]:
2) реалізація політики безпеки;
3) підтримка політики безпеки.

Процес аналізу інформаційних ризиків містить в собі визначення того, що варто захищати, від чого захищати і як це робити. Необхідно розглянути всі можливі ризики і ранжувати їх в залежності від потенційного розміру збитку. Цей процес складається з безлічі економічних рішень. Давно визначено, що витрати на захист не повинні перевищувати вартості інформації, що захищається (об'єкта інформації).

Процес аналізу ризиків розділимо на два етапи [63]: ідентифікація активів та ідентифікація загроз. Розглянемо більш докладніше ці етапи.

1. *Ідентифікація активів*. Це один з етапів аналізу ризиків і складається з ідентифікації всіх об'єктів, що потребують захисту. Необхідно прийняти до уваги все, що може постраждати від порушення режиму безпеки. Тому необхідно з початку класифікувати активи:

- апаратура: процесори, модулі, клавіатури, термінали, робочі станції, персональні комп'ютери, принтери, дисководи, мережі зв'язку, термінальні сервери, маршрутизатори;
- програмне забезпечення, вихідні тексти, об'єктні модулі, утиліти, діагностичні та комунікаційні програми, операційні системи;

- дані (інформація) безпосередньо доступні, архівовані, оброблювані, збережені у вигляді резервної копії, реєстраційні журнали, бази даних, що передаються по комунікаційних мережах;
- люди: користувачі, обслуговуючий персонал;
- документація: по програмах, по апаратурі, системна, по адміністративних процедурах;
- випадкові матеріали: папір, форми, фарбуючи стрічки, магнітні носії.

2. *Ідентифікація загроз*. Після того, як були виявлені активи, що потребують захисту, необхідно ідентифікувати загрози цим активам і розміри можливого збитку та втрат. Це допоможе зрозуміти, яких загроз ватро побоюватися більше всього.

Типова загроза від впливу для більшості об'єктів інформаційного захисту – це несанкціонований доступ до інформації на об'єкті, що захищається, може приймати різні форми. Ступінь важливості проблеми несанкціонованого доступу для різних об'єктів різна.

Несанкціоноване (нелегальне) ознайомлення з інформацією – друга розповсюджена загроза від впливу. Дуже важливо правильно визначити ступінь конфіденційності інформації, що зберігається в ІС об'єкта.

Відмовлення в обслуговуванні порушують цілісність системи і виникають по різних причинах, і виявляються по-різному. Мережа може прийти в непрацездатний стан від підробленого пакета, від перевантаження чи через відмовлення компонента. Вірус здатний сповільнити чи паралізувати роботу інформаційної системи.

При розробці ПІБ необхідно дати відповіді на ряд питань:
- хто має право використовувати ресурси;
- як правильно використовувати ресурси;
- хто наділений правом давати привілеї і дозволяти використання;
- хто може мати адміністративні привілеї;
- які права й обов'язки користувачів;

- які права й обов’язки системних адміністраторів стосовно звичайних користувачів;
- як працювати з конфіденційною інформацією.

Власне, організаційна ПІБ описує порядок надання і використання прав доступу користувачів, а також вимоги звітності користувачів за свої дії в питаннях безпеки.

Для інформаційних мереж можна виділити наступні ймовірні загрози, які необхідно враховувати при визначенні ПІБ: випадкові та навмисно створювані загрози.

Розглянемо послідовно ці загрози.

До випадкових загроз можна віднести:

- помилки обслуговуючого персоналу та користувачів;
- втрата чи руйнування інформації, обумовлені неправильним збереженням архівних даних на магнітних носіях;
- випадкове знищення чи зміна даних;
- збої устаткування електроживлення;
- збої кабельної системи;
- перебої в електроживленні;
- збої апаратури запису та зйому інформації;
- збої системи архівування даних;
- збої роботи серверів, робочих станцій, мережевих карт і т.п.;
- руйнування файлових структур через некоректну роботу чи програми апаратних засобів;
- зміна даних при помилках у програмному забезпеченні;
- зараження системи вірусами;
- несанкціонований доступ;
- випадкове ознайомлення з конфіденційною інформацією сторонніх осіб.

До випадкових (ненавмисних) загроз мають відношення також випадки руйнації, втрати або зміни даних, конфіденційної інформації або ресурсів під

час природних катаклізмів, які не підвладні людині (пожари, землетруси, повені, магнітні бурі та радіоактивні випромінювання).

А до навмисно створених загроз слід відносити такі:

- ознайомлення працівників з інформацією, до якої вони не повинні мати доступу;
- несанкціонований доступ сторонніх осіб, що не належать до числа працівників, до конфіденційної інформації і мережевих ресурсів;
- розкриття і модифікація інформації і програм;
- копіювання інформації і програм;
- розкриття чи модифікація або підміна трафіку передачі інформації по мережі;
- розробка і поширення комп'ютерних вірусів;
- введення в програмне забезпечення логічних бомб;
- крадіжка магнітних та паперових носіїв, що містять конфіденційну інформацію;
- крадіжка розрахункових документів;
- крадіжка устаткування та апаратури;
- руйнування архівної інформації або навмисне її знищення;
- фальсифікація повідомлень, переданих по каналах зв'язку;
- відмовлення від авторства повідомлення, переданого по каналах зв'язку;
- відмовлення від факту одержання інформації;
- нав'язування раніше переданого повідомлення;
- перехоплення й ознайомлення з інформацією, що передана по каналах зв'язку і т.п.

Головною метою діяльності в області інформаційної безпеки є забезпечення властивостей кожного активу:

- доступності (можливість користування деякими ресурсами інформаційної системи й інформацією в довільний момент);

- конфіденційності (недоступність інформації чи сервісів для користувачів, яким апріорно не надана можливість використання зазначених сервісів або інформації);
- цілісності (незалежність властивостей інформації і ресурсів у будь-який момент часу від моменту їх появи чи введення у систему);
- ймовірності (збереження інформацією своїх семантичних властивостей у будь-який момент часу від моменту введення в систему).

При аналізі загроз варто брати до уваги їхній вплив на активи по чотирьох названих напрямках.

На підставі вище зазначеного розроблений зразковий алгоритм роботи по оцінці інформаційних ризиків (див. рис. 2.6).

Оцінка ймовірності появи вище перерахованих ймовірних загроз і очікування розмірів втрат – складний і тривалий процес, але коректно визначити вимоги до системи захисту об’єкта ще складніше, тому ПІБ повинна визначатися наступними мірами:

- ідентифікація користувачів;
- перевірка дійсності та контроль доступу користувачів до об’єкту, що захищається, у приміщення, до ресурсів ІС;
- поділ повноважень користувачів, що мають доступ до обчислювальних ресурсів;
- реєстрація та облік роботи користувачів;
- реєстрація спроб порушення повноважень;
- шифрування або кодування конфіденційної інформації на основі криптографічних алгоритмів високої стійкості;
- застосування цифрового підпису для передачі інформації по каналах зв’язку;
- забезпечення антивірусного захисту та відновлення інформації, зруйнованої вірусними впливами;
- контроль цілісності програмних засобів та інформації, що обробляється;

- відновлення зруйнованої архівної інформації, навіть при значних втратах;
- наявність адміністратора захисту інформації в системі;
- розробка та дотримання необхідних організаційних мір;
- застосування технічних засобів, що забезпечують безперебійну роботу устаткування.

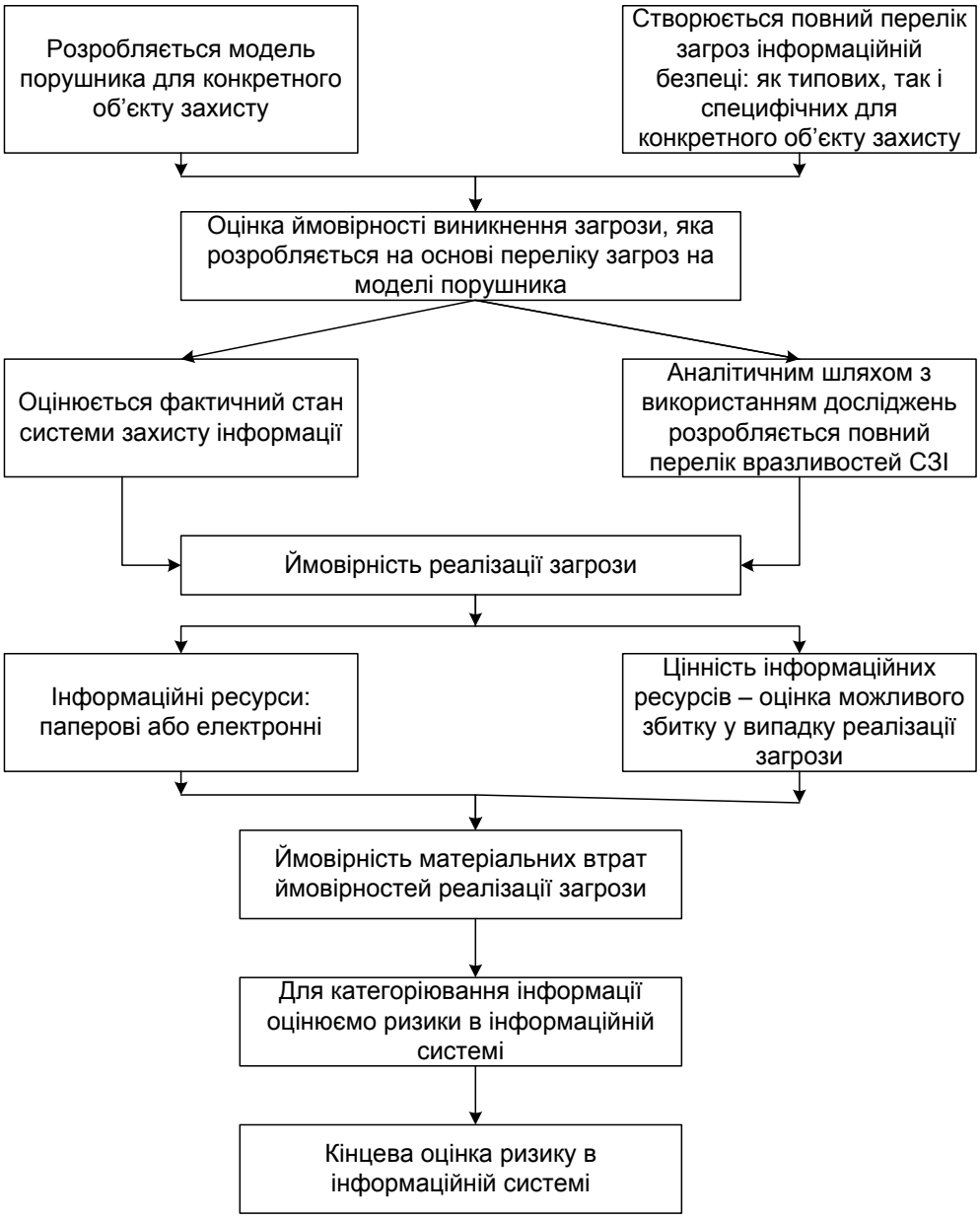


Рис.2.6. Алгоритм роботи з оцінки ризиків в ІС

Реалізація ПІБ об'єкта починається з проведення розрахунку фінансових втрат і вибору відповідних засобів для виконання цих задач. При цьому необхідно врахувати такі фактори як безконфліктність роботи обраних засобів, репутація постачальників засобів захисту, можливість одержання

повної інформації про механізми захисту і надані гарантії. Також варто враховувати основні положення по безпеці інформації:

- економічна ефективність – вартість засобів захисту повинна бути менше, ніж розміри можливого збитку;
- кожен користувач повинний мати мінімальний набір привілеїв, необхідний при роботі;
- простота системи захисту об’єкта – захист буде тим більше ефективний, чим легше користувачу з ним працювати;
- відключення захисту при нормальному функціонуванні – захист не повинен відключатися, за винятком особливих випадків, коли співробітник із спеціальними повноваженнями може мати можливість відключити систему захисту;
- відкритість проектування і функціонування механізму захисту (для можливості адекватного реагування обслуговуючого персоналу на виникнення збоїв у системі);
- незалежність системи захисту від суб’єктів захисту – розроблювачами не повинні бути ті, кого вона буде контролювати;
- загальний контроль без яких-небудь виключень з безлічі контрольованих суб’єктів;
- звітність і підконтрольність системи захисту;
- відповідальність осіб, що займаються інформаційною безпекою;
- об’єкти захисту доцільно розділити на групи так, щоб порушення захисту в одній групі не впливало на безпеку інших груп;
- відмова від замовчування – при збої засобів захисту доступ до обчислювальних ресурсів повинен бути заборонений;
- система захисту об’єкту повинна бути цілком специфікована, протестована та погоджена;
- система повинна допускати зміну своїх параметрів адміністратором;

- важливі критичні рішення повинні прийматися людиною, а не комп’ютером;
- система захисту об’єкта повинна проектуватися в розрахунку на вороже оточення і припускати, що користувачі мають найгірші наміри, будуть робити помилки і шукати шляхи обходу механізмів захисту;
- інформація про існування механізмів захисту повинна бути, по можливості, схована від користувачів, робота яких контролюється.

При підтримці ПІБ потрібно постійне спостереження за вторгненнями зловмисників, які відбуваються, у мережу, виявлення вад і "дір" у системі захисту об’єкта інформації, обліку випадків несанкціонованого доступу до конфіденційних даних.

При цьому основна відповідальність за підтримку ПІБ мережі (об’єкта інформації) лежить на системному адміністраторі, що повинен оперативно реагувати на всі випадки злому конкретної системи захисту, аналізувати їх і використовувати необхідні апаратні та програмні засоби захисту з урахуванням максимальної економії фінансових засобів.

Очевидно, що будь-яка офіційна політика поза залежністю від її відношення до інформаційної безпеки, час від часу порушується. Порушення може бути наслідком недбалості користувачів, випадкової помилки, відсутності надійної та належної інформації про поточну політику чи її нерозуміння. Можливо, також, що деяка особа – група осіб свідомо роблять дії, що прямо суперечать затвердженій політиці безпеки.

Необхідно заздалегідь визначити характер дій, що починаються у випадку виявлення порушень ПІБ, щоб ці дії були швидкими й правильними. Варто організувати розслідування, щоб зрозуміти, як і чому порушення стало можливим. Після цього потрібно внести корективи в систему захисту. Тип і серйозність коректив залежить від типу порушення, яке сталося.

Політику безпеки можуть порушувати різні особи. Деякі з них є своїми, місцевими користувачами, інші – здійснюють напади ззовні. Корисно визначити самі поняття "свої" і "чужі," виходячи з адміністративних,

правових чи політичних положень. Ці положення окреслюють характер санкцій, які можна застосувати до порушника – від письмової догани до залучення до суду. Таким чином, послідовність відповідних дій залежить не тільки від типу порушення, але й від виду порушника; вона повинна бути продумана задовго до першого інциденту, хоча це і непросто.

Варто пам’ятати, що правильно організоване навчання – кращий захист. Керівництво об’єкта, що захищає свою конфіденційну інформацію, зобов’язано поставити справу так, щоб не тільки внутрішні, але і зовнішні легальні користувачі знали положення ПІБ об’єкта.

Проблеми з нелегальними користувачами, загалом, ті ж самі. Потрібно одержати відповіді на питання про те, як типи користувачів порушують політику, як і навіщо вони це роблять. У залежності від результатів розслідування можна просто закрити "діру" у системі захисту та задовольнитися отриманим уроком чи зволіти більш жорстокі міри.

Кожний об’єкт повинен заздалегідь визначити набір адміністративних санкцій, застосованих до місцевих користувачів, які порушують ПІБ сторонньої організації чи об’єкта. Крім того, необхідно подбати про захист від відповідних дій сторонньої організації. При розробці ПІБ варто враховувати всі юридичні положення, які застосовуються до подібних ситуацій.

Політика безпеки об’єкта повинна мати процедури для взаємодії з зовнішніми організаціями, у число яких входять правоохоронні органи, інші організації, команди "швидкого реагування", засобів масової інформації. У процедурах повинно бути визначено, хто має право на такі контакти, і як саме вони відбуваються.

Крім політичних положень, необхідно продумати й описати процедури, що виконуються у випадку виявлення порушень режиму безпеки. Для усіх видів порушень повинні бути заготовлені відповідні процедури.

Коли на об’єкт відбувається напад, що загрожує порушенням інформаційної безпеки, стратегія відповідних дій може будуватися під впливом двох протилежних підходів.

1. Якщо керівництво побоюється вразливості об’єкта, воно може віддати перевагу стратегії "захиститися і продовжити". Головною метою подібного підходу є захист інформаційних ресурсів і максимально швидке відновлення нормальної роботи користувачів. Діям порушника виявляється максимальна протидія, подальший доступ запобігається, після чого негайно починається процес оцінки нанесених ушкоджень і відновлення інформації. Можливо, при цьому прийдеться виключити комп’ютерну систему, закрити доступ до мережі чи почати інші жорсткі міри. Зворотній бік даної моделі полягає в тому, що поки зловмисник невиявлений, він може знову напасти на ту ж саму чи іншу організацію колишнім чи новим способом.

2. Інший підхід, "вистежити і засудити", спирається на інші філософію та систему цілей. Основна мета полягає в тому, щоб дозволити зловмиснику продовжувати свої дії, доки об’єкт не зможе встановити його особистість. Такий підхід подобається правоохоронним органам. Нажаль, ці органи не зможуть звільнити об’єкт від відповідальності, якщо користувачі звернуться до суду з позивом із приводу збитку, нанесеного їхнім програмам та інформації.

Відомо з [21,39], що в основу методики оцінки впливів на дані в ІС доцільно покласти методики побудови моделі зловмисника та аналізу загроз від впливів на ресурси ІС. Такі моделі створюються на підставі детального аналізу можливих загроз від впливів, способів та каналів їх реалізації. В свою чергу, моделі зловмисника та моделі впливів (загроз) ресурсам ІС є основою для подальшого проведення аналізу ризиків і формування вимог до системи протидії впливам [4-12].

У кожному конкретному випадку, виходячи з технології обробки інформації, розробляється модель зловмисника, яка має бути адекватна реальному зловмиснику для даної ІС. Слід враховувати, що модель

зловмисника – абстрактний формалізований або неформалізований опис дій зловмисника, який відображає його практичні та теоретичні можливості, апріорні знання, час та місце дії тощо. Для побудови цієї моделі рекомендується виконати аналіз та упорядкування наступної інформації.

Зловмисника слід розглядати як особу, яка прагне чи може одержати несанкціонований доступ до інформації, циркулюючого у ІС. При побудові моделі зловмисника слід враховувати, що особливістю ресурсів ІС, в першу чергу інформаційних, є їх принадливість для окремих осіб чи певних груп осіб, які з метою використання цих ресурсів прагнуть бути чи є користувачами інформації, що циркулює у ІС. Ця принадливість найчастіше є обумовленою характером та об'ємом інформації, яка вводиться , обробляється, зберігається та циркулює в ІС. Якщо та чи інша особа – користувач ресурсами ІС здійснює спробу несанкціонованого доступу до об'єктів захисту, то такий користувач є порушником.

По відношенню до ІС порушники можуть бути внутрішніми (з числа співробітників, користувачів системи) або зовнішніми (сторонні особи або будь-які особи, що знаходяться за межами контрольованої зони).

Модель зловмисника має визначати:

- категорії осіб, з числа яких може бути зловмисник;
- рівень можливостей зловмисника;
- припущення про кваліфікацію та можливий рівень знань зловмисника;
- методи і способи, що використовуються при здійсненні порушень;
- можливу мету зловмисника та її градацію за ступенями небезпечності для ІС;
- можливі місця здійснення порушень;
- можливі способи для здійснення загроз в ІС;
- припущення про характер дій зловмисника.

До категорій осіб, як можуть бути зловмисниками, слід відносити:

- суб’єктів інформаційної діяльності - працівників організації - власника ІС - внутрішніх зловмисників; для їх визначення слід детально розглянути можливості несанкціонованого доступу до ресурсів ІС кожного із працівників організації;

- сторонніх осіб, що отримують тим чи іншим шляхом доступ до ресурсів ІС – зовнішні зловмисники; для їх визначення слід детально розглянути їх можливості відвідувачів організації щодо несанкціонованого доступу до ресурсів ІС з урахуванням наявної системи організаційного обмеження їх доступу.

За рівнем можливостей, що надаються їм штатними засобами ІС, зловмисників доцільно класифікувати за чотирма рівнями можливостей. Класифікація є ієрархічною, тобто кожний наступний рівень включає в себе функціональні можливості попереднього:

- перший рівень визначає найнижчий рівень можливостей проведення діалогу з ІС – можливість запуску фіксованого набору програм (завдань), що реалізують заздалегідь передбачені функції обробки інформації;

- другий рівень визначається можливістю створення і запуску власних програм з новими функціями обробки інформації;

- третій рівень визначається можливістю управління функціонування ІС, тобто впливом на базове програмне забезпечення системи і а склад і конфігурацію її устаткування;

- четвертий рівень визначається всім обсягом можливостей осіб, що здійснюють проектування, реалізацію і ремонт апаратних компонентів ІС, аж до включення до складу ІС власних засобів з новими функціями обробки інформації.

Зрозуміло, що найбільш небезпечні зловмисники можуть знати:

1) склад, розміщення, функціональні особливості, умови та режими функціонування елементів ІС, включаючи траси прокладених чи можливих

ліній зв’язку комунікаційних мереж та трафіку відповідних каналів передачі даних;

2) порядок, засоби та режими здійснення охорони елементів ІС, місць їх розташування та прилеглої території;

3) порядок, засоби та режими здійснення організаційно-правових та технічних заходів захисту ресурсів ІС;

4) основні закономірності формування в ІС баз даних та потоків запитів до них.

За використовуваними методами і способами зловмисників можна класифікувати, як таких, що використовують:

- виключно агентурні методи одержання інформації;
- пасивні технічні засоби перехоплення інформаційних сигналів;
- способи і засоби активного впливу на ІС, що змінюють конфігурацію системи;
- виключно штатні засоби ІС або недоліки проектування КСЗІ для реалізації спроб НСД.

Така класифікація зловмисників є корисною для використання в процесі оцінки ризиків, аналізу вразливості системи, ефективності існуючих і планованих заходів захисту.

Також необхідно визначити, якими з можливих способів можуть здійснюватися загрози ІС:

- технічними каналами, що включають канали побічних електромагнітних випромінювань і наводок, акустичні, віброакустичні, акустоелектричні, оптичні, радіо- та радіотехнічні та інші канали;
- канали спеціального впливу шляхом формування полів і сигналів з метою руйнування системи захисту або порушення цілісності інформації;
- НСД шляхом підключення до апаратури та мереж зв’язку, маскування під зареєстрованого користувача, подолання заходів захисту з метою використання інформації або нав’язування хибної інформації,

застосування закладних пристроїв чи програм та вкорінення комп'ютерних вірусів.

За характером дій зловмисник може здійснювати як активні, так і пасивні загрози ресурсам ІС. Слід також враховувати, що порушення з боку цих осіб можуть бути як ненавмисними, так і зловмисними. Особливу небезпеку слід очікувати від зловмисних порушень. Ненавмисний порушник може здійснювати випадкові загрози ресурсам ІС під час виконання своїх функціональних обов'язків внаслідок помилкових дій, за рахунок неуважності чи недбалості.

Така класифікація дозволяє більш чітко визначити способи несанкціонованих дій зловмисника – перелік загроз ресурсам ІС та засобів, які потрібні для їх унеможливлення.

Для аналізу загроз ресурсам ІС необхідним є, перш за все, визначення можливих каналів та видів загроз ресурсам ІС чи інформації, що можуть бути реалізовані відносно ІС, слід здійснювати аналіз основних джерел їх походження. Як відомо [1-5], основними видами джерел загроз є:

1) зміна умов фізичного середовища (стихійні лиха й аварії, землетрус, пожежа чи інші випадкові події);

2) наслідки помилок під час проектування і розробки компонентів ІС;

3) збої і відмовлення в роботі устаткування та технічних засобів ІС;

4) помилки персоналу (користувачів) комп'ютерних систем під час експлуатації;

5) навмисні дії чи спроби потенційних зловмисників – спроби НСД до інформаційних ресурсів ІС.

Впливи, джерела яких мають природу 1-го та 2-го видів, розглядати не доцільно, оскільки засобів технічного захисту інформації від них не існує сьогодні.

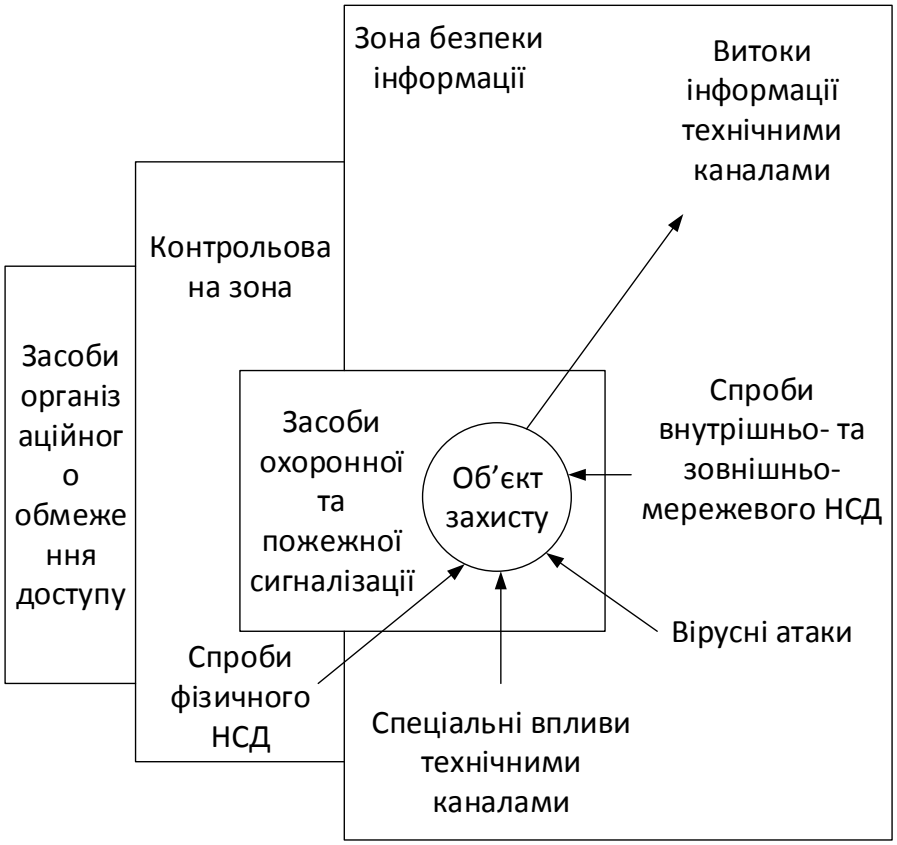


Рис. 2.7. Модель захищеного об'єкта

Аналіз впливів, які створюються навмисними діями потенційних порушників, доцільно розглядати з використанням моделі захищеного об'єкта, яка наведена на рис. 2.7.

Для моделі об'єкта, що підлягає захисту, слід визначати механізми впливів загроз на об'єкт захисту. Для визначення будемо вважати, що об'єктом захисту є ресурси інформаційної системи та сама система, яка, в свою чергу, є елементом інформаційної мережі та інформаційного простору держави. Для таких умов слід вважати, що загрози об'єкту захисту (інформаційним ресурсам ІС) можуть здійснюватися шляхом несанкціонованого доступу при безпосередніх чи дистанційних впливах на об'єкти захисту наступними можливими способами:

1. Безпосередній вплив (з безпосереднім доступом до об'єкту захисту) з можливим при умові подолання зловмисником:

- засобів організаційного обмеження доступу;
- засобів охоронної сигналізації;

- засобів адміністрування доступу (проблемно-орієнтованих засобів захисту базового ПЗ, організаційних систем та систем управління базами даних, включаючи маскування під зареєстрованого користувача з метою використання інформації чи нав'язування помилкової інформації, застосування заставних пристроїв чи програм і впровадженням комп'ютерних вірусів).

2. Дистанційний вплив можливий за рахунок:

- технічних каналів побічних електромагнітних випромінювань і наведень, акустичних каналів;
- каналів спеціального впливу шляхом формування полів і сигналів з метою руйнування системи захисту чи порушення цілісності інформації.

Модель загроз визначає перелік можливих загроз і класифікацію їх за результатами впливу на інформацію, тобто на порушення яких властивостей вони спрямовані (конфіденційності, цілісності і доступності інформації), а також порушення спостереженості і керованості інформаційних систем.

Випадковими впливами суб'єктивної природи (дії, що здійснюються персоналом чи користувачами через неуважність, недбалість, незнання і тому подібне, але без навмисного наміру) є:

- дії, що приводять до відмовлення ІС або окремих компонентів, руйнування апаратних, програмних, інформаційних ресурсів (устаткування, видалення даних, програм та ін.);
- ненавмисне ушкодження носіїв інформації;
- неправомірна зміна режимів роботи інформаційних систем (окремих компонентів, устаткування, програмного забезпечення і т.п.), ініціювання тестуючих чи технологічних процесів, здатних привести до необоротних змін у системі (наприклад, форматування носіїв інформації);
- ненавмисне зараження ПЗ комп'ютерними вірусами;
- невиконання вимог до організації заходів захисту діючих ІС розпорядницьких документів;

- помилки при введенні даних у систему, видача даних за невірними адресами пристроїв, внутрішніх абонентів і т.п.;
- будь-які дії, що можуть привести до розголошення конфіденційних відомостей, атрибутів розмежування доступу, втрати атрибутів і т.п.
- неправомірне впровадження і використання забороненого політикою безпеки ПЗ (наприклад, навчальні й ігрові програми й ін.);
- наслідки некомпетентного застосування засобів захисту.

Навмисними загрозами суб'єктивної природи, спрямованими на дезорганізацію роботи ІС (окремих компонентів) чи виводу її з ладу, проникнення в систему й одержання можливостей несанкціонованого доступу до її ресурсів, є:

- порушення фізичної цілісності ІС (окремих компонентів, пристроїв, устаткування, носіїв інформації);
- порушення режимів функціонування або вивід з ладу систем життєзабезпечення ІС (електроживлення, заземлення, охоронної сигналізації, вентиляції й ін.);
- порушення режимів функціонування ІС (устаткування і ПЗ);
- впровадження і використання комп'ютерних вірусів, заставних (апаратних і програмних) пристроїв, що підслуховують та інших засобів розвідки;
- використання засобів перехоплення побічних електромагнітних випромінювань і наведень, акустоелектричних перетворень інформаційних сигналів;
- використання (шантаж, підкуп і т.п.) з корисливою метою персоналу ІС;
- крадіжки носіїв інформації, виробничих відходів (роздруківок, записів і т.п.);
- несанкціоноване копіювання носіїв інформації;

- читання залишкової інформації з оперативної пам’яті ПЕОМ, зовнішніх накопичувачів;
- одержання атрибутів доступу з наступним їхнім використанням для маскування під зареєстрованого користувача;
- впровадження і використання забороненого політикою безпеки ПЗ чи несанкціоноване використання ПЗ, за допомогою якого можна одержати доступ до критичної інформації (наприклад, аналізаторів безпеки мереж).

Впливи, пов’язані з діяльністю зареєстрованих користувачів, в свою чергу, можуть розподілятися на випадкові чи навмисні. Випадковими загрозами є загрози, які здійснюються персоналом або користувачами по неуважності, недбалості, незнанню тощо, але без спеціального наміру. Зрозуміло, що кожна з загроз від впливу здійснюється з деякою ймовірністю, може порушувати ту чи іншу функціональну властивість захищеної системи, має своїм наслідком (особливо навмисні загрози) певні страти або шкоду та джерело виникнення чи активізації. Врахування цього надає можливість подальшої розробки ефективних засобів системи технічного захисту інформації, які в першу чергу забезпечують захист від найбільш імовірних та шкідливих загроз.

З цією метою слід визначити найбільш імовірні властивості захищеності інформації, які порушуються внаслідок впливу загроз кожного з їх типів, тобто здійснити їх ідентифікацію у вигляді переліку загроз з констатацією відповідності властивостям захищеності ресурсів ІС, на порушення яких вони спрямовані [конфіденційності (к), цілісності (ц), доступності (д), спостереженості та керованості (с) ІС]. Приклад такої ідентифікації наведено в табл. 2.1.

Таблиця 2.1.

Характеристика впливів на ресурси ІС та їх наслідки

	Вид впливу	Ймовірність	Що порушує	Рівень шкоди	Джерело

	2	3	4	5	6
1.	Порушення фізичної цілісності ІС (її окремих компонентів), пристроїв, обладнання, носіїв інформації	висока	к, ц, д, с	неприпустимо високий	внут. зовн.
2.	Доступ до даних з порушенням встановлених правил розмежування доступу з метою ознайомлення, модифікації, копіювання, знищення даних тощо	низька	к, ц, д, с	неприпустимо високий	внут. зовн.
3.	Модифікація інформаційних ресурсів, в тому числі програмного забезпечення	низька	ц, д, с	неприпустимо високий	внут. зовн.
4.	Несанкціоноване змінювання повноваження інших користувачів	низька	к, ц, д, с	неприпустимо високий	внут. зовн.
5.	Порушення режимів функціонування (виведення з ладу) систем життєзабезпечення ІС (електроживлення, заземлення, охоронної чи пожежної сигналізації, вентиляції та ін.)	висока	ц, д, с	неприпустимо високий	внут. зовн.
6.	Порушення режимів функціонування ІС (обладнання та ПЗ)	висока	к, ц, д, с	неприпустимо високий	внут. зовн.
7.	Впровадження і використання комп’ютерних вірусів, закладних	висока	к, ц, д, с	середній	внут. зовн.

	(апаратурних і програмних) і пристроїв для підслуховування, інших засобів технічної розвідки, навмисно включати до складу програмного забезпечення спеціальні блоки для порушення безпеки даних				
8.	Використання персоналу ІС (шантаж, підкуп тощо) з корисливою метою	висока	к, ц, д, с	високий	внут. зовн.
9.	Видавання власних несанкціонованих запитів за запити операційної системи	середня	к, ц, д, с	середній	внут.
10.	Отримання захищених даних за допомогою спеціально організованої серії санкціонованих запитів	середня	к, ц, д, с	середній	внут. зовн.
11.	Читання залишкової інформації з оперативної та зовнішньої пам’яті ЕОМ	низька	к	високий	внут.
12.	Одержання атрибутів доступу з наступним їх використанням для маскування під зареєстрованого користувача, незаконне розширювання своїх повноважень, видавання себе за зареєстрованого користувача, вивчання права доступу інших користувачів	низька	к, ц, д, с	неприпустимо високий	внут. зовн.
	Неправомірне підключення (в	неприп	к, ц, д, с	неприпу	зовн.

13.	тому числі, наприклад, "врізання" в канал пар типу "модем – модем") до каналів зв'язку, перехоплення даних, що передаються, зміна (модифікація) інформації повідомлень (в тому числі службові, наприклад, адрес передавача та отримувача повідомлень	устимо висока		стимо високий	
14.	Маскування захищених даних під незахищені	дуже висока	к	високий	внут.
15.	Впровадження і використання забороненого політикою безпеки ПЗ або несанкціоноване використання ПЗ, за допомогою якого можна одержати доступ до критичної інформації (наприклад, аналізаторів безпеки мереж) та ін.	висока	к, ц, д, с	високий	внут. зовн.
16.	Несанкціоноване копіювання носіїв інформації	висока	к	висока	внут.
17.	Крадіжки носіїв інформації, виробничих відходів (роздруківок, записів тощо)	низька	к	середній	внут.
18.	Фальсифікація фактів формування та видачі даних	висока	ц	високий	внут.
19.	Підтвердження отримання від деякого користувача даних, сформованих самим порушником	висока	ц	високий	внут.

20.	Підтвердження передачі якому-небудь користувачеві даних, які не передавались	висока	ц	середній	внут.
21.	Фальсифікація фактів отриманих даних	висока	ц	середній	внут.
22.	Розкриття змісту даних у каналах зв'язку	висока	к	високий	внут.
23.	Виконання аналізу потоку даних (трафіку)	висока	д, с	низький	внут. зовн.
24.	Змінювання потоку даних, наприклад, шляхом генерації несправжніх повідомлень для перевантаження системи	висока	ц, д, с	високий	внут. зовн.
25.	Переривання передачі потоку даних, наприклад, шляхом генерації несправжніх повідомлень для перевантаження системи	дуже висока	ц, д	неприпустимо високий	внут. зовн.
26.	Виконання ініціації фіктивного з'єднання	середня	ц, д	високий	внут.
27.	Дії, що призводять до відмови ІС чи окремих її елементів, руйнування апаратурних ресурсів (в тому числі обчислювальних ресурсів – процесорів та носіїв даних) та обладнання, в тому числі телекомунікаційного, засобів вводу/виводу, програмних та	низька	к, ц, д, с	неприпустимо високий	внут.

	інформаційних ресурсів (як базових так і прикладних, файлів, наборів даних тощо)				
28.	Ненавмисне пошкодження носіїв інформації чи інформації, яка зберігається на цих носіях	низька	к, ц	низький	внут.
29.	Неправомірна зміна режимів роботи ІС (її окремих компонентів, обладнання, програмних засобів тощо), ініціювання технологічних чи тестуючих процесів, які здатні призвести до незворотних змін у системі (наприклад форматування носіїв інформації)	низька	к, ц, д, с	неприпустимо високий	внут.
30.	Навмисне зараження програмних засобів (ПЗ) комп'ютерними вірусами	значна	к, ц, д, с	неприпустимо високий	внут.
31.	Невиконання організаційних заходів щодо порядку і правил експлуатації чи використання ресурсів ІС, передбачених "Планом ТЗІ", посадовими чи іншими, в тому числі технологічними інструкціями	низька	к, ц, д, с	неприпустимо високий	внут.
32.	Помилки при введенні даних в систему, видачі даних за невірними адресами пристроїв, внутрішніх та зовнішніх абонентів тощо	низька	к, ц, д, с	високий	внут.

33.	Неправомірне впровадження і використання забороненого політикою безпеки програмного забезпечення (системне, прикладне ПЗ, навчальні та ігрові програми та ін.)	низька	к, ц, д, с	низький	внут.
34.	Некомпонентне застосування засобів захисту	висока	к, ц, д, с	високий	внут.
35.	Наслідки викривлень під час проектування та розробки компонентів ІС (технічних засобів, технології обробки інформації, програмних засобів, засобів захисту, структур даних тощо)	низька	к, ц, д, с	неприпустимо високий	внут.
36.	Зміна умов фізичного середовища (стихійні лиха, як землетрус, повінь, пожежа і аварії або інші випадкові події)	низька	ц, д, с	неприпустимо високий	зовн.
37.	Збої та відмови у роботі обладнання та технічних засобів ІС, аварійне відключення живлення та т.п.	низька	ц, д, с	неприпустимо високий	внут.
38.	Впливи природних завад (грозові розряди, іскріння в електромережах, під час електрозварювання та т.п.)	низька	ц, д, с	низький	зовн.

В цій таблиці показано також оцінку ризиків, тобто ймовірності здійснення впливів та рівень збитків (шкоди) від порушень по кожному з

видів порушень і джерела (чи джерело) виникнення впливу, які внутрішні чи зовнішні суб'єкти можуть ініціювати вплив. Оцінка ризиків здійснення згідно з рекомендаціями нормативних документів у вигляді якісної оцінки ймовірностей реалізації впливів (не значна, низька, висока, неприпустимо висока) при допущенні, що закон розподілу ймовірностей кожної з них є найгіршим для реалізації захисту – рівномірним. Оцінка рівня шкоди внаслідок реалізації впливу розглядається як очікувані збитки від втрати об'єктами захисту кожної з властивостей захищеності (к, ц, д) або втрати спостереженості та керованості (с). Ця оцінка здійснена також за якісною шкалою (відсутня, низька, висока, неприпустимо висока).

Серед найбільш розповсюджених загроз шляхом несанкціонованого доступу до інформаційних ресурсів ІС – методів подолання (зламу) засобів управління доступом – слід відзначити:

1. Комплексний пошук можливих методів НСД, зловмисники винятково ретельно вивчають системи безпеки перед проникненням у неї, дуже часто вони знаходять очевидні й дуже прості методи подолання системи, які розробники просто "прогляділи", створюючи можливо дуже гарну систему ідентифікації або шифрування;

2. НСД через термінали захищеної ІС – точки входу користувача в інформаційну мережу, у тому випадку, коли до них мають доступ кілька користувачів або взагалі будь-який бажаючий, при їхньому проектуванні й експлуатації необхідно ретельно дотримуватися комплексу заходів безпеки, в тому числі, а можливо і насамперед, організаційних;

3. НСД шляхом спроб входу в систему зовсім без знання пароля, ґрунтуючись на викривленнях у реалізації програмного або апаратурного забезпечення, тобто шляхом пароля;

4. НСД шляхом маскування під авторизованого користувача передбачає попереднє отримання паролю тим чи іншим чином, наприклад, на основі помилок адміністратора та користувачів.

Модель загроз ресурсам ІС – максимально повний і деталізований перелік загроз ІС, розробляється для аналізу загроз впливів та їх наслідків. Для побудови такої моделі слід здійснити аналіз моделі порушника і визначити несанкціоновані дії (навмисні чи випадкові), які може здійснити кожен із таких порушників (зловмисників відносно ресурсів ІС, перш за все інформаційних). Окрім того, слід проаналізувати та врахувати також впливи природних факторів. Такі несанкціоновані дії, а також інші обставини, що можуть бути причиною порушення політики безпеки інформації і/або нанести втрати ІС, прийнято називати загрозами впливів. Перелік таких можливих загроз є основою для розроблення моделі загроз впливів. Нижче пропонується методика розроблення моделі загроз від впливів у вигляді таблиці. Методика розроблення такої моделі полягає в тому, що в один із стовпчиків таблиці заноситься по можливості повний перелік видів загроз від впливів (вони наведені в стовпчику 2).

Надалі для кожної із можливих загроз впливів шляхом їх аналізу (можливо і методом експертних оцінок) необхідно визначити:

- ймовірність виникнення таких загроз. В табл. 2.1 наведена якісна оцінка їх ймовірності – неприпустимо викоса, дуже висока, висока, значна, середня, низька, знехтувано низька (стовпчик 3);
- на порушення яких властивостей інформації або ІС вона спрямована (рекомендується використовувати чотири основні градації – порушення конфіденційності – *к*, цілісності – *ц*, доступності – *д* інформації, а також порушення спостереженості та керованості – *с* ІС) (стовпчик 4);
- можливий (такий, що очікується) рівень шкоди (стовпчик 5);
- джерела виникнення (які суб'єкти ІС, зовнішні чи внутрішні відносно неї, можуть ініціювати загрозу) (стовпчик 6).

Для створення цієї моделі було проаналізовано велику кількість доступних інформаційних джерел та спиралися на досвід розробки політики безпеки інформації для ІС у вигляді розподілених інформаційних мереж.

Слід враховувати, що наведені оцінки ймовірностей та величини можливої шкоди кожної із загроз впливів в моделі загроз носить узагальнений характер. Для конкретних ІС ці величини повинні бути визначеними службою захисту відповідного об'єкта.

Зрозуміло також, що для кожної ІС перелік загроз може бути звуженим чи, навпаки, розширеним, але інформації, наведеної в табл. 2.1, як основи для подальших міркувань, досить, ніж достатньо.

З моделі загроз впливів можна зробити висновок, що для реалізації загроз тій чи іншій властивості захищеності інформації зловмисник може діяти дистанційно (через засоби зв'язку, витоки інформації чи навпаки через засоби спеціального спливу технічними каналами) або безпосередньо (в тому числі і шляхом фізичного впливу) на елементи інформаційних мереж та інформаційного простору. В останньому випадку зловмиснику необхідно отримати фізичний доступ до загальних елементів інформаційних мереж (тобто подолати засоби організаційного обмеження доступу та, при необхідності, охоронної сигналізації). Ці обставини можуть суттєво вплинути на склад засобів захисту відповідних властивостей захищеності інформації.

Модель загроз від впливів є також основою для аналізу можливих збитків внаслідок відсутності засобів чи заходів захисту, а відтак, і для визначення можливих контрзаходів. З моделі загроз витікає необхідність захисту від впливу загроз усім властивостям захищеності інформації, насамперед від загроз, наслідком реалізації яких може бути неприпустимо високий чи високий рівень шкоди (загрози №1-10, 12, 13, 15, 27, 29-38), оскільки такі загрози мають комплексний, тобто одночасний вплив на декілька властивостей захищеності. Такі загрози прийнято називати найбільш суттєвими загрозами. Величину втрат, збитків, шкоди тощо, які може потерпати власник інформації або ІС внаслідок того, що в силу недосконалості, а, можливо, і відсутності, заходів та засобів захисту частка загроз зможе вплинути на функціональні властивості захищеності інформації. Цей ризик має назву залишкового.

Зрозуміло, що визначення найбільш суттєвих (найбільш небезпечних, найбільш імовірних) загроз від впливу є основою для визначення в подальшому потрібних засобів захисту відповідних функціональних властивостей захищеності інформаційних ресурсів ІС, а отже визначення складу потрібних контрзаходів для забезпечення припустимої захищеності, необхідних для захисту засобів, підсистем, механізмів та функцій захисту, тобто дає змогу будувати відповідні моделі систем захисту.

В свою чергу, знання можливих чи потрібних контрзаходів дає можливість визначення складу, характеристик та можливостей застосування тих чи інших способів, механізмів, функцій, здатних протистояти чи зменшити вплив кожної із визначеної множини загроз.

2.3. Метод знаходження оптимальної конфігурації ІС

При проектуванні інформаційних мереж, розробці трафіків передачі інформації постійно приходиться зіткатися з задачами оптимізації. При цьому особливу увагу звичайно приділяють задачам визначення в мережі оптимальних конфігурацій, які мають структуру вихідних (зростаючих) лісів.

У багатьох задач синтезу мереж виникає наступна задача.

Задача 2.1. Задан орграф $G = (X, \theta), |X| = n$, з коренем (джерелом) $x_0 \in X$, причому кожна дуга $u \in \theta$ має довжину $l(u) > 0$. Потрібно знайти суграф $G' = (X, \theta'), \theta' \subset \theta$, в якому існує шлях з вершини x_0 в будь-яку іншу вершину $x \in X \backslash \{x_0\}$ та сума довжин дуг якого є мінімальною.

Легко помітити, що суграф G' завжди буде мати структуру вихідного дерева з коренем у вершині $x_0 \in X$. Для цього достатньо показати, що в кожну вершину $x \in X \backslash \{x_0\}$ суграфа G' заходить рівно одна дуга $u \in U$. Насправді, якщо це було б не так, то беручи довільну вершину $y \in X \backslash \{x_0\}$, в яку заходить більше однієї дуги, завжди можливо обрати таку дугу, що заходить $u \in \theta$, яка належить одному з простих шляхів $P(x_0, y)$ з x_0 в y. З видаленням інших дуг, що заходять в y досяжність вершин $x \in X \backslash \{x_0\}$ з x_0 не

порушується. Таким чином, отримаємо новий суграф, сума довжин дуг якого менша, ніж у початкового.

Зрозуміло, що задача 2.1 є деяким узагальненням задачі про побудову мінімального (за сумою довжин ребр) пов'язуючого дерева у зваженому неорієнтованому графі [54], для рішення якої існує доволі простий та ефективний алгоритм Прима-Краскала. Але рішення задачі 1 потребує суттєво іншого підходу та алгоритму.

Ефективний алгоритм рішення даної задачі (у декілька іншій інтерпретації) запропоновано Едмондо [96]. В роботах [95,97,100,] з'явилися інші модифікації; найбільш цікавою з них є модифікація Фалкерсона [97] для проблеми оптимальної упаковки орієнтованих корінних резервів. Цей алгоритм описаний в [58], де відмічається, що складна його частина це зворотній хід відновлення цікавого нам суграфа за його редукцією. Тому, хоча сам алгоритм є не дуже складним, зворотній його хід потрібно чітко визначити та акуратно реалізувати.

З цієї причини в роботі приводиться розроблений алгоритм, який охоплює деталі, пов'язані з зворотнім ходом побудови оптимального вихідного дерева та не представлені в роботах, що згадувалися вище [85]. На практиці запропонованим алгоритмом вирішується більш загальна задача.

Задача 2.2. Задано орграф $G = (X, \theta), |X| = n$, кожна дуга $u = \theta$ якого має довжину $l(u) > 0$, та деяка підмножина вершин $X_0 \subset X, |X_0| = p (p < n)$ володіє наступною властивістю:

для будь-якого $y \in X \backslash X_0$ існує шлях $P(x, y)$ з деякої $x \in X_0$ в y. (2.21)

Треба знайти суграф $G^{\hat{}} = (X, \theta^{\hat{}}), \theta^{\hat{}} \subset \theta$, який задовольняє умові (2.21) та має мінімальну суму довжин дуг.

На перший погляд розглядання цієї задачі не дає нічого нового, тому що додавання до орграфу G нової вершини z (в якості кореня) та нових дуг $V_i, i = 1,2,\dots,p$ (виходячих з z і заходячих у відповідні $x_i \in X_0$) з $l(V_i) = \varepsilon (0 < \varepsilon < \min_{u \in U} l(u))$ зводиться до задачі 2.1. Насправді, її вивчення є

суттєвим як для модифікації вищезгаданих алгоритмів, так і для дослідження питання оптимального розбиття орграфа G на певну кількість підграфів з урахуванням побудови мінімальних (за сумою довжини дуг) суграфа з коренями у відповідних підграфах.

Окрім цього, на відміну від Едмонса та Фалкерсона, які для обгрунтування запропонованих їми алгоритмів використовували методи лінійного програмування, дано наочне обґрунтування, що не виходить за рамки теоретико-графових міркувань. Такий підхід, як буде показано є корисним для вирішення й інших оптимізаційних задач, пов'язаних з вибором не тільки оптимальної структури необхідного суграфа $G^{`}$, який розшукується, але й відповідної підмножини $X_0{}' \subset X$, в чому й полягає суть даної роботи.

Для зручності подальшого викладення введемо наступні визначення та позначення.

Визначення 2.1. Орграф $T = (X, W), |X| = n$, назвемо вихідним лісом з базой $X_0 \subset X, |X_0| = p$, якщо він складається з p компонент зв'язності $T_i = (X_i, \theta_i), X_i \subset X$, $\theta_i \subset \theta, i = 1,2, \dots, p$, де кожна компонента T_i представяє вихідне дерево з коренем $x_i \in X_0$.

Легко помітити, що цікавий нам суграф $G^{`}$ в задачі 2.2 буде мати завжди структуру вихідного ліса з базой $X_0 \subset X$.

Для будь-якого $Y \subset X$ позначимо через $\theta_G(Y)$ підмножину тих дуг $u \in \theta$, які заходять у вершини Y; через L_G – суму довжини всього орграфа G.

Якщо в орграфі $G = (X, \theta)$ позначена підмножина $X_0 \subset X$, яка володіє властивістю (2.1), тоді можемо записати $t(G) = X_0$.

Визначення 2.2. Вихідний ліс $T^* = (X, \theta^*)$ з базой $X_0 \subset X$ назвемо мінімальним вихідним лісом для орграфа G з $t(G) = X$, якщо $\theta^* \subset \theta$ та $L_{T^*} = \min\limits_{W \subset \theta} L$, а вихідний ліс $T^0 = (X, \theta^0)$ з базой $X_0 \subset X$ – максимальний вихідний ліс для орграфа G з $t(G) = X_0$, якщо $\theta^0 \subset \theta$ та $L_{T^0} = \max\limits_{W \subset \theta} L$, та $t(T) = X_0$.

Визначення 2.3. Нехай $Y \subset X$ – довільна підмножина вершин. Перетином $\sigma_G(Y)$ орграфа G по Y назвемо підмножину дуг $\theta' \subset \theta$, що мають початок в $X \backslash Y$ та кінець в Y.

Визначення 2.4. Приведенням орграфа G по $\sigma_G(Y)$ назвемо операцію зменшення довжини усіх дуг $u \in \sigma_G(Y)$ на величину $t(u^*) = \min_{u \in \sigma_G(Y)} t(u)$.

Дуга $u^* \in \sigma_G(Y)$ буде виділеною дугою по $\sigma_G(Y)$, а величина $t(u^*)$ - константою приведення за множиной Y.

Метод рішення задачі 2.2 починається з формування простого програмного лічильника CAL та масива MASS. У лічильнику CAL накопичується значення L_T мінімального вихідного лісу, а у масиві MASS - відповідні дуги, які йому належать.

Запропонований метод включає наступне:

1. Приводим орграф G по $\sigma_G(\{x\})$, $V_x \in X \backslash X_0$, та додаємо суму констант приведення до лічильника CAL (до початку роботи алгоритму вміст лічильника дорівнює нулю).
2. Берем $i = I$.
3. Всім виділеним дугам $u \in U$ приписуємо позначки $a(u)=i$.
4. Знаходим суграф $G^i = (X, \theta^i)$, де $\theta^i \subset \theta$ - множина усіх виділених дуг.
5. Перевіряєм, чи задовільняє суграф G^i умові задачі 2. Якщо так, то переходим до п. 10, якщо ні - до п.6.
6. Знаходим сильно зв'язкові компоненти $G_j^i=(X_j^i, \theta_j^i)$, $j=1,2,...,q_i$, в суграфі G^i, які не містять вершин $x \in X_0$.
7. Приводим орграф G по $\sigma_G(X_j^i)$, $j=1,2,...,q_i$ та суму констант приведення додаємо до лічильника CAL.
8. Новим отриманим виділеним дугам $u \in \theta$ приписуєм позначки $a(u) = i + 1$.
9. Замінюємо i на $i+1$ та переходим до п.4.

10. Берем множину $Z=X_0$.

11. У множині всіх виділених дуг $\theta^* \subset \theta$, що належать перетину $\sigma_G(X\backslash Z)$, обираємо одну з $u \in \theta^*$, яка має найменшу *a(u)*.

12. Знаходим величину $x \in X\backslash Z$, в яку заходить обрана дуга $u \in \sigma_G(X\backslash Z)$.

13. Дуги u включаємо до масиву MASS, а множину Z замінюємо на *ZU(x)*.

14 Перевірим, чи має місце *Z=X*. Якщо так, то переходим до наступного пункту, якщо ні - до п.11.

15. Виводимо зміст CAL та MASS на дисплей або друк.

Зауваження 2.1. В цьому алгоритмі можна виділити два етапи: прямий хід алгоритму - пункти 1-9 та зворотній хід - пункти 10-15. На відміну від алгоритмів, які викладені в [96,97], тут не потрібне виконання операції стягування, що значно полегшує реалізацію зворотнього алгоритму.

Зауваження 2.2. Позначки *a(u),* що застосовуються у викладеному вище алгоритмі, цілі числа від 1 до *к*, де *к* - число ітерацій прямого хода алгоритма (одна ітерація визначається переходом до 5-го пункту алгоритму). У якості позначок можуть бути використані довільні елементи деякої упорядкованої множини.

Особливу увагу слід приділити 6-му пункту алгоритму. Для знаходження сильно зв'язкових компонент орграфа в [35] запропоновано ефективний алгоритм. Оскільки структура сильно зв'язкових компонент $G_j^i = (X_j^i, U_j^i), j = 1,2,\dots,q_i$ суграфа G_{j-1}^i є такою, що кожна з сильно зв'язкових копонент $G_j^{i-1} = (X_j^{i-1}, \theta_j^{i-1}), j = 1,2,\dots,q_i$ суграфа G_{j-1}^i міститься в якості підграфа в однієї з G_j^i, то при використанні тут цього алгоритму на кожній ітерації треба виходити з початкового розбиття множини вершин на класи (результат застосування згаданого алгоритму на попередній ітерації), а далі проводиться без змін.

При аналізі запропонованого алгоритму (п.5) виникає питання: чи може існувати сильно зв'язкова компонента $G_r^i = (X_r^i, \theta_r^i)$, яка не містить вершин $x \in X_0$ та така, що перетин $\sigma_{G^i}(X_r^i) \neq \emptyset$, якщо суграф G^i не володіє властивістю (2.21)? На це питання можна отримати відповідь.

Лема 2.1. Нехай $G' = (X, \theta')$ - довільний суграф орграфа G. Тоді G' володіє властивістю (2.21) в тому і тільки в тому випадку, коли $\sigma_{G^i}(Y) \neq \emptyset$, для будь-якого $Y \subseteq X \backslash X_0$.

Доведення. Необхідність очевидна та при цьому будемо доводити лему від зворотнього. Припустимо, що $\sigma_{G^i}(Y) \neq \emptyset$, $\forall Y \subseteq X \backslash X_0$, але суграф G' не володіє властивістю (2.21). Візьмемо будь-яку величину $x \in X \backslash X_0$ до якої немає шляху з X_0 , та розглянемо сильно зв'язкову компоненту $G_x^l = (X_x^l, \theta_x^l)$ суграфа G', яка містить вершину x. Тоді не одна з вершин X_x^l не може бути досягнута з X_0, інакше вершини X_x^l були б досягнуті з X_0 та отримали б суперечність з початковою пропозицією. Перетин $\sigma_{G^i}(X_x^l \cup Z_1) \neq \emptyset$, звідки виходять дуги $u \in \sigma_{G^i}(X_x^l \cup Z_1 \cup Z_2) = \emptyset$, звідки аналогічно знаходимо множину Z_3 тощо.

Оскільки цей процес не може бути нескінченим, ми прийдемо до випадку, коли для деякого i_0, множина Z_{i0} буде містити принаймні одну вершину $y \in X_0$. Але це значить, що вершини множини X_x^l, а відповідно і вершина x, досяжні з деякої $y \in X_0$ всупереч припущенням. Лему доведено.

Таким чином, якщо суграф $G^i = (X, \theta^i)$ на деякій ітерації прямого хода алгоритму не володіє властивістю (2.21), то обов'язково існує сильно зв'язкова компонента $G_j^i=(X_j^i, \theta_j^i)$, $\theta_j^i \subset \theta$, є такою, що $\sigma_{G^i}(X_j^i) = \emptyset$.

$$L_{G^i}(X_r^i) = \sum_{u \in \theta_{G^i}(X_r^i)} l(u) = \sum_{x \in X_r^i} \sum_{u \in \theta_{G^i}(\{x\})} l(u) =$$

$$= \sum_{x \in X_r^i} \sum_{u \in \theta_{G^i}(\{x\})} f(\{x\}) l_1(u) =$$

$$\sum_{x\in X_r^k}\left|\sigma_{G^i}(\{x\})\right| f(\{x\})+\sum_{x\in X_r^k}\sum_{u\in\theta_{G^i}(\{x\})} l(u)=$$

$$=\sum_{\{x\}\subset X_r^k}\left|\left|\sigma_{G^i}(\{x\})\right|f(\{x\})+\sum_{u\in\theta_{G^i}(\{x_r^k\})} l_1(u).$$

Після виконання кожної ітерації прямого ходу алгоритму довжина дуг змінюється. Тому поряд з позначеннями, введеними при описі алгоритму, використовуємо ще одне: $l_1(u)$ – довжина дуги після виконання i-ої ітерації.

Будемо рахувати, що суграф $G^i=(X,\theta^i)$ при $i=0$, тобто при нульовій ітерації, є суграф $G^0=(X,\emptyset)$ і кожна його вершина $x\in X\backslash X_0$ являє собою сильно зв'язну компоненту.

Нехай A – множина всіх $X_j^i\subset X$, $i=0,1,2,\dots,k-1; j=1,2,\dots,q_i$, які виникають в результаті виконання прямого ходу алгоритму. Для множини $X_j^i, X_r^s\in A$ будемо вважати рівними $(X_j^i=X_r^s)$, якщо вони містять однакові елементи та $i=s$. У випадку, коли X_j^i містить усі елементи множини X_r^s або однакові елементи, але $i>s$, можемо записати $X_r^s\subset X_j^i$.

Зауваження 2.1. Структура множини $X_j^i\in A$ є такою, що будь-які $X_j^{i1}, X_j^{i2}\in A$ або не мають спільних вершин, або одне з них цілком міститься в іншому.

Розглянемо тепер функцію $f: A\to D$, де $f(X_j^i)$ – значення константи приведення за множиною $X_j^i\subset X$ після виконання i-ої ітерації. Тоді має місце лема 2.2.

Лема 2.2. Нехай $G^i=(X,\theta^i)$ – довільний суграф орграфа G, а $G_r^s=(X_r^s,\theta_r^s)$ – одна з сильно зв'язних компонент сугрофа $G^s=(X,\theta^s), \theta^s\subset\theta$, отриманого після s-й ітерації минулого хода алгоритму. Тоді

$$L_{G^i}(X_s^r)=\sum_{X_j^i\subset X_r^s}\left|\sigma_{G^i}(X_j^i)\right|\cdot f(X_j^i)++\sum_{u\in\theta_{G^i}(X_r^s)} t_s(u) \qquad (2.22)$$

Доведення. Доведення проведем індукцією за кількістю ітерацій. Припустимо, що виконана одна ітерація прямого хода алгоритму та суграф

$G^l = (X, \theta^l)$, породжений множиною виділених дуг, які утворилися, містить сильно зв'язану компоненту $G_r^l = (X_r^l, \theta_r^l), \theta_r^l \subset \theta$ (G_r^l не містить вершин X_0). Тоді формула (2.22) при $s = 1$ підтверджується.

Припустимо тепер, що ця формула є справедливою для всіх $X_j^{s-1} \subset X, j = 1,2,\dots, q_{s-1}$, отриманих після виконання $(s-1)$-ї ітерації прямого ходу алгоритму ($s < k-1$), та припустимо, що після виконання s-ї ітерації виник суграф $G_s = (X, \theta^s), \theta^s \subset \theta$. Розглянемо одну з сильно зв'язаних компонент $G_r^s = (X_r^s, \theta_r^s)$ цього суграфа, яка не містить X_0.

Нехай $G_{j1}^{s-1}=(X_{j1}^{s-1}, U_{j1}^{s-1})$, $j = 1,2,\dots, q_{s-1}$ – сильно зв'язані компоненти, отримані після виконання $(s-1)$-ї ітерації та містяться в G_r^{s-1} в якості підграфів. Згідно припущенню індукції для кожного з $X_{j1}^{s-1} \subset X_r^s$, $j = 1,2,\dots, q_{s-1}$, справедливою є формула

$$L_{G^l}(X_{j1}^{s-1}) = \sum_{X_j^i \subset X_{j_1}^{s-1}} \left|\sigma_{G^l}(X_j^i)\right| f(X_j^i) + \\ + \sum_{u \in \theta_{G^*}(X_{j1}^{s-1})} l_{s-1}(u). \qquad (2.23)$$

Другий доданок можна представити у вигляді

$$\sum_{u \in \sigma_{G^*}(X_{j1}^{s-1})} l_{s-1}(u) + \sum_{u \in \theta_{G^*}(X_{j1}^{s-1}) \setminus \sigma_{G^*}(X_{j1}^{s-1})} l_{s-1}(u)$$

Оскільки довжина дуг $u \in \theta_{G^*}(X_{j1}^{s-1}) \setminus \sigma_{G^*}(X_{j1}^{s-1})$ в результаті виконання s-ї ітерації не змінюються, тоді

$$\sum_{u \in \theta_{G^*}(X_{j_1}^{s-1}) \setminus \sigma_{G^*}(X_{j_1}^{s-1})} l_{s-1}(u) = \sum_{u \in \theta_{G^*}(X_{j_1}^{s-1}) \setminus \sigma_{G^*}(X_{j_1}^{s-1})} l_s(u),$$

$j_1 = 1,2,\dots, q_{s-1}$.

Таким чином

$$\sum_{u \in \theta_{G^*}(X_{j_1}^{s-1})} l(u) = \sum_{u \in \sigma_{G^*}(X_{j_1}^{s-1})} \left(f(X_{j1}^{s-1})\right) + l_s(u) + \\ + \sum_{u \in \theta_{G^*}(X_{j1}^{s-1}) \setminus \sigma_{G^*}(X_{j1}^{s-1})} l_s(u),\ j = 1,2,\dots, q_{s-1},$$

звідки

$$\sum_{u\in\theta_{G'}(X_{j1}^{s-1})} l_{s-1}(u) = \left|\sigma_{G'}(X_{j1}^{s-1})\right| f(X_{j1}^{s-1}) +$$

$$+\sum_{u\in\sigma_{G'}(X_{j1}^{s-1})} l_s(u) + \sum_{u\in\theta_{G'}(X_{j1}^{s-1})\setminus\sigma_{G'}(X_{j1}^{s-1})} l_s(u),$$

тобто

$$\sum_{u\in\theta_{G'}(X_{j1}^{s-1})} l_{s-1}(u) = \left|\sigma_{G'}(X_{j1}^{s-1})\right| f(X_{j1}^{s-1}) +$$

$$+\sum_{u\in\theta_{G'}(X_{j1}^{s-1})} l_s(u), \qquad (2.24)$$

Підставив вираз (2.24) в рівняння (2.23), знаходим

$$L_{G'}(X_{j1}^{s-1}) = \sum_{X_j^i\subset X_{j1}^{s-1}} \left|\sigma_{G'}(X_j^i)\right| f(X_j^i) +$$

$$+\left|\sigma_{G'}(X_{j1}^{s-1})\right| f(X_{j1}^{s-1}) + \sum_{u\in\theta_{G'}(X_{j1}^{s-1})} l_s(u) =$$

$$- \sum_{X_j^i\subseteq X_{j1}^{s-1}} \left|\sigma_{G'}(X_j^i)\right| f(X_j^i) + \sum_{u\in\theta_{G'}(X_{j1}^{s-1})} l_s(u),$$

тобто

$$L_{G'}(X_{j1}^{s-1}) = \sum_{X_j^i\subseteq X_{j1}^{s-1}} \left|\sigma_{G'}(X_j^i)\right| f(X_j^i) +$$

$$+ \sum_{u\in\theta_{G'}(X_{j1}^{s-1})} l_s(u), \qquad (2.25)$$

$j_1 = 1,2,\dots,q_{s-1}$.

Додаючи співвідношення (2.25) за j_1, отримаєм потрібну формулу (2.22). Лему 2.2 доведено.

Лема 2.3. Якщо $T^* = (X,\theta^*)$ мінімальний вихідний ліс для орграфа G з базой $X_0 \subset X$, тоді для кожного з множини $X_r^s \subset X$ перетин $\sigma_{T^*}(X_r^s)$ містить не більше однієї дуги $u \in \theta\setminus\theta^s$ (θ^s – множина всіх виділених дуг, отриманих після виконання s-й ітерації).

Доведення. Розглянемо довільну множину $X_r^s \subset X$, яка виникає після виконання s-й ітерації прямого хода алгоритму, та запропонуємо зворотнє,

тобто, що перетин $\sigma_{T^*}(X_r^s)$ містить дуги $u_1, u_2, \dots, u_m (m \geq 2)$, що належать множині $\theta \backslash \theta^s$.

Оскільки T^* - вихідний ліс з базой $X_0 \subset X$, то в ньому існує хоча б один простий шлях $P(x, y), x \in X_0, y \in X_r^s$, в якому одна з дуг $u_{i0} \in \sigma_{T^*}(X_r^s)$ є останньою при русі від x до y та який не містить інші дуги $u \in \sigma_{T^*}(X_r^s)$.

З самого смислу структури компоненти $G_r^s = (X_r^s, \theta_r^s)$ витікає, що відносно вершини y можна побудувати вихідне дерево $T_r^s = (X_r^s, V_r^s)$, $V_r^s \subset \theta_r^s$, з джерелом в ній таким чином, щоб для кожної множини $X_j^i \subset X_r^s$, що не містить y, мало б місто $|\sigma_{T_r^s}(X_j^i)|=1$.

Відмітимо, що якщо в вихідному лісі T^* замінити дуги $u \in \theta^*$, які заходять до вершини $x \in X_r^s \backslash \{y\}$, на дуги, які заходять $u \in V_r^s$, то отриманий орграф $T_1^* = (X, \theta_1^*), \theta_1^* \subset \theta$ буде також вихідним лісом з базою $X_0 \subset X$ для орграфа G з $t(G) = X_0$. Дійсно, $|\sigma_{T_1^*}(\{x\})| = 1, \forall x \in X \backslash X_0$ та будь-яка вершина $x \in X \backslash X_0$ досягається з деякої вершини $z \in X_0$.

Покажемо, що $L_{T_1^*} < L_{T^*}$. Насправді,

$$L_{T^*} = L_{T^*}((X \backslash X_0) \backslash X_r^s) + L_{T^*}(X_r^s); \quad (2.26)$$

$$L_{T_1^*} = L_{T_1^*}((X \backslash X_0) \backslash X_r^s) + L_{T_1^*}(X_r^s). \quad (2.27)$$

З побудови вихідного лісу T_1^* маємо

$$L_{T_1^*}((X \backslash X_0) \backslash X_r^s) = L_{T^*}((X \backslash X_0) \backslash X_r^s).$$

Згідно з лемою 2.1:

$$L_{T^*}(X_r^s) = \sum_{X_j^i \subset X_r^s} |\sigma_{T^*}(X_j^i)| f(X_j^i) + \sum_{q=1}^{m} l_r(u_q); \quad (2.28)$$

$$L_{T_1^*}(X_r^s) = \sum_{X_j^i \subset X_r^s} f(X_j^i) + l_r(u_{i0}). \quad (2.29)$$

В (4.25) $|\sigma_{T^*}(X_j^i)| \geq 1, \forall X_j^i \subset X_r^s$,

оскільки T^* - вихідний ліс з базой $X_0 \subset X$ і в кожну множину X_j^i заходить зовні в крайньому випадку одна дуга. Тому перший доданок в (2.28) не менший ніж перший доданок в (2.29). Порівняв другі доданки в цих

співвідношеннях помітимо, що $\sum_{q=1}^{m} l_r(u_q) > l(u_{i0})$, тому що u_{i0} співпадає з однією з дуг $u_q, q = 1,2,\dots,m; m \geq 2$.

Таким чином,

$L_{T^*}(X_r^s) > L_{T_1^*}(X_r^s)$.

В силу (2.26), (2.27) отримана нерівність тягне за собою $L_{T_1^*} < L_{T^*}$ всупереч тому, що $T^* = (X, \theta^*)$ мінімальний вихідний ліс для орграфа G з базой $X_0 \subset X$ з $t(G) = X_0$. Тому припущення є невірним, лему доведено.

Наслідок 2.1. Мінімальний вихідний ліс T^* не може містити дуги $u \in \theta \backslash \theta^*$ (θ^* – множина всіх виділених дуг, отриманих після виконання прямого ходу алгоритму).

Оскільки в мінімальному вихідному лісі T^* перетин $\sigma_{T^*}(X_j^i) \neq \emptyset, \forall X_j^i \subset X$, тоді $L_{T^*} \geq \sum_{X_j^i \in A} f(X_j^i)$. З іншого боку, в суграфі $G^* = (X, \theta^*)$ можна побудувати вихідний ліс $T = (X, V), V \subset \theta^*$, таким чином, щоб для кожного $X_j^i \subset X$ мало місце $|\sigma_T(X_j^i)| = 1$. Тоді $L_T = \sum_{X_j^i \in A} f(X_j^i)$ на основі леми 2.1.

Тому

$$L_{T^*} = \sum_{X_j^i \in X} f(X_j^i). \qquad (2.30)$$

Звернувшись до леми 2.3, помітимо, що якщо $l_s(u_{i0})$=0, то дуга u_{i0} має помітку $\alpha(u_{i0}) \leq s$, причому перетин $\sigma_G(X_r^s)$ не містить дуг з помітками $\alpha(u_{i0})$. Якщо $l_s(u_{i0}) \neq 0$, то на основі наслідка 1 дуга u_{i0} повинна мати помітку $\alpha(u_{i0}) = s_1 > s$, тобто $l_s(u_{i0})$=0, а $l_{s_1-1}(u_{i0}) > 0$. Це означає, що існує множина $X_{j1}^{s-1} \subset X$, для якого $u_i \in \sigma_G(X_{j1}^{s-1})$, при цьому в даному перетині не містяться дуги з помітками, меншими за s.

З відміченого вище витікає необхідна нам як наслідок теорема: алгоритм реалізує оптимальне рішення, та для мінімального вихідного лісу T^* з заданой базою $X_0 \subset X$ для орграфа G з $t(G) = X_0$, коли дугам $u \in \theta$ приписані довільні речові числа, не обов'язково позитивні. Якщо до довжини

усіх дуг $u \in \theta$, що заходять у деяку вершину x$\in X$, додати або відняти позитивне число h_x, то структура мінімального лісу T^* не зміниться, а сума довжини дуг L_{T^*} відповідно збільшиться або зменшиться на h_x. Тому, якщо обрати $h = \max_{u \in \theta} |l(u)|$ та збільшити довжину дуг $u \in \theta$ на h, то цей випадок зведеться до випадку з позитивними довжинами дуг. Якщо в орграфі G з $t(G) = X_0$ треба знайти максимальний вихідний ліс $T^0 = (X, \theta^0)$ з базою $X_0 \subset X$, тоді для цього достатньо змнити знаки величин *l(u)* на протилежні та шукати в орграфі *G* з новою довжиною дуг $l'(u) = -l(u)$ мінімальний вихідний ліс T_1^* з базой $X_0 \subset X$. Тоді $T_1^* = T^0$.

Метод знаходження оптимальної конфігурації ІС (рис. 2.8) побудований на теоретико-графовому підході і реалізується у два етапи – прямого та зворотного ходу [85]. Перший етап складається з блоків: обробки даних (БОД), знаходження суграфу (БЗС), перевірки умови 1 (БПУ1), знаходження сильно-зв'язкових компонентів (БСЗК); другий етап містить блоки: виділення множин (БМ), вибору мінімальної довжини дуги (БМД), знаходження величини дуги (БЗД), перевірки умови 2.21 (БПУ).

Таким чином отримали результати:

1. Для довільного графа із заданою базою та визначеними довжинами дуг вирішена задача побудови суграфу з аналогічними вершинами та мінімальною сумою довжин дуг.
2. Запропоновано новий метод оптимізації структури мережі, який на відміну від алгоритмі, запропонованих в роботах Пріма-Краскала, Едмондо, Фалкерсона, використовує зворотній хід побудови оптимального вихідного дерева.
3. При знаходженні оптимальної структури мережі сформульовано та розв'язано 2 задачі, доведено 3 леми та 1 теорема.

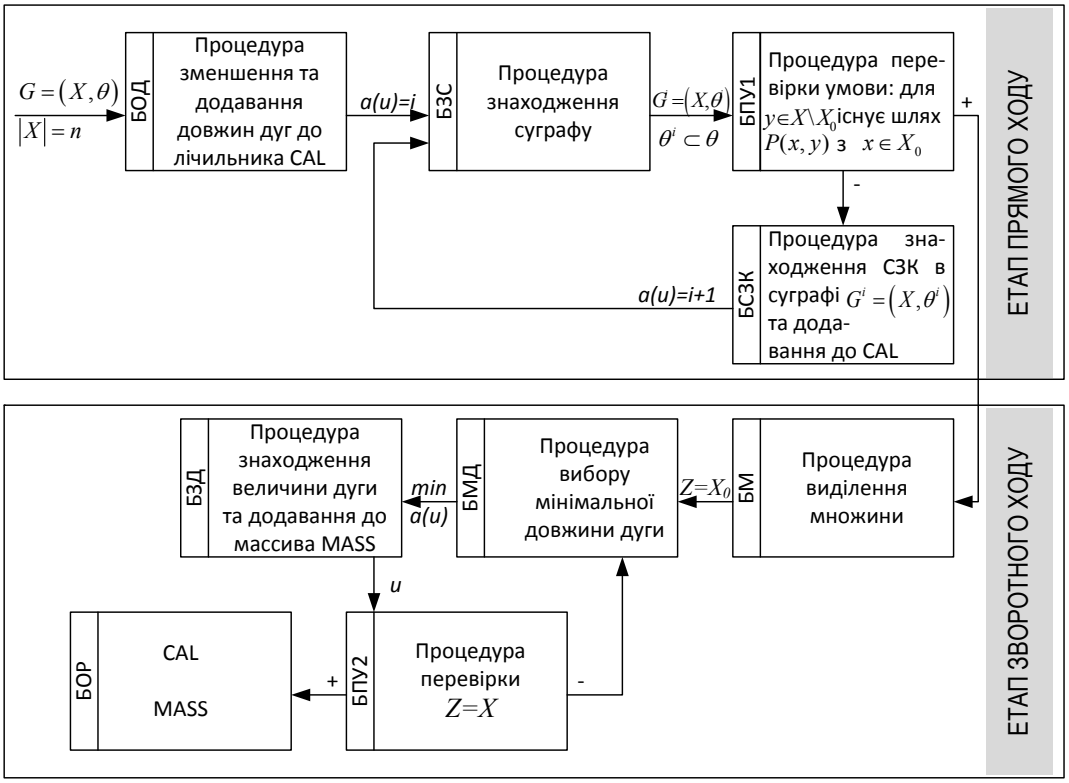


Рис. 2.8. Схематичне відображення методу знаходження оптимальної конфігурації ІС

2.4. Висновки до другого розділу

Розроблений метод знаходження оптимальної конфігурації інформаційної системи за рахунок використання теоретико-графового моделювання зворотного ходу побудови оптимального вихідного дерева дозволяє визначати оптимальну архітектуру інформаційної системи в умовах інформаційних впливів.

Запропонована методика оцінки уразливостей і впливів на інформаційні системи дозволяє ідентифікувати уразливості інформаційних систем в умовах впливів за рахунок використання логіко-ймовірнісних пар зв'язок «параметри → уразливості».

РОЗДІЛ 3. МЕТОДИ ОПТИМІЗАЦІЇ ІНФОРМАЦІЙНИХ СИСТЕМ В УМОВАХ ВПЛИВІВ

3.1. Теорія моделювання критеріїв оптимальності та обмеження загроз інформації

Для створення будь-якої системи, в тому числі й системи захисту інформації, процедура аналізу ефективності та оптимальності рішень у загальному випадку повинна містити наступні необхідні етапи:

- визначення практичної потреби;
- вибір цілей та формування вимог до системи, яка повинна забезпечити досягнення поставлених цілей;
- визначення зовнішніх умов функціонування системи;
- визначення систем, з якими буде взаємодіяти нова система, що розробляється;
- вибір критеріїв ефективності (оптимальності) системи та побудова їх математичних моделей;
- вибір та аналіз можливих способів вирішення поставлених задач;
- виявлення та дослідження необхідних ресурсів та обмежень на їх використання;
- розробка математичних моделей обмежень як функцій від керованих та некерованих змінних;
- порівняльний аналіз ефекту та затрат ресурсів, можливих варіантів побудови системи;
- порівняння альтернатив, пошук та вибір оптимального рішення;
- аналіз адекватності та чуттєвості математичних моделей, критеріїв та обмежень до змін керованих змінних параметрів.

Сучасні системи захисту інформації представляють собою складні ієрархічні багаторівневі системи [17]. Основними характеристиками таких

систем є вертикальна та горизонтальна декомпозиція на самостійні підсистеми, які мають свої цілі, критерії та органи керування, пріоритет прийняття рішень, залежність рішень, що приймаються на кожному рівні та у кожній підсистемі від рішень, які приймаються на інших рівнях та в інших підсистемах, необхідність узгодження критеріїв та рішень, координації виконання рішень та дій. Процес керування критеріями та рішеннями підсистем здійснюється в умовах невизначеності, яка обумовлена неповною інформацією про поведінку інших підсистем, а також про їх зовнішнє оточення [67].

При виборі критеріїв та обмежень в ієрархічних системах можливі наступні проблемні ситуації:

- одноріневий вибір критеріїв при наявності однієї мети;
- одноріневий багатоцільовий вибір критеріїв;
- багаторівневий вибір критеріїв при умові, що кожний рівень керується однією метою;
- багаторівневий багатоцільовий процес формування критеріїв.

Відповідно, побудова математичних моделей критеріїв ефективності та обмежень є ключовою проблемою в усіх задачах аналізу, синтезу та оптимізації систем, що розробляються, тому побудова самих процедур формалізації критеріїв та обмежень само по собі є важливою та актуальною проблемою [32,42,86].

Тобто необхідні розробка та застосування системи правил для математичного моделювання критеріїв оптимальності та обмежень як певних функцій від керованих, так й некерованих змінних. Формалізація побудови математичних моделей дозволяє змістовно ставити та вирішувати задачі аналізу, синтезу та оптимізації систем за обраними критеріями та виявленим обмеженням. Некеровані змінні, як правило, відіграють роль параметрів родини рішень та визначають зазвичай ті чи інші умови функціонування та взаємодії систем та/або області існування та єдності оптимальних рішень.

Тому потрібно сформулювати систему правил, для чого використовуються три основних принципи:

1. Критерії ефективності повинні дозволяти оптимальне керування, тобто готувати та приймати оптимальні рішення, у тому числі й при наявності обмежень.

2. Так як в задачах оптимізації обмеження відіграють роль критеріїв, то математичні моделі обмежень конструюють також й моделі критеріїв.

3. Будь-яка задача з обмеженнями може бути перетворена у послідовність задач без обмежень, тому для вибору канонічних форм можна використовувати допоміжну функцію Лагранжа як узагальнений критерій оптимальності, який враховує обмеження.

Система правил математичного моделювання критеріїв оптимальності та обмежень будується на необхідних та достовірних умовах існування екстремумів функцій та функціоналів. Вона дозволяє розробляти канонічні форми рівнянь оптимізації, як рівнянь балансу [72,86], критеріїв оптимізації та обмежень, як інтегральних перетворень цих канонічних форм.

Розглянемо послідовно та детально запропоновану систему правил.

Правило оптимальності. Будь-яка безперервна двічі диференційована функція $OC(cv_1,...,cv_\varepsilon)$ від ε аргументів може бути критерієм оптимальності ОС (optimality criterion) цільової функції, а самі аргументи є керованими змінними cv (controlled variables), якщо для області існування ОС дотримуються необхідні та достатні умови існування екстремумів.

Правило обмеження. Будь-яка безперервна двічі диференційована функція $L(cv_1,...,cv_\varepsilon)$ від ε незалежних аргументів може бути обмеженням (limitation), а самі аргументи є керованими змінними, якщо для області існування L дотримуються необхідні та достатні умови існування екстремумів та задані обмеження у вигляді:

$$L_1(cv_1,...,cv_\varepsilon) = L_1^*,...,L_\mu(cv_1,...,cv_\varepsilon) = L_\mu^*; \qquad (3.1)$$

де μ – число обмежень.

Правило існування. Для того, щоб оптимальне рішення існувало та було єдиним, необхідно щоб число керованих змінних та число обмежень задовольняли умові:

$$\varepsilon > \mu. \tag{3.2}$$

Правило зведення. У випадках, коли обмеження (3.1) задані у вигляді нерівностей, оптимізація зводиться до відомих способів введення фіктивних допоміжних змінних. Якщо цільові функції та обмеження можуть мінятися місцями, то в задачах оптимізації повинна виконуватися необхідна умова (3.2).

Правило допоміжної функції. У задачах оптимізації з обмеженнями за критерій оптимізації використовується допоміжна функція Лагранжа виду:

$$\begin{aligned} &AL(cv_1,...,cv_\varepsilon) = OC(cv_1,...,cv_\varepsilon) + (\lambda_1\left[L_1(cv_1,...,cv_\varepsilon) - L_1^*\right] + ... \\ &+\lambda_\mu\left[L_\mu(cv_1,...,cv_\varepsilon) - L_\mu^*\right]), \end{aligned} \tag{3.3}$$

де λ_k – допоміжні невизначені множники Лагранжа, $k = \overline{1,\mu}$.

Правило канонічності. Система з $\varepsilon + \mu$ рівнянь оптимізації:

$$\begin{cases} \dfrac{\partial AL(cv_1,\lambda_1)}{\partial cv_1} = 0,...,\dfrac{\partial AL(cv_\varepsilon,\lambda_\varepsilon)}{\partial cv_\varepsilon} = 0 \\ \dfrac{\partial AL(cv_1,\lambda_1)}{\partial \lambda_1} = 0,...,\dfrac{\partial AL(cv_\mu,\lambda_\mu)}{\partial \lambda_\mu} = 0, \end{cases} \tag{3.4}$$

може бути подана у канонічній формі виду

$$\begin{cases} \dfrac{\partial AL_1(cv_1,\lambda_1)}{\partial cv_1} = \dfrac{\partial AL_2(cv_1,\lambda_1)}{\partial cv_1},...,\dfrac{\partial AL_1(cv_\varepsilon,\lambda_\varepsilon)}{\partial cv_\varepsilon} = \dfrac{\partial AL_2(cv_\varepsilon,\lambda_\varepsilon)}{\partial cv_\varepsilon} \\ L_1(cv_1,...,cv_\varepsilon) = L_1^*,...,L_\mu(cv_1,...,cv_\varepsilon) = L_\mu^*. \end{cases} \tag{3.5}$$

Таким чином систему (3.5) будемо називати першою канонічною формою представлення системи рівнянь оптимізації. Елементи обох частин рівнянь (3.5) будемо називати типовими елементами першої канонічної форми.

Правило критеріїв. Використання першої канонічної форми (3.5) системи рівнянь оптимізації дозволяє створювати критерії оптимізації у вигляді сепарабельних адитивних критеріїв:

$$OC(cv_1,...,cv_\varepsilon)=\sum_{i=1}^{\varepsilon}(\int\frac{\partial AL_1(cv_1,...,cv_\varepsilon;\lambda_1,...,\lambda_\mu)}{\partial cv_i}dcv_i-$$
$$-\int\frac{\partial AL_2(cv_1,...,cv_\varepsilon;\lambda_1,...,\lambda_\mu)}{\partial cv_i}dcv_i), \quad (3.6)$$

Сепарабельність $OC(cv_1,...,cv_\varepsilon)$ означає, що всі недіагональні елементи матриці других часткових похідних цієї функції дорівнюють нулю.

Правило сепарабельного програмування. Сепарабельну форму та адитивність також зручно використовувати для обмежень виду (3.5):

$$OC_{1k}(cv_1)+...+OC_{\varepsilon k}(cv_\varepsilon)=OC_k^*. \quad (3.7)$$

Задачу оптимізації, у якій критерій оптимізації представлений у вигляді (3.6), а обмеження у вигляді (3.7), будемо називати задачею сепарабельного програмування. Якщо $OC(cv_1,...,cv_\varepsilon)$ є випуклою функцією, а $L_k(cv_1,...,cv_\varepsilon)$ – угнутою, існує рішення прямих задач сепарабельного програмування. Для зворотних задач функції $OC(cv_1,...,cv_\varepsilon)$ та $L_k(cv_1,...,cv_\varepsilon)$ повинні володіти протилежними властивостями. Властивості сепарабельності та адитивності дозволяють створювати ефективні обчислювальні алгоритми пошуку оптимальних рішень. Представлення критерію оптимізації у вигляді (3.6) називається другою канонічною формою постановки задачі оптимізації. У задачах оптимізації при побудові допоміжних функцій Лагранжа (3.3) критерій та одне з обмежень міняються місцями. При цьому змінюється і характер екстремуму, і вимоги випуклості та вгнутості цільових функцій та обмежень. Доданки суми (6) будемо називати типовими елементами другої канонічної форми.

Запропонована система правил дозволяє створити загальну теорію математичного моделювання сепарабельних критеріїв оптимізації та обмежень. Вони засновані на виборі типових елементів канонічних форм (3.5), (3.6) та методах сепарабельного програмування. Параметри канонічних

форм грають роль параметрів сімейства оптимальних рішень, їх зручно використовувати як параметри середовища (зовнішнього оточення) або як параметри, які характеризують взаємодію системи, що розглядається з іншими системами.

Для класифікації типових елементів першої канонічної форми (3.5) корисно використовувати методи аналітичної та диференційної геометрії, які володіють високою наочністю. У ролі типових елементів форм можуть бути обрані алгебраїчні функції (поліноми) q-го порядку, показові, експоненціальні, тригонометричні, трансцендентні та інші.

Виходячи з цього, розглянемо випадок, коли $\varepsilon = 1, \mu = 0$. Це означає, що в ролі критерія оптимальності обирається функція однієї керуючої змінної, а обмеження відсутні. Припустимо, що перший типовий елемент $OC'(cv)$ є поліномом нульового порядку:

$$OC_1'(cv, a_{10}) = a_{10}, \tag{3.8}$$

а другий типовий елемент $OC_2'(cv, a_{21}, a_{20})$ є поліномом першого порядку:

$$OC_2'(cv, a_{21}, a_{20}) = a_{21}cv + a_{20}. \tag{3.9}$$

Покажемо вид канонічної форми (3.5) рівняння оптимізації, вид канонічної форми (3.6) критерія оптимальності. Побудуємо математичну модель критерія, тобто знайдемо оптимальне значення cv_{opt} керуючої змінної та екстримальне значення критерію. Дослідимо вид екстремума в залежності від параметрів a_{10}, a_{20}, a_{21} типових елементів форми (3.5).

У відповідності з (3.5) рівняння оптимізації має вигляд:

$$a_{10} = a_{20} + a_{21}cv. \tag{3.10}$$

Розв’язуючи це рівняння відносно x, отримаємо оптимальне значення керуючої змінної

$$cv_{opt} = \frac{a_{10} - a_{20}}{a_{21}}. \quad (3.11)$$

За допомогою другої канонічної форми (3.6) визначимо математичну модель критерія:

$$OC(a_{10}, a_{20}, a_{21}, cv) = a_{10}cv + c_{11} - a_{20}cv - a_{21}\frac{cv^2}{2} - c_{21} =$$

$$= -a_{21}\frac{cv^2}{2} - (a_{20} - a_{10})cv - (c_{21} - c_{11}). \quad (3.12)$$

З аналізу виразу (3.12) витікає, що друга канонічна форма (3.6) критерія є поліномом другого порядку, екстремуми якого визначають параметри першої канонічної форми (3.5). Таким чином, якщо перша канонічна форма є лінійною і містить поєднання поліномів нульового та першого порядків, то друга канонічна форма (3.6) для критерія оптимальності є поліномом другого порідку. Отже, перші канонічні форми типу (3.12) породжують клас задач квадратичного програмування.

Лінійна апроксимація перших канонічних форм рівнянь оптимізації володіє відносно широкими можливостями для моделювання задач лінійного та нелінійного програмування. В цьому випадку лінійна канонічна форма включає чотири параметри: $a_{10}, a_{11}, a_{20}, a_{21}$ та дозволяє апроксимувати чимало класів критеріїв (середньоквадратичні критерії, критерії максимальної правдоподібності тощо) варіацією поєднань цих параметрів як морфологічних параметрів форми.

Визначимо екстремальні значення критерія оптимальності (3.12) при $cv = cv_{opt}$ (3.11). Підставимо значення cv_{opt} з (3.11) до (3.12) та отримаємо:

$$OC_{ext}(a_{10}, a_{11}, a_{21}, cv_{opt}) = -a_{21}\frac{(a_{10} - a_{20})^2}{2a_{21}^2} +$$

$$+ \frac{(a_{10} - a_{20})^2}{a_{21}} - (c_{21} - c_{11}) = \frac{(a_{10} - a_{20})^2}{2a_{21}} - (c_{21} - c_{11}). \quad (3.13)$$

Для уточнення виду екстремуму виконаємо диференціювання ПКФ за керованою змінною x, отримаємо значення другої похідної критерію:

$$ОС''(cv) = a_{21}. \quad (3.14)$$

Отже, значення параметру a_{21} ПКФ (3.5) визначає вид екстремуму. Якщо $a_{21} > 0$, тоді екстремум є мінімумом:

$$ОС_{ext}(a_{10}, a_{11}, a_{21}, cv_{opt}) = ОС_{min}(a_{10}, a_{11}, a_{21}, cv_{opt}). \quad (3.15)$$

Якщо $a_{21} < 0$, тоді екстремум є максимумом:

$$ОС_{ext}(a_{10}, a_{11}, a_{21}, cv_{opt}) = ОС_{max}(a_{10}, a_{11}, a_{21}, cv_{opt}). \quad (3.16)$$

Якщо $a_{21} = 0$ лінійна форма (3.5) першого порядку вироджується у канонічну форму нульового порядку (сингулярний випадок), квадратична форма критерія вироджується в лінійну форму

$$ОС_0(a_{10}, a_{11}, a_{21} = 0, cv) = (a_{10} - a_{20})cv + c_{11} - c_{21}, \quad (3.17)$$

яка, як відомо з лінійного програмування, має екстремальні значення критерію лише на границях області існування cv.

Частіше за все такі границі задаються, виходячи з обмежень та вимог до допустимого значення критерію. Наприклад, якщо, як обмеження, задано необхідне значення $ОС_0^*$, тоді значення cv_{opt} визначають з нерівності

$$(a_{10} - a_{20})cv + c_{11} - c_{21} \geq ОС_0^*. \quad (3.18)$$

З рівняння (3.18) витікає, що

$$cv_{opt} \geq \frac{ОС_0^* - c_{11} + c_{21}}{a_{10} - a_{20}}. \quad (3.19)$$

Таким чином, лінійну канонічну форму (3.5) зручно розглядати як деяку перехідну форму, яка в граничному розумінні пов'язує між собою задачі лінійного та нелінійного програмування. Постійні інтегрування c_{11}, c_{12}

можна розглядати як деякі вільні параметри, значення яких обирають, виходячи з конкретного логічного розуміння та змісту задачі оптимізації.

Якщо ж, припустити, що за логічним змістом екстремум критерія оптимізації повинен бути мінімумом та мінімальне значення критерію повинно бути рівним нулю, тоді $a_{21} \geq 0$ та

$$\frac{(a_{10}-a_{20})^2}{2a_{21}}-(c_{21}-c_{11})=0. \tag{3.20}$$

Звідси різниця постійних інтегрування, яку можна розглядати як одну постійну інтегрування, і вона повинна мати значення

$$c_{21}-c_{11}=\frac{(a_{10}-a_{20})^2}{2a_{21}}. \tag{3.21}$$

Система правил дозволяє ввести таку форму представлення системи рівнянь оптимізації (3.5), яка за допомогою її інтегрального перетворення (3.6) дозволяє синтезувати морфологічним методом сепарабельні адитивні критерії та обмеження у вигляді (3.6). Тобто дозволяє оцінювати захищеність ІС з урахуванням дозволених границь гарантованого рівня захисту інформації.

3.2. Метод оптимізації ІС на основі теорії диференціальних ігор

Розглянемо задачу диференціальної гри у наступній постановці. Вектори стану супротивників A і B – розподілених динамічних систем захисту інформації – описуються векторними диференціальними рівняннями з частковими похідними виду

$$\frac{\partial \phi_1}{\partial t}=F_i\left(\phi_{i=A,B},\frac{\partial \phi_{i=A,B}}{\partial X},\ldots,\frac{\partial \phi^{(n)}_{i=A,B}}{\partial X^{(n)}},X,t\right)+$$

$$+F_{i_0}\left(\phi_{i=A,B},\frac{\partial \phi_{i=A,B}}{\partial X},\ldots,\frac{\partial \phi^{(n)}_{i=A,B}}{\partial X^{(n)}},\mathrm{X},t\right)U_i\left(\phi_{i=A,B},X,t\right), \tag{3.22}$$

де $\varphi_i = \varphi_i(X,t)$ – вектор станів розподіленої системи – супротивників, *i=A,B*; *X* – вектор аргументу; F_i, F_{i0} – відомі нелінійні вектори і матричні функції; $U_i = U_i(\varphi_{i=A,B}, X, t)$ – вектори ігрового управління.

Від кожного *i*-го учасника, який точно знає поточний стан свій і супротивника, потрібно вибирати управління U_i, так щоб мінімізувати деякий заданий функціонал якості $J_{1i}(\varphi_{i=A(B)})$ при одночасній максимізації другого $J_{2i}(\varphi_{i=A(B)})$. Так, наприклад, в задачах інформаційної боротьби іточнику інформації *A* необхідно забезпечити мінімум відхилення субвектора параметрів φ_{SA} електромагнітного потоку від вектора заданих значень *g* у відповідній області аргумента X^*

$$J_{1A} = \int_{X^*} [\phi_{sa} - g]^T [\phi_{sa} - g] dX ,$$

а об'єкт, що створює перешкоди – мінімум його відхилення від вектора значень *h*, необхідних учаснику подій *B* (наприклад, нульових)

$$J_{1B} = \int_{X^*} [\phi_{sa} - h]^T [\phi_{sa} - h] dX .$$

В більш складному варіанті подій учасникові *A* ще додатково потрібна станція *B*, тобто забезпечити мінімум функціонала $J_{2A} = \int_{X^*} \phi_{SB}^T \phi_{SB} dX$, а учасникові *B* – зберегти параметри свого потоку в заданих межах, тобто мінімізувати $J_{2B} = \int_{X^*} [\phi_{SB} - q]^T [\phi_{SB} - q] dX$, де q – вектор відомих необхідних значень.

В узагальненій формі існуючі для розподілених систем критерії J_{ji} можна представити, згідно [24,25,37,47], у вигляді

$$J_{ji} = \int_X \Phi_{ji}[X, \phi_{i=A,B}(X,t)] dX ,$$

де Φ_{ji} - відома нелінійна функція векторного аргументу, *i=A,B; j=1,2,….*

Слід при цьому відмітити, що в більшості практичних випадків (як видно з викладеного вище) функція Φ_{ji} обирається або монотонно зростаючою на відомому інтервалі аргументу, або квадратичною, що дозволяє у подальших міркуваннях зробити припущення про її позитивну визначеність.

Перед остаточною формалізацією постановки задачі об'єднаємо систему векторних рівнянь (3.22)

$$\frac{\partial \phi_A}{\partial t} = F_A + F_{A0} U_A(\phi_A, \phi_B, X, t),$$

$$\frac{\partial \phi_B}{\partial t} = F_B + F_{B0} U_B(\phi_A, \phi_B, X, t),$$

в єдине векторне рівняння

$$\frac{\partial \phi}{\partial t} = F + F_1 U_A(\phi, X, t) + F_2 U_B(\phi, X, t), \qquad (3.23)$$

де $\phi = \begin{vmatrix} \phi_A \\ \phi_B \end{vmatrix}$, $F = \begin{vmatrix} F_A \\ F_B \end{vmatrix} = F(\phi, X, t)$,

$$F_1 = \begin{vmatrix} F_{A0} \\ 0 \end{vmatrix} = F_1(\phi, X, t), \; F_2 = \begin{vmatrix} 0 \\ F_{B0} \end{vmatrix} = F_2(\phi, X, t),$$

а також врахуємо, що при синтезі реальних динамічних систем, окрім розглянутих критеріїв, які вирішують задачу досягнення заданих вимог до динаміки стану системи (3.23), при формуванні вектора управління вводять, як правило, критерій, мінімізація якого забезпечує мінімум «енергетики», управління в вільний поточний момент часу і який може бути записаний у загальному вигляді в формі

$$J_{U_i} = \int_{t_0}^{t} \int_{X} \Phi_{U_i}[U_i(\varphi, X, t)] dX dt \;\; J_{U_B} = \int_{t_0}^{t} \int_{X} \Phi_{U_B}[U_B(\varphi, X, t)] dX dt$$

де Φ_{U_i} - відома нелінійна функція, яка обирається в більшості випадків квадратичною: $\Phi_{U_i} = U_i^T U_i$; $i=A,B$.

Тоді, згідно з викладеним, організація процедури синтезу ігрових управлінь, яка розшукуються, потребує вибору векторів U_A, U_B з умови мінімуму відповідних функціоналів.

$$J_A = \int_X \Phi_A[X,\phi]dX + \int_{t_0}^{t}\int_X \Phi_{U_A}[U_A]dXdt\,,$$

$$J_B = \int_X \Phi_B[X,\phi]dX + \int_{t_0}^{t}\int_X \Phi_{U_B}[U_B]dXdt\,, \qquad (3.24)$$

одночасно визначених на множині рішень рівняння

$$\frac{\partial\phi}{\partial t} = F + F_1U_A + F_2U_B\,, \qquad (3.25)$$

Згідно розглянутої вище позитивної визначеності функціоналів $J_{A(B)}$, а також їх «енергетичних» складових $\Phi_{U_{A(B)}}$, для рішення поставленої задачі доцільно використовувати той відомий факт, що при невід'ємно визначеній критеріальній функції для забезпечення її мінімального значення в кожний момент часу достатньо, щоб похідна її по часу, яка взята зі зворотнім знаком, мала максимум [24,29,37,71]. На першому етапі синтезу при пошуку керування U_A, це приводить до умови

$$\max_{U_A}(-J_A) = \max_{U_A}\{-\int_X(\frac{\partial\Phi_A}{\partial\phi}\phi + \Phi_{U_A}[U_A])dX\} =$$
$$= \max_{U_A}\{-\int_X(\frac{\partial\Phi_A}{\partial\phi}[F + F_1U_A + F_2U_B] + \Phi_{U_A}[U_A])dX\}\,,$$

Аналіз отриманого рівняння показує, що рішення поставленої задачі зводиться до класичної задачі пошуку вектор-функції U_A, яка реалізує мінімум визначеного інтегралу

$$\int_X(\frac{\partial\Phi_A}{\partial\phi}\,[F + F_1U_A + F_2U_B] + \Phi_{U_A}[U_A])dX\,.$$

При цьому вектор-функція U_A, яка розшукується, повинна задовольняти рівнянню Ейлера

$$\frac{\partial \Phi_A}{\partial \phi} F_1 - \frac{\partial}{\partial U_A} \Phi_{U_A}[U_A] = 0,$$

або

$$(\frac{\partial \Phi_{U_A}}{\partial U_A})^T = F_1^T \frac{\partial \Phi_A^T}{\partial \phi}, \tag{3.26}$$

з якого випливає, що у загальному випадку визначення вектора U_A потребує рішення нелінійного векторного рівняння, яке представляє непросту обчислювальну задачу.

У окремому випадку квадратичної форми функції Φ_{U_A} рішення рівняння легко знаходиться аналітично:

$$(2U_{A_{opt}}^T)^T = F_1^T \frac{\partial \Phi_A^T}{\partial \phi},$$

тобто

$$U_{Aopt} = \frac{1}{2} F_1^T \frac{\partial \Phi_A^T}{\partial \phi} = \frac{1}{2} F_{A_0}^T \frac{\partial \Phi_A^T}{\partial \phi}) \tag{3.27}$$

Тут функція φ визначається вже з рішення рівняння, отриманого підстановкою U_{Aopt} у рівняння (3.23):

$$\frac{\partial \phi}{\partial t} = \mathrm{F} + \frac{1}{2} F_1 F_1^T \frac{\partial \Phi_A^T}{\partial \phi} + F_2 U_B = F^* + F_2 U_B. \tag{3.28}$$

Рівняння (3.27) і (3.28) завершують 1-й шаг (етап) синтезу потрібного ігрового управління, після чого починається процедура 2-го шагу – пошук оптимального вектору U_B з умови мінімуму критерія J_B:

$$J_B = \int_X \Phi_B[X, \phi] dX + \int_{t_0}^{t} \int_X \Phi_{U_B}[U_B] dX dt. \tag{3.29}$$

Зрозуміло, що внаслідок збігу структур рівняння (3.28):

$$\frac{\partial \phi}{\partial t} = F^* + F_2 U_B,$$

і рівняння (3.25), а також критеріїв J_A і J_B, вектор U_B може бути сформований з використанням підходу, який співпадає з приведеним. Таким чином, задача 2-го етапу – синтез оптимального рівняння $U_B(\varphi,X,t)$ – може бути сформована як задача пошуку вектор-функції U_B, яка доставляє мінімум (3.29) на множині функцій $\varphi(X,t)$, задовольняючих рішенню (3.28). Так як дана задача з точністю до позначень співпадає з приведеною вище, то й алгоритм її рішення виявляється тим же. Повторюючи попередні обчислення, приходимо до рівняння для оптимального управління $U_B(\varphi,X,t)$, аналогічного (3.26):

$$(\frac{\partial \Phi_{U_B}}{\partial U_B})^T = F_2^T \frac{\partial \Phi_B^T}{\partial \varphi},$$

звідки для традиційного випадку квадратичної форми Φ_{U_B} одержуємо

$$U_{Bopt} = \frac{1}{2} F_2^T \frac{\partial \Phi_B^T}{\partial \varphi} = \frac{1}{2} F_{B_0}^T \frac{\partial \Phi_B^T}{\partial \varphi} \tag{3.30}$$

Логічно, що в цьому випадку вектор-функція φ, яка визначає вираз як для $U_{Aopt}(\varphi,X,t)$, так і для $U_{Bopt}(\varphi,X,t)$, являє собою рішення рівняння:

$$\frac{\partial \varphi}{\partial t} = F + \frac{1}{2} F_1 F_1^T \frac{\partial \Phi_A^T}{\partial \varphi} + \frac{1}{2} F_2 F_2^T \frac{\partial \Phi_B^T}{\partial \varphi}, \tag{3.31}$$

інтегрування якого (кожним учасником подій для свого вектора стану) завершує процес рішення поставленої задачі.

Слід відмітити, що з обчислювальної точки зору розв'язання рівняння (3.31) виявляється не набагато складніше, ніж розв'язання рівняння (3.24). Більше того, схожість структур (3.23) і (3.31) обумовлює можливість використання у повному обсязі методів, розроблених для розв'язання рівняння (3.23) в працях [37,71].

Для зображення можливості практичного використання запропонованого підходу розглянемо наступну ситуацію.

Нехай об'єкт *A*, який описується нелінійним стохастичним рівнянням

$$\dot{x} = -x - 0{,}01x^2 - 0{,}2y + U_A + \xi_x ,$$

де ξ_x – білий гаусовський нормований шум, функціонує в умовах протидії супротивника B, який описується у свою чергу рівнянням

$$\dot{y} = -y^3 - 0{,}1x^2 + U_B + \xi_y ;$$

де ξ_y – також білий гаусовський нормований шум.

Учасникові ситуації *A*, який спостерігає за станом своїм та супротивника за допомогою вимірювача

$$z_x = 1{,}5x^2 + y + \xi_x ,$$

де ξ_x – білий гаусовський центрований шум з інтенсивністю D_x, потрібно забезпечити в кожний поточний момент часу близьке до гаусовського розподілення координати *x* з нульовим середнім математичним очікуванням $m_x=0$ та дисперсією $D_x=0{,}8$ при одночасному «нав'язуванні» супротивникові близького до гаусовського розподілення з математичним очікуванням $m_y=3{,}5$ та дисперсією $D_y=50$. Аналогічно протидіючий йому супротивник *B*, який спостерігає за своїм станом і станом об'єкту *A* за допомогою контролюючої апаратури

$$z_y = y^2 + x + \xi_y ,$$

де ξ_y – білий гаусовський центрований шум з інтенсивністю D_y, має за мету досягти для себе гаусовського розподілення зі середнім математичним очікуванням, дорівнюючим 0,5, та дисперсією 0,6, а для супротивника – зі середнім математичним очікуванням, дорівнюючим 7, і дисперсією 50. Так як мета ситуації, що склалася – забезпечення відповідних розподілень, то для її досягнення необхідне знання відповідної щільності розподілення $\varphi=\varphi(x,y)$, яка описується в даному випадку рівнянням Стратоновича [37,71].

$$\frac{\partial \phi}{\partial t} = (1 + 0,02x + 3y^2)\phi + (x + 0,01x^2 + 0,2y)\ \frac{\partial \phi}{\partial x} + (y^3 + 0,1x^2)\frac{\partial \phi}{\partial y} +$$

$$+ \frac{1}{2}\left(\frac{\partial^2 \phi}{\partial x^2} + \frac{\partial^2 \phi}{\partial y^2}\right) + [\theta - \theta_0]\phi - U_A \frac{\partial \phi}{\partial x} - U_B \frac{\partial \phi}{\partial y} - \frac{\partial U_A}{\partial x}\phi - \frac{\partial U_B}{\partial y}\phi, \qquad (3.32)$$

$$\theta = \frac{1}{2}\left[z - \begin{vmatrix} 1,5x^2 + y \\ y^2 + x \end{vmatrix} \right]^T \begin{vmatrix} D_x^{-1} & 0 \\ 0 & D_y^{-1} \end{vmatrix} \left[z - \begin{vmatrix} 1,5x^2 + y \\ y^2 + x \end{vmatrix} \right],$$

яке співпадає за своєю структурою з рівнянням (3.25).

Функціонали, які мінімізуються, в даному випадку приймають вигляд:

$$J_A = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} \left\{\phi(x,y) - G_1\left[(0;0,8;x),(3,5;50;y)\right]\right\}^2 dxdy + \int_{t_0}^{t}\int_{-\infty}^{\infty} U_A^2(x,y,t)dxdydt,$$

де $G_i[(m_x, D_x, x),(m_y, D_y, y)]$, *i=1,2.* – двомірне гаусовське розподілення з відповідними характеристиками.

Слідуючи міркуванням, які привели до виразу для оптимальних законів управління (3.27) і (3.30) аналогічно отримуємо:

$$U_{Aopt}(x,y) = \frac{\partial}{\partial x}(G_1 - \phi)\phi,$$

$$U_{Bopt}(x,y) = \frac{\partial}{\partial x}(G_2 - \phi)\phi, \qquad (3.33)$$

де функція φ визначається інтегруванням рівняння (3.32) після підстановки до нього законів (3.33).

Дане рівняння розв'язано методом прямокутних сіток в області $(x,y) \in [-230,230]$ з шагом $\Delta x = \Delta y = 0,05$ при $D_x = D_y = 1,5$, $\varphi(x,y,t_0) = G[(0,1;0,3;x),(0,4;0,4;y)]$ для $Z(t_i)$, які отримані в результаті чисельного моделювання рівнянь об'єктів та спостерігачів на інтервалі $t \in [0,100]$ за методом Рунге-Кутта 4-го порядку з шагом $\Delta t = 0,05c$ (формування управління здійснювалось у масштабі часу надходження вимірювальної інформації, тобто для кожного часового кроку моделювання

t_i. По закінченню часу моделювання інтегральні квадратичні відхилення φ виявились такими:

- при відсутності протидії зі сторони супротивника *B* (управління $U_B=0, J_B=0$) відхилення φ від G_1 склало ≈0,26;
- при відсутності протидії зі сторони того, хто захищається $A(U_A=0, J_A=0)$ відхилення φ від G_2 склало ≈0,18;
- при реалізації ситуації у повному обсязі (як було розглянуто вище при синтезі управлінь U_A, U_B) відхилення φ від G_1 склало ≈0,21; від G_2 склало ≈0,23.

3.3. Метод оптимізації поведінки систем захисту інформації в умовах впливів

На підставі досліджень, які були проведені у попередніх підрозділах, будемо вважати, що типовою задачею дослідження поведінки СЗІ в умовах впливів на інформацію є оптимальний розподіл ресурсів гравця безпеки відносно ресурсів гравця впливів.

Нехай є дві системи. Одна із систем – система впливів (СВ) – є гравцем, що впливає на інформацію другої системи системи (СБІ), гравця, що забезпечує безпеку. Для цього СВ використовує певну кількість методів і засобів впливів. Засоби впливу СВ складаються з S_1 типів, причому в деяких умовних одиницях кількість засобів m-го типу дорівнює a_m. Сумарний атакуючий ресурс (потенціал) СВ M_1 становить величину, що дорівнює $M_1 = \sum_{m=1}^{S_1} a_m$. Аналогічно СБІ складається з S_2 типів підсистем безпеки, причому кількість засобів безпеки j-го типу в умовних одиницях дорівнює d_j. Сумарний захисний потенціал СБІ M_2 визначається як $M_2 = \sum_{j=1}^{S_2} d_j$.

Інформація, яка підлягає захисту, має n інформаційних блоків $B_i, \ldots, B_n$, причому цінність B_i-го блоку оцінюється деякою умовною величиною v_i, де $i = 1, \ldots, n$. Нехай також інформаційні блоки $B_i, \ldots, B_n$ упорядковані за їх цінністю, тобто $v_i \geq \ldots \geq v_n$.

Припустимо, що кожен незахищений інформаційний блок B_i під час впливу на інформацію та реалізації одного впливу засобами m-го типу втрачає свої властивості – цілісність, доступність та конфіденційність. Величина втрат від впливу на інформацію в СЗІ на B_i-й інформаційний блок оцінюється величиною $v_i \varepsilon_m$.

Сумарні втрати цілісності, доступності та конфіденційності інформації $I(\lambda, \mu)$, які визначають її захищеність в СБІ за умови наявності впливів та протидії ним можна оцінити величиною, пропорційною різниці їх сумарної кількості, якщо вона позитивно визначена, і рівною нулю у протилежному випадку, тобто

$$I(\lambda, \mu) = \sum_{i=1}^{n} v_i \max\left\{0, \sum_{m=1}^{S_1} \varepsilon_m \left(\mu_{im} - \sum_{j=1}^{S_2} \lambda_{mj} \lambda_{ij} \right)\right\}, \tag{3.34}$$

де μ_{im} – інтенсивність потоку інформаційних впливів, виділених СВ для впливу на B_i-й інформаційний блок засобами впливу m-го типу;

λ_{ij} – інтенсивність потоку дій, виділених СБІ для забезпечення безпеки B_i-го інформаційного блоку засобами забезпечення безпеки j-го типу;

λ_{mj} – інтенсивність потоку дій, що виділяється СБІ для відбиття впливу від засобів m-го типу засобами забезпечення безпеки j-го типу.

Розподіл засобів забезпечення безпеки j-го типу, що виділяються СБІ для відбиття впливу від засобів m-го типу за умови $\sum_{m=1}^{S_1} \lambda_{mj} = 1$, $1 \leq j \leq S_2$ та $1 \leq m \leq S_1$, може бути поданий у матричному вигляді:

$$\Lambda = \left\| \lambda_{m\,j} \right\|, \tag{3.35}$$

за відповідних обмежень

$$0 \le \lambda_{m\,j} \le \lambda_{m\,j_{\max}}, \tag{3.36}$$

де $\lambda_{m\,j_{\max}}$ – максимальна інтенсивність потоку дій , щодо забезпечення безпеки $\lambda_{m\,j_{\max}} = 1$.

Нехай сумарна величина втрат інформації в СБІ $I(\lambda, \mu)$ (3.34) виступатиме основною характеристикою інформаційного конфлікту, джерелом якого є протиріччя інтересів СБІ та СВ. При цьому СБІ намагається підвищити захищеність інформації шляхом зменшення величини сумарних втрат (3.34), що наносяться діями впливів СВ. Метою СВ є протилежною, тому функція (3.34) може бути прийнята як плата системи забезпечення безпеки інформації системі впливів. У результаті задача синтезу оптимальної поведінки в системі безпека-вплив зводиться до антагоністичної гри двох гравців з опуклою по одній змінній λ функцією виграшу $I(\lambda, \mu)$ (3.34) при довільному фіксованому значенні другої змінної μ.

Виходячи з методики знаходження рішень антагоністичних ігор для опуклих по одній змінній функцій виграшу [24,25,29], сформулюємо задачу синтезу оптимальної поведінки в системі безпека-вплив у вигляді наступної теореми.

Теорема 3.1. Нехай плата $I(\lambda, \mu)$ є неперервною за двома змінними λ та μ функцією виграшу для антагоністичної гри, яка строго опукла по λ для кожного довільно фіксованого μ і така, що має на одиничному інтервалі першу похідну по λ. Тоді існує єдина оптимальна стратегія захисту для СБІ λ^{opt}, що є східчастою функцією плати $I(\lambda^{opt}, \mu)$, причому $\lambda^{opt} = const$, та єдиним розв'язком рівняння

$$I\left(\lambda^{opt},\mu\right)=\max_{0\le\mu\le1} I\left(\lambda^{opt},\mu\right)\ . \tag{3.37}$$

У разі вибору обома гравцями СВ та СБІ оптимальних стратегій μ^{opt} та λ^{opt} відповідно ціна гри I^* може бути визначена як

$$I^*=\min_{0\le\lambda\le1}\max_{0\le\mu\le1} I\left(\lambda^{opt},\mu^{opt}\right). \tag{3.38}$$

Доведення. Оптимальна стратегія гравця впливу μ^{opt} може бути визначена залежно від значення оптимальної стратегії гравця забезпечення безпеки λ^{opt}. Якщо гравець забезпечення безпеки обирає одну з оптимальних стратегій:

$$\lambda^{opt}=\begin{cases}1, & \dfrac{\partial I\left(\lambda^{opt},\mu^{opt}\right)}{\partial\lambda}\le 0;\\[2ex] 0, & \dfrac{\partial I\left(\lambda^{opt},\mu^{opt}\right)}{\partial\lambda}>0,\end{cases} \tag{3.39}$$

то гравець впливу обиратиме таку оптимальну стратегію $\mu^{opt}=const$, що буде задовольняти умовам

$$0\le\mu^{opt}\le1, \tag{3.40}$$

та вразу (3.38).

Якщо гравець забезпечення безпеки відхиляється від оптимальної стратегії λ^{opt} у межах $0<\lambda<1$, то гравець впливу обиратиме стратегію вигляду

$$\mu(\alpha)=\alpha I\left(\lambda,\mu_1\right)+(1-\alpha)I\left(\lambda,\mu_2\right), \tag{3.41}$$

де α, μ_1, μ_2 – довільні сталі, що задовольняють умовам

$$\begin{gathered}0\le\alpha\le1,\quad 0\le\mu_1\le1,\quad 0\le\mu_2\le1,\quad I\left(\lambda^{opt},\mu_1\right)=I\left(\lambda^{opt},\mu_2\right)=I,\\ \frac{\partial I\left(\lambda^{opt},\mu_1\right)}{\partial\lambda}\ge0,\ \frac{\partial I\left(\lambda^{opt},\mu_2\right)}{\partial\lambda}\le0,\ \alpha\frac{\partial I\left(\lambda^{opt},\mu_1\right)}{\partial\lambda}+(1-\alpha)\frac{\partial I\left(\lambda^{opt},\mu_2\right)}{\partial\lambda}=0.\end{gathered} \tag{3.42}$$

Зауваження. Накладені на функцію плати $I(\lambda,\mu)$ (3.34) вимоги можливо послабити.

По-перше, можна знехтувати умовами існування похідних. Але у даному випадку передбачається існування односторонніх похідних функції $I(\lambda,\mu)$ у кожній точці інтервалу її визначення. Тоді умови, накладені на похідні $\frac{\partial I\left(\lambda^{opt},\mu_1\right)}{\partial\lambda}$ і $\frac{\partial I\left(\lambda^{opt},\mu_2\right)}{\partial\lambda}$, замінюються відповідними умовами для односторонніх похідних у вказаних точках.

По-друге, умову строгої опуклості функції виграшу $I(\lambda,\mu)$ можна послабити, замінивши її умовою, що вона є просто опуклою. Але це призводить до того, що оптимальні стратегії як для першого μ^{opt}, так і для другого λ^{opt} гравців не єдині.

На основі теореми 3.1 та з урахуванням зауваження чиста оптимальна стратегія забезпечення безпеки СБІ λ^{opt} може бути визначена з рівняння

$$\inf_{\lambda}\ \sup_{\mu} I(\lambda,\mu)=\sup_{\mu} I\left(\lambda^{opt},\mu\right)=I\,. \tag{3.43}$$

Врахувавши (3.43), СВ обирає змішану оптимальну стратегію $\mu^{*}(\alpha)$, що є певною опуклою комбінацією скінченної кількості чистих стратегій.

Введемо деякі позначення. Нехай $X_i=\left\|\mu_{i1},\ldots,\mu_{iS_1}\right\|$, $Y_i=\left\|\lambda_{i1},\ldots,\lambda_{iS_2}\right\|$, $\xi_i=\left\|\nu_i\varepsilon_1,\ldots,\nu_i\varepsilon_{S_1}\right\|$. Тоді плата (3.34) з урахуванням прийнятих позначень може бути подана у матричній формі:

$$I(\lambda,\mu)=\sum_{i=1}^{n}\max\left\{0,\ \xi'\left(X_i-\Lambda Y_i\right)\right\}, \tag{3.44}$$

де ξ' – транспонована матриця до матриці ξ.

Оскільки функція плати $I(\lambda,\mu)$ (3.34) опукла по λ для кожного довільно фіксованого μ, то СА при побудові оптимальної стратегії μ^{opt} може

використовувати рандомізовану лише серед тих чистих стратегій, які є вершинами симплекса:

$$\mu^{opt} = \left\{ \sum_{i=1}^{S_1} \delta_i \, \alpha_i \right\}, \tag{3.45}$$

де $\delta_i \geq 0$, $\sum_{i=1}^{S_1} \delta_i = 1$.

При цьому плата (3.34) з урахуванням (3.45) набуватиме вигляду

$$I(\lambda, \mu) = I\left(\lambda, \sum_{i=1}^{S_1} \delta_i \, \alpha_i \right) \leq \sum_{i=1}^{S_1} \delta_i \, I(\lambda, \alpha_i). \tag{3.46}$$

Позначимо через I_m частину ціни гри I^*, яка може бути отримана СВ за рахунок застосування засобів впливу m-го типу, так що $\sum_{m=1}^{S_1} I_m = I^*$ і $Q = \| a_1, \ldots, a_{S1} \|$. Тоді для визначення стратегії забезпечення безпеки B_i-го інформаційного блоку для СБІ згідно із сформульованою теоремою 3.1 отримуємо матричне рівняння

$$Q - \Lambda Y_i = I_i. \tag{3.47}$$

Для розв'язку матричного рівняння (3.47) доцільно застосувати узагальнену обернену матрицю Мура-Пенроуза, вперше введену в роботі [102].

Нехай для прямокутної матриці Λ (3.35) існує узагальнена обернена матриця Мура-Пенроуза Λ^+, для якої справедливі такі умови [102]:

$$\Lambda \Lambda^+ \Lambda = \Lambda, \qquad \Lambda^+ \Lambda \Lambda^+ = \Lambda^+, \qquad \left(\Lambda \Lambda^+ \right)^* = \Lambda \Lambda^+, \qquad \left(\Lambda^+ \Lambda \right)^* = \Lambda^+ \Lambda, \tag{3.48}$$

де Λ^* – ермітово спряжена матриця, яка для матриці Λ над полем дійсних чисел є транспонованою, тобто $\Lambda^* = \Lambda'$.

Так, для неособливої квадратної матриці Λ (3.35) визначено узагальнену обернену матрицю Λ^{+}, яка збігається зі звичайною оберненою матрицею Λ^{-1}, тобто $\Lambda^{+} = \Lambda^{-1} = \left\| \beta_{ij} \right\|$.

З урахуванням властивостей узагальненої оберненої матриці (3.48) з матричного рівняння (3.47) отримуємо

$$Y_i = \Lambda^{+} \left(Q - I_i \right), \tag{3.49}$$

звідки стратегія забезпечення безпеки B_i-го інформаційного блоку засобами забезпечення безпеки j-го типу СЗІ λ_{ij}, що визначає інтенсивність потоку дій щодо забезпечення безпеки з урахуванням прийнятих вище позначень, набуває вигляду

$$\lambda_{ij} = \sum_{m=1}^{S_1} \beta_{jm} \left(a_m - \frac{I_m}{v_i \varepsilon_m} \right). \tag{3.50}$$

Припустимо, що СБІ розміщує свої засоби протидії j-го типу серед найбільш цінної інформації $\psi(j)$, тобто

$$\lambda_{\psi(j)+1,j} = \lambda_{\psi(j)+2,j} = \ldots = \lambda_{n,j} = 0. \tag{3.51}$$

Сумуючи величини (3.50) за всіма n інформаційними блоками $B_i, \ldots, B_n$ та враховуючи припущення (3.51), визначаємо стратегію для гравця на випадок забезпечення безпеки для найбільш цінної інформації:

$$\sum_{i=1}^{\psi(j)} \lambda_{ij} = \psi(j) \sum_{m=1}^{S_1} \beta_{jm} a_m - L_{\psi(j)} \sum_{m=1}^{S_1} \beta_{jm} \frac{I_m}{\varepsilon_m}, \tag{3.52}$$

де $L_{\psi(j)} = \sum_{i=1}^{\psi(j)} \frac{1}{v_i}$.

Оскільки $\sum_{i=1}^{\psi(j)} \lambda_{ij} = d_j$ згідно з припущенням, то з (3.52) маємо

$$\sum_{m=1}^{S_1} \beta_{jm} \frac{I_m}{\varepsilon_m} = \frac{1}{L_{\psi(j)}} \left[\psi(j) \sum_{m=1}^{S_1} \beta_{jm} a_m - d_j \right]. \qquad (3.53)$$

Позначимо

$$W = \left\| \frac{I_1}{\varepsilon_1}, \ldots, \frac{I_{S_1}}{\varepsilon_{S_1}} \right\|, \; S = \left\| \begin{matrix} \frac{\psi(1)}{L_{\psi(1)}} & 0 & \ldots & 0 \\ & \frac{\psi(2)}{L_{\psi(2)}} & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & \frac{\psi(S_2)}{L_{\psi(S_2)}} \end{matrix} \right\|, \; R = \left\| \frac{d_1}{\psi(1)}, \ldots, \frac{d_{S_1}}{\psi(S_2)} \right\|.$$

Виходячи з прийнятих позначень перейдемо від рівняння (3.53) до його матричної форми

$$\Lambda^+ W = S\left(\Lambda^+ Q - R\right). \qquad (3.54)$$

Скориставшись властивостями узагальненої оберненої матриці (3.48) з виразу (3.54) після спрощень, маємо

$$W = \Lambda S\left(\Lambda^+ Q - R\right), \qquad (3.55)$$

звідки частина ціни гри I_m, що є платою СБІ за втрати найбільш цінної інформації, визначається як

$$I_m = \varepsilon_m \sum_{j=1}^{S_2} \frac{\lambda_{mj}}{L_{\psi(j)}} \left[\psi(j) \sum_{m=1}^{S_1} \beta_{jm} a_m - d_j \right]. \qquad (3.56)$$

СВ діятиме оптимально, якщо буде впливати на найбільш цінну інформацію $\psi = \max \psi(j)$, для якої забезпечує безпеку СБІ з деякою ймовірністю p_i. При цьому ціна гри для СВ може бути визначена як

$$I^* = \sum_{m=1}^{S_1} I_m = \sum_{m=1}^{S_1} \sum_{j=1}^{S_2} \frac{\varepsilon_m \lambda_{mj}}{L_{\psi(j)}} \left[\psi(j) \sum_{m=1}^{S_1} \beta_{jm} a_m - d_j \right]. \qquad (3.57)$$

Висновок з теореми 3.1. Математичне сподівання виграшу від впливу всіма засобами впливу на кожен блок інформації B_i, для якої забезпечується безпека всіма засобами забезпечення безпеки СБІ, не залежить від номера інформаційного блоку i, тобто $p_i v_i = c = const$. Врахувавши умову нормування $\sum_{i=1}^{\psi} p_i = 1$, маємо

$$p_i = \begin{cases} c/v_i, & 1 \le i \le \psi; \\ 0, & i > \psi, \end{cases}$$

де $c = \left(\sum_{i=1}^{\psi} \frac{1}{v_i} \right)^{-1} = \frac{1}{L_\psi}$.

Таким чином, синтез оптимальної поведінки СБІ–СВ визначається оптимальними стратегіями гравців в інформаційному конфлікті, вирази (3.39) та (3.45) відповідно.

Приклад. Нехай СБІ обирається довільна стратегія забезпечення безпеки, але така, що не є оптимальною (3.39), тоді вибір СВ оптимальної стратегії (3.45) гарантує їй виграш у платі E_1 не менше від ціни гри I^* (3.57), тобто

$$\begin{aligned} E_1 &= \sum_{i=1}^{\psi} \frac{1}{v_i L_\psi} \sum_{m=1}^{S_1} \varepsilon_m \left[a_m - \sum_{j=1}^{S_2} \lambda_{mj} \lambda_{ij} \right] = \\ &= \frac{\psi}{L_\psi} \varepsilon_m \left[\sum_{j=1}^{S_2} \sum_{m=1}^{S_1} \beta_{jm} a_m \lambda_{mj} \right] - \sum_{i=1}^{\psi} \frac{1}{L_\psi} \sum_{m=1}^{S_1} \varepsilon_m \sum_{j=1}^{S_2} \lambda_{mj} \lambda_{ij} \ge \\ &\ge \sum_{m=1}^{S_1} \varepsilon_m \sum_{j=1}^{S_2} \left[\psi(j) \sum_{m=1}^{S_1} \beta_{jm} a_m \lambda_{mj} \right] \frac{1}{L_{\psi(j)}} - \sum_{m=1}^{S_1} \varepsilon_m \sum_{j=1}^{S_2} \frac{\lambda_{mj} d_j}{L_{\psi(j)}} = \\ &= \sum_{m=1}^{S_1} \sum_{j=1}^{S_2} \frac{\varepsilon_m \lambda_{mj}}{L_{\psi(j)}} \left[\psi(j) \sum_{m=1}^{S_1} \beta_{jm} a_m - d_j \right] = I^*. \end{aligned} \tag{3.58}$$

Нехай стратегія впливу СВ не є оптимальною, тоді, виходячи з матричного рівняння (3.44), втрати інформації в СБІ не перевищуватимуть величини E_2:

$$E_2 = v_i \sum_{m=1}^{S_1} \varepsilon_m \left\{ \mu_{im} - \sum_{j=1}^{S_2} \lambda_{mj} \left[\beta_{jm} \left(a_m - \frac{I_m}{v_i\, \varepsilon_m} \right) \right] \right\} \le$$

$$\le v_i \left\{ \sum_{m=1}^{S_1} \varepsilon_m \left[a_m - \sum_{j=1}^{S_2} \sum_{m=1}^{S_1} \beta_{jm}\, a_m\, \lambda_{mj} + \sum_{j=1}^{S_2} \sum_{m=1}^{S_1} \beta_{jm} \frac{I_m}{v_i\, \varepsilon_m} \lambda_{mj} \right] \right\} = \qquad (3.59)$$

$$= v_i \left\{ \sum_{m=1}^{S_1} \varepsilon_m\, a_m - \left[\sum_{m=1}^{S_1} \varepsilon_m\, a_m + \sum_{m=1}^{S_1} \frac{I_m}{v_i} \right] \right\} = I\,.$$

Виходячи з даних співвідношень, випливає справедливість сформульованих згідно з теоремою 3.1 тверджень. Отже, теорема 3.1 доведена.

3.4. Висновки до третього розділу

Запропоновано систему правил щодо моделювання критеріїв оптимальності, які, за рахунок синтезу морфологічним методом сепарабельних адитивних критеріїв та обмежень, дозволяють розв’язувати задачі аналізу, синтезу та оптимізації систем за обраними критеріями та виділеними обмеженнями, а також оцінювати рівень захищеності інформаційних систем з урахуванням дозволених границь гарантованого рівня захисту інформації.

Запропоновано диференціально-ігровий метод оптимізації параметрів інформаційних систем, що, за рахунок врахування стратегії гравця впливу, критерію оптимізації ресурсів гравців у процесі оптимізації і енергетичної складової у заданий період часу, дозволяє визначати у реальному часі оптимальну стратегію безпеки інформації в інформаційних системах.

РОЗДІЛ 4. ЕКСПЕРИМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ ВПЛИВІВ НА ІНФОРМАЦІЙНІ СИСТЕМИ ТА ОЦІНКА ЇХ УРАЗЛИВОСТЕЙ

4.1. Методика проведення експериментального дослідження

Метою експериментального дослідження є вивчення якостей оцінюваних об'єктів, перевірка правильності формування та достовірності гіпотез, глибоке вивчення досліджуваної наукової тематики [15,44]. Правильний вибір методики експерименту займає особливе значення при його проведенні. Методика експериментального дослідження – визначена послідовність процесів, у результаті якої досягається мета дослідження.

Перший крок у проведенні експериментального дослідження займає складання плану – програми дослідження [23,26]:

1. Мета та задачі експерименту:

1.1. Оцінити прогнозований та поточний рівень захищеності інформаційних ресурсів для таких стратегій побудови систем безпеки, як: ешелонована система захисту з n бар'єрів захисту [23,24]; стратегія відведення гравця впливу на хибний інформаційний ресурс з подальшим втягуванням його в інформаційний конфлікт [24]; стратегія оцінювання рівня захищеності за шаблоном нормальної поведінки системи [25]. Перевірити достовірність методу оптимізації поведінки систем безпеки інформації в умовах впливів.

1.2. Відповідно до визначених параметрів ІС провести моделювання її поточних станів для перевірки можливості ідентифікації уразливості інформаційних систем в умовах впливів на основі розробленої методики оцінки уразливостей.

2. Вибір вхідних та вихідних параметрів:

2.1. Вхідні параметри: обрані типи впливів, типи підсистем захисту та стратегії побудови систем безпеки. Вихідні параметри: прогнозований $I\left(\lambda^{opt},\mu^{opt}\right)$ та поточний $I\left(\lambda,\mu\right)$ рівні захищеності інформаційних ресурсів,

залежно від стратегій λ та μ, які обираються гравцями – суб'єктами конфлікту на визначеному інтервалі $[t_0, T]$.

2.2. Вхідні параметри: визначений список параметрів, лінгвістичних змінних, інтервалів, типів уразливостей, лінгвістичних ідентифікаторів, еталонів та правил, що дозволять ідентифікувати тип уразливості інформаційних систем в умовах впливів. Вихідні параметри: Оцінені уразливості ІС.

3. Послідовність дій:

3.1. На основі обраної стратегії побудови систем безпеки визначити вирази оцінки рівня захищеності ІС. Після чого визначити кроки зміни параметрів λ, μ і t: $\Delta\lambda$, $\Delta\mu$ та Δt відповідно. Для кожної комбінації λ, μ і t розрахувати поточний $I(\lambda, \mu)$ рівні захищеності інформаційних ресурсів в момент часу t, $\lambda \in \overline{0,1}$, $\mu \in \overline{0,1}$, $t \in \overline{t_0, T}$.

3.2. Визначений список параметрів, лінгвістичних змінних, інтервалів, типів уразливостей, лінгвістичних ідентифікаторів. Далі слід сформувати еталони та правила визначення уразливостей. Після чого провести моделювання станів ІС.

4. Вибір кроку зміни чинників:

4.1. $\Delta\lambda$ змінюється від 0 до 1 із кроком 0,1; $\Delta\mu$ змінюється від 0 до 1 із кроком 0,1; Δt змінюється від 0 до 1 із кроком 0,1 с.

5. Використовувані засоби: Технологічна платформа 1С:Підприємство 8.2 (для створення програмних засобів, що дозволяють провести дослідження).

6. Аналіз результатів наведено п.3.3 роботи.

Другий крок, здійснюється після затвердження методики, – це визначення об'єму експериментальних досліджень та необхідних програмних засобів [26]. *Третім кроком є безпосереднє проведення експерименту*, а заключним кроком – обробка експериментальних даних, систематизація усіх

числових даних, перевірка зведення до єдиної системи одиниць, побудова графіків залежностей, таблиць, діаграм[24,26].

4.2. Розробка програмних засобів і проведення експериментального дослідження

У якості середовища розробки програмних засобів обрано технологічну платформу 1С: Підприємство 8.2 [13,22,23]. Технологічна платформа надає об'єкти (даних і метаданих) і механізми управління об'єктами [44]. Об'єкти (дані та метадані) описуються у вигляді конфігурацій. При автоматизації будь-якої діяльності (розробці програмних засобів) складається своя конфігурація об'єктів, яка і являє собою закінчене прикладне рішення. Конфігурація створюється в спеціальному режимі роботи програмного продукту під назвою «Конфігуратор», потім запускається режим роботи під назвою «1С: Підприємство», в якому користувач отримує доступ до основних функцій, реалізованим в даному прикладному рішенні (конфігурації). Сама платформа не є програмним продуктом для використання кінцевими користувачами, а слугує фундаментом для розробки та роботи прикладних рішень.

Опишемо основні ключові можливості технологічної платформи 1С: Підприємства 8.2 [13,22]:

1. Можливість використання трьох клієнтських програм: Товстий клієнт, Тонкий клієнт, Веб-клієнт.

Товстий клієнт дозволяє реалізовувати повні можливості 1С: Підприємства 8.2 як в плані розробки, адміністрування, так і в плані виконання прикладного коду. Однак він не підтримує роботу з інформаційними базами через Інтернет, вимагає попередньої установки на комп'ютер користувача і має досить значний обсяг дистрибутива.

Тонкий клієнт не дозволяє розробляти й адмініструвати прикладні рішення, однак може працювати з інформаційними базами через Інтернет. Він також вимагає попередньої установки на комп'ютер користувача, але має значно менший розмір дистрибутива, ніж товстий клієнт.

Веб-клієнт не вимагає будь-якої попередньої установки на комп'ютер. На відміну від товстого і тонкого клієнтів, він виконується не в середовищі

операційної системи комп'ютера, а в середовищі інтернет-браузера (Microsoft Internet Explorer або Mozilla Firefox).

2. Багатоплатформеність. У версії 1С: Підприємство 8.2, завдяки появі веб-клієнта, всі компоненти системи можуть працювати на комп'ютерах як під управлінням Windows, так і під управлінням Linux. Причому в будь-яких можливих поєднаннях.

3. Відмовостійкий масштабований кластер з динамічним розподілом навантаження. В 1С: Підприємстві 8.2 розвиток кластера серверів виконано відразу по декількох напрямках: масштабованість, відмовостійкість, динамічний розподіл навантаження.

3.1. Масштабованість. Можна управляти розподілом навантаження, яке раніше виконувалось єдиним менеджер кластеру. Тепер це навантаження може бути розподілене між кількома менеджерами кластера, що дозволяє розвантажити головний менеджер кластера і підвищити надійність його роботи.

3.2. Відмовостійкість кластера в цілому досягається за рахунок того, що в 1С: Підприємство 8.2 кілька кластерів можуть бути об'єднані в групу резервування. Кластери, що знаходяться в одній групі резервування синхронізуються автоматично. Відмовостійкість робочих процесів досягається за рахунок їх резервування. Кожному робочому процесу можна вказати варіант його використання. Якщо який-небудь робочий процес завершився аварійно, кластер запускає замість нього один з неактивних резервних процесів і автоматично перерозподіляє навантаження на нього.

3.3. Динамічний розподіл навантаження. Завантаженість робочих процесів аналізується динамічно і при необхідності клієнт автоматично перемикається на більш продуктивний робочий процес. Таке перемикання відбувається абсолютно непомітно для користувача.

4. Новий інтерфейс. 1С: Підприємство 8.2 повністю змінює весь шар роботи з інтерфейсом. Сюди відноситься і командний інтерфейс, і форми, і

віконна система. При цьому не тільки змінюється модель розробки користувальницького інтерфейсу в конфігурації, але і пропонується нова архітектура поділу функціональності між клієнтським додатком і сервером. Новий інтерфейс орієнтований на комфортну ефективну роботу, відповідає сучасним тенденціям і в той же час враховує сильні сторони колишнього інтерфейсу.

5. Нова модель клієнт-серверної взаємодії. Архітектура керованого додатку орієнтована на максимальний перенос виконання всієї функціональності на сервер і максимальне «полегшення» клієнта. У попередніх версіях платформи форма і командний інтерфейс повністю розташовувалися на клієнті і звернення до сервера виконувалися в основному для зчитування та запису прикладних даних. Також на сервер могли переноситися окремі частини обчислень за допомогою серверних загальних модулів. У керованому додатку вся робота прикладних об'єктів виконується тільки на сервері. Функціональність форм і командного інтерфейсу також реалізована на сервері. На сервері виконується підготовка даних форми, розташування елементів, запис даних форми після зміни. На клієнті відображається вже підготовлена на сервері форма, виконується введення даних і виклики сервера для запису введених даних та інших необхідних дій. Аналогічно командний інтерфейс формується на сервері і відображається на клієнті. Також і звіти формуються повністю на сервері і відображаються на клієнті. При цьому механізми системи орієнтовані на мінімізацію обсягу даних, переданих на клієнтський комп'ютер. Наприклад, дані списків, табличних частин і звітів передаються з сервера не відразу, а в міру перегляду їх користувачем.

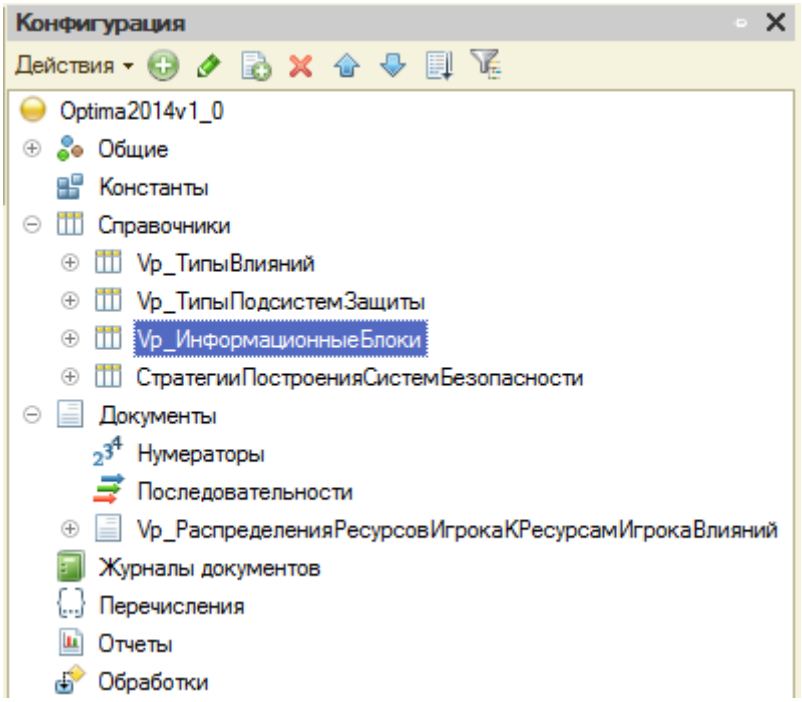
Усі вище перечисленні можливості використання 1С: Підприємства 8.2 свідчать про те, що дана технологічна платформа може слугувати зручним засобом не тільки для автоматизації бухгалтерського та управлінського обліків підприємств, але й може знаходить своє застосування в областях, далеких від власне бухгалтерських завдань, наприклад для проведення

наукових досліджень. Саме, тому дану платформу обрано для проведення експериментальних досліджень розроблених рішень.

Програмне забезпечення «Optima – 2014 v.1.0»

Для проведення експерименту, на основі методу оптимізації поведінки систем безпеки інформації в умовах впливів (див. п.3.3), було розроблено програмне забезпечення «Optima – 2014 v.1.0». Дане програмне забезпечення реалізує оцінювання прогнозованого та поточного рівнів захищеності інформаційного ресурсу для таких стратегій побудови систем безпеки, як: ешелонована система захисту з n бар'єрів захисту; стратегія відведення гравця впливу на хибний інформаційний ресурс з подальшим втягуванням його в інформаційний конфлікт; стратегія оцінювання рівня захищеності за шаблоном нормальної поведінки системи. Дані стратегії побудови систем безпеки були описані у роботі [23]. Зазначимо даний список стратегій не є кінцевим, користувачу дана можливість його розширення.

Структура розробленого програмного засобу (прикладного рішення) у режимі роботи «Конфігуратор» наведена на рис. 4.1.



На рис. 4.1. Структура ПЗ «Optima – 2014 v.1.0» у режимі роботи «Конфігуратор»

Сам інтерфейс користувача дуже простий (див. рис. 4.2).

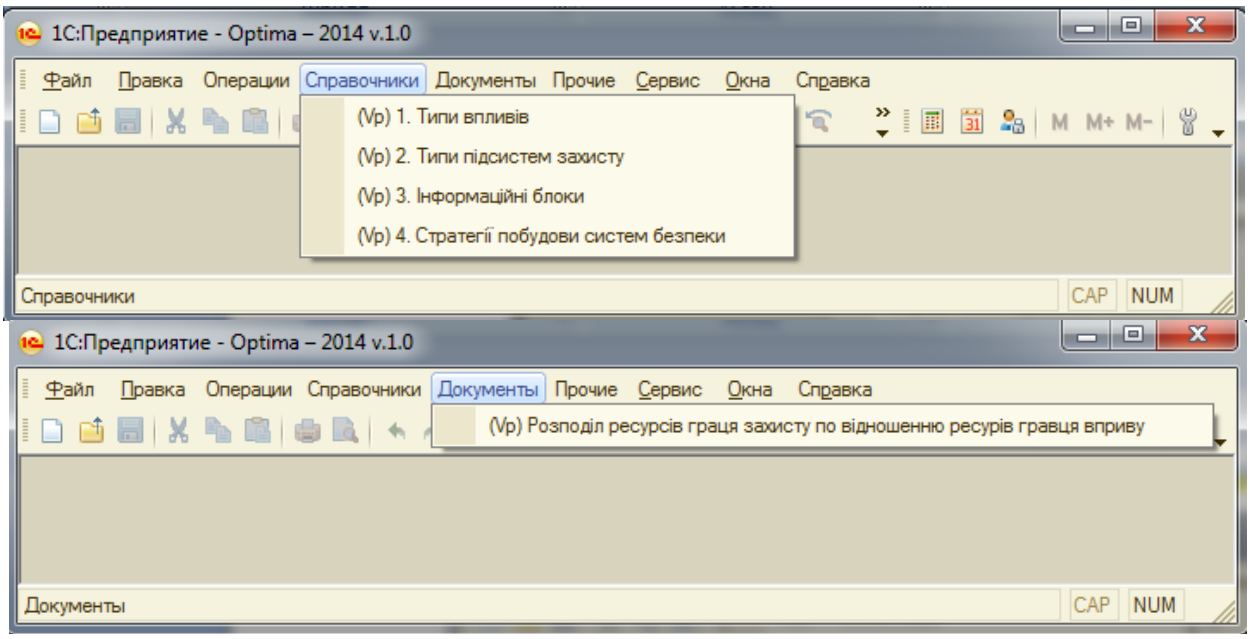


Рис. 4.2. Інтерфейс користувача ПЗ «Optima – 2014 v.1.0»

Як видно з рис. 4.1 − 4.2 розроблене ПЗ складається лише з чотирьох довідників і одного документа. Дані об’єкти дозволяють описати стратегії побудови систем безпеки та провести їх експериментальне дослідження.

Опишемо дані об’єкти:

1. Довідник «Типи впливів» призначений для зберігання та налаштування параметрів типів впливів на ІС. На рис. 4.3 наведено приклад вікна форми списку довідника «Типи впливів».

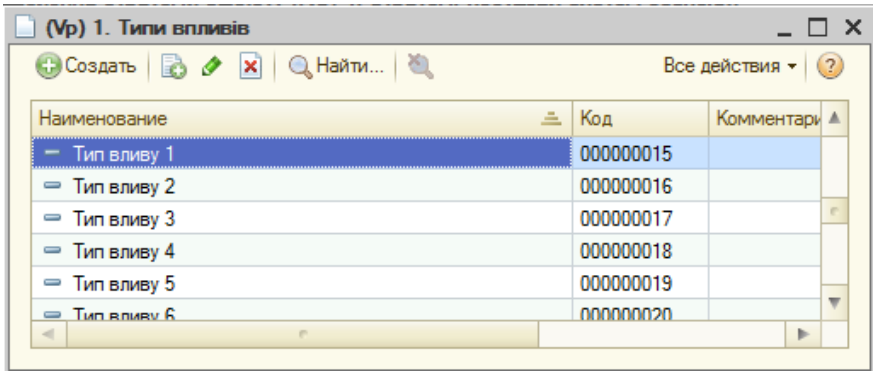


Рис. 4.3. Вікно форми списку довідника «Типи впливів»

2. Довідник «Типи підсистем захисту» використовується для зберігання та налаштування підсистем захисту ІС (приклад форми списку див. рис. 4.4).

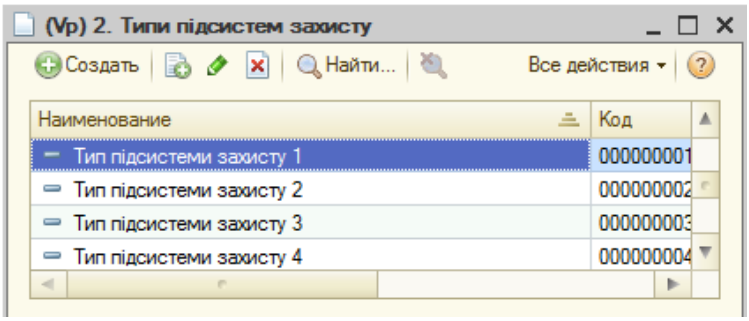


Рис. 4.4. Вікно форми списку довідника «Типи підсистем захисту»

3. Довідник «Інформаційні блоки» призначений для зберігання та налаштування інформаційних блоків ІС (приклад форми списку див. рис. 4.5).

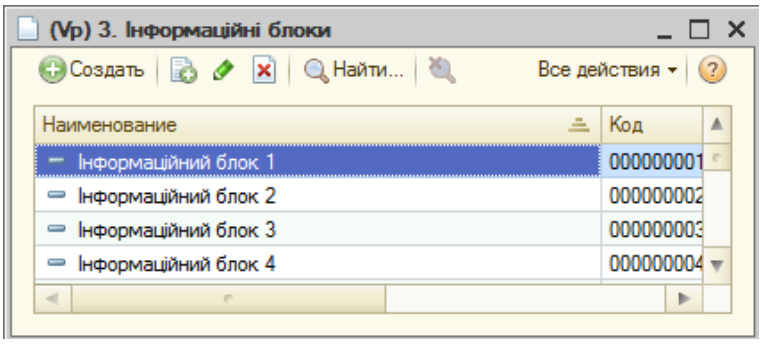


Рис. 4.5. Вікно форми списку довідника «Інформаційні блоки»

4. Довідник «Стратегії побудови систем безпеки» використовується для налаштування різноманітних стратегії захисту. На рис. 4.6–4.7 наведено його вікно форми списку та форми елементу відповідно.

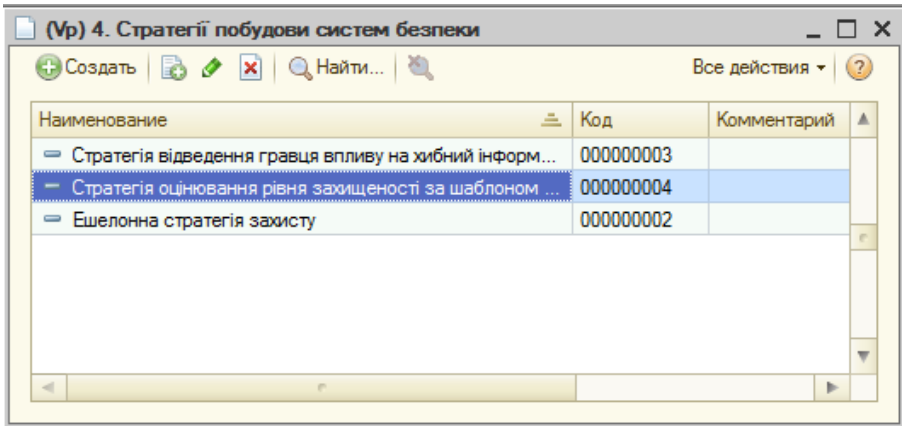


Рис. 4.6. Вікно форми списку довідника «Стратегії побудови систем безпеки»

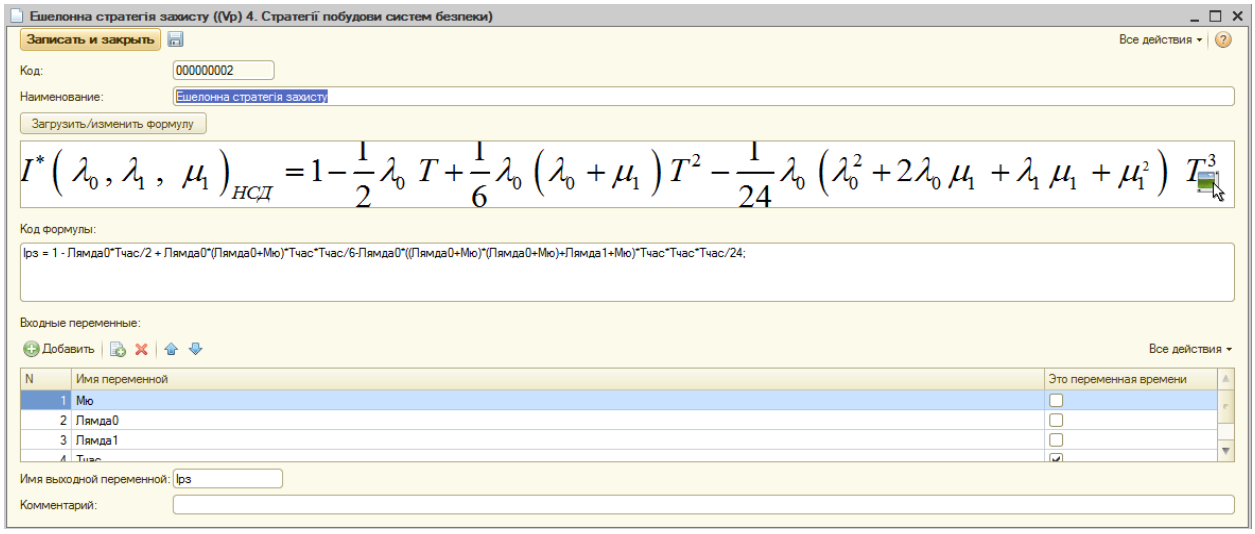


Рис. 4.7. Вікно форми елементу довідника «Стратегії побудови систем безпеки»

5. Документ «Розподіл ресурсів гравця захисту по відношенню ресурсів гравця впливу» призначений для синтезу оптимальної поведінки системи безпеки в умовах впливів. Саме в цьому документі можна для різних стратегій побудови систем безпеки можна оцінити прогнозований та поточний рівнів захищеності інформаційних ресурсів. На рис. 4.8 наведено вікно форми «Розподіл ресурсів гравця захисту по відношенню ресурсів гравця впливу».

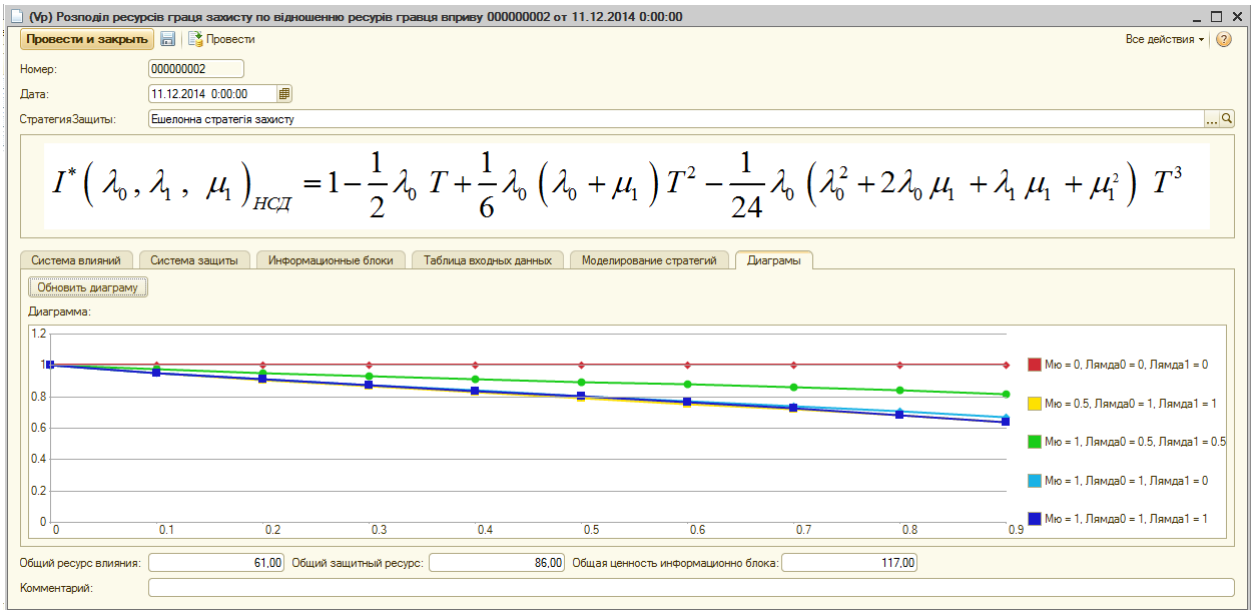


Рис. 4.8. Вікно форми документу «Розподіл ресурсів гравця захисту по відношенню ресурсів гравця впливу»

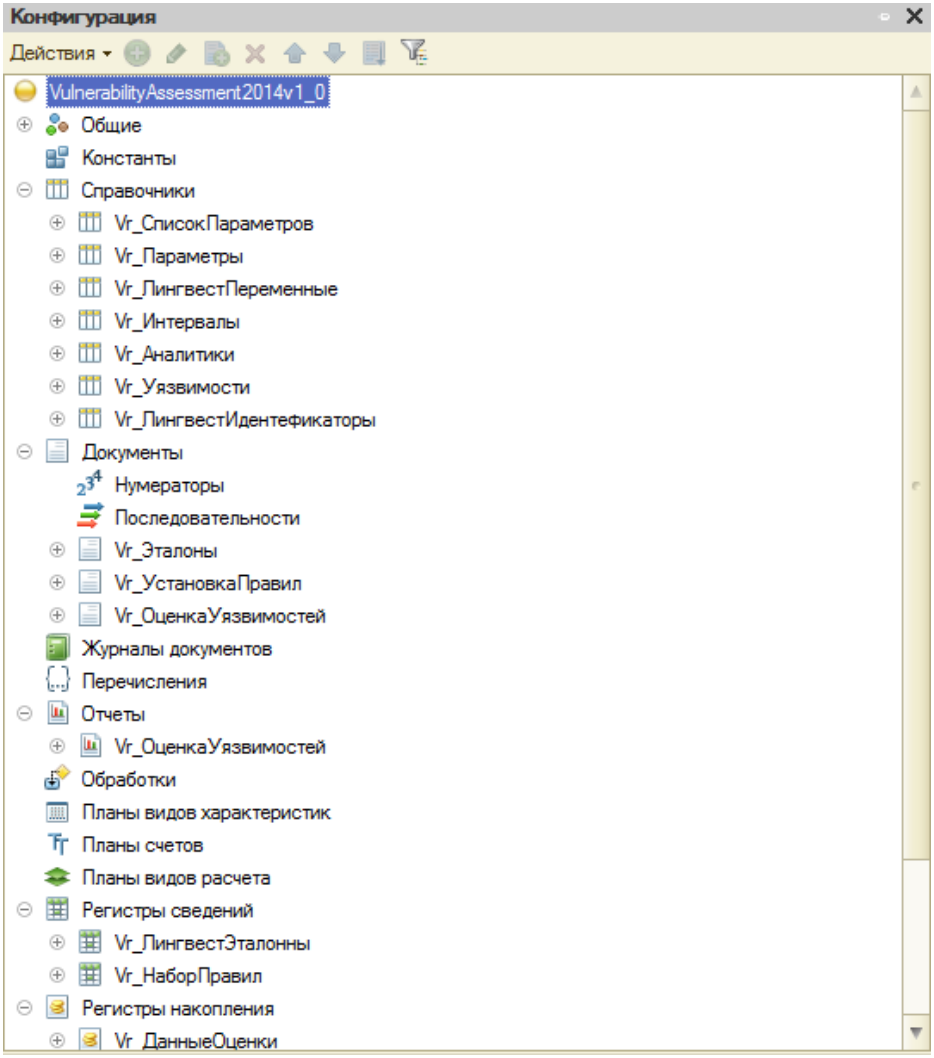
Для використання даного програмного засобу (прикладного рішення) потрібно виконати наступне:

1. Заповнити та налаштувати довідник «Типи впливів».
2. Заповнити та налаштувати довідник «Типи підсистем захисту».
3. Заповнити та налаштувати довідник «Інформаційні блоки».
4. Заповнити довідник «Стратегії побудови систем безпеки».
5. Для кожної стратегії побудови систем безпеки потрібно створити документ «Розподіл ресурсів гравця захисту по відношенню ресурсів гравця впливу», в якому вказати: які впливи реалізовує гравець впливу; які підсистеми захисту використовуються в інформаційній системі; які інформаційні блоки є в системі і їх важливість. Після чого на визначеному інтервалі $[t_0, T]$ (t_0 − момент часу початку інформаційного конфлікту, T − час його завершення) розрахується прогнозований $I(\lambda^{opt}, \mu^{opt})$ та поточний $I(\lambda, \mu)$ рівні захищеності інформаційних ресурсів, залежно від стратегій λ та μ, які обираються гравцями – суб'єктами конфлікту.

Програмне забезпечення «Vulnerability Assessment – 2014 v.1.0»

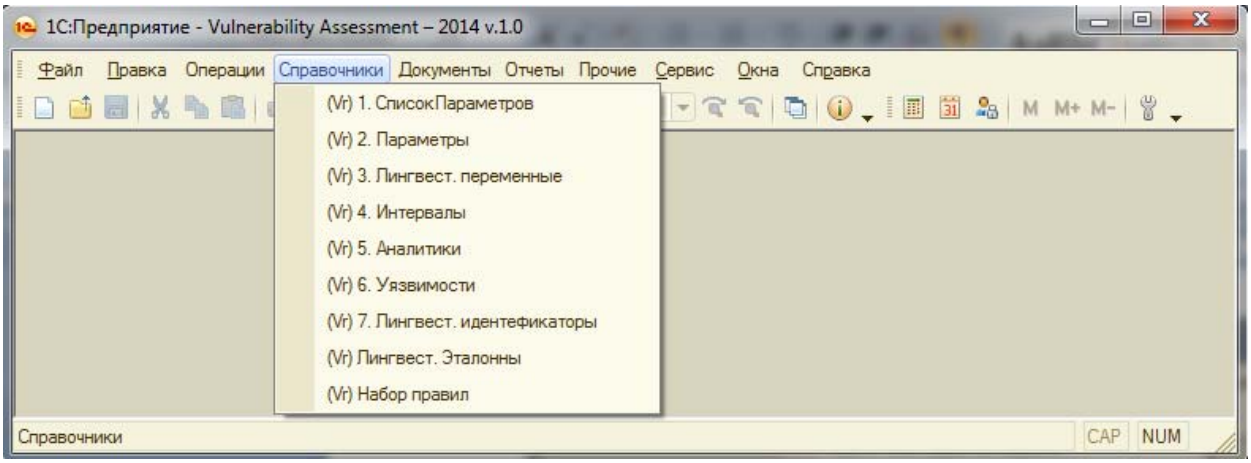
З метою оцінювання уразливостей ІС реалізовано програмний засіб «Vulnerability Assessment – 2014 v.1.0». Цей засіб дозволяє ідентифікувати уразливості інформаційних систем в умовах впливів. Відповідно до зазначених у роботі мережевих та хостових параметрів проведено моделювання поточних станів ІС. Принцип роботи даного ПЗ базується на [26]. Дане ПЗ дозволяє формувати правила визначення уразливостей окремо кожним користувачем системи. Користувач програми може доповнювати список визначених ним параметрів ІС, змінювати встановлювані ним правила та адаптувати для різноманітних ІС.

Структура даного програмного засобу у режимі роботи «Конфігуратор» наведена на рис. 4.9.



На рис. 4.9. Структура ПЗ «Vulnerability Assessment – 2014 v.1.0» у режимі роботи «Конфігуратор»

Сам інтерфейс користувача простий і зображений на рис. 4.10.



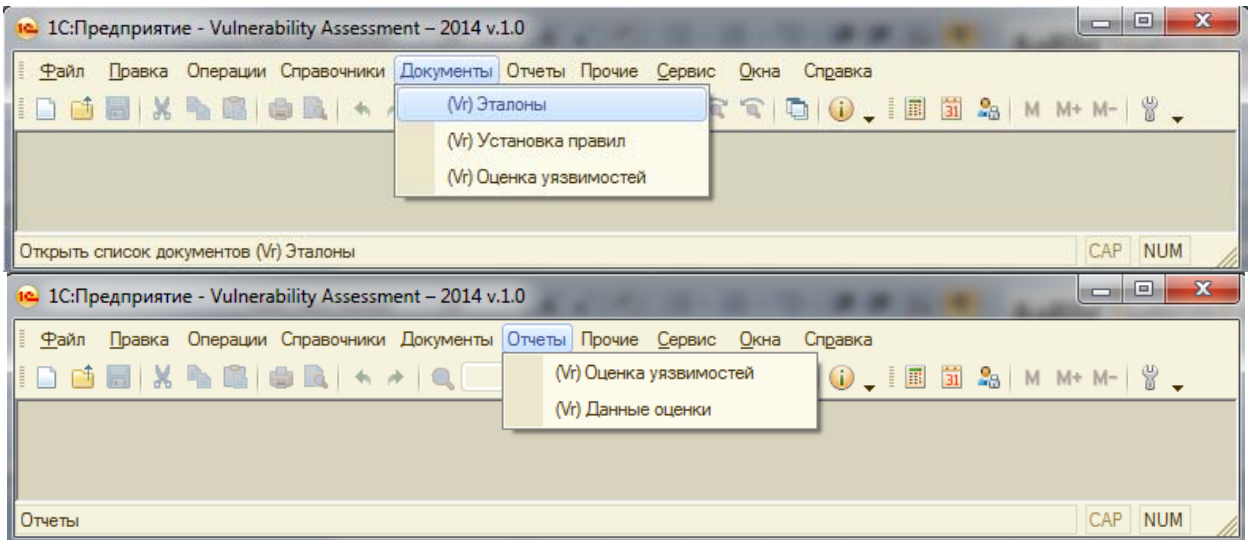


Рис. 4.10. Інтерфейс користувача ПЗ «Vulnerability Assessment – 2014 v.1.0»

Як видно з рис. 4.9 − 4.10 розроблене ПЗ складається з семи довідників, трьох документів, одного звіту, двох регістрів відомостей та одного регістра накопичення. Дані об’єкти дозволяють сформувати правила ідентифікації уразливостей інформаційних систем в умовах впливів.

Опишемо дані об’єкти:

1. Довідник «Список параметрів» використовується для зберігання та налаштування кортежу параметрів на основі якого будуть визначатись уразливості інформаційних систем. На рис. 4.11 наведено приклад вікна форми елементу цього довідника.

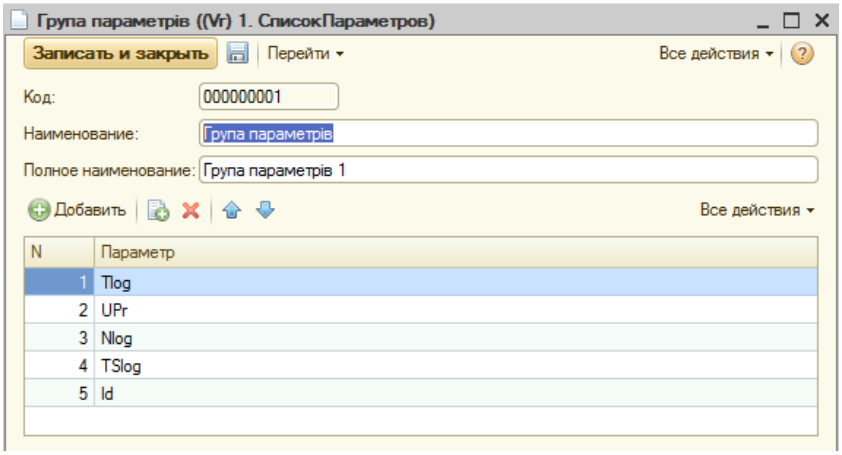


Рис. 4.11. Вікно форми елементу довідника «Список параметрів»

2. Довідник «Параметри» призначений для зберігання списку параметрів, що можуть використовуватись для визначення уразливостей інформаційних систем.

3. Довідник «Лінгвістичні змінні» використовується для зберігання списку можливих лінгвістичних змінних, що будуть використовуватись при налаштуванні еталонів.

4. Довідник «Інтервали» призначений для зберігання списку можливих інтервалів, що будуть використовуватись при налаштуванні еталонів.

5. Довідник «Аналітики» використовується для зберігання списку усіх можливих аналітиків, що можуть складати еталони та формувати правила ідентифікації уразливостей інформаційних систем в умовах впливів.

6. Довідник «Вразливості» використовується для зберігання списку уразливостей, що може ідентифікувати даний ПЗ. На рис. 4.12 наведено приклад вікна форми списку даного довідника.

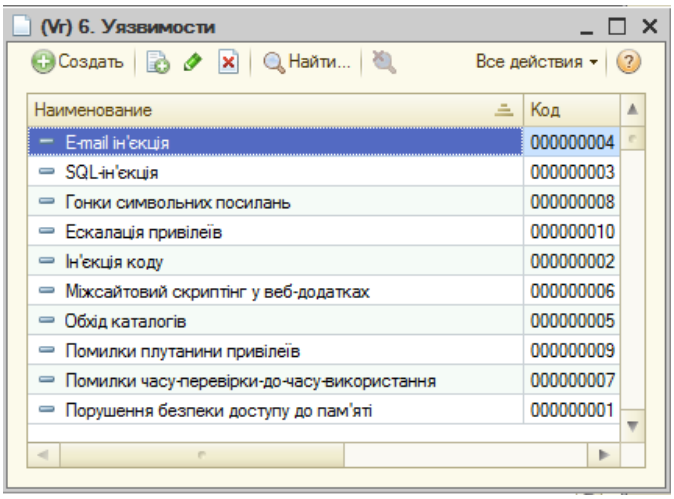


Рис. 4.12. Вікно форми списку довідника «Вразливості»

7. Довідник «Лінгвістичні ідентифікатори» використовується для зберігається інформація по всім лінгвістичним ідентифікаторам, що може використовуватись в дослідженні.

8. Документ «Еталони» призначений для налаштування еталонів можливих значень параметрів, що може окремо задавати кожен користувач (аналітик). На рис. 4.13 наведено приклад фрагменту вікна форми даного документа.

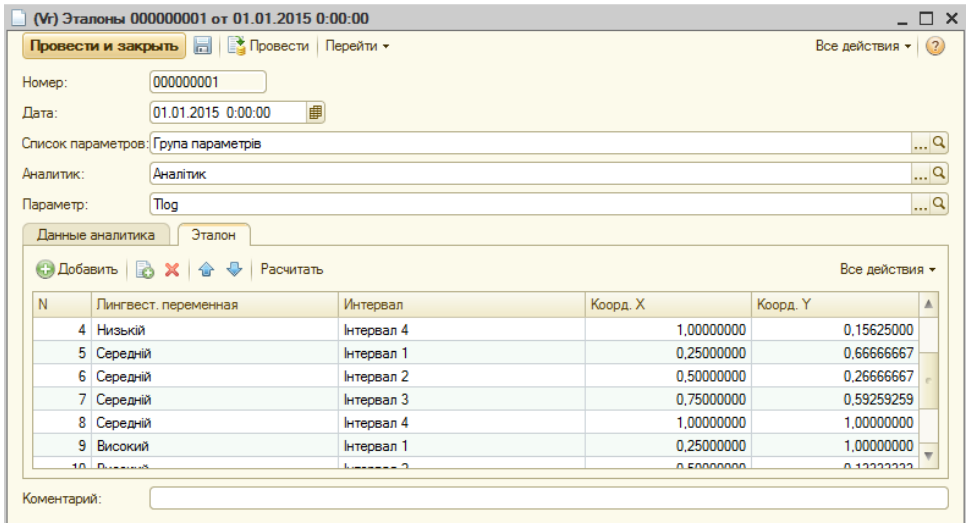


Рис. 4.13. Вікно форми документа «Еталони»

9. Регістр відомостей «Лінгвістичні еталони» використовується для більш ефективного зберігання та використання сформованих еталонів. Даний регістр заповняється автоматично при проведенні документа «Еталони».

10. Документ «Установка правил» призначений для налаштування правил визначення уразливостей на основі вхідного кортежу даних. На рис. 4.14 наведено приклад фрагменту вікна форми даного документа.

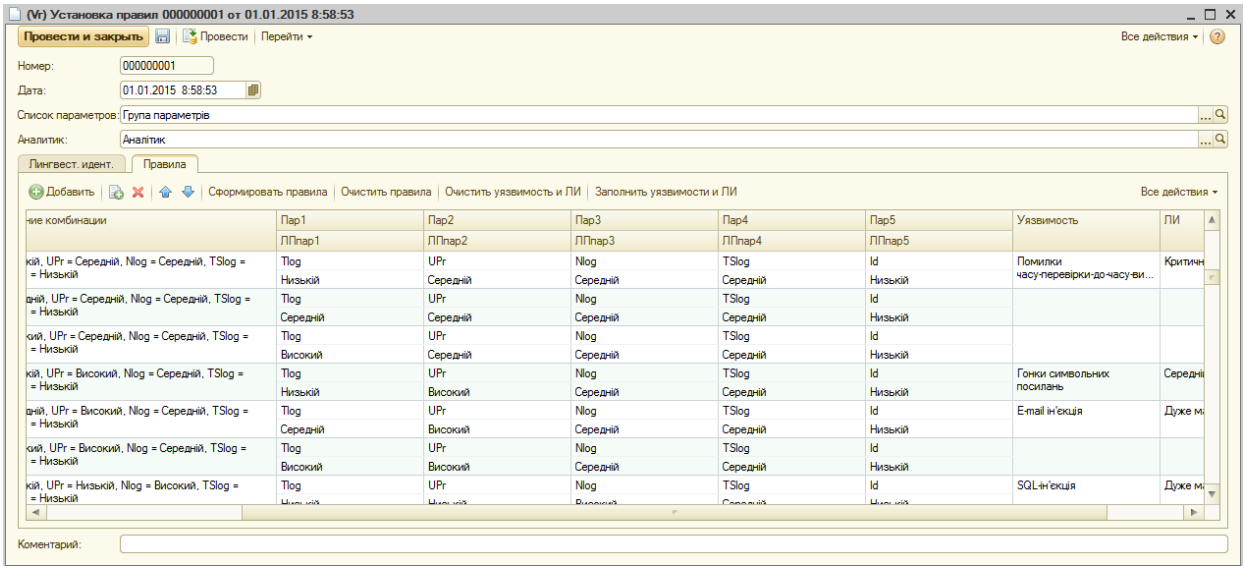


Рис. 4.14. Вікно форми документа «Установка правил»

11. Регістр відомостей «Набор правил» призначений для більш ефективного зберігання та використання сформованих користувачем правил. Даний регістр заповняється автоматично при проведенні документа «Установка правил».

12. Документ «Оцінка уразливостей» призначений для самої оцінки уразливостей на основі моделювання поточних станів ІС. На основі встановлених еталонів та правил ПЗ дозволяє визначити вразливість ІС. На рис. 4.15 наведено приклад фрагменту вікна форми даного документа.

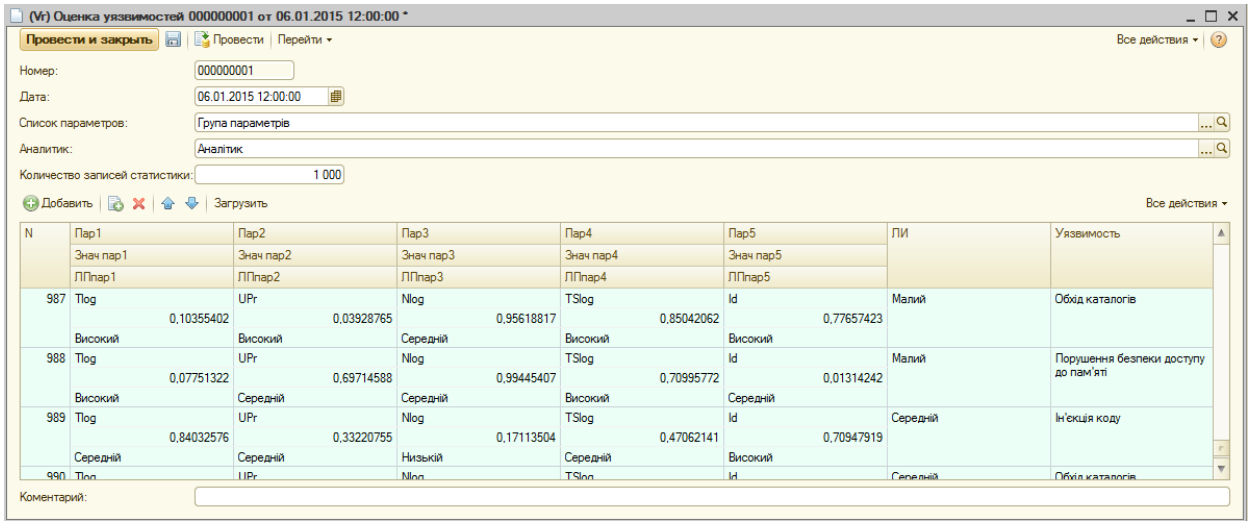


Рис. 4.15. Вікно форми документа «Оцінка уразливостей»

13. Регістр накопичення «Оцінки» використовується для більш ефективного зберігання визначених документами «Оцінка уразливостей» уразливості інформаційних систем в умовах впливів на основі сформованих користувачем правил. Даний регістр заповняється автоматично при проведенні документа «Оцінка уразливостей».

14. Звіт «Оцінка уразливостей» призначений для виведення звіту за період по ідентифікованих уразливостей інформаційних систем в умовах впливів. Користувач може сам настроювати даний звіт в залежності від необхідної йому інформації (налаштування виконуються, якщо у формі звіту нажати кнопку «Настройки»). На рис. 4.16 див. приклад звіту.

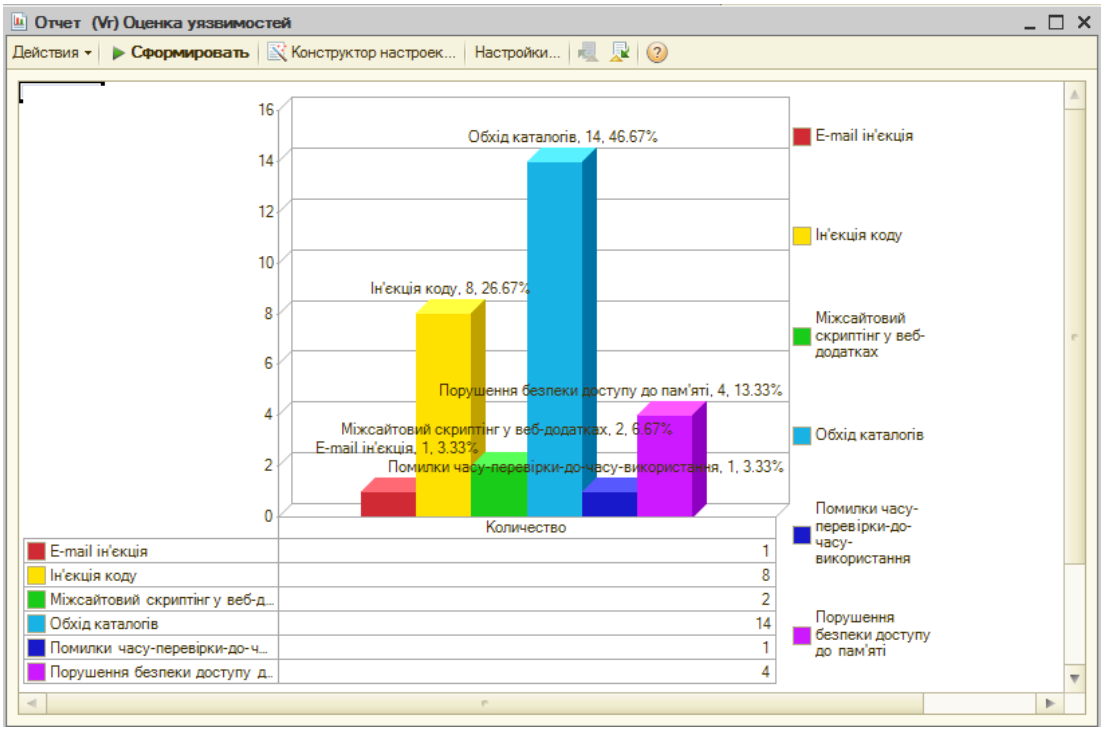


Рис. 4.16. Вікно звіту «Оцінка уразливостей»

Для використання даного програмного засобу потрібно виконати наступне:

1. Заповнити довідники «Список параметрів», «Параметри», «Лінгвістичні змінні», «Інтервали», «Аналітики», «Вразливості», «Лінгвістичні ідентифікатори».
2. Кожний користувач (аналітик) формує еталони поведінки ІС документом «Еталони» та формує список правил визначення уразливостей документом «Установка правил».
3. Після чого промоделювати стани параметрів стану ІС документом «Оцінка уразливостей».
4. Сформувати звіт та отримати дані про ідентифіковані уразливості ІС в умовах впливів.

4.3. Верифікація отриманих результатів

Оцінка прогнозованого та поточного рівня захищеності інформаційних ресурсів для різних стратегій побудови систем безпеки.

Задача синтезу оптимальної поведінки з використанням розробленого програмного забезпечення дозволяє оцінювати прогнозований $I\left(\lambda^{opt},\mu^{opt}\right)$ та поточний $I(\lambda,\mu)$ рівні захищеності інформаційного ресурсу, залежно від стратегій λ та μ, які обираються гравцями – суб'єктами конфлікту на визначеному інтервалі $[t_0,T]$, де t_0 − момент часу початку інформаційного конфлікту, T − час його завершення. Процедура оцінювання зводиться до моделювання антагоністичної гри двох гравців.

У роботі досліджуються три стратегії побудови систем безпеки [23]: стратегія побудови ешелонованої система захисту з n бар'єрів захисту, стратегія відведення гравця впливу на хибний інформаційний ресурс з подальшим втягуванням його в інформаційний конфлікт та стратегія оцінювання рівня захищеності за шаблоном нормальної поведінки системи.

Згідно опису методу оптимізації поведінки системи безпеки інформації в умовах впливів рівень захищеності, залежно від обраних стратегій побудови таких систем, у загальному вигляді визначається згідно з (3.34). При цьому для різних стратегій захисту систем безпеки, які обираються гравцем захисту, прогнозований $I\left(\lambda^{opt},\mu^{opt}\right)$ та поточний $I(\lambda,\mu)$ рівні захищеності інформаційного ресурсу набувають значень, які варіюють у діапазоні $I\in[0,1)$. Оцінимо прогнозований та поточний рівень захищеності інформаційних ресурсів для кожної з них.

Стратегія побудови ешелонованої система захисту з n бар'єрів захисту описана в роботах [23,26]. На рис. 4.17 зображена графова модель процесу нападу (впливу) на ешелоновану систему захисту.

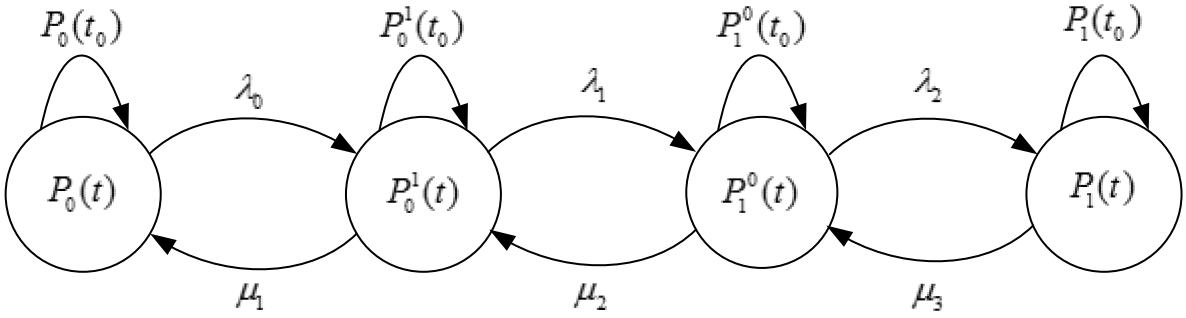


Рис. 4.17. Графова модель процесу нападу (впливу) на ешелоновану систему захисту

На рис. 4.17 $P_0(t)$ - ймовірність перебування системи захисту під впливом методів НСД, $P_0^1(t)$ - ймовірність перебування системи захисту під впливом методів НСД при дії методів захисту, $P_1^0(t)$ - ймовірність перебування системи захисту під впливом методів захисту при дії методів НСД, $P_1(t)$ - ймовірність перебування системи захисту під впливом методів захисту, λ_0, λ_1, λ_2, μ_1, μ_2, μ_3 - інтенсивності потоків захисних дій та інформаційних атак при відповідних імовірностей. $P_0(t_0)$, $P_0^1(t_0)$, $P_1^0(t_0)$, $P_1(t_0)$ - початкові умови для відповідних ймовірностей.

Для даної стратегії у роботі [23] було показано, що при використанні ешелонованої системи захисту з чотирьох бар'єрів захисту ($n=4$) та довільних стратегій захисту і впливу вираз оцінки (3.34) набуває вигляду:

$$I^*\left(\lambda_0, \lambda_1, \mu_1\right)_{НСД} = 1 - \frac{1}{2}\lambda_0 T + \frac{1}{6}\lambda_0\left(\lambda_0 + \mu_1\right)T^2 - \frac{1}{24}\lambda_0\left(\lambda_0^2 + 2\lambda_0\mu_1 + \lambda_1\mu_1 + \mu_1^2\right)T^3$$

На основі даного виразу та кроку зміни параметрів λ (інтенсивності захисних дій в одиницю часу), μ (інтенсивність впливів за одиницю часу) і t визначених у п. 4.1 та використанні програмного забезпечення «Optima – 2014 v.1.0» отримані наступні залежності рівня захищеності (табл. 4.1).

Таблиця 4.1

Рівень захищеності системи безпеки при використанні ешелонованої системи захисту

λ	μ	$T=0,2$ с	$T=0,4$ с	$T=0,6$ с	$T=0,8$ с	$T=1$ с
0,00	1,00	1,000	1,000	1,000	1,000	1,000
0,25	0,00	0,975	0,952	0,929	0,906	0,885
0,25	0,25	0,976	0,953	0,932	0,912	0,893
0,25	0,50	0,976	0,955	0,935	0,917	0,900
0,25	0,75	0,977	0,956	0,938	0,921	0,906
0,25	1,00	0,977	0,957	0,940	0,925	0,911
0,50	0,00	0,952	0,906	0,864	0,824	0,786

0,50	0,25	0,952	0,909	0,870	0,834	0,801
0,50	0,50	0,953	0,912	0,876	0,843	0,813
0,50	0,75	0,954	0,915	0,880	0,850	0,822
0,50	1,00	0,955	0,917	0,885	0,856	0,828
0,75	0,00	0,929	0,864	0,805	0,751	0,701
0,75	0,25	0,930	0,868	0,813	0,764	0,719
0,75	0,50	0,931	0,872	0,821	0,775	0,732
0,75	0,75	0,932	0,876	0,827	0,784	0,742
0,75	1,00	0,933	0,879	0,833	0,791	0,748
1,00	0,00	0,906	0,824	0,751	0,685	0,625
1,00	0,25	0,908	0,829	0,761	0,700	0,643
1,00	0,50	0,909	0,834	0,770	0,712	0,656
1,00	0,75	0,911	0,839	0,777	0,721	0,664
1,00	1,00	0,912	0,843	0,784	0,728	0,667

На рис. 4.18 показано залежність зміни рівня захищеності $I(\lambda,\mu)$ від часу t.

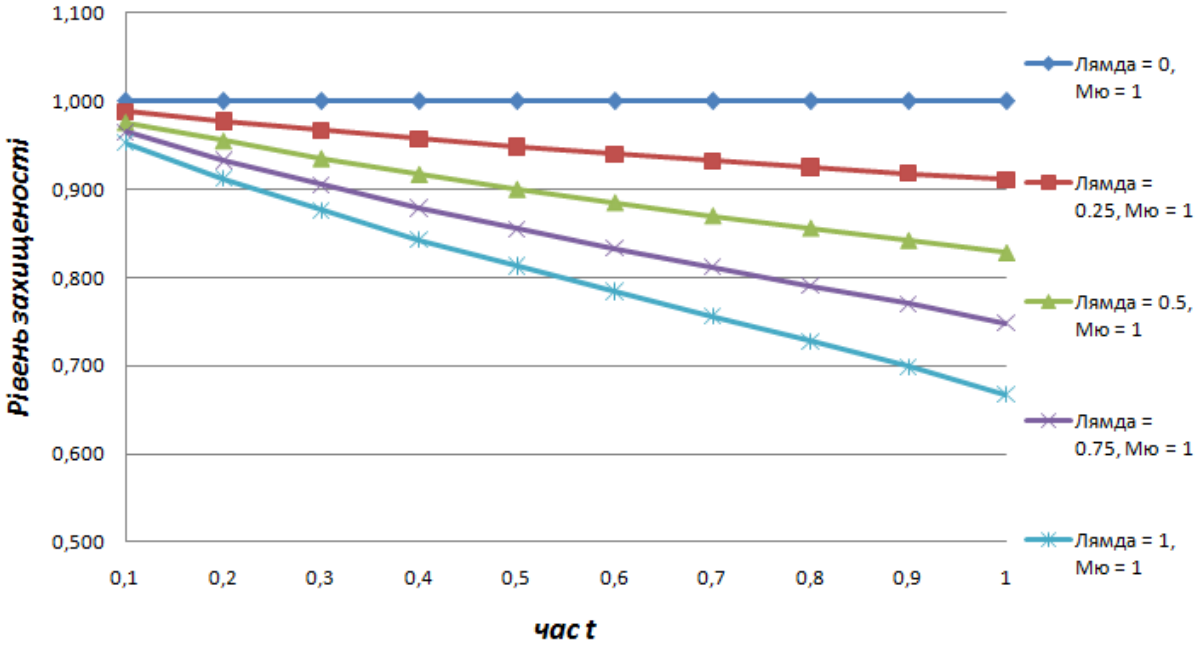


Рис. 4.18. Залежність зміни рівня захищеності $I(\lambda,\mu)$ від часу t при використанні ешелонованої системи захисту

Як видно з табл. 4.1 та рис. 4.18 при виборі гравцями оптимальних стратегій захисту та впливу відповідно прогнозований рівень захищеності інформаційного ресурсу при ешелонованій організації системи безпеки дорівнює 0,667 (для $T=1$ с), тобто $I\left(\lambda^{opt},\mu^{opt}\right)=0.667$. Для решти випадків, при відхиленні гравців від оптимальних стратегій, його величина варіює в діапазоні заданих обмежень.

Стратегія відведення гравця впливу на хибний інформаційний ресурс з подальшим втягуванням його в інформаційний конфлікт описана у роботах [23,26]. На рис. 4.19 зображена графова модель процесу нападу (впливу) на систему захисту, що використовує стратегію відведення гравця впливу на хибний інформаційний ресурс з подальшим втягуванням його в інформаційний конфлікт.

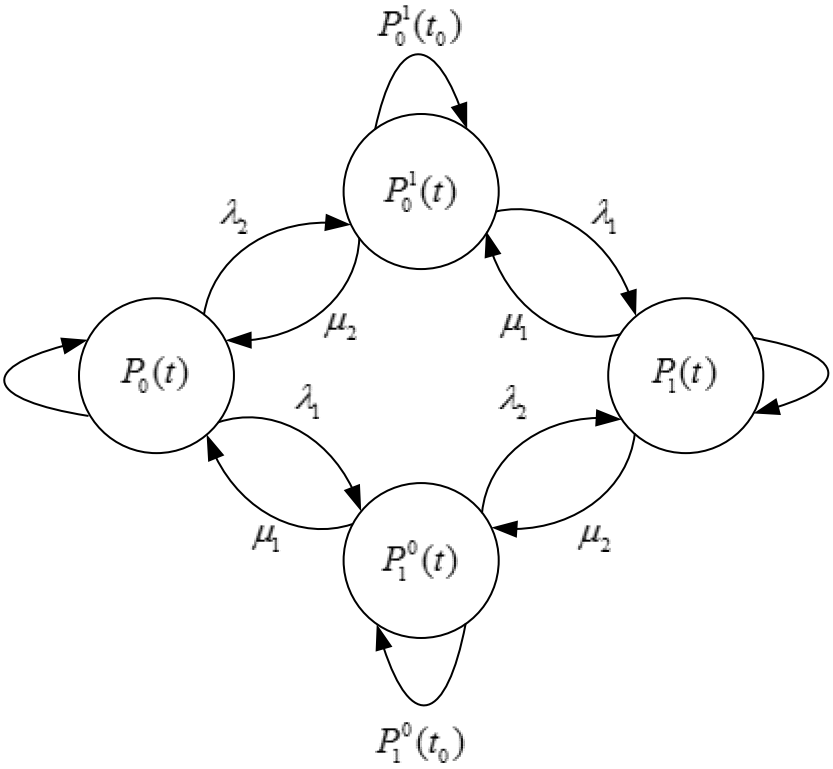


Рис. 4.19 Графова модель процесу нападу на систему захисту, що використовує стратегію відведення гравця впливу на хибний інформаційний ресурс з подальшим втягуванням його в інформаційний конфлікт

На рис. 4.19 $P_0(t)$ - ймовірність перебування системи захисту під впливом методів НСД, $P_0^1(t)$ - ймовірність перебування системи захисту під впливом методів НСД при дії методів захисту, $P_1^0(t)$ - ймовірність перебування системи захисту під впливом методів захисту при дії методів НСД, $P_1(t)$ - ймовірність перебування системи захисту під впливом методів захисту, λ_0, λ_1, λ_2, μ_1, μ_2, μ_3 - інтенсивності потоків захисних дій та інформаційних атак при відповідних імовірностей.

Для даної стратегії у роботі [23] було показано, що при довільних стратегіях захисту і впливу вираз оцінки (3.34) набуває вигляду:

$$I^*\left(\lambda_1, \lambda_2, \mu_1, \mu_2\right)_{НСД} = 1 - \frac{1}{2}\left(\lambda_1 + \lambda_2\right)T + \frac{1}{6}\left(\left(\lambda_1 + \lambda_2\right)^2 + \lambda_1\mu_1 + \lambda_2\mu_2\right)T^2 -$$

$$-\frac{1}{24}\left(\left(\lambda_1 + \lambda_2\right)\left(\left(\lambda_1 + \lambda_2\right)^2 + \lambda_1\mu_1 + \lambda_2\mu_2 + \lambda_1\mu_1\left(2\lambda_2 + \lambda_1 + \mu_1\right) + \lambda_2\mu_2\left(2\lambda_1 + \lambda_2 + \mu_2\right)\right)\right)T^3$$

На основі даного виразу та кроку зміни параметрів λ (інтенсивності захисних дій в одиницю часу), μ (інтенсивність впливів за одиницю часу) і t визначених у п. 4.1 та використанні програмного забезпечення «Optima – 2014 v.1.0» отримані наступні залежності рівня захищеності (табл. 4.2).

Таблиця 4.2

Рівень захищеності системи безпеки при використанні стратегії відведення гравця впливу на хибний інформаційний ресурс з подальшим втягуванням його в інформаційний конфлікт

λ_1	λ_2	μ_1	μ_2	$T = 0,6$ с	$T = 0,8$ с	$T = 1$ с
0,00	0,00	1,00	1,00	1,000	1,000	1,000
0,50	0,50	0,50	0,50	0,768	0,707	0,646
0,50	0,50	0,50	1,00	0,774	0,712	0,646
0,50	0,50	1,00	0,50	0,774	0,712	0,646
0,50	0,50	1,00	1,00	0,780	0,717	0,646
0,50	0,75	0,50	0,50	0,715	0,636	0,549
0,50	0,75	0,50	1,00	0,720	0,633	0,529
0,50	0,75	1,00	0,50	0,717	0,633	0,532
0,50	0,75	1,00	1,00	0,722	0,630	0,512
0,50	1,00	0,50	0,50	0,663	0,560	0,438
0,50	1,00	0,50	1,00	0,662	0,541	0,380
0,50	1,00	1,00	0,50	0,661	0,547	0,401
0,50	1,00	1,00	1,00	0,660	0,528	0,344
0,75	0,50	0,50	0,50	0,715	0,636	0,549
0,75	0,50	0,50	1,00	0,717	0,633	0,532
0,75	0,50	1,00	0,50	0,720	0,633	0,529
0,75	0,50	1,00	1,00	0,722	0,630	0,512
0,75	0,75	0,50	0,50	0,662	0,558	0,434
0,75	0,75	0,50	1,00	0,660	0,541	0,385
0,75	0,75	1,00	0,50	0,660	0,541	0,385
0,75	0,75	1,00	1,00	0,659	0,524	0,336
0,75	1,00	0,50	0,50	0,606	0,472	0,296
0,75	1,00	0,50	1,00	0,597	0,432	0,197
0,75	1,00	1,00	0,50	0,598	0,438	0,215
0,75	1,00	1,00	1,00	0,589	0,398	0,116
1,00	0,50	0,50	0,50	0,663	0,560	0,438
1,00	0,50	0,50	1,00	0,661	0,547	0,401
1,00	0,50	1,00	0,50	0,662	0,541	0,380
1,00	0,50	1,00	1,00	0,660	0,528	0,344
1,00	0,75	0,50	0,50	0,606	0,472	0,296
1,00	0,75	0,50	1,00	0,598	0,438	0,215
1,00	0,75	1,00	0,50	0,597	0,432	0,197
1,00	0,75	1,00	1,00	0,589	0,398	0,116

1,00	1,00	0,50	0,50	0,547	0,371	0,125
1,00	1,00	0,50	1,00	0,528	0,307	0
1,00	1,00	1,00	0,50	0,528	0,307	0
1,00	1,00	1,00	1,00	0,508	0,243	0

На рис. 4.20 показано залежність зміни рівня захищеності $I(\lambda,\mu)$ від часу t.

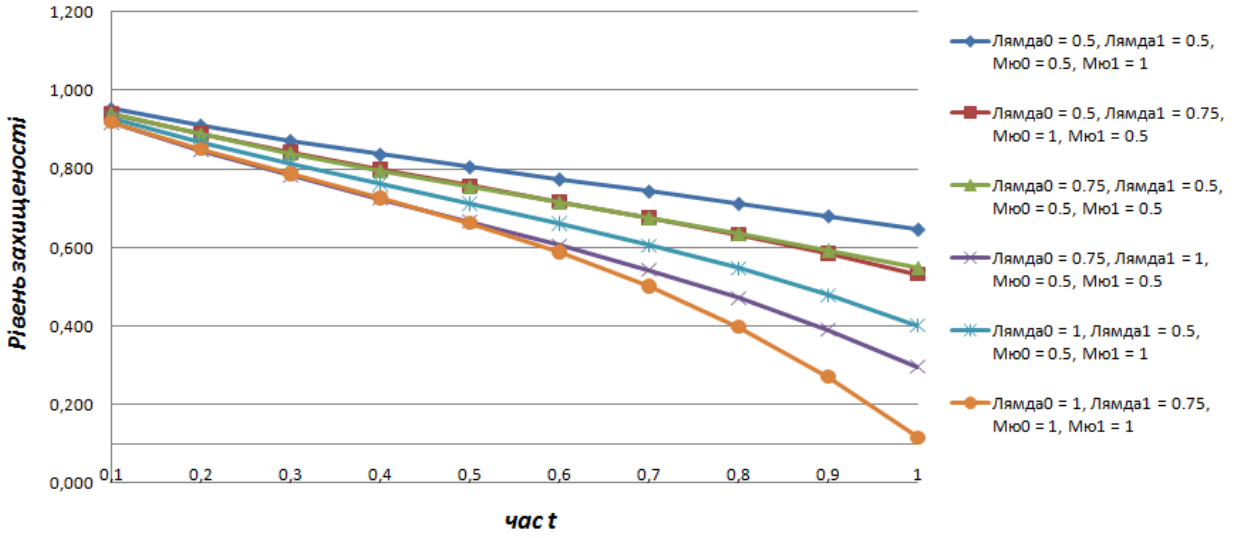
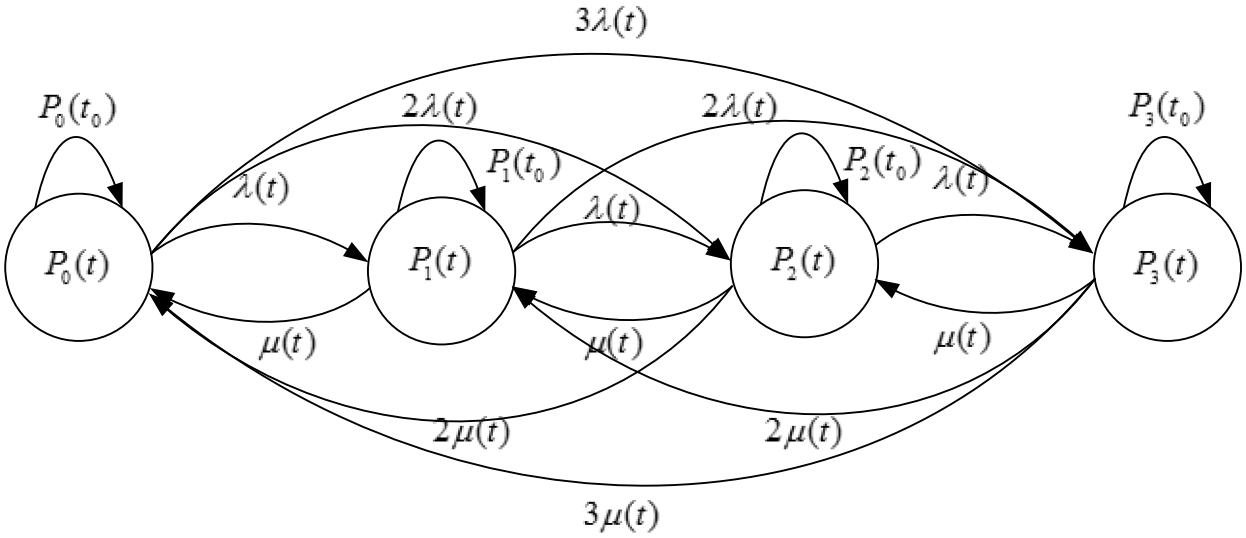


Рис. 4.20. Залежність зміни рівня захищеності $I(\lambda,\mu)$ від часу t при використанні стратегії відведення гравця впливу на хибний інформаційний ресурс з подальшим втягуванням його в інформаційний конфлікт

Як видно з табл. 4.2 та рис. 4.20 при виборі гравцями оптимальних стратегій захисту та впливу відповідно прогнозований рівень захищеності інформаційного ресурсу при використанні стратегії відведення гравця впливу на хибний інформаційний ресурс з подальшим втягуванням його в інформаційний конфлікт дорівнює 0,6044 (для $T=1$ с), тобто $I(\lambda^{opt},\mu^{opt})\approx 0.6044$. Для решти випадків, при відхиленні гравців від оптимальних стратегій, його величина варіює в діапазоні заданих обмежень.

Стратегія оцінювання рівня захищеності за шаблоном нормальної поведінки системи описана у роботах [23,26]. На рис. 4.21 зображена графова модель процесу нападу (впливу) на систему захисту, що використовує стратегію оцінювання рівня захищеності за шаблоном нормальної поведінки системи.



На рис. 4.21 Графова модель процесу нападу на систему захисту, що використовує стратегію оцінювання рівня захищеності за шаблоном нормальної поведінки системи

На рис. 4.21 $P_0(t)$ - ймовірність відмови системи від обслуговування під впливом атаки, $P_1(t)$ - ймовірність перебування системи під впливом атаки при дії методів захисту інформації, $P_2(t)$ - ймовірність перебування сервера під впливом МЗІ при дії атаки, $P_3(t)$ - ймовірність перебування сервера під впливом МЗІ, $\lambda(t)$, $\mu(t)$ − інтенсивності потоків захисних дій та інформаційних атак, що обираються гравцями конфлікту.

Для даної стратегії у роботі [24] було показано, що при довільних стратегіях захисту і впливу вираз оцінки (3.34) набуває вигляду:

$$I^*(\lambda_0,\ \mu_0)_{НСД} = 1-\lambda_0 T^2+\frac{1}{20}\lambda_0(18\lambda_0+7\mu_0)T^4-\frac{1}{84}\lambda_0\left(3\lambda_0(18\lambda_0+7\mu_0)+\frac{1}{4}\mu_0(77\lambda_0+53\mu_0)\right)T^6$$

На основі даного виразу та кроку зміни параметрів λ (інтенсивності захисних дій в одиницю часу), μ (інтенсивність впливів за одиницю часу) і t визначених у п. 4.1 та використанні програмного забезпечення «Optima – 2014 v.1.0» отримані наступні залежності рівня захищеності (табл. 4.3).

Таблиця 4.3

Рівень захищеності системи безпеки при використанні стратегії стратегії оцінювання рівня захищеності за шаблоном нормальної поведінки системи

λ	μ	$T=0,2$ с	$T=0,4$ с	$T=0,6$ с	$T=0,8$ с	$T=1$ с
0,00	1,00	1,000	1,000	1,000	1,000	1,000
0,25	0,00	0,990	0,961	0,917	0,860	0,796
0,25	0,25	0,990	0,962	0,919	0,867	0,808
0,25	0,50	0,990	0,962	0,921	0,872	0,815
0,25	0,75	0,990	0,963	0,923	0,876	0,817
0,25	1,00	0,990	0,963	0,925	0,878	0,814
0,50	0,00	0,980	0,925	0,845	0,751	0,645
0,50	0,25	0,980	0,926	0,849	0,760	0,654
0,50	0,50	0,980	0,927	0,853	0,766	0,653
0,50	0,75	0,981	0,928	0,856	0,770	0,642
0,50	1,00	0,981	0,929	0,859	0,771	0,621
0,75	0,00	0,971	0,892	0,783	0,656	0,485
0,75	0,25	0,971	0,893	0,788	0,664	0,476
0,75	0,50	0,971	0,895	0,792	0,667	0,452
0,75	0,75	0,971	0,896	0,796	0,666	0,413
0,75	1,00	0,971	0,897	0,799	0,662	0,360
1,00	0,00	0,961	0,860	0,727	0,560	0,257
1,00	0,25	0,962	0,862	0,732	0,562	0,215
1,00	0,50	0,962	0,864	0,736	0,559	0,153
1,00	0,75	0,962	0,865	0,740	0,550	0,072
1,00	1,00	0,962	0,867	0,742	0,537	0

На рис. 4.22 показано залежність зміни рівня захищеності $I(\lambda,\mu)$ від часу t.

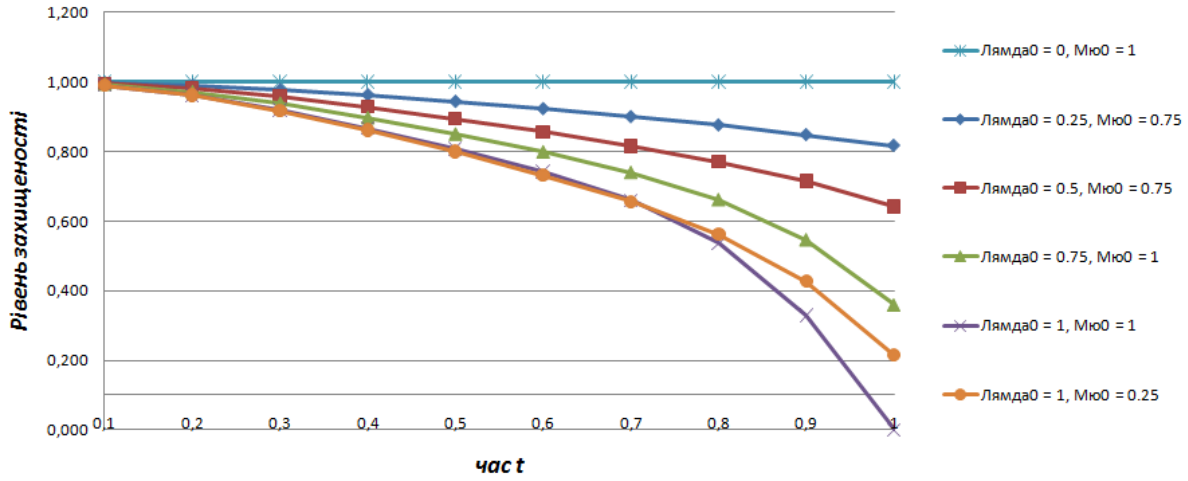


Рис. 4.22. Залежність зміни рівня захищеності $I(\lambda,\mu)$ від часу t при використанні стратегії стратегії оцінювання рівня захищеності за шаблоном нормальної поведінки системи

Як видно з табл. 4.3 та рис. 4.22 при виборі гравцями оптимальних стратегій захисту та впливу відповідно прогнозований рівень захищеності інформаційного ресурсу при використанні стратегії стратегії оцінювання рівня захищеності за шаблоном нормальної поведінки системи дорівнює

0,215 (для $T=1$ с), тобто $I\left(\lambda^{opt},\mu^{opt}\right)\approx 0.215$. Для решти випадків, при відхиленні гравців від оптимальних стратегій, його величина варіює в діапазоні заданих обмежень.

Отже, за допомогою програмного забезпечення «Optima – 2014 v.1.0» було оцінено прогнозований та поточний рівень захищеності інформаційних ресурсів для трьох стратегій побудови систем безпеки: стратегія ешелонованої системи захисту, стратегія відведення гравця впливу на хибний інформаційний ресурс з подальшим втягуванням його в інформаційний конфлікт та стратегія оцінювання рівня захищеності за шаблоном нормальної поведінки системи. Визначено, прогнозований рівень захищеності інформаційного ресурсу для кожної із розглянутих стратегій побудови системи безпеки. Як видно із результатів гравець безпеки може спрогнозувати рівень захищеності та оптимізувати свої ресурси, в тому числі, для тих випадків коли гравець впливу використовує оптимальну стратегію.

Моделювання поточних станів ІС для перевірки можливості ідентифікації уразливості інформаційних систем в умовах впливів.

Для оцінки уразливостей ІС обрано наступні параметри: інтенсивність дій ($I_{дій}$), об'єм завантаженої оперативної пам'яті ($V_{оп}$), завантаженість процесора ($P_{проц}$), час виконання процесу ($T_{проц}$), кількість виконуваних процесів ($K_{Впроц}$), тип виконуваних файлів впливу ($F_{тип}$), Кількість збоїв та помилок ($K_{збоїв}$), невластиві процеси ($K_{НеВлПроц}$).

У процесі атаки (впливу) порушник, діючи на систему, змінює певні її параметри, створює або припиняє властиві їй процеси тощо. Всі ці дії відображаються на стані системи. Оцінюючи ці параметри можна провести виявлення факту та ідентифікувати уразливість ІС в умовах впливів [25]. Оскільки процес виявлення та ідентифікації уразливості відбувається в умовах невизначеності, а ряд вище наведених параметрів носять нечіткий характер, то функціонування такої системи має грунтуватись на нечіткій логіці. Для ідентифікації порушника можна використовувати логіко-

лінгвістичний підхід і базову модель параметрів, частково описану в [26], які були основою розробленого ПЗ.

За допомогою розробленого ПЗ експертним шляхом була побудована модель еталонів лінгвістичних змінних для нечітких параметрів ідентифікації порушника з обраної множини параметрів використовуючи роботу [23].

Експертним шляхом сформовані правила направлені на виявлення уразливостей в умовах впливів. Дані правила дозволяють виявити аномальний стану ІС, спричиненого діяльністю порушника, на основі використання методів нечіткої логіки, експертних оцінок та моделей еталонів параметрів, необхідних для виявлення порушника. Побудова правил здійснено за допомогою відповідної моделі [26], для створення якої введено множину лінгвістичних ідентифікаторів $LI = \bigcup_{i=1}^{d} LI = \{LI_1, LI_2, ..., LI_d\}$, де d - кількість елементів множини, необхідних для відображення аномального стану, а LI_i $(i = 1,d)$ - елементи LI, кожен з яких приймає одне з текстових значень, що характеризують в лінгвістичній формі рівень аномального стану системи, яке може бути породжене атакуючими діями.

На основі множин ідентифікаторів LI і набору лінгвістичних зв'язок LC побудовано множину правил для виявлення уразливостей $ER = \left\{ \bigcup_{i=1}^{n} ER_i \right\} = \{ER_1, ER_2, ..., ER_n\}$, де ER_i $(i=1,n)$ - підмножина можливих правил для виявлення i-го аномального стану, породженого i-ою атакою (впливом), при цьому $\bigcup_{i=1}^{n} ER_i = \bigcup_{i=1}^{n} \left\{ \bigcup_{j=1}^{r_n} ER_{ij} \right\} = \{ER_{11}, ER_{12}, ..., ER_{1r_1}\}, \{ER_{21}, ER_{22}, ..., ER_{2r_2}\}, ..., \{ER_{n1}, ER_{n2}, ..., ER_{nr_n}\}$, де ER_{ij} $(i=1,n, j=1,r_n)$ - j-е правило i-ої підмножини можливих правил, а r_i $(i=1,n)$ - загальна кількість можливих правил, спрямованих на виявлення i-ої аномалії. Із роботи [23] слідує

$$ER = \bigcup_{i=1}^{n}\left\{\bigcup_{j=1}^{r_i} ER_{ir_j}\right\} = \bigcup_{i=1}^{n}\left\{\bigcup_{j=1}^{r_i}(LC_{ir_j} \to LI_{ir_j})\right\} =$$

$$\left\{\bigcup_{i=1}^{n}\left\{\bigcup_{j=1}^{r_i} ER_{ir_j} = (LC_{ir_j} \to LI_{ir_j})\right\}\right\},$$

де ER_{ir_j} є r_j-е правило виявлення аномалії породженої *i*-ою атакою, яке буквально інтерпретується як: "Якщо LC_{ir_j} істинно, то рівень аномального стану, який може бути породжений *i*-ою атакою, буде LI_{ir_j} ".

Відповідно до зазначених мережевих та хостових параметрів проведено моделювання поточних станів ІС.

У процесі проведення експерименту, за допомогою розробленого ПЗ Vulnerability Assessment – 2014 v.1.0, відповідно до зазначених параметрів, було здійснене моделювання 10 000 поточних станів ІС, з яких 866 були характерними визначених категорій уразливостей. Контроль усіх поточних станів ІС здійснювався за допомогою 6561 правил, при цьому загальний розподіл уразливостей у відсотках за категоріями такий: порушення безпеки доступу до пам'яті (10,16%), ін'єкція коду (10,51%), SQL-ін'єкція (8,31%), e-mail ін'єкція (23,44%), обхід каталогів (4,27%), міжсайтовий скриптінг у веб-додатках (13,86%), помилки часу-перевірки-до-часу-використання (12,01%), гонки символьних посилань (3,46%), помилки плутанини привілеїв (9,12%) та ескалація привілеїв (4,85%). Такий розподіл (рис. 4.23-4.24) на 100% є очікуваним і відповідає умовам моделювання. Кожна вразливість була однозначно ідентифікована відповідною групою сформованих правил.

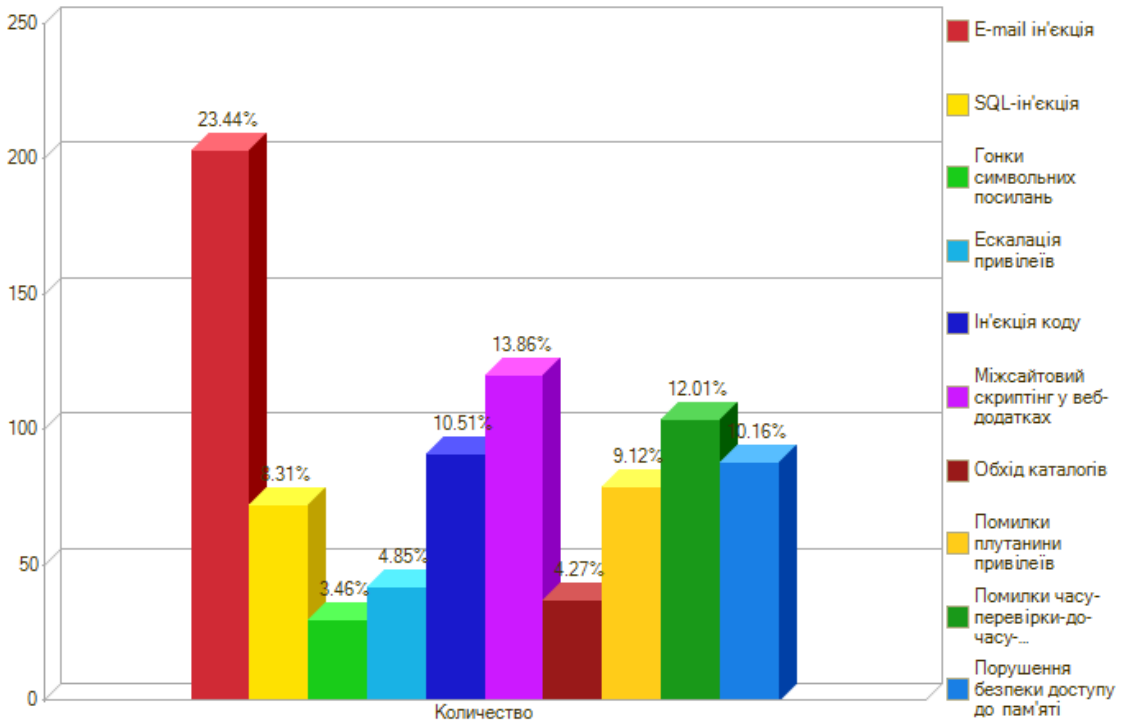
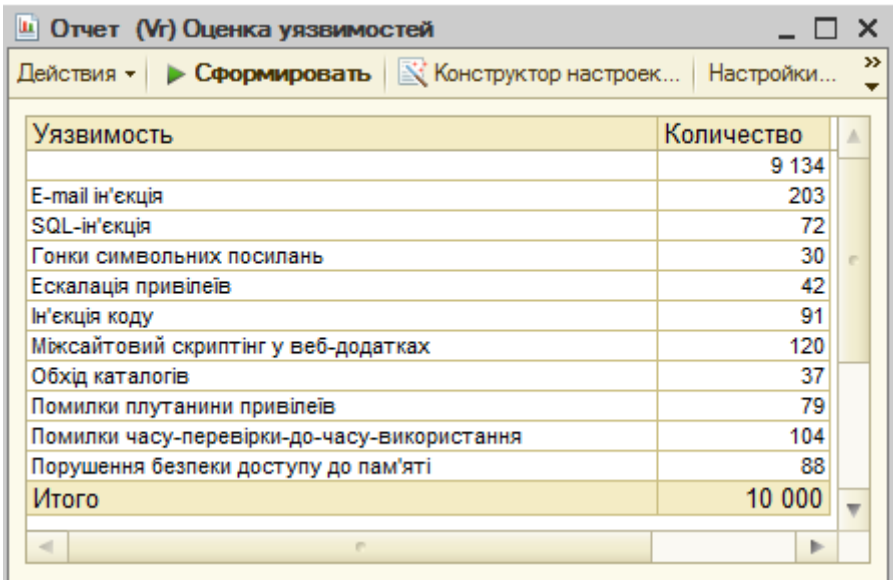


Рис. 4.23. Діаграма розподілу виявлених уразливостей інформаційних систем в умовах впливів



Уязвимость	Количество
	9 134
E-mail ін'єкція	203
SQL-ін'єкція	72
Гонки символьних посилань	30
Ескалація привілеїв	42
Ін'єкція коду	91
Міжсайтовий скриптінг у веб-додатках	120
Обхід каталогів	37
Помилки плутанини привілеїв	79
Помилки часу-перевірки-до-часу-використання	104
Порушення безпеки доступу до пам'яті	88
Итого	10 000

Рис. 4.24. Кількість виявлених уразливостей при моделюванні 10000 поточних станів ІС

Отже, за допомогою програмного забезпечення «Vulnerability Assessment – 2014 v.1.0» проведено моделювання поточних станів ІС, що дозволило ідентифікації уразливості інформаційних систем в умовах впливів.

4.4. Висновки до четвертого розділу

4.1. Запропоновано методику проведення експериментального дослідження, що дозволило провести експериментальне дослідження.

4.2. Розроблено програмне забезпечення «Optima – 2014 v.1.0», що дозволило оцінити прогнозований та поточний рівень захищеності інформаційних ресурсів для таких стратегій побудови систем безпеки, як: ешелонована система захисту з n бар'єрів захисту; стратегія відведення гравця впливу на хибний інформаційний ресурс з подальшим втягуванням його в інформаційний конфлікт; стратегія оцінювання рівня захищеності за шаблоном нормальної поведінки системи. Отримані результати підтвердили достовірність розробленого методу оптимізації поведінки систем безпеки інформації в умовах впливів.

4.3. Розроблено програмне забезпечення «Vulnerability Assessment – 2014 v.1.0», що дозволило ідентифікувати уразливості інформаційних систем в умовах впливів при зазначених станах ІС. Отримані результати підтвердили достовірність розробленої методики оцінки уразливостей.

ВИСНОВКИ

Результатом виконаної роботи є розв’язання наукової задачі побудови і дослідження методів моделювання впливів на інформаційні системи, оцінювання уразливостей та оптимізації показників систем захисту, що можуть використовуватися для підвищення ефективності сучасних систем захисту інформації. У процесі виконання дисертаційної роботи отримані такі вагомі результати:

1. Проведено аналіз існуючих методів і засобів оцінки уразливостей інформаційних систем, що дозволило виявити їх недоліки і формалізувати завдання щодо розробки більш ефективного засобу; аналіз сучасних методів моделювання впливів на інформаційні системи дав можливість визначити найбільш ефективний підхід і використати його з метою оптимізації параметрів систем захисту.

2. Запропоновано систему правил щодо моделювання критеріїв оптимальності, які, за рахунок синтезу морфологічним методом сепарабельних адитивних критеріїв та обмежень, дозволяють розв’язувати задачі аналізу, синтезу та оптимізації систем за обраними критеріями та виділеними обмеженнями, а також оцінювати рівень захищеності інформаційних систем з урахуванням дозволених границь гарантованого рівня захисту інформації.

3. Запропоновано диференціально-ігровий метод оптимізації параметрів інформаційних систем, що, за рахунок врахування стратегії гравця впливу, критерію оптимізації ресурсів гравців у процесі оптимізації і енергетичної складової у заданий період часу, дозволяє визначати у реальному часі оптимальну стратегію безпеки інформації в інформаційних системах.

4. Запропоновано метод оптимізації систем захисту інформації, що, за рахунок врахування параметрів системи безпеки (кількість засобів безпеки,

тип підсистеми безпеки, сумарний ресурс безпеки та цінність інформації), дозволяє визначати оптимальну поведінку в системі «вплив-безпека»;

5. Удосконалено метод знаходження оптимальної конфігурації інформаційної системи, який, за рахунок використання теоретико-графового моделювання зворотного ходу побудови оптимального вихідного дерева, дозволяє визначати оптимальну архітектуру інформаційної системи в умовах інформаційних впливів.

6. Розроблено методику оцінки уразливостей і впливів на інформаційні системи, які, за рахунок використання логіко-ймовірнісних пар зв'язок «параметри $\rightarrow$ уразливості», дозволяють ідентифікувати уразливості інформаційних систем в умовах впливів.

7. Розроблено алгоритми та програмне забезпечення для реалізації розроблених методів, за допомогою якого проведено експериментальне дослідження, що підтвердило адекватність запропонованих методів з точки зору оптимізації параметрів інформаційних систем в умовах інформаційних впливів.

8. Зазначені результати роботи впроваджено у діяльність в/ч К-1410 (14.06.2012 р.), ТОВ «Конзьюмер Експрес» (17.11.2014 р.), Національного авіаційного університету (10.02.2015 р.), Державного університету інформаційно-комунікаційних технологій (26.06.2012 р.) та Кіровоградського національного технічного університету (17.09.2014 р.), що підтверджено відповідними актами впровадження, які містяться у додатках до дисертаційної роботи.

Додаток А. Документи, що підтверджують впровадження результатів

Додаток Б. Лістинги (коди) програмних засобів

Оскільки розроблені програмні засоби побудовані на технологічній платформі 1С: Підприємство 8.2 більшість функціонала реалізована налаштуваннями конфігурацій при їх створенні. Наведемо лише коди модулей об’єктів конфігурацій.

ПЗ Optima – 2014 v.1.0

Код форми елементу довідника Стратегії побудови систем безпеки

```
&НаКлиенте
Процедура ЗагрузитьИзменитьФормулу(Команда)
    ВыбранноеИмя = "";
    АдресВременногоХранилища = "";
    Если ПоместитьФайл(АдресВременногоХранилища,"",ВыбранноеИмя,Истина,
        УникальныйИдентификатор) Тогда
        Файл = Новый Файл(ВыбранноеИмя);
        ИмяФайлаКартинки = Файл.Имя;
        АдресКартинки = АдресВременногоХранилища;
        Модифицированность = Истина;
    КонецЕсли;
КонецПроцедуры

&НаСервере
Процедура ПередЗаписьюНаСервере(Отказ, ТекущийОбъект, ПараметрыЗаписи)
    Если ЭтоАдресВременногоХранилища(АдресКартинки) Тогда
        ДвоичныеДанные = ПолучитьИзВременногоХранилища(АдресКартинки);
        ТекущийОбъект.КартинкаФормулыМодели =
        Новый ХранилищеЗначения(ДвоичныеДанные, Новый СжатиеДанных());
        ТекущийОбъект.ИмяФайлаКартинки = ИмяФайлаКартинки;
    КонецЕсли;
КонецПроцедуры

&НаСервере
Процедура ПриЗаписиНаСервере(Отказ, ТекущийОбъект, ПараметрыЗаписи)
```

```
        Если ЭтоАдресВременногоХранилища(АдресКартинки) Тогда
            УдалитьИзВременногоХранилища(АдресКартинки);
            АдресКартинки = ПолучитьНавигационнуюССылку(
            ТекущийОбъект.Ссылка, "КартинкаФормулыМодели");
        КонецЕсли;
КонецПроцедуры
&НаСервере
Процедура ПриСозданииНаСервере(Отказ, СтандартнаяОбработка)
        Если Объект.ИмяФайлаКартинки <> "" Тогда
            АдресКартинки = ПолучитьНавигационнуюССылку(
            Объект.Ссылка, "КартинкаФормулыМодели");
        КонецЕсли;
КонецПроцедуры
```

Код форми документа Стратегії побудови систем безпеки

```
&НаКлиенте
Процедура МодельПриИзменении(Элемент)
        АдресКартинки = ПолучитьНавигационнуюССылку(Объект.Модель,
"КартинкаФормулыМодели");
КонецПроцедуры

&НаСервере
Процедура ПриСозданииНаСервере(Отказ, СтандартнаяОбработка)
        АдресКартинки = ПолучитьНавигационнуюССылку(Объект.Модель,
"КартинкаФормулыМодели");
КонецПроцедуры

&НаКлиенте
Процедура ЗаполнитьСистемуВлияний(Команда)
        ГСЧ = Новый ГенераторСлучайныхЧисел();
        Объект.СистемаВлияний.Очистить();
        Выборка = Справочники.Vp_ТипыВлияний.Выбрать();
        Пока Выборка.Следующий() Цикл
            Если Выборка.ПометкаУдаления Тогда
                Продолжить;
```

```
            КонецЕсли;
            СлучЧисло = ГСЧ.СлучайноеЧисло(1, 4294967295);
            СлучЧисло = СлучЧисло % 20;
            НоваяСтрока = Объект.СистемаВлияний.Добавить();
            НоваяСтрока.ТипВлияния = Выборка.Ссылка;
            НоваяСтрока.Количество = СлучЧисло;
        КонецЦикла;
        Объект.СистемаВлияний.Сортировать("Количество Убыв");
        ПересчитатьИтоговыеПоля();
КонецПроцедуры

&НаКлиенте
Процедура ЗаполнитьСистемуЗащиты(Команда)
        ГСЧ = Новый ГенераторСлучайныхЧисел();
        Объект.СистемаЗащиты.Очистить();
        Выборка = Справочники.Vp_ТипыПодсистемЗащиты.Выбрать();
        Пока Выборка.Следующий() Цикл
            Если Выборка.ПометкаУдаления Тогда
                Продолжить;
            КонецЕсли;
            СлучЧисло = ГСЧ.СлучайноеЧисло(1, 4294967295);
            СлучЧисло = СлучЧисло % 20;
            НоваяСтрока = Объект.СистемаЗащиты.Добавить();
            НоваяСтрока.ТипПодсистемыЗащиты = Выборка.Ссылка;
            НоваяСтрока.Количество = СлучЧисло;
        КонецЦикла;
        Объект.СистемаЗащиты.Сортировать("Количество Убыв");
        ПересчитатьИтоговыеПоля();
КонецПроцедуры

&НаКлиенте
Процедура ЗаполнитьИнформационныйБлок(Команда)
        ГСЧ = Новый ГенераторСлучайныхЧисел();
        Объект.ИнформационныеБлоки.Очистить();
        Выборка = Справочники.Vp_ИнформационныеБлоки.Выбрать();
```

```
        Пока Выборка.Следующий() Цикл
            Если Выборка.ПометкаУдаления Тогда
                Продолжить;
            КонецЕсли;
            СлучЧисло = ГСЧ.СлучайноеЧисло(1, 4294967295);
            СлучЧисло = СлучЧисло % 25;
            НоваяСтрока = Объект.ИнформационныеБлоки.Добавить();
            НоваяСтрока.ИнформационныйБлок = Выборка.Ссылка;
            НоваяСтрока.ЦенностьБлока = СлучЧисло;
        КонецЦикла;
        Объект.ИнформационныеБлоки.Сортировать("ЦенностьБлока Убыв");
        ПересчитатьИтоговыеПоля();
КонецПроцедуры

&НаКлиенте
Процедура ЗаполнитьТаблицуВходныхДанных(Команда)
        Объект.ТаблицаВходныхДанных.Очистить();
        Для Каждого Строка Из Объект.Модель.ТаблицаВходныхДанных Цикл
            НоваяСтрока = Объект.ТаблицаВходныхДанных.Добавить();
            ЗаполнитьЗначенияСвойств(НоваяСтрока, Строка);
            НоваяСтрока.НачальноеЗначение = 0;
            НоваяСтрока.Шаг = 0.25;
            НоваяСтрока.КонечноеЗначение = 1;
        КонецЦикла;
        Объект.ТаблицаВходныхДанных.Сортировать("ИмяПеременной Возвр");
        Объект.МоделированиеСтратегий.Очистить();
        УстановитьВидимость();
КонецПроцедуры

&НаКлиенте
Процедура СистемаВлияний ПриОкончанииРедактирования(Элемент, НоваяСтрока,
ОтменаРедактирования)
        ПересчитатьИтоговыеПоля();
КонецПроцедуры
```

```
&НаКлиенте
Процедура СистемаЗащитыПриОкончанииРедактирования(Элемент, НоваяСтрока,
ОтменаРедактирования)
	ПересчитатьИтоговыеПоля();
КонецПроцедуры

&НаКлиенте
Процедура ИнформационныеБлокиПриОкончанииРедактирования(Элемент,
		НоваяСтрока, ОтменаРедактирования)
	ПересчитатьИтоговыеПоля();
КонецПроцедуры

&НаКлиенте
Процедура СистемаВлиянийПослеУдаления(Элемент)
	ПересчитатьИтоговыеПоля();
КонецПроцедуры

&НаКлиенте
Процедура СистемаЗащитыПослеУдаления(Элемент)
	ПересчитатьИтоговыеПоля();
КонецПроцедуры

&НаКлиенте
Процедура ИнформационныеБлокиПослеУдаления(Элемент)
	ПересчитатьИтоговыеПоля();
КонецПроцедуры

&НаКлиенте
Процедура ПересчитатьИтоговыеПоля()
	Объект.ОбщийРесурсВлияния = Объект.СистемаВлияний.Итог("Количество");
	Объект.ОбщийЗащитныйРесурс = Объект.СистемаЗащиты.Итог("Количество");
	Объект.ОбщаяЦенностьИнформационноБлока =
	 Объект.ИнформационныеБлоки.Итог("ЦенностьБлока");
КонецПроцедуры
```

```
&НаКлиенте
Процедура РасчетСтратегий(Команда)
	Объект.МоделированиеСтратегий.Очистить();
	ТаблицаЗначений = ПолучитьТаблицуЗначениеВходныхДанных();
	ТаблицаЗначений.Колонки.Добавить("ТекущееЗначение");
	МассивПеременнойВремени = ТаблицаЗначений.НайтиСтроки(
	 Новый Структура("ЭтоПеременнаяВремени", Истина));
	МассивПеременных = ТаблицаЗначений.НайтиСтроки(
	 Новый Структура("ЭтоПеременнаяВремени", Ложь));
	Если МассивПеременных.Количество() = 0 ИЛИ
МассивПеременнойВремени.Количество() = 0 Тогда
		Возврат;
	КонецЕсли;
	СтрокаВремени = МассивПеременнойВремени[0];
	РасчитатьУровеньЗащищености(МассивПеременных, СтрокаВремени, 0);
КонецПроцедуры

&НаСервере
Функция ПолучитьТаблицуЗначениеВходныхДанных()
	Возврат Объект.ТаблицаВходныхДанных.Выгрузить();
КонецФункции

&НаКлиенте
Процедура РасчитатьУровеньЗащищености(МассивПеременных,
		СтрокаВремени, ИндексМасиваПеременных = 0)
	ИндексПеременных = ИндексМасиваПеременных;
	Если ИндексПеременных < МассивПеременных.Количество() Тогда
		СтрокаПеременной = МассивПеременных[ИндексПеременных];
		СтрокаПеременной.ТекущееЗначение = СтрокаПеременной.НачальноеЗначение;
		Пока СтрокаПеременной.ТекущееЗначение <=
СтрокаПеременной.КонечноеЗначение Цикл
			РасчитатьУровеньЗащищености(МассивПеременных, СтрокаВремени,
			 ИндексПеременных + 1);
			СтрокаПеременной.ТекущееЗначение =
СтрокаПеременной.ТекущееЗначение
```

```
                + СтрокаПеременной.Шаг;
            КонецЦикла;
        Иначе
            НоваяСтрока = Объект.МоделированиеСтратегий.Добавить();
            СтрокаПеременных = "";
            КодВыполнения = "";
            ИндПеременной = 0;
            Пока ИндПеременной < МассивПеременных.Количество() Цикл
                НоваяСтрока["ИмяПеременной" + (ИндПеременной + 1)] =
                  МассивПеременных[ИндПеременной].ИмяПеременной;
                НоваяСтрока["ЗначениеПеременной"      + (ИндПеременной + 1)] =
                  МассивПеременных[ИндПеременной].ТекущееЗначение;
                СтрокаПеременных = СтрокаПеременных +
                МассивПеременных[ИндПеременной].ИмяПеременной + " = " +
                  Формат(МассивПеременных[ИндПеременной].ТекущееЗначение,"ЧРД=.;
ЧН=0; ЧГ=") + ", ";
                КодВыполнения = КодВыполнения +
                  МассивПеременных[ИндПеременной].ИмяПеременной + " = " +
                  Формат(МассивПеременных[ИндПеременной].ТекущееЗначение,"ЧРД=.;
ЧН=0; ЧГ=") + ";"
                  + Символы.ПС;
                ИндПеременной = ИндПеременной + 1;
            КонецЦикла;
            СтрокаПеременных = Лев(СтрокаПеременных, СтрДлина(СтрокаПеременных) -
2);
            НоваяСтрока.СтрокаПеременных = СтрокаПеременных;
            КодВыполненияВремя = "";
            СтрокаВремени.ТекущееЗначение = СтрокаВремени.НачальноеЗначение;
            ИндСтрокиВремени = 0;
            Пока ИндСтрокиВремени < 10 Цикл
                КодВыполненияВремя = КодВыполненияВремя +
СтрокаВремени.ИмяПеременной + " = " +
                  Формат(СтрокаВремени.ТекущееЗначение,"ЧРД=.; ЧН=0; ЧГ=") + ";" +
Символы.ПС;
                КодВыполненияВремя = КодВыполненияВремя +
```

```
                Объект.Модель.ИмяВыходнойПеременной + " = 0;" + Символы.ПС;
            КодВыполненияВремя = КодВыполненияВремя +
Объект.Модель.КодФормулы +
                Символы.ПС;
            КодВыполненияВремя = КодВыполненияВремя +
"НоваяСтрока.УровниЗащищенностиТ" +
                (ИндСтрокиВремени + 1) + " = " +
Объект.Модель.ИмяВыходнойПеременной + ";" +
                Символы.ПС;
            КодВыполненияВремя = КодВыполненияВремя +
"НоваяСтрока.УровниЗащищенностиТ" +
                (ИндСтрокиВремени + 1) + " = " + "?(НоваяСтрока.УровниЗащищенностиТ"
+
                (ИндСтрокиВремени + 1) + " > 1, 1, НоваяСтрока.УровниЗащищенностиТ"
+
                (ИндСтрокиВремени + 1) + ");" + Символы.ПС;
            КодВыполненияВремя = КодВыполненияВремя +
"НоваяСтрока.УровниЗащищенностиТ" +
                (ИндСтрокиВремени + 1) + " = " + "?(НоваяСтрока.УровниЗащищенностиТ"
+
                (ИндСтрокиВремени + 1) + " < 0, 0, НоваяСтрока.УровниЗащищенностиТ"
+
                (ИндСтрокиВремени + 1) + ");" + Символы.ПС;
            Попытка
                Выполнить(КодВыполнения + КодВыполненияВремя);
            Исключение
                Сообщить(ОписаниеОшибки());
            КонецПопытки;
            СтрокаВремени.ТекущееЗначение = СтрокаВремени.ТекущееЗначение +
                СтрокаВремени.Шаг;
            ИндСтрокиВремени = ИндСтрокиВремени + 1;
        КонецЦикла;
    КонецЕсли;
КонецПроцедуры
```

```
&НаКлиенте
Процедура ПриОткрытии(Отказ)
	УстановитьВидимость();
	ОбновитьДиаграму();
КонецПроцедуры

&НаКлиенте
Процедура ТаблицаВходныхДанныхПриОкончанииРедактирования(Элемент,
НоваяСтрока, ОтменаРедактирования)
	Объект.МоделированиеСтратегий.Очистить();
	УстановитьВидимость();
КонецПроцедуры

&НаКлиенте
Процедура ТаблицаВходныхДанныхПослеУдаления(Элемент)
	Объект.МоделированиеСтратегий.Очистить();
	УстановитьВидимость();
КонецПроцедуры

&НаКлиенте
Процедура УстановитьВидимость()
	МассивПеременных = Объект.ТаблицаВходныхДанных.НайтиСтроки(Новый
	 Структура("ЭтоПеременнаяВремени", Ложь));
	КоличествоПараметров = МассивПеременных.Количество();
	ЭтаФорма.Элементы.МоделированиеСтратегийГруппа1.Видимость =
(КоличествоПараметров >= 1);
	ЭтаФорма.Элементы.МоделированиеСтратегийГруппа2.Видимость =
(КоличествоПараметров >= 2);
	ЭтаФорма.Элементы.МоделированиеСтратегийГруппа3.Видимость =
(КоличествоПараметров >= 3);
	ЭтаФорма.Элементы.МоделированиеСтратегийГруппа4.Видимость =
(КоличествоПараметров >= 4);
	ЭтаФорма.Элементы.МоделированиеСтратегийГруппа5.Видимость =
(КоличествоПараметров >= 5);
КонецПроцедуры
```

```
&НаКлиенте
Процедура ОбновитьДиаграмуВывода(Команда)
	ОбновитьДиаграму();
КонецПроцедуры

&НаКлиенте
Процедура ОбновитьДиаграму()
	МассивПоискаСтратегий	= Объект.МоделированиеСтратегий.НайтиСтроки(
	Новый Структура("ВыводитьДиаграму", Истина));
	МассивВремени	= Новый Массив;
	МассивПоискаВремени = Объект.ТаблицаВходныхДанных.НайтиСтроки(
	Новый Структура("ЭтоПеременнаяВремени", Истина));
	СтрокаВремени = МассивПоискаВремени[0];
	ТекущееЗначение = СтрокаВремени.НачальноеЗначение;
	ИндСтрокиВремени = 0;
	Пока ИндСтрокиВремени < 10 Цикл
		МассивВремени.Добавить( Формат(ТекущееЗначение,"ЧРД=.; ЧН=0; ЧГ="));
		ТекущееЗначение		= ТекущееЗначение + СтрокаВремени.Шаг;
		ИндСтрокиВремени	= ИндСтрокиВремени + 1;
	КонецЦикла;
	ТзДляВывода = Новый ТаблицаЗначений;
	ТзДляВывода.Колонки.Добавить("Серия");
	Инд = 1;
	Для Каждого ЭлементМассива Из МассивВремени Цикл
		ТзДляВывода.Колонки.Добавить("Т"+Инд);
		Инд = Инд + 1;
	КонецЦикла;
	Для Каждого СтрокаПоиска Из МассивПоискаСтратегий Цикл
		НоваяСтрока = ТзДляВывода.Добавить();
		Серия = СтрокаПоиска.СтрокаПеременных;
		НоваяСтрока.Серия = Серия;
		Инд = 1;
		Для Каждого ЭлементМассива Из МассивВремени Цикл
			ИмяКолонки = "Т"+Инд;
```

```
                НоваяСтрока[ИмяКолонки] = СтрокаПоиска["УровениЗащищоностиТ" +
Инд];
                ТзДляВывода.Колонки[ИмяКолонки].Заголовок = "" + ЭлементМассива;
                Инд = Инд + 1;
            КонецЦикла;
        КонецЦикла;
        ЭтаФорма.Диаграмма.Очистить();
        ЭтаФорма.Диаграмма.ТипДиаграммы       = ТипДиаграммы.График;
        ЭтаФорма.Диаграмма.СерииВСтроках      = Истина;
        ЭтаФорма.Диаграмма.ИсточникДанных     = ТзДляВывода;
КонецПроцедуры
```

ПЗ Vulnerability Assessment – 2014 v.1.0

Код загального модуля Доп.Процедури

```
Функция ПолучитьКомбинациюПараметров(СписокПараметров, Инд = 0,
            СтрокаТЧДокумента = Неопределено) Экспорт
        Результат = "";
        Если Не ЗначениеЗаполнено(СписокПараметров) Тогда
            Возврат Результат;
        КонецЕсли;
        КоличествоВсегоКомбинаций = 1;
        Для Каждого СтрокаТЧ Из СписокПараметров.СписокПараметров Цикл
            КоличествоВсегоКомбинаций = КоличествоВсегоКомбинаций *
             СтрокаТЧ.Параметр.ЛингвестПерем.Количество();
        КонецЦикла;
        ТекИнд = Инд;
        Если ТекИнд < 0 Тогда
            ТекИнд = 0;
        ИначеЕсли ТекИнд >= КоличествоВсегоКомбинаций Тогда
            ТекИнд = КоличествоВсегоКомбинаций - 1;
        КонецЕсли;
        ИндПараметра = 1;
        Для Каждого СтрокаТЧ Из СписокПараметров.СписокПараметров Цикл
            ИндСоответствия = ?( СтрокаТЧ.Параметр.ЛингвестПерем.Количество() = 0, 0,
```

```
            ТекИнд % СтрокаТЧ.Параметр.ЛингвестПерем.Количество() );
            Параметр = СтрокаТЧ.Параметр;
            Соответствие =
СтрокаТЧ.Параметр.ЛингвестПерем[ИндСоответствия].Переменная;
            Если СтрокаТЧДокумента <> Неопределено Тогда
                СтрокаТЧДокумента["Пар" + ИндПараметра]    = Параметр;
                СтрокаТЧДокумента["ЛПпар" + ИндПараметра]          = Соответствие;
            КонецЕсли;
            ТекИнд = ?( СтрокаТЧ.Параметр.ЛингвестПерем.Количество() = 0, 0,
             Цел(ТекИнд / СтрокаТЧ.Параметр.ЛингвестПерем.Количество()));
            Результат = Результат + ?(ЗначениеЗаполнено(Результат), ", ", "") + Параметр
             + " = " + Соответствие;
            ИндПараметра = ИндПараметра + 1;
        КонецЦикла;
        Возврат Результат;
КонецФункции
```

Код форми документа Еталони

```
&НаКлиенте
Процедура ЗаполнитьДанные(Команда)
        Объект.ДанныеАналитика.Очистить();
        Объект.Эталон.Очистить();
        МассивЛингвестПеременные =
ПолучитьТаблицуЛингвестическихПеременных(Объект.Параметр);
        МассивИнтервалы = ПолучитьТаблицуИнтервалов(Объект.Параметр);
        Для Каждого ЭлементЛП Из МассивЛингвестПеременные Цикл
            Для Каждого ЭлементИ Из МассивИнтервалы Цикл
                НоваяСтрока = Объект.ДанныеАналитика.Добавить();
                НоваяСтрока.ЛингвестПеременная = ЭлементЛП;
                НоваяСтрока.Интервал = ЭлементИ;
                НоваяСтрока.Значение = 0;
            КонецЦикла;
        КонецЦикла;
КонецПроцедуры
```

```
&НаКлиенте
Функция ПолучитьТаблицуЛингвестическихПеременных(Параметр)
	Возврат Параметр.ЛингвестПерем.ВыгрузитьКолонку("Переменная");
КонецФункции

&НаКлиенте
Функция ПолучитьТаблицуИнтервалов(Параметр)
	Возврат Параметр.Интервалы.ВыгрузитьКолонку("Интервал");
КонецФункции

&НаКлиенте
Процедура Расчитать(Команда)
	Объект.Эталон.Очистить();
	Если Объект.ДанныеАналитика.Количество() = 0 Тогда
	    Возврат;
	КонецЕсли;
	// Этап 0. Полуем Количество Разных интервалов и ЛП
	МассивИнтервалы = ПолучитьМассив("Интервал");
	МассивЛингвестПеременные = ПолучитьМассив("ЛингвестПеременная");
	КоличествоИ = МассивИнтервалы.Количество();
	КоличествоЛП = МассивЛингвестПеременные.Количество();
	// Этап 1. Полуем рядок К
	ТзК = ПолучитьТаблицуЗначений("Интервал","Значение");
	// Этап 2. Ищем максимальный элемент ТзК
	Кмакс = 0;
	Для Каждого СтрокаТз Из ТзК Цикл
	    Если СтрокаТз.Значение > Кмакс Тогда
	        Кмакс = СтрокаТз.Значение;
	     КонецЕсли;
	КонецЦикла;
	// Этап 3. Обчислюем ТЗ_С.
	ТзС = ПолучитьТаблицуЗначений("ЛингвестПеременная, Интервал","Значение");
	ТзС.Очистить();
	ИндИ = 0;
```

```
Пока ИндИ < КоличествоИ Цикл
    МассивПоиска1 = ТзК.НайтиСтроки(Новый Структура("Интервал", МассивИнтервалы[ИндИ]));
    КСтолбца = МассивПоиска1[0].Значение;
    ИндЛП = 0;
    Пока ИндЛП < КоличествоЛП Цикл
        Если КСтолбца <> 0 Тогда
            МассивПоиска2 = Объект.ДанныеАналитика.НайтиСтроки(
              Новый Структура("ЛингвестПеременная, Интервал",
              МассивЛингвестПеременные[ИндЛП], МассивИнтервалы[ИндИ]));
            НоваяСтрока = ТзС.Добавить();
            НоваяСтрока.ЛингвестПеременная = МассивЛингвестПеременные[ИндЛП];
            НоваяСтрока.Интервал = МассивИнтервалы[ИндИ];
            НоваяСтрока.Значение = МассивПоиска2[0].Значение * Кмакс / КСтолбца;
        Иначе
            НоваяСтрока = ТзС.Добавить();
            НоваяСтрока.ЛингвестПеременная = МассивЛингвестПеременные[ИндЛП];
            НоваяСтрока.Интервал = МассивИнтервалы[ИндИ];
            Инд1 = ?((ИндИ-1) < 0, КоличествоИ -1, ИндИ-1);
            Инд2 = ?((ИндИ+1) >= КоличествоИ, 0, ИндИ+1);
            МассивПоиска3 = Объект.ДанныеАналитика.НайтиСтроки(
              Новый Структура("ЛингвестПеременная, Интервал",
              МассивЛингвестПеременные[ИндЛП], МассивИнтервалы[Инд1]));
            МассивПоиска4 = Объект.ДанныеАналитика.НайтиСтроки(
              Новый Структура("ЛингвестПеременная, Интервал",
              МассивЛингвестПеременные[ИндЛП], МассивИнтервалы[Инд2]));
            НоваяСтрока.Значение= (МассивПоиска3[0].Значение+ МассивПоиска4[0].Значение)/2;
        КонецЕсли;
        ИндЛП = ИндЛП + 1;
    КонецЦикла;
    ИндИ = ИндИ + 1;
```

```
КонецЦикла;
// Этап 4. Ищем ТЗ_М
ТЗМ = ТзС.Скопировать();
ТзМ.Очистить();
ИндЛП = 0;
Пока ИндЛП < КоличествоЛП Цикл
    /// ищем C_i_max
    МаксЕл = 0;
    ИндИ1 = 0;
    МассивПоиска1 = ТзС.НайтиСтроки(Новый Структура("ЛингвестПеременная",
     МассивЛингвестПеременные[ИндЛП]));
    Пока ИндИ1 < КоличествоИ Цикл
        Если МассивПоиска1[ИндИ1].Значение > МаксЕл Тогда
            МаксЕл = МассивПоиска1[ИндИ1].Значение;
        КонецЕсли;
        ИндИ1 = ИндИ1 + 1;
    КонецЦикла;
    /// M_i_j = C_i_j / C_i_max
    ИндИ2 = 0;
    Пока ИндИ2 < КоличествоИ Цикл
        МассивПоиска2 = ТзС.НайтиСтроки(Новый
Структура("ЛингвестПеременная, Интервал",
         МассивЛингвестПеременные[ИндЛП], МассивИнтервалы[ИндИ2]));
        НоваяСтрока = ТЗМ.Добавить();
        НоваяСтрока.ЛингвестПеременная = МассивЛингвестПеременные[ИндЛП];
        НоваяСтрока.Интервал = МассивИнтервалы[ИндИ2];
        НоваяСтрока.Значение = ?(МаксЕл = 0, 0, МассивПоиска2[0].Значение /
МаксЕл);
        ИндИ2 = ИндИ2 + 1;
    КонецЦикла;
    ИндЛП = ИндЛП + 1;
КонецЦикла;
/// Этап 5. Заполнение ТЧ
Для Каждого ЭлементЛП Из МассивЛингвестПеременные Цикл
    Для Каждого ЭлементИ Из МассивИнтервалы Цикл
```

```
                НоваяСтрока = Объект.Эталон.Добавить();
                НоваяСтрока.ЛингвестПеременная = ЭлементЛП;
                НоваяСтрока.Интервал = ЭлементИ;
                МассивПоиска1 = ТзМ.НайтиСтроки(Новый
Структура("ЛингвестПеременная, Интервал",
                  ЭлементЛП, ЭлементИ));
                //НоваяСтрока.КоордХ = МассивПоиска1[0].Значение;
                НоваяСтрока.КоордY = МассивПоиска1[0].Значение;
                МассивПоиска = Объект.Параметр.Интервалы.НайтиСтроки(Новый
Структура(
                 "Интервал", ЭлементИ));
                Если МассивПоиска.Количество() <> 0 Тогда
                    //НоваяСтрока.КоордY = МассивПоиска[0].Коэффициент;
                        НоваяСтрока.КоордХ = МассивПоиска[0].Коэффициент;
                КонецЕсли;
            КонецЦикла;
        КонецЦикла;
КонецПроцедуры

&НаСервере
Функция ПолучитьМассив(ИмяРеквизита)
    Тз = Объект.ДанныеАналитика.Выгрузить();
    Тз.Свернуть(ИмяРеквизита,"");
    Массив = Тз.ВыгрузитьКолонку(ИмяРеквизита);
    Возврат Массив;
КонецФункции

&НаСервере
Функция ПолучитьТаблицуЗначений(ИмяРеквизита, ИмяРесурса)
    Тз = Объект.ДанныеАналитика.Выгрузить();
    Тз.Свернуть(ИмяРеквизита,ИмяРесурса);
    Возврат Тз;
КонецФункции
```

Код модуля документа Еталони

```
Процедура ОбработкаПроведения(Отказ, РежимПроведения)
	ПроверитьЗаполнениеПолей(Отказ);
	Если Не Отказ ТОгда
		ДвиженияДокумента();
	КонецЕсли;
КонецПроцедуры

Процедура ДвиженияДокумента()
	Движения.Vr_ЛингвестЭталонны.Очистить();
	Для Каждого Строка Из Эталон Цикл
		Движение = Движения.Vr_ЛингвестЭталонны.Добавить();
		Движение.Период = Дата;
		Движение.Регистратор = Ссылка;
		Движение.СписокПараметров = СписокПараметров;
		Движение.Аналитик = Аналитик;
		Движение.Параметр = Параметр;
		Движение.ЛингвестПеременная = Строка.ЛингвестПеременная;
		Движение.Интервал = Строка.Интервал;
		Движение.КоордX = Строка.КоордX;
		Движение.КоордY = Строка.КоордY;
	КонецЦикла;
	Движения.Vr_ЛингвестЭталонны.Записать();
КонецПроцедуры
```

Код форми документа Установка правил

```
&НаКлиенте
Процедура ПриОткрытии(Отказ)
	УстановитьВидимость();
КонецПроцедуры

&НаКлиенте
Процедура СписокПараметровПриИзменении(Элемент)
	Объект.ЛингвестИдент.Очистить();
	Объект.Правила.Очистить();
	УстановитьВидимость();
КонецПроцедуры
```

```
&НаКлиенте
Процедура ЗаполнитьЛИ(Команда)
	Объект.ЛингвестИдент.Очистить();
	Выборка =
Справочники.Vr_ЛингвестИдентефикаторы.Выбрать(,Объект.СписокПараметров);
	Пока Выборка.Следующий() Цикл
		Если Выборка.ПометкаУдаления Тогда
			Продолжить;
		КонецЕсли;
		НоваяСтрока = Объект.ЛингвестИдент.Добавить();
		НоваяСтрока.ЛИ = Выборка.Ссылка;
		НоваяСтрока.Порядок = Выборка.Ссылка.Порядок;
	КонецЦикла;
	Объект.ЛингвестИдент.Сортировать("Порядок Возвр");
КонецПроцедуры

&НаКлиенте
Процедура СформироватьПравила(Команда)
	ПроверкаПройдена = Истина;
	Если Не ЗначениеЗаполнено(Объект.СписокПараметров) Тогда
		Сообщить("Заполните список параметров!");
		ПроверкаПройдена = Ложь;
	КонецЕсли;
	Если Объект.ЛингвестИдент.Количество() = 0 Тогда
		Сообщить("Заполните ТЧ лингвест. идент.!");
		ПроверкаПройдена = Ложь;
	КонецЕсли;
	Если Не ПроверкаПройдена Тогда
		Возврат;
	КонецЕсли;
	КоличествоВсегоКомбинаций = 1;
	Для Каждого СтрокаТЧ Из Объект.СписокПараметров.СписокПараметров Цикл
		КоличествоВсегоКомбинаций = КоличествоВсегоКомбинаций *
		СтрокаТЧ.Параметр.ЛингвестПерем.Количество();
```

```
        КонецЦикла;
        Объект.Правила.Очистить();
        Инд = 0;
        Пока Инд < КоличествоВсегоКомбинаций Цикл
            ОбработкаПрерыванияПользователя();
            Состояние("" + (Инд + 1) + " / " + КоличествоВсегоКомбинаций);
            НоваяСтрока = Объект.Правила.Добавить();
            НоваяСтрока.ИндКомбинацииПараметра = Инд + 1;
            НоваяСтрока.НаименованиеКомбинации=
ДопПроцедуры.ПолучитьКомбинациюПараметров(
             Объект.СписокПараметров, Инд, НоваяСтрока);
            Инд = Инд + 1;
        КонецЦикла;
КонецПроцедуры

&НаКлиенте
Процедура ОчиститьПравила(Команда)
        Объект.Правила.Очистить();
КонецПроцедуры

&НаКлиенте
Процедура ПравилаИндКомбинацииПараметраПриИзменении(Элемент)
        ТекСтрока = ЭтаФорма.ТекущийЭлемент.ТекущиеДанные;
        Если ТекСтрока.ИндКомбинацииПараметра = 0 Тогда
            ТекСтрока.ИндКомбинацииПараметра = 1;
        КонецЕсли;
        ТекСтрока.НаименованиеКомбинации =
ДопПроцедуры.ПолучитьКомбинациюПараметров(
        Объект.СписокПараметров, ТекСтрока.ИндКомбинацииПараметра - 1, ТекСтрока);
КонецПроцедуры

&НаКлиенте
Процедура ОчиститьУязвимостьИЛИ(Команда)
        Для Каждого СтрокаТЧ Из Объект.Правила Цикл
            СтрокаТЧ.ЛИ  = Неопределено;
```

```
            СтрокаТЧ.Уязвимость = Неопределено;
        КонецЦикла;
КонецПроцедуры

&НаКлиенте
Процедура УстановитьВидимость()
        КоличествоПараметров =
Объект.СписокПараметров.СписокПараметров.Количество();
        ЭтаФорма.Элементы.ПравилаГруппа1.Видимость          = (КоличествоПараметров
>= 1);
        ЭтаФорма.Элементы.ПравилаГруппа2.Видимость          = (КоличествоПараметров
>= 2);
        ЭтаФорма.Элементы.ПравилаГруппа3.Видимость          = (КоличествоПараметров
>= 3);
        ЭтаФорма.Элементы.ПравилаГруппа4.Видимость          = (КоличествоПараметров
>= 4);
        ЭтаФорма.Элементы.ПравилаГруппа5.Видимость          = (КоличествоПараметров
>= 5);
        ЭтаФорма.Элементы.ПравилаГруппа6.Видимость          = (КоличествоПараметров
>= 6);
        ЭтаФорма.Элементы.ПравилаГруппа7.Видимость          = (КоличествоПараметров
>= 7);
        ЭтаФорма.Элементы.ПравилаГруппа8.Видимость          = (КоличествоПараметров
>= 8);
        ЭтаФорма.Элементы.ПравилаГруппа9.Видимость          = (КоличествоПараметров
>= 9);
        ЭтаФорма.Элементы.ПравилаГруппа10.Видимость = (КоличествоПараметров >=
10);
КонецПроцедуры

&НаКлиенте
Процедура ЗаполнитьУязвимостиИЛИ(Команда)
        Для Каждого СтрокаТЧ Из Объект.Правила Цикл
            СтрокаТЧ.ЛИ = Неопределено;
            СтрокаТЧ.Уязвимость = Неопределено;
```

```
    КонецЦикла;
    КоличествоЛИ = 0;
    МассивЛИ = Новый Массив;
    Для Каждого Строка Из Объект.ЛингвестИдент Цикл
        КоличествоЛИ = КоличествоЛИ + 1;
        МассивЛИ.Добавить(Строка.ЛИ);
    КонецЦикла;
    КоличествоУязвимостей = 0;
    МассивУязвимостей = Новый Массив;
    Выборка = Справочники.Vr_Уязвимости.Выбрать();
    Пока Выборка.Следующий() Цикл
    Если Выборка.ПометкаУдаления Тогда
        Продолжить;
    КонецЕсли;
    КоличествоУязвимостей = КоличествоУязвимостей + 1;
        МассивУязвимостей.Добавить(Выборка.Ссылка);
    КонецЦикла;
    ГСЧ = Новый ГенераторСлучайныхЧисел();
    Для Каждого СтрокаТЧ Из Объект.Правила Цикл
       СлучЧисло = ГСЧ.СлучайноеЧисло(1, 4294967295);
       СлучЧисло = СлучЧисло % 10;
        Если СлучЧисло <= 1 Тогда
            СлучЧисло1 = ГСЧ.СлучайноеЧисло(1, 4294967295);
            СлучЧисло2 = ГСЧ.СлучайноеЧисло(1, 4294967295);
            СлучЧисло1 = СлучЧисло1 % КоличествоЛИ;
            СлучЧисло2 = СлучЧисло2 % КоличествоУязвимостей;
            СтрокаТЧ.ЛИ = МассивЛИ[СлучЧисло1];
            СтрокаТЧ.Уязвимость = МассивУязвимостей[СлучЧисло2];
        КонецЕсли;
    КонецЦикла;
КонецПроцедуры
```

Код модуля документа Установка правил

Код форми документа Оцінка вразливостей

```
&НаКлиенте
Процедура ПриОткрытии(Отказ)
	УстановитьВидимость();
КонецПроцедуры

&НаКлиенте
Процедура СписокПараметровПриИзменении(Элемент)
	Объект.ТаблицаДанных.Очистить();
	УстановитьВидимость();
КонецПроцедуры

&НаКлиенте
Процедура УстановитьВидимость()
	КоличествоПараметров =
Объект.СписокПараметров.СписокПараметров.Количество();
	ЭтаФорма.Элементы.ТаблицаДанныхГруппа1.Видимость	=
(КоличествоПараметров >= 1);
	ЭтаФорма.Элементы.ТаблицаДанныхГруппа2.Видимость	=
(КоличествоПараметров >= 2);
	ЭтаФорма.Элементы.ТаблицаДанныхГруппа3.Видимость	=
(КоличествоПараметров >= 3);
	ЭтаФорма.Элементы.ТаблицаДанныхГруппа4.Видимость	=
(КоличествоПараметров >= 4);
	ЭтаФорма.Элементы.ТаблицаДанныхГруппа5.Видимость	=
(КоличествоПараметров >= 5);
	ЭтаФорма.Элементы.ТаблицаДанныхГруппа6.Видимость	=
(КоличествоПараметров >= 6);
	ЭтаФорма.Элементы.ТаблицаДанныхГруппа7.Видимость	=
(КоличествоПараметров >= 7);
	ЭтаФорма.Элементы.ТаблицаДанныхГруппа8.Видимость	=
(КоличествоПараметров >= 8);
	ЭтаФорма.Элементы.ТаблицаДанныхГруппа9.Видимость	=
(КоличествоПараметров >= 9);
```

```
        ЭтаФорма.Элементы.ТаблицаДанныхГруппа10.Видимость       =
(КоличествоПараметров >= 10);
КонецПроцедуры

&НаКлиенте
Процедура Загрузить(Команда)
        ПроверкаПройдена = Истина;
        Если Не ЗначениеЗаполнено(Объект.СписокПараметров) Тогда
            Сообщить("Заполните список параметров!");
            ПроверкаПройдена = Ложь;
        КонецЕсли;
        Если Не ЗначениеЗаполнено(Объект.Аналитик) Тогда
             Сообщить("Заполните аналитика!");
             ПроверкаПройдена = Ложь;
        КонецЕсли;
        Если Не ЗначениеЗаполнено(Объект.КоличествоЗаписейСтатистики) Тогда
             Сообщить("Заполните количество записей статистики!");
             ПроверкаПройдена = Ложь;
        КонецЕсли;
        Если Не ПроверкаПройдена Тогда
             Возврат;
        КонецЕсли;
        Инд = 1;
        ПараметрыСпискаПараметров = Новый Структура;
        Для Каждого СтрокаТЧ Из Объект.СписокПараметров.СписокПараметров Цикл
            ПараметрыСпискаПараметров.Вставить("Пар" + Инд, СтрокаТЧ.Параметр);
            ПараметрыСпискаПараметров.Вставить("КолЛП" + Инд,
             СтрокаТЧ.Параметр.ЛингвестПерем.Количество());
            Инд = Инд + 1;
        КонецЦикла;
        ПараметрыСпискаПараметров.Вставить("КоличествоВсегоПараметров", Инд-1);
        ТзЭталонов = ПолучитьТзЭталонов();
        ТзПравил         = ПолучитьТзПравил();
        ГСЧ = Новый ГенераторСлучайныхЧисел();
        Объект.ТаблицаДанных.Очистить();
```

```
        Инд1 = 0;
        Пока Инд1 < Объект.КоличествоЗаписейСтатистики Цикл
            ОбработкаПрерыванияПользователя();
            Состояние("" + (Инд1+1) + " / " + Объект.КоличествоЗаписейСтатистики);
            НоваяСтрока = Объект.ТаблицаДанных.Добавить();
            ЗаполнитьЗначенияСвойств(НоваяСтрока, ПараметрыСпискаПараметров );
            Инд2 = 1;
            Для Каждого СтрокаТЧ Из Объект.СписокПараметров.СписокПараметров Цикл
                СлучЧисло = ГСЧ.СлучайноеЧисло(1, 100000000);
                СлучЧисло = СлучЧисло * 0.00000001;
                  НоваяСтрока["ЗначПар" + Инд2]           = СлучЧисло;
                НоваяСтрока["ЛППар" + Инд2]      = УстановитьЛП(ТзЭталонов,
                  НоваяСтрока["Пар" + Инд2],НоваяСтрока["ЗначПар" + Инд2]);

                Инд2 = Инд2 + 1;
            КонецЦикла;
            ИндексКомбинации        =
ПолучитьИндексКомбинации(ПараметрыСпискаПараметров,
             НоваяСтрока);
            НоваяСтрока.ИндКомбинацииПараметра = ИндексКомбинации;
            Правило = НайтиПравило(ИндексКомбинации, ТзПравил);
            Если Правило <> Неопределено Тогда
                НоваяСтрока.ЛИ = Правило.ЛИ;
                НоваяСтрока.Уязвимость = Правило.Уязвимость;
            КонецЕсли;
            Инд1 = Инд1 + 1;
        КонецЦикла;
КонецПроцедуры

&НаСервере
Функция ПолучитьТзЭталонов()
        Запрос = Новый Запрос;
        Запрос.Текст =
        "ВЫБРАТЬ
        | ЛингвестЭталонныСрезПоследних.СписокПараметров,
```

```
	| ЛингвестЭталонныСрезПоследних.Аналитик,
	| ЛингвестЭталонныСрезПоследних.Параметр,
	| ЛингвестЭталонныСрезПоследних.ЛингвестПеременная,
	| ЛингвестЭталонныСрезПоследних.Интервал,
	| ЛингвестЭталонныСрезПоследних.КоордX,
	| ЛингвестЭталонныСрезПоследних.КоордY
	|ИЗ
	| РегистрСведений.Vr_ЛингвестЭталонны.СрезПоследних(
	|		&Дата,
	|		СписокПараметров = &СписокПараметров
	|			И Аналитик = &Аналитик) КАК
ЛингвестЭталонныСрезПоследних";
	Запрос.УстановитьПараметр("Дата", Объект.Дата);
	Запрос.УстановитьПараметр("СписокПараметров", Объект.СписокПараметров);
	Запрос.УстановитьПараметр("Аналитик", Объект.Аналитик);
	Возврат Запрос.Выполнить().Выгрузить();
КонецФункции

&НаСервере
Функция ПолучитьТзПравил()
	Запрос = Новый Запрос;
	Запрос.Текст =
	"ВЫБРАТЬ
	| НаборПравилСрезПоследних.СписокПараметров,
	| НаборПравилСрезПоследних.Аналитик,
	| НаборПравилСрезПоследних.ИндКомбинацииПараметра,
	| НаборПравилСрезПоследних.Уязвимость,
	| НаборПравилСрезПоследних.ЛИ
	|ИЗ
	| РегистрСведений.Vr_НаборПравил.СрезПоследних(
	|		&Дата,
	|		СписокПараметров = &СписокПараметров
	|			И Аналитик = &Аналитик) КАК
НаборПравилСрезПоследних";
	Запрос.УстановитьПараметр("Дата", Объект.Дата);
```

```
        Запрос.УстановитьПараметр("СписокПараметров", Объект.СписокПараметров);
        Запрос.УстановитьПараметр("Аналитик", Объект.Аналитик);
        Возврат Запрос.Выполнить().Выгрузить();
КонецФункции

&НаКлиенте
Функция УстановитьЛП(ТзЭталонов, Параметр, ЗначениеПараметра)
        Результат = Неопределено;
        Если Не ЗначениеЗаполнено(Параметр) Тогда
              Возврат Результат;
        КонецЕсли;
        Интервал = Справочники.Vr_Интервалы.ПустаяСсылка();
        НомерСТрокиИнтервала = 0;
        ЗначПрошлогоИнтервала      = 0;
        Для Каждого СтрокаТч Из Параметр.Интервалы Цикл
            Если ( ЗначПрошлогоИнтервала <= ЗначениеПараметра ) И
                  ( ЗначениеПараметра <= СтрокаТч.Коэффициент ) Тогда
                Интервал = СтрокаТч.Интервал;
                НомерСТрокиИнтервала = СтрокаТЧ.НомерСтроки;
                Прервать;
            КонецЕсли;
            ЗначПрошлогоИнтервала = СтрокаТч.Коэффициент;
        КонецЦикла;

        ТЗЛП = Новый ТаблицаЗначений;
        ТЗЛП.Колонки.Добавить("ЛП");
        ТЗЛП.Колонки.Добавить("Коорд");

        Для Каждого СтрокаЛП Из Параметр.ЛингвестПерем Цикл
            МассивПоискаКон = ТзЭталонов.НайтиСтроки(Новый
Структура("СписокПараметров,
             Аналитик, Параметр, ЛингвестПеременная, Интервал",
Объект.СписокПараметров,
             Объект.Аналитик, Параметр, СтрокаЛП.Переменная, Интервал));
            X2 = МассивПоискаКон[0].КоордX;
```

```
            Y2 = МассивПоискаКон[0].КоордY;
            Если (НомерСТрокиИнтервала-2) < 0 Тогда
                X1 = 0;
                Y1 = Y2;
            Иначе
                МассивПоискаНач = ТзЭталонов.НайтиСтроки(Новый
Структура("СписокПараметров,
                 Аналитик, Параметр, ЛингвестПеременная, Интервал",
Объект.СписокПараметров,
                 Объект.Аналитик, Параметр, СтрокаЛП.Переменная,
                 Параметр.Интервалы[НомерСТрокиИнтервала-2].Интервал));
                X1 = МассивПоискаНач[0].КоордX;
                Y1 = МассивПоискаНач[0].КоордY;
            КонецЕсли;
            Попытка
                Ykоорд = (ЗначениеПараметра - X1) * (Y2 - Y1) / (X2 - X1) + Y1;
            Исключение
                Ykоорд = 0;
            КонецПопытки;
            НоваяСтрока = ТЗЛП.Добавить();
            НоваяСтрока.ЛП = СтрокаЛП.Переменная;
            НоваяСтрока.Коорд = Ykоорд;
        КонецЦикла;
        ТЗЛП.Сортировать("Коорд Убыв, ЛП Убыв");
        Возврат ТЗЛП[0].ЛП;
КонецФункции

&НаКлиенте
Функция ПолучитьИндексКомбинации(ПараметрыСпискаПараметров, СтротаТЧ)
    ДляПереноса = 0;
    ИндПолный = 0;
    Инд = ПараметрыСпискаПараметров.КоличествоВсегоПараметров;
    Пока Инд > 0 Цикл
        Пар = ПараметрыСпискаПараметров["Пар" + Инд];
        МассивПоиска = Пар.ЛингвестПерем.НайтиСтроки(Новый
```

```
Структура("Переменная",
            СтротаТЧ["ЛППар" + Инд]));
            ИндПолный = МассивПоиска[0].НомерСтроки;
            ИндПолный = ИндПолный + ДляПереноса *
ПараметрыСпискаПараметров["КолЛП" + Инд];
            ДляПереноса        = ИндПолный - 1;
            Инд = Инд - 1;
        КонецЦикла;
        Возврат ИндПолный;
КонецФункции

&НаКлиенте
Функция НайтиПравило(ИндКомбинацииПараметра, ТзПравил)
        Результат = Неопределено;
        МассивПоиска = ТзПравил.НайтиСтроки(Новый Структура("СписокПараметров,
Аналитик,
        ИндКомбинацииПараметра", Объект.СписокПараметров, Объект.Аналитик,
        ИндКомбинацииПараметра));
        Если МассивПоиска.Количество() > 0 Тогда
            Результат = МассивПоиска[0];
        КонецЕсли;
        Возврат Результат;
КонецФункции

&НаКлиенте
Процедура Очистить(Команда)
        Объект.ТаблицаДанных.Очистить();
КонецПроцедуры
```

Код модуля документа Оцінка вразливостей

```
Процедура ОбработкаПроведения(Отказ, РежимПроведения)
        ПроверитьЗаполнениеПолей(Отказ);
        Если Не Отказ ТОгда
            ДвиженияДокумента();
```

```
        КонецЕсли;
 КонецПроцедуры

Процедура ПроверитьЗаполнениеПолей(Отказ)

КонецПроцедуры

Процедура ДвиженияДокумента()
        Движения.Vr_ДанныеОценки.Очистить();
        Для Каждого СтрокаТЧ Из ТаблицаДанных Цикл
            Движение = Движения.Vr_ДанныеОценки.Добавить();
            Движение.Период = Дата;
            Движение.Регистратор = Ссылка;
            Движение.СписокПараметров    = СписокПараметров;
            Движение.Аналитик = Аналитик;
            Движение.НомерЭксперимента = СтрокаТЧ.НомерСтроки;
            Движение.ЛИ = СтрокаТЧ.ЛИ;
            Движение.Уязвимость = СтрокаТЧ.Уязвимость;
            Движение.НаименованиеКомбинации   =
ДопПроцедуры.ПолучитьКомбинациюПараметров(
             СписокПараметров, СтрокаТЧ.ИндКомбинацииПараметра);
            Движение.Количество      = 1;
        КонецЦикла;
        Движения.Vr_ДанныеОценки.Записать();
КонецПроцедуры
```

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Алексеев А. Управление рисками. Метод CRAMM / А. Алексеев // IT Expert. – Электрон. дан. – М. : ЗАО “ИТ Эксперт”, 2010. – Режим доступа: WorldWideWeb. – URL: http://www.itexpert.ru/rus/ITEMS/ITEMS_CRAMM.pdf.
2. Андреєв В.І. Основи інформаційної безпеки / Андреєв В.І., Хорошко В.О., Чередниченко В.С., Шелест М.Є. – К.: Вид. ДУІКТ, 2009. – 292 с.
3. Астахов А. Актуальные вопросы вявления сетевых атак. Jet Info №3 (106), 2002. – На сайте http://www.jetinfo.ru/2002/3/1/article 1.3.2002.html.
4. Астахов А. Анализ защищенности корпоративных систем // Оперативные системы. №07-08/2002. – На сайте http://www.osp.ru/os.
5. Астахов А.М. Искусство управления информационными рисками / Астахов А.М. – М : ДМК Пресс, 2010. – 314 с.
6. Берж К. Теория графов и ее применение. – М.: ИЛ, 1962. – 308 с.
7. Будько М.М. Визначення залишкового ризику при оцінці захищеності інформації в інформаційно-обчислювальних системах / Будько М.М. // Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні, Вип. 8, 2004. – С. 20-26.
8. Будько М.М. Методи оцінки загроз для інформації автоматизованих систем / Будько М.М. // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, Вип. 10, 2005. – С. 35-46.
9. Будько М.М. Методика оцінки захищеності інформації в ЛОМ / Будько М.М., Василенко В.С., Проскурін В.М. // ВІТІ НТТУ "КПІ", Збірник доповідей на II НТК.
10. Буравльов Є.П. Глобалізація: проблеми безпеки / Буравльов Є.П. – К.: Ін-т проблем нац. безпеки, 2007 – 160 с.

11. Бурушкин А.А. Использование аппарата сетей Петри-Маркова для оценки характеристик динамики реализации угроз безопасности информации в компьютерных сетях / А.А. Бурушкин, А.А. Панфилов, Ю.К. Язов // Противодействие угрозам терроризма. – М.: ІСТТ, 2007. - №10. – С. 162-169.

12. Василенко В.С. Методики визначення вихідних даних для оцінки залишкових ризиків у ЛОМ / Василенко В.С., Будько М.М. // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, Вип. 9, 2004. – С. 110-120

13. Васильев В. В. Моделирование задач оптимизации и дифференциальных игр / В. В. Васильев, В. Л. Баранов. – К. : Наукова думка, 1989. – 286 с.

14. Волобуев С.В. О систематизации выявления и анализа каналов утечки. Прямые и косвенные носители информации / Волобуев С.В. // Вопросы защиты информации, №1, 2000. – С. 26-37.

15. Воробьев А. А. Оценивание защищённости автоматизированных систем на основе методов теории игр / А. А. Воробьёв, Г. В. Куликов, А. В. Непомнящих // Информационные технологии (приложение). – М. : Новые технологии, 2007. – 24 с.

16. Воронин А.Н. Векторная оптимизация динамических систем / А.Н. Воронин, Ю.К. Зиатдинов, А.И. Козлов, В.С. Чабанюк; под ред. А.Н. Воронина. – К.: Техніка, 1999. – 284 с.

17. Вунш Г. Теория систем / Вунш Г. – М.: Сов. радио, 1978. – 288 с.

18. Габович А.Г. Методика оцінки рівня безпеки інформації / Габович А.Г., Горобець А.Ю., Горобець А.Ю., Хорошко В.О. // Вісник НУ «Львівська політехніка», №551, Автоматика, вимірювання та керування, 2006. – С. 48-53.

19. Гнатюк С.О. Теоретичні основи побудови та функціонування систем управління інцидентами інформаційної безпеки / С.О. Гнатюк, Ю.Є. Хохлачова, А.О. Охріменко, А.К. Гребенькова // Захист інформації. – 2012. – № 1(54). – С. 121-126.

20. Голубенко А.Л. Информационные технологии и киберпреступность / Голубенко А.Л., Хорошко В.А., Петров А.С., Белозеров Е.В. // Вісник СНУ ім. В. Даля, №9 (103), 2006. – С. 7-10.

21. Голубенко О.Л. Політика інформаційної безпеки / Голубенко О.Л., Хорошко В.О., Петров О.С., Головань С.М., Яремчук Ю.Є. – Луганськ: Вид. СНУ ім. В. Даля, 2009. – 300 с.

22. Горелик В.А. Исследование операций / Горелик В.А., Ушаков И.А. – М.: Машиностроение, 1986. – 288 с.

23. Грищук Р.В. Теоретичні основи моделювання процесів нападу на інформацію методами теорії диференційних ігор та диференційних перетворень: Монографія / Р.В. Грищук. – Житомир: Рута, 2010. – 280 с.

24. Грищук Р.В. Ігрові методи кібератак на інформаційну сферу / Р.В. Грищук, С.Ж. Піскун, В.О. Хорошко, Ю.Є. Хохлачова // Захист інформації. – 2012. – № 1(54). – С. 86-93.

25. Грищук Р.В. Синтез оптимальної поведінки в системі захист-атака / Грищук Р.В., Хорошко В.О. // Проблеми створення, випробування та експлуатації складних інформаційних систем. – Житомир : ЖВІ ім. С.П. Корольова НАУ, 2011, №5. – С. 60-66.

26. Грищук Р.В. Теоретичні основи моделювання процесів нападу на інформацію методами теорій диференціальних ігор та диференціальних перетворень: монографія / Грищук Р.В. – Житомир: Вид. Рута, 2012. – 280 с.

27. Даник Ю.Г. Національна безпека запобігання критичним ситуаціям / Даник Ю.Г., Катков Ю.І., Пічугін М.Ф. – Житомир: Рута, 2006. – 387 с.

28. Девянин В.Д. Модели безопасности компьютерных систем / В.Д. Девьянин. – М.: Издательский центр "Академия", 2005. – 144 с.

29. Дружинин В.В. Введение в теорию конфликта / Дружинин В.В., Конторов Д.С., Конторов М.Д. – М.: Радио и связь, 1989. – 298 с.

30. Захаров А.И. Информационные системы: оценка рисков / А.И. Захаров // Information Security (Информационная безопасность) – 2005. – №6 – С. 18–19.

31. Иванченко Е.В. Обработка информационных потоков и составление для них расписаний в системах защиты информации / Е.В. Иванченко, В.А. Хорошко, Ю.Е. Хохлачева // Інформатика та математичні методи в моделюванні. – 2014. – Т. 4. – № 3. – С. 256-260.

32. Игнатов В.А. Аксиоматическая теория математического моделирования критериев оптимальности и ограничений / Игнатов В.А., Минаев Ю.Н., Гузий Н.Н. // Захист інформації, №4, 2005. – С. 46-56.

33. Іванченко Є.В. Алгоритм прогнозування технічного стану комплексних систем захисту інформації / Є.В. Іванченко, В.О. Хорошко, Ю.Є. Хохлачова // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2013. – № 2(25). – С 9-16.

34. Ігнатенко О.П. Конфліктна задача взаємодії двох гравців у відкритому інформаційному середовищі / О.П. Ігнатенко // Проблеми програмування. – К. : Ін-т ПС НАН України, 2009. – № 2. – С. 1–9.

35. Капустян М.В., Хорошко В.А. Алгоритм нахождения оптимальной конфигурации сети с заданной базой. // Вісник ДУІКТ. – 2006. – №4. – С 298-308.

36. Ковтун И.А. Виды информационных воздействий / Ковтун И.А., Мухан В.И., Набока Ю.И. // Вопросы защиты информации, 2001, №1 (52). – С. 2-7.

37. Коменюк В.Б. Элементы теории целевой оптимизации / Коменюк В.Б. – М. : Наука, 1983. – 288 с.

38. Крапивин В.Ф. Теоретико-игровые методы синтеза сложных систем в конфликтных ситуациях / Крапивин В.Ф. – М. : Советское радио, 1972. – 192 с.

39. Ленков С.В. Методы и средства защиты информации. В 2-х томах / Ленков С.В., Перегудов Д.А., Хорошко В.А. – К.: Арий, 2008.

40. Майника Є. Алгоритмі оптимизации на сетях и графах. – М.: Мир, 1981. – 323 с.

41. Мастяниця Й.І. Захист інформаційних ресурсів України: проблеми і шляхи їх розв'язування / Мастяниця Й.І., Соскін О.В., Шиманський Л.Є. – К.: Нац. інст. стратегічних досліджень, 200. – 98 с.

42. Мину М. Математическое программирование. Теория и алгоритмы / Мину М. – М.: Наука, 1990. – 488 с.

43. Мухин В.Е. Комплексная система мониторинга безопасности на основе анализа целей субъектов компьютерных систем и сетей / В.Е. Мухин, А.Н. Волокита // Управляющие системы и машины. – К.: УСиМ, 2006. - №5. – С. 85-92.

44. Нейман Дж. Теория игр и экономическое поведение / Дж. Нейман, О. Моргенштерн; пер. с англ. – М. : Наука, 1970. – 707 с.

45. Нестеров С. А. Анализ и управление рисками в информационных системах на базе операционных систем Microsoft : [Учебный курс.] / Нестеров С. А. – Санкт-Петербург. : Издательство "INTUIT", 2009. – 136 с.

46. Николаев Ю.А. Оборонная достаточность: критерии и методы оценки / Николаев Ю.А. // Военная мысль, 1992, №4-5. – С. 47-52.

47. Нэш Д. Бескоалиционные игры. В кн.: Матричные игры / Нэш Д. – М. : Физматгиз, 1961. – С. 42-59.

48. Оре О. Теория графов. – М.: Наука, 1980. – 336 с.

49. Петренко С.А Управление информационными рисками. Экономически оправданная безопасность / С. А. Петренко, С. В. Симонов. – М.: Компания АйТи, ДМК Пресс, 2004. – 384 с.

50. Петренко С.А. Политика информационной безопасности / Петренко С.А., Курбатов В.А. – М.: Компания Ай Ти, 2006. – 400 с.

51. Петров А.О. Синтез систем захисту інформації / А.О. Петров, В.Д. Степанов, В.О. Хорошко, Ю.Є. Хохлачова // Інформаційна безпека. – 2012. – № 1(7). – С. 48-54.

52. Піскун С.Ж. Оцінка безпеки інформаційної сфери / С.Ж. Піскун, В.О. Хорошко, Ю.Є. Хохлачова // Сучасна спеціальна техніка. – 2013. – № 1(32). – С. 93-100.

53. Поченцов Г.Г. Информационные войны. Основы военно-коммуникативных исследований / Поченцов Г.Г. – М.: Рефл-бук, К.: Ваклер, 200. – 576 с.

54. Прим Р.К. Кратчайшие связывающие сети и некоторые обобщения. // Кибернетический сборник. – 1961. – №2. – С.95-107.

55. Расторгуев С.П. Информационная война / Расторгуев С.П. – М.: Радио и связь, 1999. – 416 с.

56. Расторгуев С.П. Программные методы защиты информации в компьютерных сетях / Расторгуев С.П. – М.: Агенство Яхтсмен, 1993. – 128 с.

57. Расторгуев С.П. Философия информационной войны / Расторгуев С.П. – М.: Московский психолого-социальный институт, 2003. – 486 с.

58. Романовский И.В. Алгоритмы решения экстремальных задач. – М.: Наука, 1987. – 284 с.

59. Симонов С. В. Анализ рисков в информационных системах. Практические аспекты. Защита информации / С. В. Симонов // Конфидент. Безопасность компьютерных систем – 2001. – №2. – С. 48-53.

60. Симонов С. В. Технологии и инструментарий для управления рисками / С. В. Симонов // Информационный бюллетень Jet Info. – 2003. – № 2 (117)/2003. – С. 3 – 32.

61. Сірченко Г.А. Алгоритм визначення показників для оцінки надійності систем спеціального призначення / Г.А. Сірченко, В.О. Хорошко, Ю.Є. Хохлачова // Інформаційна безпека. – 2013. – № 1(9). – С. 142-147.

62. Современные методы и средства анализа и контроля рисков информационных систем компаний CRAMM, RiskWatch и ГРИФ [Электронный ресурс] / И. С. Медведовский // SecurityLab. Электрон. дан. – Мн. : SecurityLab, 2004. – Режим доступа: World Wide Web. – URL: http://www.ixbt.com/cm/informationsystem-risks012004.shtml.

63. Соколов А.В. Защита от комп'ютерного терроризма / Соколов А.В., Степанюк О.М. – СПб: БХВ-Петербург, Арлей, 2002. – 496 с.

64. Стратегія управління інформаційною безпекою / В. І. Андрєєв, В. Д. Козюра, Л. М. Скачек, В. О. Хорошко. – К. : ДУІКТ, 2007. – 272 с.

65. Терейковський І.А. Нейронні мережі в засобах захисту комп'ютерної інформації / І.А. Терейковський. – К.: ПоліграфКонсилтинг. – 2007. – 209 с.

66. Технологии анализа рисков. [Электронный ресурс] : / Группа компаний “Компьюлинк”. –Электрон. дан. – М. : Группа компаний “Компьюлинк”. –2003. – Режим доступа: World Wide Web. – URL: http://www.glossary.ru/. – Загл. с экрана (просмотрено 25 марта 2010).

67. Тиснина Е.О. Абсолютная устойчивость положения равновесия системы поддержки принятия решений в системе защиты информации / Тиснина Е.О., Хорошко В.А. // Сучасний захист інформації, №4, 2010. – С. 74-79.

68. Управление надежностью. Анализ риска технологических систем : ГОСТ Р 51901 – 2002. – Введ. 2003.09.01. – М. : ИПК “Издательство стандартов”, 2002. – 21 с.

69. Феллер В. Введение в теорию вероятностей и ее приложения. В 2-х томах / Феллер В. – М.: Мир, 1967.

70. Фишберн П. Теория полезности для принятия решений / П. Фишберн. – М. : Наука, 1978. – 352 с.

71. Хан Г. Статистические модели в инженерных задачах / Хан Г., Шапиро С. – М. : Мир, 1969. – 306 с.

72. Хоменюк В.В. Элементы теории многоцелевой оптимизации / Хоменюк В.В. – М.: Наука, 1983. – 343 с.

73. Хорошко В.А. Виды информационных воздействий / Хорошко В.А., Чередниченко В.С. // Захист інформації, Спец. випуск, 2007 – С 6-8.

74. Хорошко В.А. Информационная война. Сущность и содержание / Хорошко В.А., Чередниченко В.С. // Всеукраинский межведомственный НТС «Радиотехника», Вып. 155. – Харьков: ХНУРЕ, 2009. – С. 49-54.

75. Хорошко В.А. Методы и средства защиты информации / Хорошко В.А., Чекатков А.А. – К.: Изд. Юниор, 2003. – 504 с.

76. Хорошко В.О. Методичний підхід щодо оцінки рівня безпеки інформації / Хорошко В.О., Чередниченко В.С. // Збірник наук. праць Військового інституту Київського національного університету ім. Т. Шевченка, №14, 2008. – с. 176-181.

77. Хорошко В.А. Особенности защиты информации в сетях связи / В.А. Хорошко, Ю.Е. Хохлачева // Вісник східноукраїнського національного університету ім. В. Даля. – 2013. – № 15(204). – С. 219-221.

78. Хорошко В.А. Синтез систем защиты информации, имеющих допусковый разброс параметров / В.А. Хорошко, Ю.Е. Хохлачева, Е.П. Сластенко // Інформаційна безпека. – 2013. – №4 (12). – С. 130-134.

79. Хорошко В.О. Методика оцінювання рівня безпеки юридичної особи / В.О. Хорошко, В.Д. Козюра, С.Ж. Піскун, Ю.Є. Хохлачова // Інформаційна безпека людини, суспільства, держави. – 2013. – № 1(11). – С 121-126.

80. Хорошко В.О. Оптимізація параметрів систем захисту в мережах передачі інформації / В.О. Хорошко, Ю.Є. Хохлачова // Інформатика та математичні методи в моделюванні. – 2013. – Т. 3. – № 1. – С. 69-75.

81. Хорошко В.О. Особливості оцінки безпеки інформаційних систем / В.О. Хорошко, Ю.Є. Хохлачова // Захист інформації. – 2012. – № 2(55). – С. 9-15.

82. Хорошко В.О. Оцінка захищеності інформаційних систем / В.О. Хорошко, Ю.Є. Хохлачова // Сучасний захист інформації. – 2012. – № 4. – С. 50-58.

83. Хорошко В.О. Оцінка захищеності систем зв'язку в інформаційно-комунікаційних системах / В.О. Хорошко, І.С. Іванченко, Ю.Є. Хохлачова // Системи обробки інформації. – 2013. – № 3(110). – С. 112-117.

84. Хохлачова Ю.Є. Сучасні підходи до оцінювання уразливостей і моделювання впливів на інформаційні системи / Ю.Є. Хохлачова,

С.С. Чумаченко, О.П. Дуксенко // Вісник Інженерної академії України. – 2014. – № 4. – С. 121-126.

85. Хохлачова Ю.Є. Алгоритм знаходження оптимальної конфігурації мережі / Ю.Є. Хохлачова // Системи обробки інформації. – 2014. – № 2(118). – С. 101-106.

86. Хохлачова Ю.Є. Моделювання критеріїв оптимальності та обмежень для захисту інформаційних систем / Ю.Є. Хохлачова // Захист інформації. – 2012. – № 4 (57). – С. 106-109.

87. Хохлачова Ю.Є. Політика інформаційної безпеки об'єкта / Ю.Є. Хохлачова // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2012. – № 2(24). – С. 23-29.

88. Хохлачова Ю.Є. Принципи побудови моделей загроз інформаційним системам / Ю.Є. Хохлачова // Сучасний захист інформації. – 2012. – №2. – С. 6-9.

89. Хохлачова Ю.Є. Уразливість інформаційних систем / Ю.Є. Хохлачова // Сучасний захист інформації. – 2012. – № 3. – С. 18-23.

90. Чарлз Хант. Разведка на службе вашего предприятия / Чарлз Хант, Вахе Зартаньян. – К.: Укрзакордонвизасервис, 1992. – 160 с.

91. Anderson Risk Management / Anderson, Alison Shain, Michael Shain // Information Security Handbook. – New York : Stockton Press, 1991, P. 75–127.

92. Biskup J. Security in computing systems: challenges, approaches and solutions : monograph / J. Biskup. – Berlin : Springer, 2009. – 694 p.

93. Caelli W. Information Security for Managers. Information Security Handbook / W. Caelli, D. Longley, M. Shain. – UK. : Stockton Press, 1989. – 26 p.

94. Compliant Information Security Risk Assessment Tool: vsRisk [Electronic resource] / IT Governance Ltd. – Electronic data – Boise : IT Governance Ltd, 2011. – Access mode: World Wide Web. – URL: http://www.27001.com/products/31.

95. Dörfler, Willibald. Der lerbores zenzengraph eines gerichteten Grafen. // Math.Nachr. – 1974. – №1-6. – P.35-49.

96. Edmonda J. Optimum Branching. // J.res.Nat. bureau standards. Ser.B. – 1967. – №4. – P.233-240.

97. Fulkerson D.R. Packing rooted directed cuts in a weighted directed graf. // Math.Program. – 1974 – №1. – P.1-13.

98. Hill S. Risk Management & Corporate Security / S. Hill, M. Smith // Computers & Security. – 1995. – P. 199–204.

99. Inventory of risk assessment and risk management methods / [Reference document]. – Paris : Securing Europe's Information Society Regulation, 2004. – 460 p.

100. Karp R.M. A simple derivation of Edmonds' algorithm for optimum branching. // Network. – 1971. – №3. – P.265-272.

101. Lichtensteir S. Factors in the Selection of a Risk Assessment Method / S. Lichtensteir // Information Management & Computer Security. – 1993. – Vol. 4 Iss: 4 – P. 20–25.

102. Penrose R. A Generalized Inverse for Matrices // Proceedings of the Cambridge Philosophical Society / R. Penrose. – Cambridge, 1955. – V. 51. – P. 406–413.

103. Risk Management Tools. Program Risk Management Tools [Electronic resource] / The MITRE Corporation. All rights reserved – New York : Solutions That Make a Difference, 2012. – Access mode: World Wide Web. – URL:
http://mitre.org/work/systems_engineering/guide/risk_management_tools.html.

104. Smith M. Commonsense Computer Security, your practical guide to information security / M. Smith // London : McGraw – Hill, 1993 – 105 p.

105. U. S. Geological Survey: Proposed procedures for dedealing with warning and preparedness for geologic-related hazard // United States Federal Register. – 1977, 42. №70. – P. 14292–14296.