МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Кафедра економічної кібернетики

ДОПУСТИТИ ДО ЗАХИСТУ

Завідувач кафедри

економічної кібернетики

_____ Іванченко Н.О.

«____» _____ 2020 р.

КВАЛІФІКАЦІЙНА РОБОТА

(Пояснювальна записка)

здобувача освітнього ступеня «Магістр»

Тема: Ігрові ризик-моделі захисту АІС з використанням неправдивих інформаційних систем

Виконав: Павлюк Євгеній Леонідович

Керівник: д.т.н., професор Олешко Тамара Іванівна

Консультанти з розділів:

Розділ 1: д.т.н., професор Олешко Т.І.

Розділ 2: д.т.н., професор Олешко Т.І.

Розділ 3: д.т.н., професор Олешко Т.І.

Нормоконтролер із ЄСКД (ЄСПД):

к.е.н., доцент Густера О.М.

Національний авіаційний університет

Факультет економіки та бізнес-адміністрування

Кафедра економічної кібернетики

Освітній ступінь «Магістр»

Освітньо-професійна програма «Економічна кібернетика»

ЗАТВЕРДЖУЮ
Завідувач кафедри
економічної кібернетики
_____Іванченко Н.О.
«___»_____2020 р.

ЗАВДАННЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

Студента: Павлюка Євгеній Леонідовича

Тема роботи: Ігрові ризик-моделі захисту АІС з використанням неправдивих інформаційних систем затверджена наказом ректора № 1967/ст від 08.10. 2020 р.

1. Термін здачі студентом закінченої роботи на кафедру: 17.12.2020 р.

2. Вихідні дані до роботи: наукова інформація в галузі ігрових моделей та АІС зарубіжних та вітчизняних вчених.

3. Зміст дослідження:

- характеристика основних понять неправдивих інформаційних систем;
- дослідження автоматизованих інформаційних систем;
- аналіз принципів ризик-моделювання для захисту АІС;
- характеристика методології теорії ігор для захисту АІС;
- моделювання ефективності роботи неправдивої інформаційної системи;
- оптимізація ефективності використання ресурсів неправдивою інформаційною системою для здійснення захисту АІС.

4. Перелік обов'язкових демонстраційних матеріалів: 12 слайдів

Календарний план

№ п/п	Назва етапів кваліфікаційної роботи	Термін виконання	Позначки керівника про виконання завдань
1	Отримання завдання на дипломну роботу	05.10.20	
2	Огляд літератури за темою дослідження	06.10.20 – 09.10.20	
3	Характеристика сутності неправдивих інформаційних систем	10.10.20 – 15.10.20	
4	Ознайомлення з методологією оцінки ризиків	16.10.20 – 27.10.20	
5	Використання теорії ігор для захисту АІС	28.10.20 – 04.11.20	
6	Опис методів управління ефективністю роботи неправдивої інформаційної системи	05.11.20 – 09.11.20	
7	Оцінка ризиків та аналіз ефективності роботи інформаційної системи за різними ігровими сценаріями	10.11.20 – 15.11.20	
8	Аналіз ефективності використання неправдивих інформаційних систем для захисту АІС	16.11.20 – 24.11.20	
9	Оптимізація ресурсів, що витрачаються неправдивою інформаційною системою	25.11.20 – 04.12.20	
10	Створення слайдів та написання доповіді	05.12.20 – 13.12.20	
11	Попередній захист випускної роботи	14.12.20	
12	Корегування роботи за результатами попереднього захисту	15.12.20 – 17.12.20	
13	Остаточне оформлення дипломної роботи та слайдів	18.12.20 – 19.12.20	
14	Підписання відгуку та рецензії	21.12.20	
15	Захист кваліфікаційної роботи у ДЕК	23.12.20	

5. Дата видачі завдання: _____

Керівник:
д.т.н., професор _____ Олєшко Т.І.

Завдання прийняв для виконання _____ Павлюк Є.Л.

РЕФЕРАТ

Павлюк Євгеній Леонідович. Ігрові ризик-моделі захисту АІС з використанням неправдивих інформаційних систем. - Кваліфікаційна робота магістра зі спеціальності 051 «Економіка», ОПП «Економічна кібернетика». Національний авіаційний університет Міністерства освіти і науки України, м. Київ, 2020.

Дипломна робота містить 89 сторінок, 8 таблиць, 15 рисунків, список використаних джерел з 74 найменувань.

Об'єктом дослідження є процес захисту АІС з використанням ігрових ризик моделей.

Предметом дослідження є методи захисту АІС.

Мета дослідження полягає в розробці ігрової моделі захисту з використанням неправдивих інформаційних систем.

Наукова новизна дослідження полягає в застосуванні методології теорії ігор для підвищення ефективності при здійсненні захисту АІС.

При написанні роботи використовувалися методи дослідження: аналіз та синтез, порівняльні та статистичні методи, методи лінійного програмування, методологія теорії ігор.

Ключові слова: *помилкова інформаційна система, автоматизована інформаційна система, теорія ігор, оцінка ризиків .*

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ОДИНИЦЬ

АІС – автоматизована інформаційна система

ПІС – помилкова інформаційна система

МТІ – методи теорії ігор

НСД – несанкціонований доступ

ПЗ – програмне забезпечення

АС – автоматизована система

ВСТУП

Мережа надає дуже взаємопов'язану всесвітню платформу для кожного, щоб поширювати інформацію мільйонам людей протягом декількох хвилин, практично без будь-яких витрат.

В ІС завжди присутня ймовірність наявності невідомих вразливостей, а також вразливостей в програмному забезпеченні самих засобів захисту. У такій ситуації традиційні підходи до захисту інформації не можуть забезпечити потрібний рівень захисту інформації при прийнятних фінансових витратах. Тому сьогодні все більш актуальним стає застосування неправдивих інформаційних систем, що реалізують стратегію обману. Реалізуючи захист інформаційної системи за їх допомогою, тим самим відволікаючи порушника на неправдивий інформаційний ресурс, можна не тільки захистити інформаційну систему, а й знайти уразливості цієї системи, які раніше були невідомі.

Актуальність теми дослідження. В силу того, що поведінка зловмисника при реалізації атаки в автоматизованій інформаційній системі рідко має детермінований характер, використання математичного апарату теорії ігор при прийнятті рішень помилковою інформаційною системою по стратегії захисту має величезну область дослідження. Застосовність теорії ігор в рамках роботи помилкової інформаційної системи мало досліджена як у вітчизняних, так і зарубіжних джерелах. У зв'язку з цим робота з оцінки ефективності розроблюваних помилкових інформаційних систем, що використовують теорію ігор при прийнятті стратегій захисту, є актуальною.

Метою дослідження є розробка та формалізація ігрової моделі захисту АІС з використанням неправдивих інформаційних систем.

Для досягнення мети, були виділені наступні завдання:

– характеристика основних понять неправдивих інформаційних систем;;

– дослідження автоматизованих інформаційних систем;

– аналіз принципів ризик-моделювання для захисту автоматизованих інформаційних систем;

– характеристика методології теорії ігор для захисту автоматизованих інформаційних систем;

– моделювання ефективності роботи неправдивої інформаційної системи;

– оптимізація ефективності використання ресурсів помилковою інформаційною системою для здійснення захисту АІС.

Об'єктом дослідження є процес захисту АІС з використанням ігрових ризик моделей.

Предметом дослідження є методи захисту АІС.

РОЗДІЛ 1
ТЕОРЕТИЧНІ АСПЕКТИ ПОМИЛКОВИХ ІНФОРМАЦІЙНИХ СИСТЕМ

1.1. Характеристика помилкових інформаційних систем та причини їх використання

Інформаційна система - це інтегрований набір компонентів для збору, зберігання та обробки даних, а також для надання інформації, знань та цифрових продуктів.

Бізнес-фірми та інші організації покладаються на інформаційні системи для здійснення та управління їх діяльністю, взаємодію зі своїми клієнтами та постачальниками та врегулювання конкуренції на ринку.

Інформаційні системи використовуються для управління між-організаційними ланцюгами поставок та електронними ринками. Наприклад, корпорації використовують інформаційні системи для обробки фінансових рахунків, управління своїми людськими ресурсами та охоплення своїх потенційних клієнтів за допомогою онлайн-акцій.

Багато великих компаній повністю побудовані на основі інформаційних систем. Сюди входять:

- eBay, як аукціонний ринок;
- Amazon, як електронний торговий центр;
- Alibaba, як електронний ринок;
- та Google, як компанія-пошуковик, яка отримує більшу частину доходу від реклами ключових слів при пошуку в Інтернеті.

Уряди застосовують інформаційні системи для економічного надання послуг громадянам.

Тому захист інформації в нас час знаходиться в пріоритеті і повинен виконуватися безкомпромісно. Головною метою захисту будь-якої конфіденційної інформації є запобігання ознайомлення з нею порушників, які не мають на це відповідного дозволу.

Розвитку практики застосування ПІС сприяє все більше впровадження нових технологій віртуалізації та поява програмних засобів віртуалізації, таких як VMware ESX / ESXi, Microsoft, Hyper-V, Citrix Xen Server та ін., які дозволяють створити віртуальну інфраструктуру і керувати нею.

Разом з тим при використанні ПІС потрібно знати, наскільки ефективно можна обманути з її допомогою порушника і не створити складнощів для функціонування інформаційної системи в цілому, оскільки значний обчислювальний ресурс може виявитися задіяним на забезпечення функціонування ПІС.

До теперішнього часу методичне забезпечення оцінювання ефективності ПІС в тому числі побудованих з використанням засобів віртуалізації, ще не розроблялося. При цьому слід відзначити, що в таких системах вкрай важливо враховувати обмеження на споживання обчислювальних ресурсів, оскільки такі обмеження істотно впливають на кількість емульованих помилкових об'єктів, а, отже, і на ефективність захисту в цілому.

ПІС застосовують для реалізації наступних цілей системи захисту важливої інформації:

- зменшення кількості атак на цільові (важливі) системні вузли чи системи в цілому за допомогою відволікання порушника від реальних об'єктів системи та перенаправлення атаки на себе (результатом чого є зменшення впливу атак, збільшення часу їх здійснення та повне їх припинення);

- непомітне виявлення і вивчення неавторизованої активності (кількість витрат падає внаслідок зменшення помилкових спрацьовувань, тому що будь-який трафік, що фіксується за допомогою неправдивих інформаційних систем, з великою ймовірністю укладає в собі всі плановані операції порушника);

- моніторинг інцидентів несанкціонованого доступу до системи і її експлуатації;

- фіксація актів неправомірних дій, що спричиняє приведення порушника в стан обману.

Як і у випадку будь-якої глобальної системи, інформаційний простір забруднений величезною кількістю неякісного контенту, який порушує безпеку системи особистої інформації, затьмарює здатність суспільства бачити і конструктивно спілкуватися один з одним, дестабілізує і поляризує суспільство і завдає шкоди глобальному співтовариству.

Метою засобів масової інформації має бути інформування. Всі інформаційні матеріали слід перевіряти фактами, щоб переконатися в правдивості представленої інформації. Один з ключових принципів полягає в перевірці інформації з використанням декількох джерел. Деякі з неперевірених матеріалів створені навмисно, а інші можуть бути викликані просто відсутністю професійної компетенції.

Іноді мета такого контенту може полягати просто в залученні трафіку на веб-сайт і в спровоковані обговорення або конфлікту в розділі коментарів. Такі коментарі використовуються для формування громадської думки в соціальних мережах, тобто ставлення людей до певної події, людині або країні [3].

Здатність розпізнавати і обробляти помилкову або неточну інформацію- важливий навик в двадцять першому столітті.

В інформаційному середовищі існує три типи маніпулятивного змісту.

Дезінформація - це помилкова інформація, яка поширюється без наміру ввести в оману (наприклад, помилки журналістів). Незалежно від наміру, люди часто вірять такій інформації і поширюють її.

Дезінформація також є неправдивою інформацією, але вона навмисно призначена для того, щоб завдати шкоди людині, соціальній групі, організації або країні [4].

Коли люди поширюють дезінформацію, вони часто вірять у те, що поширюють. Навпаки, дезінформація створюється і поширюється, щоб навмисне вводити інших в оману. Дезінформація часто може перетворитися на дезінформацію, все залежить від того, хто нею ділиться і чому.

Велика частина дезінформації заснована на напівправді, де брехня змішана з частиною правдивої інформації. Це зроблено для більшої достовірності

неправдивої інформації. У таких повідомленнях дезінформації часто дослідження, які можуть бути повністю сфальсифіковані. Іноді дезінформація ретельно обробляється фахівцями, щоб переконати громадську думку на користь певної причини або просто посіяти сумніви або розбіжності.

І нарешті, деякі люди створюють дезінформацію просто для того, щоб пояснення або інформація здавалися спірними, хоча насправді це не так.

Неправильна інформація - це інформація, яка в цілому є правдивою, але використовується для нанесення шкоди людині, організації або країні. Це може бути витік особистої інформації компрометуючого контенту (реального або підробленого). Його основна мета - підірвати репутацію окремих осіб або організацій [5].

Багато типів інформації призначені для залучення нашої уваги, часто за рахунок гри на наших емоційних реакціях.

Фактично, люди самі є важливими елементами в цій системі, оскільки ми звикли ще більше поширювати контент через соціальні мережі.

Кожен раз, коли люди пасивно приймають і передають інформацію, не перевіряючи її, вони додають шуму і плутанини в і без того складний медіа-ландшафт. Таким чином, люди несуть таку ж відповідальність за перевірку достовірності інформації, якою ми ділимося з нашими власними мережами, як і самі творці контенту.

За способом побудови ПІС розділені на реальні і віртуальні. У реальних ПІС відсутні компоненти, що імітують поведінку апаратного забезпечення, на відміну від реальних ПІС, віртуальні містять такі компоненти.

Тип імітованого об'єкта задає функціональні можливості ПІС, а також визначає рівень взаємодії із засобами захисту від несанкціонованого доступу. Рівень взаємодії ПІС із засобами захисту від несанкціонованого доступу визначає, які можливості надає ПІС засобу захисту від несанкціонованого доступу по реалізації комп'ютерної атаки. Чим більше можливостей надається засобам захисту від несанкціонованого доступу, тим більше інформації можна зібрати про їхні дії і тим більше обсяг робіт зі встановлення та обслуговування

системи і вище ризик її компрометації. За типом імітованого об'єкта ПІС розділені на [10]:

- ті, що генерують мережевий трафік;
- мережеві служби;
- окремі вузли обчислювальної мережі;
- автоматизовані обчислювальні мережі;
- автоматизовані інформаційні системи.

ПІС, які генерують мережевий трафік, мають мінімальний набір функцій, що імітують тільки наявність певних мережевих служб цільової АС. Дані ПІС не здатні відповідати на мережні запити засобів несанкціонованого доступу.

ПІС, що імітують роботу мережевих служб, повинні забезпечувати коректну роботу мережевих протоколів, за якими працюють відповідні мережеві служби. Взаємодіючи з такою ПІС, за допомогою засобу НСД можливо отримувати лише коректні відповіді на мережеві запити, але не можна впровадити шкідливий код, використовуючи вразливості мережевих служб [12].

ПІС, що імітують роботу вузлів обчислювальної мережі, реалізують всі функції, характерні для ЕОМ або активного мережного обладнання обчислювальної мережі. Взаємодіючи з такою ПІС, за допомогою засобу НСД можливо впровадити шкідливий код, використовуючи вразливості програмного забезпечення помилкового вузла.

ПІС, що імітують роботу обчислювальної мережі, додатково включають функції по організації взаємодії між імітованими вузлами. ПІС, що імітують роботу АС, додатково включають функції по імітації роботи користувачів АС [15].

Залежно від типу структури виділені статичні, динамічні, а також ПІС які організовують свою діяльність автоматично. Статичні ПІС зберігають свою топологію і склад ПО в попередньо заданому стані. У динамічних ПІС їх структура змінюється з плином часу, наприклад, в процесі функціонування такої ПІС можуть з'являтися або зникати будь-які елементи. Якщо ж структура ПІС

змінюється в залежності від дій засобів несанкціонованого доступу, то це самоорганізована ПІС.

Рівень інтеграції в цільову ІС визначає місце ПІС щодо ІС, а також спосіб взаємодії з ІС. ПІС можуть працювати окремо, паралельно і в складі цільової ІС. ПІС, розташовані окремо від цільових ІС - це територіально розосереджені ПІС, що використовують провідні та безпровідні канали для зв'язку з ІС. ПІС, що працюють паралельно цільовим ІС, розміщуються на одній території і підключаються до ІС з використанням єдиного вузла. Також компоненти ПІС можуть перебувати в складі ІС [17].

За призначенням ПІС можуть бути:

- виробничими;
- дослідницькими;
- змішаними.

Виробничі ПІС знижують ймовірність успішного здійснення несанкціонованого доступу до інформації, що захищається за рахунок збільшення часу її пошуку. Дослідницькі ПІС застосовуються для вивчення засобів несанкціонованого доступу, використовуваних ними алгоритмів з метою побудови більш ефективних механізмів захисту інформації в цільових ІС. Змішані ПІС поєднують в собі можливості виробничих і дослідницьких ПІС.

Також суттєвою характеристикою ПІС є її ступінь подібності з цільової ІС, яка визначається рівнем кореляції складу і структури ПІС з цільової ІС. Чим більше ПІС схожа з цільовою ІС, тим важче за допомогою засобів несанкціонованого доступу визначити справжність системи, але в той же час у разі компрометації ПІС противник може отримати достовірні відомості про склад і структуру цільової ІС [19].

Одним з найбільш ефективних методів захисту від комп'ютерних атак на інформаційні системи є застосування помилкових інформаційних систем в системі захисту інформації.

Помилкові інформаційні системи - це комплекс програмно-апаратних засобів, який імітує процес роботи інформаційної системи, але ніяких корисних

обчислень не виконує. Основна мета створення ПІС - це маскування реальних об'єктів інформаційної системи та їх взаємозв'язків.

Щоб зрозуміти переваги ПІС і причини їх використання, розглянемо етапи нападу на інформаційну систему і механізми захисту інформації, які повинні виконуватися на кожному етапі атаки. Ці механізми захисту інформації та етапів життєвого циклу показано на рис. 1.1. Основні етапи інциденту безпеки можуть бути названі:

- попередження про загрозу безпеці;
- реалізація загрози і заподіяння пошкодження системі;
- відновлення ресурсів системи, що захищається після пошкодження.

Рисунок 1.1. Цикл інциденту безпеки

Загроза - будь-які обставини або події, що виникають у зовнішньому середовищі, які можуть бути причиною порушення політики безпеки інформації і нанесення збитків автоматизованій системі, що прагне заподіяти шкоду власнику, або користувачеві, що виражається в спотворенні і втраті інформації.

Загрози можна класифікувати на навмисні, що відображають наслідки умисних дій порушників, і ненавмисні, тобто викликані невірними діями співробітників, відмовами у функціонуванні технічних і програмних засобів або стихійними лихами [25].

Реалізація однієї або декількох навмисних загроз являє собою атаку. При цьому атака є спробою подолання захисту автоматизованої інформаційної системи, ступінь успіху якої залежить від уразливості системи та ефективності захисних заходів.

Основними видами загроз є загрози конфіденційності, цілісності та доступності. Загрози конфіденційності націлені на розголошення інформації, тобто в результаті реалізації цих загроз особа, яка не повинна мати доступу до даних відомостей, стає їх володарем. Це явище називається несанкціонованим доступом (НСД), під яким розуміється доступ до інформації, що порушує встановлені правила розмежування доступу.

Загрози цілісності - це спотворення або зміна інформації, що розташовується в обчислювальній системі або переданої по каналах зв'язку, особою, яка не має повноважень для даних операцій [26].

Цілісність інформації піддається порушенням як з боку порушника, так і внаслідок ненавмисних реакцій, що виходять від середовища експлуатації системи.

Загрози порушення доступності (відмови в обслуговуванні) орієнтовані на формування таких ситуацій, коли в результаті навмисних або ненавмисних дій зменшується працездатність обчислювальної системи, або її ресурси стають абсолютно недоступними.

Можна виділити наступні групи механізмів захисту інформації, реалізація яких цілком допустима на різних фазах життєвого циклу інциденту безпеки:

- попередження;
- введення в оману (обман) порушника;
- виявлення;
- реагування;

- нейтралізація та усунення наслідків;

- оцінка інциденту і вжитих заходів [27].

Механізми обману порушників – це особливий вид захисних механізмів, які визначаються для того, щоб змусити порушників приймати неправдиву інформацію як справжню інформацію. Іншими словами, неправдива інформація замість фактичної дозволяє знизити можливість реалізації загроз, спростити виявлення атак, уповільнити дії з реалізації різного роду загроз, а також вивчити наміри, стратегії і засоби злочинців.

Слід зазначити важливість механізмів обману злочинців. Такого роду захисним механізмам приділено недостатньо уваги, але їх реалізація значно підвищить ефективність захисних заходів від зовнішніх і внутрішніх вторгнень, так як дозволить уникнути нападу на реальний об'єкт, не заподіявши шкоди.

ПІС - це комплекс програмно-апаратного забезпечення, що імітує процес функціонування інформаційної системи, але не виконує ніяких корисних обчислень. Основною метою створення ПІС є приховування реальних об'єктів ІС, їх взаємозв'язків і відволікання зловмисника на помилкові об'єкти.

Як правило, причинами використання ПІС є [28]:

1. Збільшення кількості операцій і дій, що проводяться злочинцем. Злочинець змушений вжити багато додаткових заходів для виявлення наявності шахрайства - відсутності реальної уразливості;

2. Можливість відстежити зловмисника. Протягом часу, витраченого злочинцем на перевірку всіх виявлених вразливостей, включаючи помилкові, адміністратор безпеки може виявити внутрішнє порушення або зібрати інформацію про зовнішніх порушників і вжити відповідних заходів;

3. Спосіб усунути шкоду, яку може заподіяти злочинець. Якщо помилкові об'єкти нічим не відрізняються від реальних, то злочинець, здійснюючи напад, не може зрозуміти, що напад є помилковим об'єктом інформаційної системи, а не реальним [29].

1.2. Вимоги до помилкових інформаційних систем

Всі доступні способи втілення помилкових систем засновані на повній або частковій емуляції, а іноді і на використанні фізичних апаратних і програмних ресурсів. Крім того, багато систем уразливі для здійснення зловмисником тривіальних способів проникнення, наприклад, MAC-адреса емальованих операційних систем. Тобто, щоб замаскувати ознаки функціонування шахрайських систем, необхідно ввести додаткову надлишкову інформацію [30].

Звичайно, спочатку потрібно визначити, які цілі переслідуються під час роботи і які методи взаємодії системи з іншими підсистемами захисту використовуються. Від цього залежить конфігурація ПІС в мережі. Однак наступним вимогам повинні підкорятися всі ПІС без винятку:

- ПІС зобов'язані підтримувати такі установки, які гарантували б максимально можливе бажання нападника атакувати пастки;

- нападник не повинен визнавати факт існування ПІС.

Питання про можливість розрізнення реальної системи і системи пасток складний.

Якщо атакуюча сторона змогла виявити, що система, з якою вона вступає в контакт, невірна, вона може застосувати це в особистих цілях. Таким чином, необхідно створити умови для порушника апріорної невизначеності. Це повинно бути зроблено для того, щоб злочинцеві було важко виключити неправильну систему зі списку своїх цілей або провести відволікаючу атаку на неї, щоб дезінформувати оборону.

Побудова ПІС повинна виконуватися таким чином, щоб атака на неправильний об'єкт з будь-якої причини виглядала більш кращою для зловмисника. Для цього він повинен мати зовнішній вигляд одного з найбільш незахищених елементів системи або повинен володіти властивістю мети з уявним інформаційним тяжінням. Існування ПІС в цьому контексті політики безпеки і конфігурації всієї системи визначається реалізацією, проектуванням, для яких цілей і в яких випадках вони використовуються.

Моделювання різних протоколів (SMTP, FTP, POP3, HTTP і т. д.) функцій є частиною опцій, які підтримують ПІС. Один сервер, керований операційною системою, робоча станція або вся мережа також можуть бути піддані процесу моделювання.

Найбільш ефективною і складною є реалізація інтеграції ПІС в мережі, що захищається. Ця реалізація дозволяє відстежувати і зупиняти вторгнення зсередини, хоча це може викликати труднощі в налаштуванні і експлуатації. Разом з цим можна розрізняти існування ПІС окремо від захищених мереж і паралельно. Все це допомагає вивчити тенденції атак, що виявляються при проведенні НСД, а також допомагає сформулювати своєрідну методологію дій нападника.

Покладаючись на результати отриманих і проаналізованих досліджень в області забезпечення безпеки інформації, визначимо наступні ключові функції, які повинні бути реалізовані в перспективних ПІС [24]:

- захоплення даних, що має на увазі так зване прослуховування мережевого трафіку і забезпечення того, що в підсумку, будуть матися дані, які будуть піддані потім вивченню з метою аналізу;

- збір і наступне за ним об'єднання даних, що надходять від різних апаратних і програмних складових комп'ютерної системи, в даному випадку, СОВ, маршрутизаторів, сенсорів, міжмережевих екранів та ін.;

- розпізнавання типу "свій-чужий" і перенаправлення на компоненти відстеження підозрілих запитів;

- виявлення мережевих атак (вторгнень);

- фільтрація подій (з метою зосередження на подіях, що представляють інтерес, і автоматичного виявлення, що не відносяться до таких);

- прогнозування допустимих порушником дій, на підставі яких приймаються певні стратегії;

- виявлення джерела загроз, трасування та ідентифікація атакуючого (розпізнавання типу, рівня потенційних можливостей, які він може реалізувати та ін.);

- стеження за діями, які робить порушник, і своєчасне звернення уваги на їх наявність. Це знаходить відображення в блокуванні дій порушника, оповіщенні адміністратора про компрометацію, і ін.;

- заманювання і обман порушника (привернення уваги, приховування реальної структури системи, що захищається і ресурсів, камуфляж, дезінформація) за рахунок емуляції мережевих сегментів, серверів, робочих станцій, в тому числі переданого трафіку, і їх вразливостей, автоматичне реагування на дії порушника, в тому числі оповіщення адміністратора;

- визначення послідовності кроків з імітації цільової інформаційної системи, що підпорядковує діяльність компонентів ПІС;

- здійснення адміністрування із застосуванням технологій, що дозволяють дану діяльність у віддаленому режимі, введення сигнатур, документування, профілів та ін. Це допомагає централізувати управління, засноване на правилах безпеки реакції системи, уніфікувати аналіз тенденцій і підготовку звітів;

- надання інтерфейсу з адміністратором безпеки.

В обов'язковому порядку ПІС повинен забезпечити виконання як мінімум двох функцій-контролю і збору даних, на додаток до виконання дій, безпосередньо спрямованих на введення злочинця в оману. Це важлива вимога: збір даних гарантує, що всі дії зловмисників можуть бути виявлені і зареєстровані, навіть якщо вони замасковані або зашифровані.

Мета контролю даних - запобігти роботу скомпрометованих компонентів (ресурсів) ІС для виконання атаки або пошкодження інших елементів після зустрічі злочинця в ПІС [11].

1.3. Аналіз автоматизованих інформаційних систем

Основні засади побудови АІС пов’язані з основними положеннями кібернетики, тобто науки про управління в об’єктах живої та неживої природи та інформатики - науки про перетворення інформації з використанням технічних засобів. Кібернетика включає в себе поняття, зображені на рис. 1.2:

Рис. 1.2. Основні поняття кібернетики

Системою називається сукупність взаємопов'язаних елементів, які підпорядковуються одній меті. Ознаки системи показані на рис. 1.3:

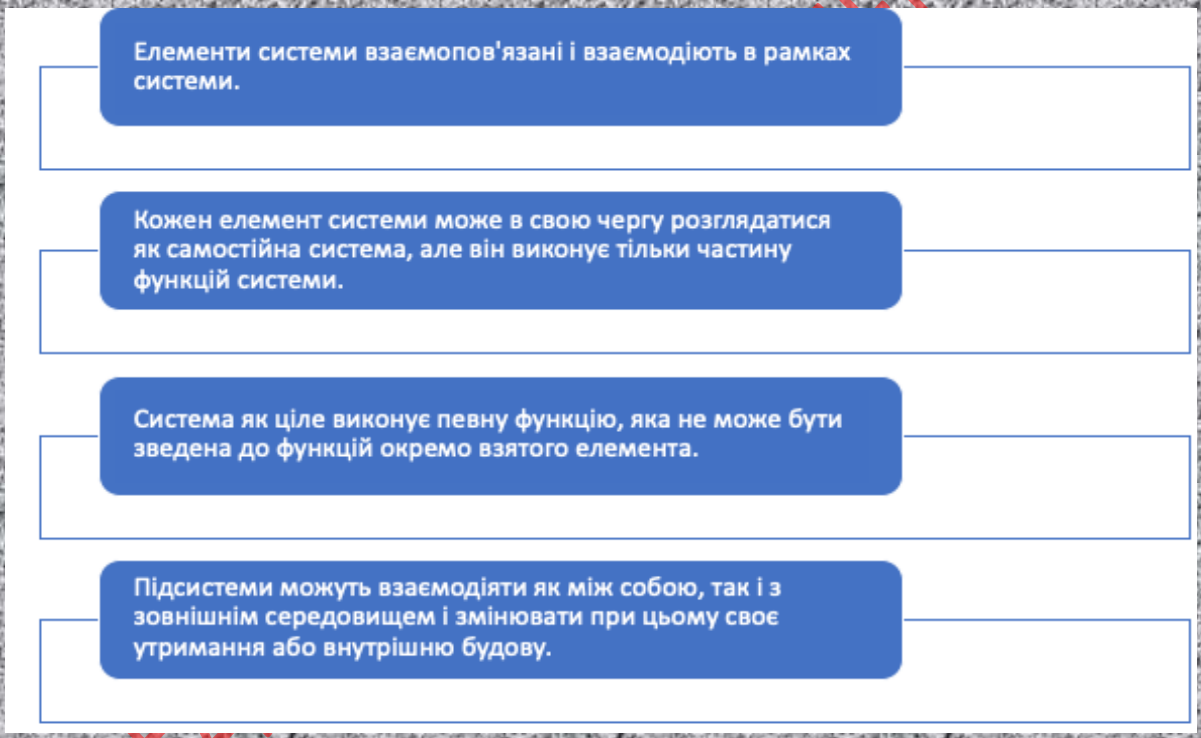

Рис. 1.3. Ознаки системи

Організації, що діють в економіці країни є складними і динамічними системами. Вони включають в себе взаємопов'язані елементи, що реалізують управлінські та виробничі функції, мають багаторівневу ієрархічну структуру.

Система управління має на меті досягнути поставлених задач та створити відповідні умови для виконання.

Система управління складається з підсистем, зображених на рис. 1.4:

Рис. 1.4. Складові системи управління

Інформаційною системою (ІС) називають сукупність та інформаційних технологій, що реалізують інформаційні процеси [11]. Розрізняють ручні та автоматизовані ЕІС.

До автоматизованих інформаційних систем належить сукупність інформації; економіко-математичних методів і моделей, технічних і програмних засобів, організованих на базі інформаційної технології.

За об'єктом управління розрізняють такі АІС, зображені на рис. 1.5:

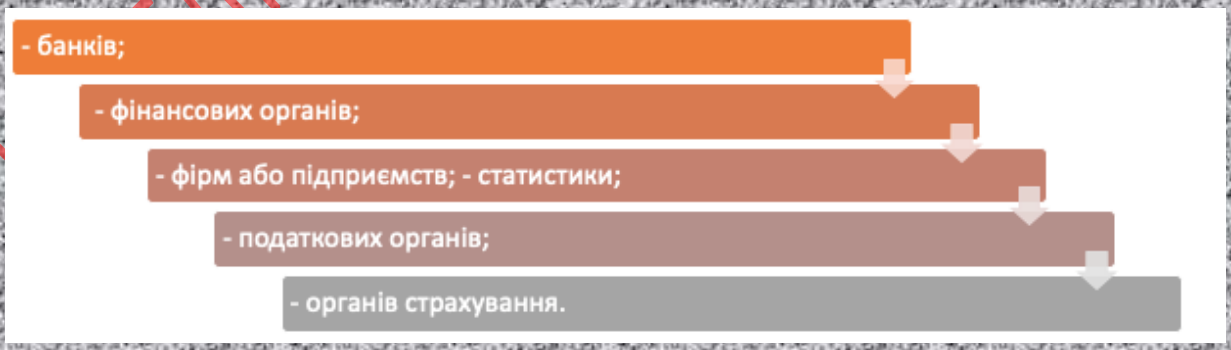

Рис. 1.5. АІС за об'єктом управління

За галузевою ознакою виділяють АІС, зображені на рис. 1.6:

Рис. 1.6. АІС за галузевою ознакою

По виду взаємодії з об'єктом управління, зображені на рис. 1.7:

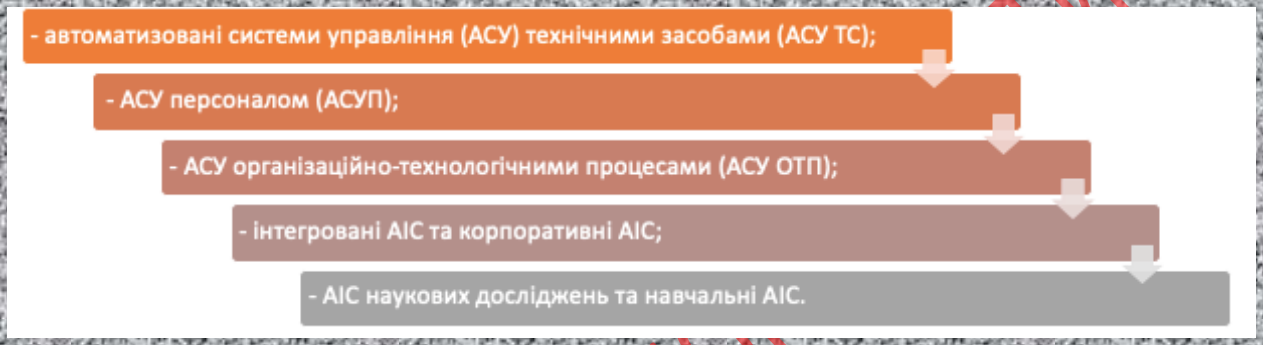

Рис. 1.7. АІС по виду взаємодії з об'єктом управління

Об'єктом управління є технічні засоби, тому взаємодія з ЕОМ здійснюється виключно каналами зв'язку.

У АСУП об'єктом управління є організаційні процеси за участю персоналу, а обмін інформацією здійснюється як по каналах зв'язку, так і документів.

Інтегровані АІС призначені для автоматизації всіх функцій управління фірмою.

Корпоративні АІС - для автоматизації всіх функцій управління фірмою або корпорацією, що має територіальну роз'єднаність між підрозділами, філіями, і т.д.

АІС наукових досліджень забезпечують рішення науково-дослідних завдань на базі математичних методів і моделей.

Навчальні АІС - для підготовки фахівців в системі освіти, при перепідготовці та підвищенні кваліфікації.

В залежності від особливостей автоматизованої професійної діяльності виділяють наступні АІС, зображені на рис. 1.8:

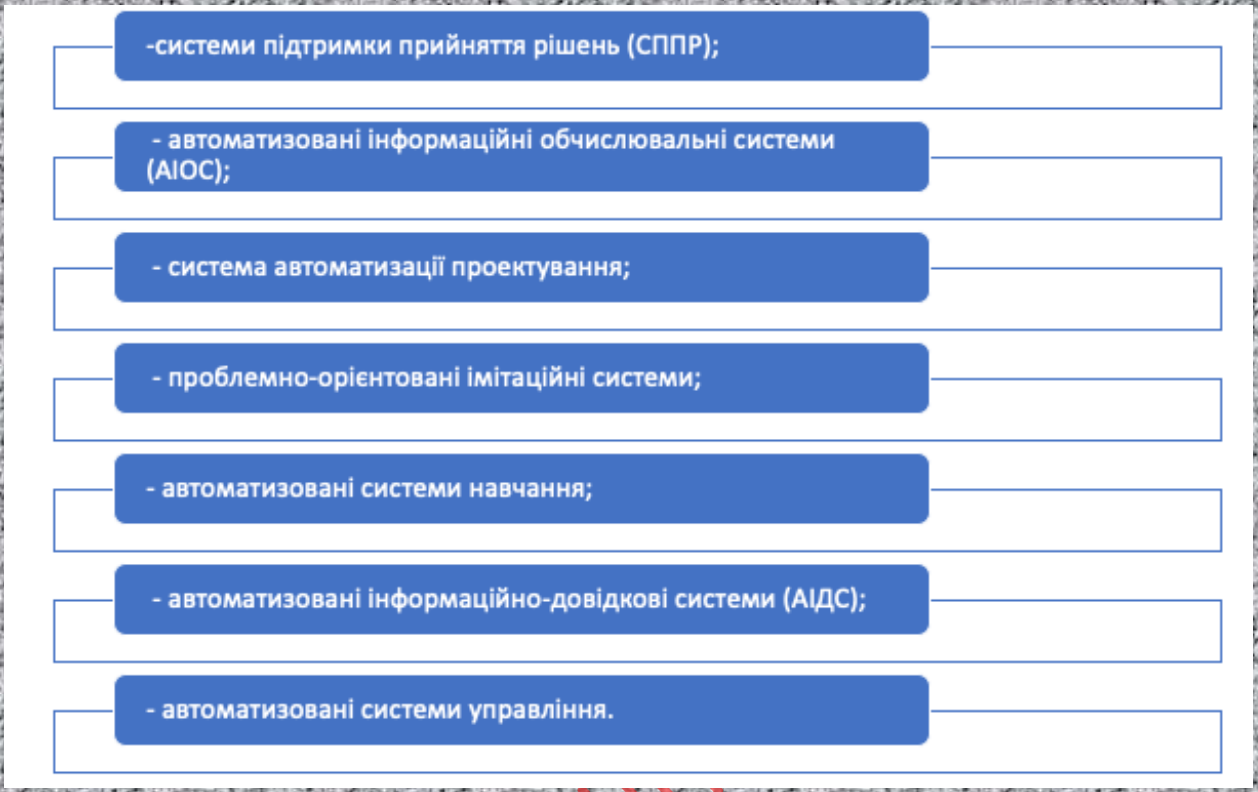

Рис. 1.8. АІС в залежності від особливостей автоматизованої професійної діяльності

Системами підтримки прийняття рішень називається АІС, призначена для автоматизації діяльності конкретних посадових осіб при виконанні своїх прямих обов'язків в процесі управління персоналом і (або) технічними засобами.

Автоматизовані інформаційно-обчислювальні системи призначені для вирішення складних в математичному плані задач, ці системи використовуються для забезпечення наукових досліджень і розробок.

Системою автоматизації проектування називається автоматизована інформаційна система, призначена для автоматизації діяльності підрозділів проектної організації.

Проблемно-орієнтовані імітаційні системи призначені для автоматизації розробки імітаційних моделей в деякій предметній сфері.

Автоматизовані системи навчання призначені для автоматизації підготовки фахівців, забезпечують навчання, підготовку навчальних курсів, управління процесом навчання і оцінку його результатів.

Автоматизовані інформаційно-довідкові системи (АІДС) - це автоматизовані інформаційні системи, призначені для збору, зберігання, пошуку і видачі інформації довідкового характеру.

За характером роботи з інформацією розрізняють АІДС, зображені на рис. 1.9:

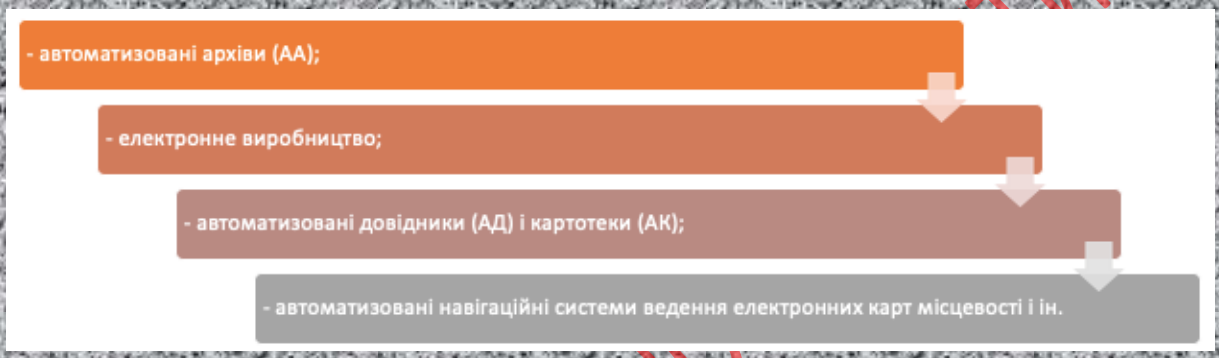

Рис. 1.9. АІС за характером роботи з інформацією

Автоматизована система управління представляє собою автоматизовану систему, призначену для автоматизації всіх або більшості завдань управління, що вирішуються колективним органом управління.

За рівнем в системі управління розрізняють АІС, зображені на рис. 1.10:

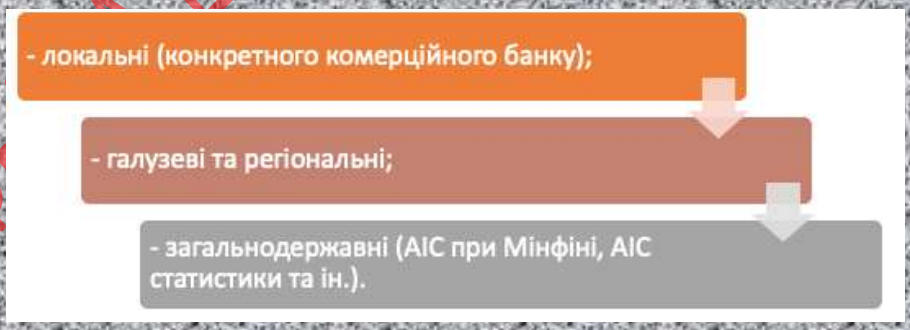

Рис. 1.10. АІС за рівнем в системі управління

Змістовну компоненту АІС складають функціональні підсистеми, що включають комплекси щодо взаємопов'язаних завдань, що реалізовують функції системи управління. При цьому під завданням розуміється отримання вихідної

інформації з безлічі вхідних даних (наприклад, складання розрахунково - платіжної відомості по обліку заробітної плати, отримання оборотної відомості по руху матеріалів і т.д.).

Склад функціональних підсистем багато в чому визначається особливостями економічної системи, її галузевою належністю, формою власності, розміром, характером діяльності підприємства.

Функціональні підсистеми АІС можуть будуватися за різними принципами:

- предметним;
- функціональним;
- проблемним;
- змішаним (предметно-функціональним).

Висновки до розділу 1

В першому розділі дипломної роботи було:

1. Охарактеризовано помилкові інформаційні системи їх види та причини використання. Помилкові інформаційні системи - це комплекс програмно-апаратного забезпечення, що імітує процес функціонування інформаційної системи, але не виконує ніяких корисних обчислень. Основною метою створення ПІС є приховування реальних об'єктів ІС, їх взаємозв'язків і відволікання зловмисника на помилкові об'єкти. Побудова ПІС повинна виконуватися таким чином, щоб атака на неправильний об'єкт з будь-якої причини виглядала більш кращою для зловмисника. ПІС повинен забезпечити виконання як мінімум двох функцій: контролю і збору даних, на додаток до виконання дій, безпосередньо спрямованих на введення злочинця в оману. Помилкові інформаційні системи впливають на підвищення рівня перешкоджання атакам порушників за рахунок відволікання на себе уваги і ресурсів порушників.

2. Досліджено вимоги до сучасних неправдивих інформаційних систем. Побудова ПІС повинна виконуватися таким чином, щоб атака на неправильний об'єкт з будь-якої причини виглядала більш кращою для зловмисника. Для цього

він повинен мати зовнішній вигляд одного з найбільш незахищених елементів системи або повинен володіти властивістю мети з уявним інформаційним тяжінням.

3. Проаналізовано сучасні автоматизовані інформаційні системи. Автоматизовані інформаційні системи – це ІС до яких належить сукупність інформації, економіко-математичних методів і моделей, технічних і програмних засобів, організованих на базі інформаційної технології. У стадії формування вимог до АІС включається комплекс науково - дослідних і організаційно-технічних заходів з обстеження, що дозволяють визначити виробничі можливості підприємства щодо підвищення прибутку, зниження витрат в результаті створення ІС. Проводиться техніко-економічне обстеження, що включає системний опис конкретного об'єкта, діагностичний аналіз в системах управління і дослідження інформаційних потоків.

РОЗДІЛ 2
ОЦІНКА РИЗИКУ КІБЕРАТАК НА ІНФОРМАЦІЙНІ СИСТЕМИ ТА ВИКОРИСТАННЯ ТЕОРІЇ ІГОР ДЛЯ ЇХ АДАПТИВНОЇ ОБОРОНИ

2.1. Принципи управління ризиками

Управління ризиками – це процес, який дозволяє IT-менеджерам збалансувати операційні та економічні витрати на захисні заходи і домогтися підвищення потенціалу місії за рахунок захисту IT-систем і даних, що підтримують місії їх організацій. Цей процес не є унікальним для IT-середовища, він пронизує процес прийняття рішень у всіх областях нашого повсякденного життя. Візьмемо, наприклад, випадок з домашньою охороною. Багато людей вирішують встановити системи домашньої безпеки і щомісяця платити постачальнику послуг за моніторинг цих систем для кращого захисту своєї власності. Очевидно, домовласники зважили вартість встановлення та моніторингу системи з цінністю своїх домашніх товарів та безпекою своєї сім'ї, що є фундаментальною «місією».

Керівник організаційного підрозділу повинен забезпечити, щоб організація володіла можливостями, необхідними для виконання своєї місії. Ці власники місій повинні визначити можливості безпеки, якими повинні володіти їх IT-системи для забезпечення бажаного рівня підтримки місій перед лицем реальних загроз. Більшість організацій мають жорсткі бюджети на IT-безпеку, тому витрати на IT-безпеку повинні розглядатися так само ретельно, як і інші управлінські рішення. Добре структурована методологія управління ризиками при ефективному використанні може допомогти керівництву визначити відповідні засоби контролю для забезпечення необхідних для місії можливостей забезпечення безпеки [31].

Мінімізація негативного впливу на організацію та необхідність надійної основи для прийняття рішень є фундаментальними причинами, за якими організації впроваджують процес управління ризиками для своїх IT-систем.

Ефективне управління ризиками має бути повністю інтегровано в життєвий цикл розробки системи (ЖЦРС). ЖЦРС ІТ-системи складається з п'яти етапів:

- ініціювання;
- розробка або придбання;
- впровадження;
- експлуатація або технічне обслуговування;
- утилізація.

У деяких випадках ІТ- система може займати кілька з цих фаз одночасно. Однак методологія управління ризиками залишається незмінною незалежно від етапу ЖЦРС, для якого проводиться оцінка. Управління ризиками - це ітеративний процес, який може виконуватися на кожному основному етапі ЖЦРС.

Таблиця 2.1

Інтеграція управління ризиками в життєвий цикл розробки системи

Фази циклу	Фазова характеристика	Підтримка діяльності з управління ризиками
Фаза 1-Початок	Виражається потреба в ІТ-системі, а також документуються мета і сфера застосування ІТ-системи	Виявлені ризики використовуються для підтримки розробки системних вимог, у тому числі вимог безпеки, а також концепції безпеки операцій (стратегія)
Фаза 2-Розробка або придбання	ІТ-система спроектована, придбана, запрограмована, розроблена або іншим чином сконструйована	Ризики, виявлені на цьому етапі, можуть бути використані для підтримки аналізу безпеки ІТ-системи, що може призвести до компромісів в архітектурі і дизайні при розробці системи
Фаза 3-Реалізація	Функції безпеки системи повинні бути налаштовані, включені, протестовані і перевірені	Процес управління ризиками підтримує оцінку впровадження системи відповідно до її вимог і в рамках модельованого операційного середовища. Рішення щодо виявлених ризиків повинні прийматися до початку роботи системи

Продовження таблиці 2.1

Фаза 4 - Експлуатація та техобслуговування	Система виконує свої функції. Як правило, система постійно модифікується шляхом додавання апаратного та програмного забезпечення, а також шляхом внесення змін в організаційні процеси, політики та процедури	Діяльність з управління ризиками здійснюється для періодичної повторної авторизації системи (або повторної акредитації) або всякий раз, коли в ІТ-систему вносяться серйозні зміни в її операційному, виробничому середовищі (наприклад, нові системні інтерфейси)
Фаза 5 – Утилізація	Ця фаза може включати в себе розміщення інформації, апаратного та програмного забезпечення. Дії можуть включати переміщення, архівування, видалення або знищення інформації, а також дезінфекцію апаратного та програмного забезпечення	Заходи з управління ризиками виконуються для компонентів системи, які будуть утилізовані або замінені, щоб забезпечити належну утилізацію апаратного і програмного забезпечення, належну обробку залишкових даних і безпечну і систематичну міграцію системи

У таблиці 2.1 описуються характеристики кожної фази ЖЦРС і вказується, як можна здійснювати управління ризиками на підтримку кожної фази.

Управління ризиками - це відповідальність керівництва. Опишемо ключові ролі персоналу, які повинні підтримувати процес управління ризиками і брати участь в ньому [32].

Вище керівництво. Відповідно до стандарту кінцевої відповідальності за виконання місії має забезпечити ефективне використання необхідних ресурсів для розвитку потенціалу, необхідного для виконання місії. Вони також повинні оцінювати та включати результати діяльності з оцінки ризиків у процес прийняття рішень. Ефективна програма управління ризиками, яка оцінює і пом'якшує ризики, пов'язані з ІТ-місією, вимагає підтримки та участі вищого керівництва.

Головний інформаційний директор. IT-директор відповідає за IT-планування, бюджетування та ефективність діяльності агентства, включаючи компоненти інформаційної безпеки. Рішення, прийняті в цих областях, повинні грунтуватися на ефективній програмі управління ризиками.

Власники систем та інформації. Власники систем та інформації несуть відповідальність за забезпечення належного контролю за цілісністю, конфіденційністю та доступністю IT-систем та даних, якими вони володіють. Як правило, власники систем та інформації несуть відповідальність за зміни в своїх IT-системах. Таким чином, вони зазвичай повинні схвалити і підписати зміни в своїх IT-системах. Тому власники системи та інформації повинні розуміти свою роль в процесі управління ризиками і повністю підтримувати цей процес.

Бізнес – та функціональні менеджери. Менеджери, відповідальні за бізнес-операції та повинні брати активну участь у процесі управління ризиками. Ці менеджери - це люди, які наділені повноваженнями і відповідальні за прийняття компромісних рішень, необхідних для виконання місії. Їх участь в процесі управління ризиками дозволяє забезпечити належну безпеку IT-систем, яка при належному управлінні забезпечить ефективність місії при мінімальних витратах ресурсів [32].

ISSO. Керівники програм IT-безпеки та співробітники з комп'ютерної безпеки несуть відповідальність за програми безпеки своїх організацій, включаючи управління ризиками. Тому вони відіграють провідну роль у впровадженні відповідної структурованої методології, що допомагає виявляти, оцінювати і мінімізувати ризики для IT-систем, що підтримують місії їх організацій. ISSO також виступають в якості основних консультантів на підтримку вищого керівництва для забезпечення того, щоб ця діяльність здійснювалася на постійній основі.

Фахівці з IT-безпеки. Фахівці з IT-безпеки (наприклад, адміністратори мереж, систем, додатків і баз даних; комп'ютерні фахівці; аналітики безпеки; консультанти з безпеки) несуть відповідальність за належне виконання вимог безпеки в своїх IT-системах. У міру того як відбуваються зміни в існуючому

середовищі IT-систем (наприклад, розширення мережевих підключень, зміни в існуючій інфраструктурі та організаційній політиці, впровадження нових технологій), фахівці з IT-безпеки повинні підтримувати або використовувати процес управління ризиками для виявлення та оцінки нових потенційних ризиків і впровадження нових засобів контролю безпеки, необхідних для захисту їх IT-систем.

Використання IT-систем і даних відповідно до політики, керівними принципами і правилами поведінки організації має вирішальне значення для зниження ризиків і захисту IT-ресурсів організації. Щоб звести до мінімуму ризик для IT-систем, вкрай важливо, щоб користувачі систем і додатків пройшли навчання з питань безпеки. Тому інструктори з IT-безпеки або фахівці в галузі безпеки/предметної області повинні розуміти процес управління ризиками, щоб вони могли розробляти відповідні навчальні матеріали і включати оцінку ризиків в навчальні програми для навчання кінцевих користувачів [33].

2.2. Методологія оцінки ризиків

Оцінка ризиків – це перший процес в методології управління ризиками. Організації використовують оцінку ризиків для визначення ступеня потенційної загрози та ризику, пов'язаного з IT-системою протягом усього її SDLC. Результати цього процесу допомагають визначити відповідні заходи контролю для зниження або усунення ризику/.

Щоб визначити ймовірність майбутньої несприятливої події, загрози для IT-системи повинні бути проаналізовані в поєднанні з потенційними вразливостями і засобами контролю, що діють для IT-системи. Вплив відноситься до величини шкоди, яка може бути заподіяна в результаті здійснення загрози уразливості. Рівень загрози визначається потенційним впливом місії і, в свою чергу, створює відносну цінність для порушених IT-активів і ресурсів (наприклад, критичність і чутливість компонентів IT-системи і даних).

При оцінці ризиків для IT-системи першим кроком є визначення обсягу зусиль. На цьому етапі визначаються межі IT-системи, а також ресурси та

інформація, що становлять систему. Характеристика IT-системи встановлює обсяг зусиль з оцінки ризику, окреслює межі дозволу на експлуатацію (або акредитації) і надає інформацію (наприклад, апаратне забезпечення, програмне забезпечення, підключення до системи і відповідальний відділ або допоміжний персонал), необхідну для визначення ризику [32].

Методологія, яка описана, може бути застосована до оцінки однієї або декількох взаємопов'язаних систем. В останньому випадку важливо, щоб область інтересу і всі інтерфейси і залежності були чітко визначені до застосування методології.

Визначення ризику для IT-системи вимагає глибокого розуміння середовища обробки системи. Тому особа або особи, які проводять оцінку ризику, повинні спочатку зібрати системну інформацію.

Загальна системна інформація для оцінки ризику повинна включати:

- обладнання;
- програмне забезпечення;
- системні інтерфейси (наприклад, внутрішнє і зовнішнє підключення);
- дані та інформація;
- особи, які підтримують і використовують IT-систему;
- місія системи (наприклад, процеси, що виконуються IT-системою);
- критичність системи та даних (наприклад, цінність або важливість системи для організації);
- чутливість системи і даних.

Додаткова інформація, що стосується операційного середовища IT-системи та її даних, включає, але не обмежується наступним:

- функціональні вимоги до IT-системи;
- користувачі системи (наприклад, користувачі системи, що надають технічну підтримку IT-системі та користувачі додатків, що використовують IT-систему для виконання бізнес-функцій);
- політика системної безпеки, що регулює IT-систему (організаційна політика, федеральні вимоги, закони, галузева практика);

- архітектура безпеки системи;

- поточна топологія мережі (наприклад, схема мережі);

- захист зберігання інформації, що забезпечує доступність, цілісність і конфіденційність системи і даних [34];

- потік інформації, що відноситься до IT-системи (наприклад, системні інтерфейси, блок-схема введення і виведення системи)

- технічні засоби контролю, що використовуються для IT-системи (наприклад, вбудований або додатковий продукт безпеки, що підтримує ідентифікацію та аутентифікацію, дискреційний або обов'язковий контроль доступу, аудит, залишковий Захист інформації, методи шифрування);

- елементи управління, що використовуються для IT-системи (наприклад, правила поведінки, планування безпеки);

- операційний контроль, використовуваний для IT-системи (наприклад, безпека персоналу, резервне копіювання, аварійні операції, поновлення та відновлення; технічне обслуговування системи; зберігання поза сайту; процедури створення та видалення облікових записів користувачів; контроль розподілу функцій, таких як привілейований доступ користувачів порівняно зі стандартним доступом користувачів)

- фізичне середовище безпеки IT-системи (наприклад, безпека об'єкта, політика центру обробки даних);

- екологічна безпека, що реалізується для середовища обробки IT-системи (наприклад, контроль вологості, води, потужності, забруднення, температури і хімічних речовин).

Для системи, що знаходиться на стадії ініціювання або проектування, системна інформація може бути отримана з документа проекту або вимог. Для розроблюваної IT-системи необхідно визначити ключові правила безпеки і атрибути, плановані для майбутньої IT-системи. Проектні документи системи і план безпеки системи можуть надати корисну інформацію про безпеку IT-системи, що знаходиться в стадії розробки.

Для операційної ІТ-системи збираються дані про ІТ-систему в її виробничому середовищі, включаючи дані про конфігурацію системи, підключення, а також документовані і недокументовані процедури і практики. Таким чином, опис системи може ґрунтуватися на безпеці, що забезпечується базовою інфраструктурою, або на майбутніх планах безпеки ІТ-системи [34].

Для збору інформації, що відноситься до ІТ-системи в межах її операційної межі, можна використовувати будь-який з наступних методів або їх комбінацію:

1. Опитування. Для збору відповідної інформації співробітники з оцінки ризиків можуть розробити перелік питань, що стосується управлінського та оперативного контролю, планованого або використовуваного для ІТ-системи. Таке анкета повинна бути поширена серед відповідного технічного та нетехнічного управлінського персоналу, який розробляє або підтримує ІТ-систему. Цю анкету можна було б також використовувати під час поїздок на місця проведення робіт і співбесіди.

2. Інтерв'ю на місці. Інтерв'ю з персоналом служби підтримки та управління ІТ-системами можуть дозволити персоналу з оцінки ризиків зібрати корисну інформацію про ІТ-систему (наприклад, про те, як вона експлуатується і управляється). Виїзди на місце також дозволяють персоналу з оцінки ризиків спостерігати і збирати інформацію про фізичну, екологічну та операційну безпеку ІТ-системи. Для систем, які все ще перебувають на стадії проектування, виїзд на місце буде являти собою особистий збір даних і може дати можливість оцінити фізичне середовище, в якому буде працювати ІТ-система.

3. Рецензування документів. Програмні документи (наприклад, законодавча документація, директиви), системна документація (наприклад, керівництво користувача системи, керівництво з адміністрування системи, документ про проектування і вимоги до системи, документ про придбання) та документація, пов'язана з безпекою (наприклад, попередній аудиторський звіт, звіт про оцінку ризиків, результати тестування системи, план безпеки системи, політика безпеки), можуть надати хорошу інформацію про засоби контролю безпеки і планованих для ІТ-системи. Аналіз впливу місії організації або оцінка

критичності активів надає інформацію про критичність і чутливість систем і даних.

4. Використання автоматизованого інструменту сканування. Активні технічні методи можуть бути використані для ефективного збору системної інформації.

Збір інформації може проводитися протягом усього процесу оцінки ризику, починаючи з етапу 1 (характеристика системи) і закінчуючи етапом 9 (документування результатів).

Наступний етап – це ідентифікація загрози. Загроза – це потенційна можливість для конкретного джерела успішно використовувати певну вразливість. Вразливість - це слабкість, яка може бути випадково викликана або навмисно використана. Джерело загрози не становить небезпеки, коли немає уразливості, яку можна використовувати. При визначенні ймовірності загрози необхідно враховувати джерела загрози, потенційні уразливості та існуючі засоби контролю.

Мета цього кроку полягає в тому, щоб визначити потенційні джерела загроз і скласти уявлення про загрозу, що перераховує потенційні джерела небезпек, застосовні до оцінюваної IT-системі.

Джерело загрози визначається як будь-яка обставина або подія, яка потенційно здатна завдати шкоди IT-системі. Загальні джерела загроз можуть бути природними, людськими або екологічними.

При оцінці джерел загроз важливо враховувати всі потенційні джерела загроз, які можуть завдати шкоди IT-системі та її середовищу обробки. Наприклад, загроза для IT-системи, яка розташована в пустелі, може не включати «природну повінь» через низьку ймовірність виникнення такої події екологічної загрози, але така загроза як розрив труби, може швидко затопити комп'ютерний зал і завдати шкоди IT-активам і ресурсам організації. Люди можуть бути джерелами загрози внаслідок навмисних дій, таких як навмисні напади на інших осіб або незадоволених співробітників, або ненавмисних дій, таких як недбалість і помилки.

Навмисна атака може бути або зловмисною спробою отримати несанкціонований доступ до IT-системи (наприклад, шляхом підбору пароля) з метою порушення цілісності системи і даних, доступності або конфіденційності, але тим не менш цілеспрямованою спробою обійти систему безпеки. Одним із прикладів останнього типу навмисної атаки є написання програмістом програми "троянський кінь" для обходу системної безпеки, щоб виконати роботу [16].

Мотивація і ресурси для проведення атаки роблять людину потенційно небезпечним джерелом загрози, типи яких більш детально наведені у таблиці 2.2.

Таблиця 2.2

Людські загрози: загроза-джерело, мотивація і дії, пов'язані із загрозою

Джерело загрози	Мотивація	Дії з погрозами
Хакер, зломщик	Виклик Незаконне розкриття інформації	Зламування Вторгнення в систему, зломи Несанкціонований доступ до системи
Комп'ютерний злочинець	Знищення інформації Незаконне розкриття інформації Грошовий прибуток Несанкціонована зміна даних	Комп'ютерні злочини (наприклад, кібер-переслідування) Шахрайська дія Інформація про хабарництво Обман Вторгнення в систему
Терорист	Шантаж Руйнування Експлуатація ІС	Інформаційна війна Системна атака Проникнення в систему Злом системи
Промислове шпигунство (компанії, іноземні уряди, інші державні інтереси)	Конкурентна перевага Економічне шпигунство	Економічна експлуатація Крадіжка інформації Вторгнення в особисте життя Соціальна інженерія Проникнення в систему Несанкціонований доступ до системи

Продовження таблиці 2.2

Інсайдери	Грошовий прибуток Помста Ненавмисні помилки і упущення (наприклад, помилка введення даних, помилка програмування)	Напад на співробітника Шантаж Перегляд конфіденційної інформації Зловживання комп'ютером Шахрайство та крадіжка Введення фальсифікованих, пошкоджених даних Перехоплення Шкідливий код (наприклад, вірус, логічна бомба, троянський кінь) Продаж особистої інформації Системні помилки Вторгнення в систему Саботаж системи Несанкціонований доступ до системи

У таблиці 2.2 представлений огляд багатьох сучасних поширених людських загроз, їх можливих мотивів і методів або дій, за допомогою яких вони можуть здійснити атаку. Ця інформація буде корисна організаціям, які вивчають своє середовище загроз для людини і налаштовують свої заяви про загрози для людини. Крім того, огляди історії системних зломів; звіти про порушення безпеки; звіти про інциденти; а інтерв'ю з системними адміністраторами, співробітниками Служби підтримки та спільнотою користувачів під час збору інформації допоможуть виявити людські загрози-джерела, які потенційно можуть завдати шкоди IT-системі та її даним і які можуть бути небезпечні там, де існує вразливість.

Оцінка мотивації, ресурсів і можливостей, які можуть знадобитися для успішної атаки, повинна бути розроблена після виявлення потенційних джерел загрози, щоб визначити ймовірність того, що загроза проявить вразливість системи [37].

Заява про загрозу або список потенційних джерел загрози повинні бути адаптовані до конкретної організації та її середовища обробки (наприклад, звички кінцевих користувачів до обчислень). В цілому, інформація про природні

загрози (наприклад, повені, землетруси, шторми) повинна бути легкодоступною. Відомі загрози були виявлені багатьма державними та приватними організаціями. Інструменти виявлення вторгнень також стають все більш поширеними, і державні та галузеві організації постійно збирають дані про події безпеки, тим самим покращуючи здатність реалістично оцінювати загрози. Джерела інформації включають, але не обмежуються ними, та поділяються на наступні:

- розвідувальні служби;
- центр реагування на комп'ютерні інциденти взлому;
- засоби масової інформації, особливо веб-ресурси, такі як SecurityFocus.com, SecurityWatch.com, SecurityPortal.com, і SANS.org.

Наступний крок - це ідентифікація вразливостей. Аналіз загрози для IT-системи повинен включати аналіз вразливостей, пов'язаних з системним середовищем. Метою цього кроку є розробка списку вразливостей системи (недоліків або слабких місць), які можуть бути використані потенційними джерелами загроз.

Таблиця 2.3

Порівняння вразливості та її загрози

Уразливість	Джерело загрози	Дія загрози
Системні ідентифікатори (ID) звільнених співробітників не видаляються з системи	Звільнені співробітники	Підключення до мережі компанії і доступ до службових даних компанії
Компанія брандмауер вхідного трафіку telnet, і посвідчення особи гостя включена на сервер	Неавторизовані користувачі (наприклад, хакери, звільнені співробітники, комп'ютерні злочинці, терористи)	Використання telnet для XYZ сервера і перегляд системних файлів з ідентифікатором гостя

Продовження таблиці 2.3

Постачальник виявив недоліки в дизайні безпеки системи, проте нові виправлення до неї не були застосовані	Неавторизовані користувачі (наприклад, хакери, незадоволені співробітники, комп'ютерні злочинці, терористи)	Отримання несанкціонованого доступу до конфіденційних системних файлів на основі відомих системних вразливостей
Центр обробки даних використовує водяні розпилювачі для придушення пожежі; брезент для захисту обладнання та обладнання від пошкодження водою не встановлений	Пожежа, недбайливі особи	У центрі обробки даних включаються водяні розбризкувачі

Рекомендованими методами виявлення вразливостей системи є використання джерел вразливостей, проведення тестування безпеки системи та розробка контрольного списку вимог безпеки.

Слід зазначити, що типи існуючих вразливостей і методологія, необхідна для визначення наявності цих вразливостей, зазвичай варіюються в залежності від характеру IT-системи і фази, в якій вона знаходиться, в SDLC:

1. Якщо IT-система ще не розроблена, пошук вразливостей повинен бути зосереджений на політиці безпеки організації, планованих процедурах безпеки і визначенні системних вимог, а також на аналізі продуктів безпеки постачальників або розробників (наприклад, технічних документах).

2. Якщо IT-система впроваджується, то ідентифікація вразливостей повинна бути розширена і включати в себе більш конкретну інформацію, таку як плановані функції безпеки, описані в проектній документації з безпеки, а також результати сертифікаційних випробувань і оцінки системи.

3. Якщо IT-система функціонує, процес виявлення вразливостей повинен включати аналіз функцій безпеки IT-системи і засобів контролю безпеки, технічних і процедурних, використовуваних для захисту системи [38].

Технічні та нетехнічні уразливості, пов'язані з середовищем обробки IT-системи, можуть бути ідентифіковані за допомогою методів збору інформації,

огляд інших галузевих джерел (наприклад, веб-сторінок постачальників, що ідентифікують системні помилки і недоліки) буде корисний при підготовці до інтерв'ю і розробці ефективних анкет для виявлення вразливостей, які можуть бути застосовні до конкретних IT-систем. Інтернет є ще одним джерелом інформації про відомі системні уразливості, що розміщуються постачальниками, поряд з виправленнями, пакетами оновленнями, патчами та іншими коригуючими заходами, які можуть бути застосовані для усунення або пом'якшення вразливостей. Документовані джерела вразливостей, які слід враховувати при ретельному аналізі вразливостей, включають, але не обмежуються ними, та поділяються на такі види:

- попередня документація з оцінки ризиків оцінюваної IT-системи;

- звіти про аудит IT-системи, звіти про аномалії системи, звіти про перевірку безпеки, звіти про тестування та оцінку системи;

- списки вразливостей, такі як база даних вразливостей nist I-CAT;

- рекомендації з безпеки, такі як бюлетені FedCIRC та Департаменту енергетики з комп'ютерних інцидентів;

- рекомендації постачальникам;

- комерційні комп'ютерні групи реагування на інциденти / надзвичайні ситуації та поштові списки (наприклад, SecurityFocus.com розсилки на форумі);

- інформаційні оповіщення про вразливості та сповіщення для військових систем;

- аналіз безпеки системного програмного забезпечення.

Про-активні методи, що використовують системне тестування, можуть бути використані для ефективного виявлення вразливостей системи в залежності від критичності IT-системи і наявних ресурсів (наприклад, виділених коштів, наявних технологій, осіб, що володіють досвідом проведення тестування). Методи випробувань включають в себе:

1. Автоматизований інструмент сканування вразливостей

2. Тестування та оцінка безпеки (ТОБ)

3. Тестування на проникнення.

Інструмент автоматичного сканування вразливостей використовується для сканування групи хостів або мережі на наявність відомих уразливих служб. Однак слід зазначити, що деякі з потенційних вразливостей, виявлених інструментом автоматичного сканування, можуть не представляти реальних вразливостей в контексті системного середовища. Наприклад, деякі з цих інструментів сканування оцінюють потенційні уразливості без урахування середовища і вимог сайту. Деякі з "вразливостей", позначених програмним забезпеченням автоматичного сканування, насправді можуть не бути вразливими для конкретного сайту, але можуть бути налаштовані таким чином, тому що їх середовище вимагає цього. Таким чином, цей метод тестування може давати помилкові спрацьовування [39].

ТОБ – це ще один метод, який може бути використаний при виявленні вразливостей IT-систем в процесі оцінки ризиків. Вона включає в себе розробку і виконання плану тестування. Метою тестування системної безпеки є перевірка ефективності засобів контролю безпеки IT-системи в тому вигляді, в якому вони застосовуються в операційному середовищі. Мета полягає в тому, щоб переконатися, що застосовувані засоби контролю відповідають затвердженій специфікації безпеки програмного і апаратного забезпечення і реалізують політику безпеки організації або відповідають галузевим стандартам.

Тестування на проникнення може бути використано для доповнення аналізу засобів контролю безпеки та забезпечення безпеки різних аспектів IT-системи. Тестування на проникнення, що застосовується в процесі оцінки ризиків, може бути використано для оцінки здатності IT-системи протистояти навмисним спробам обійти систему безпеки. Його мета-протестувати IT-систему з точки зору джерела загрози і виявити потенційні порушення в схемах захисту IT-системи.

Результати цих видів додаткового тестування безпеки допоможуть виявити уразливості системи.

На цьому етапі персонал з оцінки ризиків визначає, чи задовольняються вимоги безпеки, передбачені для IT-системи і зібрані в ході характеристики

системи, існуючими або планованими засобами контролю безпеки. Як правило, вимоги до безпеки системи можуть бути представлені у вигляді таблиці, причому кожна вимога супроводжується поясненням того, як конструкція або реалізація системи задовольняє або не задовольняє цій вимозі контролю безпеки [32].

Контрольний список вимог безпеки містить основні стандарти безпеки, які можуть бути використані для систематичної оцінки та виявлення вразливостей активів (персоналу, обладнання, програмного забезпечення, інформації), неавтоматизованих процедур, процесів і передачі інформації, пов'язаних з даною ІТ-системою, в наступних областях безпеки:

1. Управління системою безпеки.
2. Контроль безпеки.
3. Технічний захист.

У таблиці 2.4. перераховані критерії безпеки, пропоновані для використання при виявленні вразливостей ІТ-системи в кожній області безпеки.

Таблиця 2.4

Критерії Безпеки

Зона безпеки	Критерії безпеки
Безпека Управління	– Розподіл обов'язків – Безперервність підтримки – Можливість реагування на інциденти – Періодичний огляд засобів контролю безпеки – Перевірка персоналу та фонові розслідування – Оцінка ризику – Безпека та технічна підготовка – Поділ обов'язків – Авторизація та повторна авторизація системи – План безпеки системи або Програми
Оперативна безпека	– Контроль забруднюючих речовин, що переносяться повітрям (дим, пил, хімічні речовини) – Контроль за забезпеченням якості електропостачання – Доступ до носіїв даних та їх утилізація – Розподіл і маркування зовнішніх даних – Захист об'єкта (наприклад, комп'ютерний зал, дата-центр, офіс) – Контроль температури – Робочі станції, ноутбуки та автономні персональні комп'ютери

Продовження таблиці 2.4

Технічна безпека	– Комунікації (наприклад, dial-in, system interconnection, маршрутизатори) – Криптографія – Дискреційний контроль доступу – Ідентифікація та аутентифікація – Виявлення вторгнень – Повторне використання об'єктів – Системний аудит

Результатом цього процесу є контрольний списку вимог безпеки.

Наступний крок – це контрольний аналіз. Мета цього кроку полягає в тому, щоб проаналізувати засоби контролю, які були впроваджені або плануються до впровадження організацією для мінімізації або усунення ймовірності реалізації загрози уразливості системи.

Щоб отримати загальну оцінку ймовірності, яка вказує на ймовірність того, що потенційна вразливість може бути реалізована в рамках конструкції відповідного середовища загроз, необхідно розглянути питання про впровадження поточних або планованих заходів контролю. Наприклад, вразливість (системна або процедурна слабкість) навряд чи буде реалізована або ймовірність невелика, якщо існує низький рівень інтересу або можливостей джерела загрози або якщо існують ефективні засоби контролю безпеки, які можуть усунути або зменшити масштаби збитку [24].

Контроль безпеки включає в себе використання технічних і нетехнічних методів. Технічні засоби контролю - це засоби захисту, включені в комп'ютерне обладнання, програмне забезпечення або ПЗ (наприклад, механізми контролю доступу, механізми ідентифікації і аутентифікації, методи шифрування, програмне забезпечення для виявлення вторгнень).

Нетехнічний контроль - це управлінський та оперативний контроль, такий як політика безпеки, оперативні процедури, Кадрова, фізична та екологічна безпека.

Категорії контролю як для технічних, так і для нетехнічних методів контролю можуть бути додатково класифіковані як превентивні або детективні. Ці дві підкатегорії пояснюються наступним чином:

Превентивні заходи контролю перешкоджають спробам порушення політики безпеки і включають такі заходи контролю, як примусове застосування контролю доступу, шифрування і аутентифікація.

Детективні засоби контролю попереджають про порушення або спроби порушення політики безпеки і включають такі засоби контролю, як контрольні журнали, методи виявлення вторгнень і контрольні суми [26].

Впровадження такого контролю в процесі зниження ризику є прямим результатом виявлення недоліків у поточному або планованому контролі в процесі оцінки ризику.

Розробка контрольного списку вимог безпеки або використання доступного контрольного списку буде корисно для ефективного і систематичного аналізу засобів контролю. Контрольний список вимог безпеки можна використовувати для перевірки як невідповідності вимогам безпеки, так і їх відповідності.

Тому важливо оновити такі контрольні списки, щоб відобразити зміни в середовищі контролю організації (наприклад, зміни в політиках безпеки, методах і вимогах), щоб забезпечити достовірність контрольного списку.

Наступний крок - це визначення ймовірності. Щоб отримати загальну оцінку ймовірності, яка вказує на ймовірність того, що потенційна вразливість може бути реалізована в рамках конструкції пов'язаного з нею середовища загроз, необхідно враховувати наступні Керуючі фактори:

- мотивація і можливості джерела загрози;
- характер уразливості;
- наявність і ефективність поточного контролю.

Імовірність того, що потенційна вразливість може бути реалізована даним джерелом загрози, може бути описана як висока, середня або низька (табл.2.5)

Таблиця 2.5

Визначення ймовірності

Рівень ймовірності	Визначення ймовірності
Високий	Джерело загрози володіє високою мотивацією і достатніми можливостями, а заходи контролю, що запобігають реалізації уразливості, неефективні.
Середній	Джерело загрози мотиване і здатне до нанесення шкоди, але існують засоби контролю, які можуть перешкоджати успішному використанню уразливості.
Низький	У джерела загрози відсутня мотивація або здатність, або ж є засоби контролю, щоб запобігти або, принаймні, істотно перешкодити реалізації уразливості.

Наступним важливим кроком у вимірюванні рівня ризику є визначення несприятливого впливу, що виникає в результаті успішної реалізації загрози уразливості. Перед початком аналізу впливу необхідно отримати наступну необхідну інформацію, як описано вище:

1. Місія системи (наприклад, процеси, що виконуються IT-системою).

2. Критичність системи та даних (наприклад, цінність або важливість системи для організації).

3. Чутливість системи і даних.

Ця інформація може бути отримана з існуючої організаційної документації, такої як звіт про аналіз впливу місії або звіт про оцінку критичності активів.

Аналіз впливу місії визначає пріоритетність рівнів впливу, пов'язаних з компрометацією інформаційних активів організації, на основі якісної або кількісної оцінки чутливості і критичності цих активів. Оцінка критичності активів визначає пріоритетність чутливих і критично важливих інформаційних активів організації (наприклад, апаратного забезпечення, програмного забезпечення, систем, послуг і пов'язаних з ними технологічних активів), які підтримують критично важливі завдання організації [27].

Якщо ця документація не існує або такі оцінки IT-активів організації не проводилися, чутливість системи і даних може бути визначена на основі рівня захисту, необхідного для підтримки доступності, цілісності та конфіденційності системи і даних. Незалежно від методу, який використовується для визначення того, наскільки чутливі IT-система та її дані, власники системи та інформації несуть відповідальність за визначення рівня впливу для своєї власної системи та інформації. Отже, при аналізі впливу доречним підходом є опитування власника системи та інформації [41].

При проведенні аналізу впливу слід враховувати переваги і недоліки кількісних і якісних оцінок. Головна перевага якісного аналізу впливу полягає в тому, що він визначає пріоритетність ризиків і визначає області для негайного поліпшення в усуненні вразливостей. Недоліком якісного аналізу є те, що він не дає конкретних кількісних вимірювань величини впливу, що ускладнює аналіз витрат і виграшів будь-яких рекомендованих заходів контролю.

Основна перевага кількісного аналізу впливу полягає в тому, що він забезпечує вимірювання величини впливу, яке може бути використано при аналізі витрат і виграшів рекомендованих заходів контролю. Недоліком є те, що в залежності від числових діапазонів, що використовуються для вираження вимірювання, сенс кількісного аналізу впливу може бути неясним, що вимагає якісної інтерпретації результату. Для визначення величини впливу часто доводиться враховувати додаткові фактори. Вони можуть включати, але не обмежуються ними.

1. Оцінка частоти використання уразливості джерелом загрози протягом певного періоду часу (наприклад, 1 рік) .

2. Приблизна вартість кожного випадку використання уразливості джерелом загрози

3. Зважений фактор, заснований на суб'єктивному аналізі відносного впливу конкретної загрози на конкретну вразливість.

Наступний крок - це визначення ризику. Мета цього кроку-оцінити рівень ризику для ІТ-системи. Визначення ризику для конкретної пари загроза / вразливість може бути виражено як функція:

- ймовірність того, що дане джерело загрози спробує скористатися даною вразливістю;

- величина впливу, якщо джерело загрози успішно використовує вразливість;

- адекватність запланованих або існуючих заходів контролю безпеки для зниження або усунення ризику.

Наступний крок – це рекомендації щодо контролю. На цьому етапі процесу передбачені засоби контролю, які могли б пом'якшити або усунути виявлені ризики в залежності від діяльності організації [31]. Метою рекомендованих заходів контролю є зниження рівня ризику для ІТ-системи та її даних до прийнятного рівня. При рекомендаціях заходів контролю та альтернативних рішень щодо мінімізації або усунення виявлених ризиків слід враховувати наступні фактори:

1. Ефективність рекомендованих варіантів (наприклад, сумісність системи).

2. Законодавство та регулювання.

3. Організаційна політика.

4. Операційний вплив.

5. Безпека і надійність.

Рекомендації з контролю є результатами процесу оцінки ризиків і є внеском у процес зниження ризиків, в ході якого оцінюються, визначаються пріоритети і реалізуються рекомендовані процедурні та технічні засоби контролю безпеки.

Слід зазначити, що не всі можливі рекомендовані заходи контролю можуть бути реалізовані для зниження втрат. Щоб визначити, які з них необхідні і підходять для конкретної організації, слід провести аналіз витрат і виграшів, для пропонованих рекомендованих заходів контролю, щоб продемонструвати,

що витрати на впровадження заходів контролю можуть бути виправдані зниженням рівня ризику. Крім того, операційний вплив і здійсненність впровадження рекомендованого варіанту повинні бути ретельно оцінені в процесі зниження ризику [31].

Після завершення оцінки ризиків (виявлення джерел загроз і вразливостей, оцінки ризиків і надання рекомендованих заходів контролю) результати повинні бути задокументовані в офіційному звіті або брифінгу.

Звіт про оцінку ризиків – це управлінський звіт, який допомагає вищому керівництву, приймати рішення про політичні, процедурні, бюджетні та системні оперативні та управлінські зміни. На відміну від аудиторського або слідчого звіту, в якому виявляються порушення, звіт про оцінку ризиків повинен представлятися не в обвинувальній формі, а як систематичний і аналітичний підхід до оцінки ризиків, з тим щоб вище керівництво розуміло ризики і виділяло ресурси для скорочення і виправлення потенційних втрат. З цієї причини деякі люди вважають за краще розглядати загрозу та вразливість як спостереження, а не висновки в звіті про оцінку ризику.

2.3. Використання теорії ігор для захисту АІС за допомогою ігрових ризик-моделей

Теорія ігор вивчає проблеми прийняття рішень серед групи гравців і застосовується до ситуацій, коли два або більше гравців мають суперечливі цілі. Вона забезпечує кількісну основу для міркувань про рішення, прийняті в тих сценаріях, в яких гравці або не знають, або не впевнені в намірах суперників. Таким чином, теорія ігор може дати уявлення про те, коли і як стратегії повинні бути прийняті захисником або, в нашому випадку, адаптивною системою захисту з використанням автоматизованих методів обману [40].

Коротше кажучи, гра складається з гравців, дій, виплат і стратегій. У послідовних іграх гравці чергують ходи, вибираючи з набору доступних дій в кожній точці. Ми припускаємо, що ігри кінцеві в тому сенсі, що всі послідовності дій закінчуються після фіксованої кількості ходів. Стратегія - це повний опис

гравцем того, які дії слід зробити у всіх можливих точках прийняття рішення. Враховуючи набір стратегій, по одній для кожного гравця, існує функція корисності, що привласнює кожному гравцеві числове значення в якості винагороди за результат кожного, наступного обраної стратегії. Традиційний аналіз ігор – це пошук рівноважних стратегій. Найбільш часто обчислюються рівноваги, в яких гравці не мають стимулу в односторонньому порядку відхилятися від своєї стратегії, враховуючи стратегію рівноваги інших гравців.

Наведемо терміни, які використовуються для опису концепцій теорії ігор:

1. Досконала інформація: всі гравці знають попередні дії, вжиті іншими гравцями.

2. Недосконала інформація: існує принаймні один гравець, для якого ходи інших гравців частково приховані.

3. Повна інформація: стратегії та виплати відомі всім гравцям.

4. Неповна інформація: існує принаймні один гравець, який не знає всіх стратегій і виплат інших гравців.

5. Байєсівська гра: гра з неповною інформацією може бути перетворена в гру з повною, але недосконалою інформацією, в якій деякі гравці мають різні типи, визначені їх набором доступних дій, стратегій і виграшів. Інші гравці підтримують уявлення про ці типи, оновлюючи їх по ходу гри відповідно до правила Байеса.

6. Байєсівська рівновага: версія рівноваги Неша для байєсівських ігор. Досконале байєсівське рівновагу (PBE) є подальшим уточненням.

7. Гіпергейм: складна гра, в якій принаймні один гравець має неправильне уявлення про модель гри, в яку він грає. Гравці можуть:

а) не знати, що вони грають в гру;

б) не знати про можливі ходи в грі.

8. Гра з нульовою сумою: гра, в якій загальні виграші і програші для всіх гравців дорівнюють нулю. У грі з двома гравцями виграш одного гравця призводить до того, що протилежний гравець отримує еквівалентний негативний виграш [42].

Основна модель, розроблена в теорії ігор в кожному з цих видів, - це модель захисника, що розгортає пастки для виявлення атакуючого і отримання інформації про наміри атакуючого. Захисник може замаскувати нормальні системи пасток і приманок, як звичайні системи. Зловмисник спостерігає за системою, не будучи в змозі визначити її реальний тип, і не впевнений, чи варто намагатися скомпрометувати систему. Точно так же захисник може бути не впевнений в тому, як інтерпретувати дії нападника.

Розглядається одноразовий сценарій, в якому захисник спочатку вибирає, чи слід маскувати систему, після чого атакуючий вирішує, чи слід компрометувати систему. Вони визначають і характеризують ідеальну байєсівську рівновагу для цієї гри. Можна зробити висновок, що маскування є рівноважною стратегією для захисника і що ці оманливі рівноважні дії корисні для захисту мережі.

В аналогічному підході застосовують ці методи для пом'якшення атак типу "відмова в обслуговуванні" (DoS) в комп'ютерній мережі шляхом розгортання honeypots як засобу залучення зловмисника і отримання інформації про його реальні наміри. Можна відзначити, що захист від DoS-атак виявляється проблемою оптимізації з точки зору захисника, коли захисник виділяє обмежені ресурси для мінімізації витрат при максимальному стримуванні. Потім вони приступають до моделювання цієї проблеми, використовуючи сигналізацію як динамічну гру з неповною інформацією. Рішення для PBE передбачає економічно ефективне пом'якшення DoS-атак за допомогою обману.

Розширення цих концепцій від одноразової версії до повторюваних сценаріїв, які також включають неправдиву інформацію, досліджується в роботі. Тут область застосування - це мережа з підтримкою «honeypot». Серед їхніх результатів для повторної гри було показано, що байєсівська схема оновлення переконань сходиться. Доказ їх результатів було доповнено чисельним моделюванням, що підтверджує їх аналіз.

Обман був широко успішним, коли він використовувався хакерами для соціальної інженерії та військовими стратегами в інформаційній війні [26].

Обман впливає на переконання, рішення і поведінку людини. Точно так само, обман є потужним інструментом, який повинен використовуватися для захисту наших систем від людей, які хочуть проникнути в них, атакувати і заподіяти їм шкоду [44].

Роль захисника, як відомо, несправедлива, оскільки захисник прагне запобігти вторгненню в будь-яке можливе місце, і зловмиснику потрібно тільки виявити і використовувати одну вразливість, щоб порушити захист. Подібно до захисту рухомих цілей [44], використання обману для захисту дає надію на відновлення балансу цього асиметричного недоліку.

У той час як багато методів були розроблені для підвищення швидкості і точності виявлення змагальної активності з метою полегшення роботи захисника, крім апріорного зміцнення систем, було проведено менше досліджень по методам, щоб зробити роботу нападника принципово складнішою.

Активний захист в автоматизованих інформаційних системах допомагає ускладнити завдання атакуючого, додаючи непередбачуваність в простір атаки за рахунок швидкої зміни інформації. Обман може додати більше невизначеності, включаючи дезінформацію і маскуючи справжню інформацію. Це ще більше впливає на прийняття рішень зловмисниками, змушуючи їх витрачати час і зусилля. Більш того, обман може бути використаний захисником для того, щоб вселити невірну віру в атакуючого. Це неправильне переконання може викликати хвильові ефекти на кожному етапі ланцюжка і може перервати кілька атак протягом тривалого періоду часу.

Кібер-захист АІС не може покладатися тільки на захист периметра і автоматизована система повинна бути здатна реагувати на дії зловмисників з тією ж швидкістю, що і мережевий трафік. Це вимагає інтелектуальних захисних систем, які можуть автоматично реагувати на шкідливу поведінку і еволюціонувати з плином часу в міру зміни атак.

Метод штучного інтелекту, який використовується для захисної системи, повинен бути здатний дивитися вперед і динамічно розглядати, як атакуючий може вести себе в майбутньому, перш ніж вживати оборонні дії. Концепція

адаптивного або активного захисту - коли система автоматично готує і реалізує прогностичні оборонні стратегії або реагує на виявлену підозрілу активність без втручання людини, отримує визнання, але ще не отримала широкого застосування на практиці. Адаптивний захисний кібер-обман AIC поєднує в собі дві концепції для стратегічного представлення дезінформації, яка автоматично змінюється в міру спостереження за змінами в мережі або поведінці зловмисника. Адаптивний кібер-обман - це абсолютно нове, але неминуче продовження попередньої роботи, яка охоплює комп'ютерну безпеку, поведінкові науки та спільноти штучного інтелекту [60].

Є багато причин, чому методи кібер-обману повинні бути адаптивними. Наприклад, несподіванка - це один з важливих елементів, який може вплинути на процеси прийняття рішень і дії атакуючого. Коли атакуючий стикається з несподіваними результатами, він може вирішити змінити стратегію або повторити ті ж прийоми, які порушать або затримають його просування, даючи захисникам більше часу і можливостей для адекватної реакції.

Статичні методи кібер-обману AIC спочатку можуть викликати подив, але з часом їх ефект ослабне, оскільки зловмисники знайомляться з цими методами і навчаються їх очікувати. Якщо методи є адаптивними, вони виявлять, коли атакуючий виробив відповідь на обман, і відповідно змінять метод обману. Несподіванка - це лише один приклад того, як адаптивний кібер-обман AIC може негативно вплинути на атакуючого і порушити його прогрес. Є ще багато способів вплинути на атакуючого, наприклад, викликати розчарування, замішання і невпевненість в собі. Це може призвести до того, що зловмисник збільшить кількість помилок, які він робить, і зробить їх більш легкими для виявлення, затримає атаку до тих пір, поки не буде створений додатковий захист або не буде виконана критична задача, яка утримає зловмисника від переслідування певної мети [65].

2.4. Застосування методології теорії ігор для здійснення адаптивного кібер-захисту

Існує безліч методів кібер-обману AIC, які застосовуються при дослідженнях кібер-безпеки, включаючи «медові горщики» (рис. 3.1) і «медові токени», атаки відтворення, створення пакетів і зміна корисних навантажень, смоляні ями, фальшиві документи, системи приманки та інші.

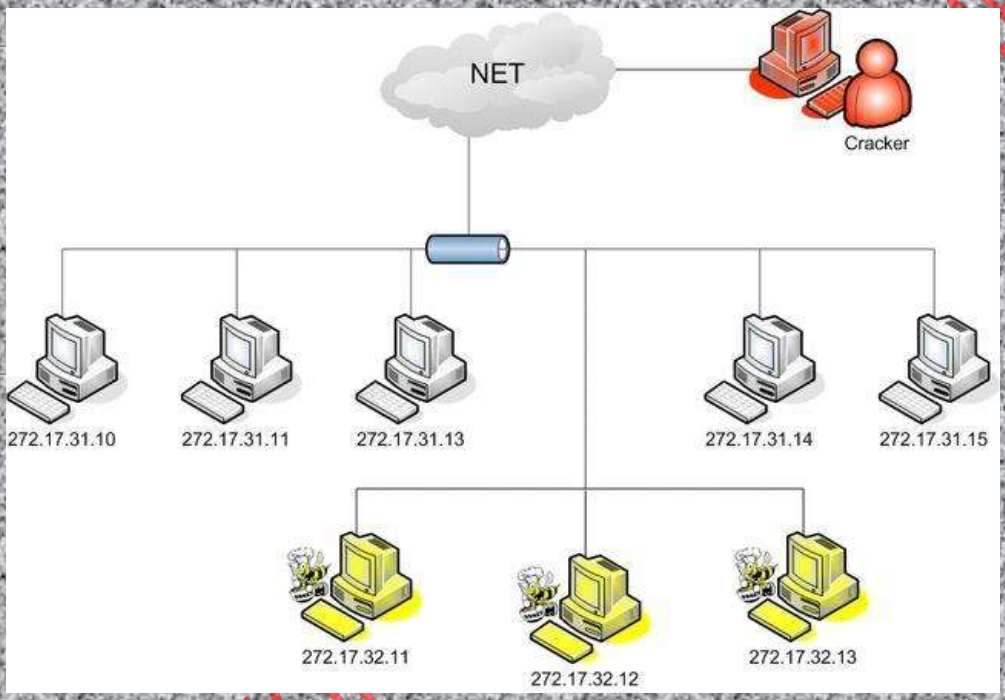

Рис. 2.1. Медові горщики в мережі

Через їх простоту, як концептуально, так і щодо реалізації, робота фокусується на використанні приманок для адаптивного обману. Наскільки відомо, ці системи ще не є адаптивними, як визначено вище, а скоріше статичними, заздалегідь сконфігурованими захистами, які, еволюціонують в системи динамічного захисту [61].

Середовище приманки складається з реалістичних та віртуальних систем, які здаються реальними системами, що виконують реальні служби з точки зору зловмисника, скануючого мережу. Вони розгортаються в реальній мережі разом з реальними системами, щоб максимізувати ймовірність швидкого виявлення та усунення атакуючого. Велика кількість помилкових активів допомагає

забезпечити асиметричну перевагу для кібер-захисників, зменшуючи ймовірність атаки на реальний актив, а також відволікаючи зловмисника від реальних активів і контенту. Це змушує зловмисника робити додаткові дії, тим самим сповільнюючи їх і збільшуючи ймовірність розкриття. Кібер-обман може піти ще далі та наштовхнути зловмисника до певного невірного переконання [59].

У доповіді Gartner 2015 року про методи обману був зроблений наступний ключовий висновок "обман як автоматизований механізм реагування являє собою значну зміну можливостей майбутньої IT-безпеки, до якого менеджери продуктів або програми безпеки не повинні ставитися легковажно" [63].

Проте адаптивні системи кібер-захисту AIC все ще перебувають у зародковому стані, і кібер-обман - це лише невелика частина системи кібер-захисту. Зосередження на адаптивних системах кібер-обману та використання теорії ігор є досить важливим для створення автономних систем кібер-обману, які можуть вирішувати, коли, де і як найкраще використовувати обман на основі поведінки атакуючого.

Пілотні дослідження, проведені з використанням спеціалістів-тестувальників, показують, що системи-приманки можуть бути дуже ефективні при порушенні мережевої розвідки, відволікаючи атакуючого, використовуючи свої когнітивні упередження проти нього, і викликаючи невпевненість в собі, що потім збільшує когнітивне навантаження на атакуючого. Також ці ефекти можна помножити, дозволивши приманкам адаптуватися до конкретних стратегій і переваг кожного противника. Крім того, ці початкові експериментальні дослідження показують, що кібер-обман автоматизованих інформаційних систем може бути таким же або більш ефективним, якщо зловмисник фактично поінформований про те, що в мережі використовується обман в оборонних цілях. Хоча ретельні дослідження, присвячені цьому питанню, вже завершені, Остаточний аналіз отриманих даних ще належить провести [51].

Реалізація адаптивної стратегії кібер-обману в реальному кібер-середовищі вимагає можливостей, які не можуть бути розгорнуті в звичайній

мережі. Зокрема, він вимагає датчиків, виконавчих механізмів і засобів логічного з'єднання входів з виходами, прийняття рішень про те, як і коли адаптуватися.

Датчики збирають інформацію для виявлення поведінкової змагальної активності, такої як виявлення активності сканування і спроб входу в систему. Більш просунуті датчики можуть виявляти такі дії, як спроба зловмисника використовувати вкрадені паролі, і можуть поширюватися на дії після експлуатації, особливо там, де приманки містять медові токени.

Приводи виконують автоматизовану дію в мережі або хості відповідно до вказівок. Приведення в дію приманок включає в себе зміну конфігурації, створення нових приманок, Зміна параметрів приманок, зміна службових банерів та інші обманні дії. Подальші пристосування-приманки можуть включати в себе зміну IP-адреси, відкриття або закриття портів, додавання або видалення служб або навіть підміну іншої операційної системи. Зазвичай такі спеціалізовані завдання зазвичай не справляються сучасними засобами управління корпоративною мережею, але ці завдання повинні бути автоматизовані, щоб швидко реагувати на підозрілу активність [62].

Крім того, ті ж самі методи кібер-обману в АІС можуть бути використані не тільки для того, щоб затримати, заплутати і здивувати зловмисника. Кібер-обман може бути використаний для більш прямого впливу на атаку. Наприклад, захисник може захотіти дізнатися щось конкретне про нападника або зібрати інформацію про конкретний тип атаки. Обман може бути використаний для того, щоб спокусити або переконати атакуючого здійснити дію, яка, невідома атакуючому, та якимось чином приносе користь захиснику. Це важливо для захисту, оскільки в міру просування до більш адаптивних кібер-захисних систем ми повинні враховувати природну еволюцію багатоступеневих ситуацій атаки / захисту. Ці просунуті засоби захисту повинні мати стратегічний вигляд, оскільки дії розглядаються на багато кроків попереду як для атакуючих, так і захисних дій [64].

Стратегія еволюції підтримує просунуті цілі захисника, такі як виявлення переваг і топологічна дезінформація. Ігрові моделі кібер-обману вимагають

додаткової складності, оскільки вони найкраще моделюються як гібридні ігри з недосконалою і неповною інформацією. Самі ігри не є кооперативними і несиметричними, захисники і нападники зазвичай мають дуже різні стратегії. Цілі захисників і нападників часто знаходяться в опозиції, і тому багато ігор можуть бути структуровані як ігри з нульовою сумою. Якщо виграшні значення конкретної стратегії не можна порівняти з виграшами для альтернативних стратегій, тоді потрібно, щоб ці стратегії були поміщені в різні ігрові дерева і проаналізовані незалежно або в контексті гіпергейму [58].

Ігри обману і неправильного сприйняття добре підходять для представлення у вигляді гіпергейму. З точки зору гіперігри можна природно і безпосередньо уявити взаємозв'язок між цілями захисника, спостереженнями, підіграми та індивідуальними стратегіями. Для визначено ігрові контексти як різні точки зору гравців на гру: контекст противника і контекст захисника.

Крім того, в моделі визначено атакуючого як "довірчивий" або "досвідчений" залежно від того, чи він усвідомлює, що обман може бути компонентом гри та стратегії в грі. Для простоти ілюстративний сценарій передбачає наївного противника, який не підозрює про обман.

Гіпергейми можуть забезпечити рішення для моделювання конфлікту, коли існує неправильне сприйняття або навмисний обман між гравцями [16]. У той час як теорія гіперігр обговорювалася для людського обману і кібер-захисту, не було стандартизовано ніяких формальних позначень для моделювання кібер-обману [56].

Гіпергейми добре підходять для моделювання кібер-обману, особливо враховуючи широкий набір потенційних цілей, стратегій і реалізацій захисного обману. Як кібер-захисник, хоча і повністю контролює ігрове поле, не можливо знати всі можливі дії, які зробить атакуючий. Це ще більш вірно для нападника, який може навіть не знати, що гра ведеться активно, і навіть якщо б він був обізнаний про неминучість обману, він не знав би, які типи обманних ходів були доступні захиснику. У грі з кібер-обманом ігрове дерево захисника може сильно відрізнятися від дерева атакуючого, а модель гіпергейму може охоплювати всі

підігрові дерева, оскільки вони розігруються для сприйняття гри кожним окремим гравцем.

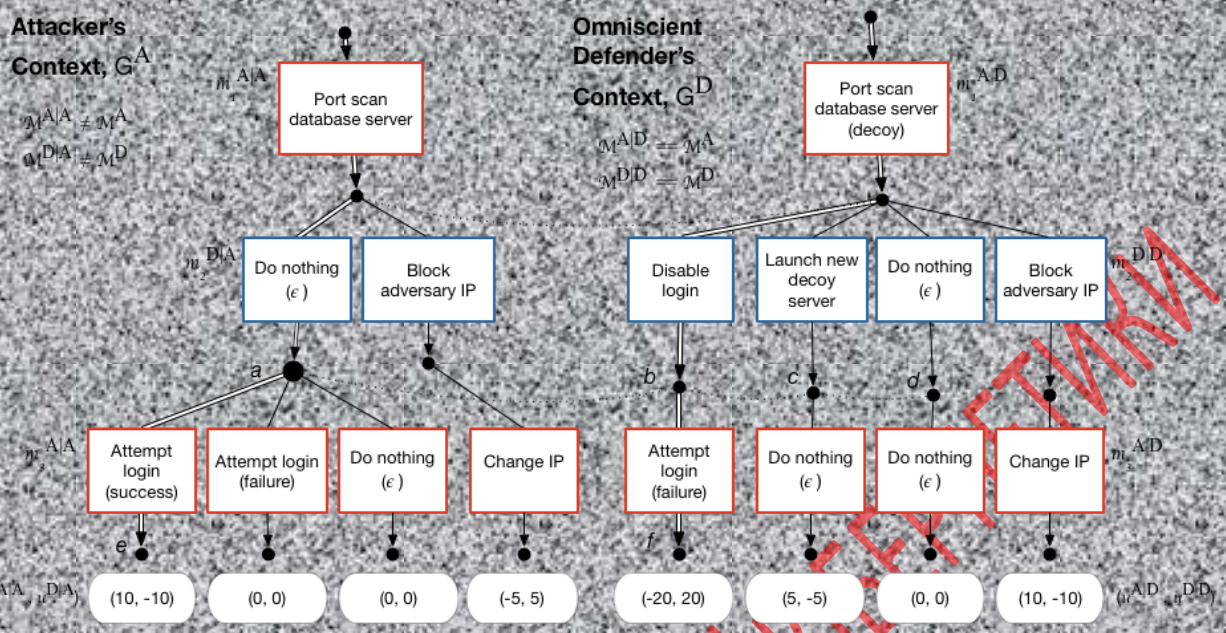

Рисунок 3.2. Ігрове дерево гіпергейму

Ліве дерево показує контекст противника (ігрове дерево для GA). Подвійні лінії вказують на сприйняття атакуючим $m^{*|A}$ послідовності ходів, що веде до їх оптимальної сприйманої виграшної парі $u^{*|A} = (10, -10)$. Праве дерево показує контекст захисника (ігрове дерево для G^D). Подвійні лінії вказують на сприйняття захисником $M^{*|D}$ послідовності ходів, що приводить до їх оптимальної сприйманої виграшної парі $u^{*/D} = (-20, 20)$. Пунктирні горизонтальні криві являють собою відповідність між інформаційними наборами гравців.

Загалом визначено кілька концепцій, які відрізняють модель адаптивного кібер-обману від традиційних моделей теорії ігор. Зокрема, сприйняття гравцем можливих ходів, результатів і справжні параметри гри.

Точно таким ж способом сприймаються ходи, як сприйняття окремим гравцем повної послідовності ходів. Наприклад, гравець «А2 сприймає повну послідовність ходів як $m^{*|A} = (m^{A|A}, m^{D|A})$. Якби це будь-яким чином відрізнялося від дійсної послідовності ходів $m = (m^A, m^D)$, гра G^A була б з недосконалої інформацією. Можна припустити всезнаючого захисника, оскільки це найкраще ілюструє потенційну перевагу, яку захисник може отримати, використовуючи

кібер-обман. Всезнаючий захисник володіє досконалою і повною інформацією, тому приймається таке спрощення в якості першого кроку в аналізі кібер-обману [55].

В цілому, ігри кібер-обману, як правило, спираються на маніпуляцію ігровими виграшами. З точки зору захисника, справжні виграші менш релевантні, ніж передбачувані виграші нападника. Це атакуюче сприйняття цінності системи - можливість, якою можливо маніпулювати за допомогою методів обману.

Ключовою концептуальною проблемою в попередніх аналізах кібер-обманних ігор є відсутність повного розуміння того, що самі сприймані виграші можуть бути порушені стратегіями обману, обраними захисниками. Захисники прагнуть змусити супротивників повірити, що системи-приманки мають високу віддачу, а реальні системи-низьку. У багатьох сценаріях маніпуляція сприйманими виграшами є ключовим параметром в оптимізації переваги захисника. Формально описуючи і моделюючи маніпуляції з оцінками виграшів атакуючих і контролюючих спостережуваних стратегій захисників, можна спостерігати динаміку, за допомогою якої ігри з кібер-обманом забезпечують підвищену перевагу захисників [61].

Таким чином контекст противника визначається як похідна гра GA, яка є поглядом атакуючого на гру G у відповідності з його сприйняттям ходів M∗ / A, утиліт $u^{*|A}$ і стратегій $\Theta^{*/A}$. Аналогічно, G^D - це погляд захисника на гру G в контексті захисника, у відповідності з їх сприйняттям послідовностей ходів $M^{*/D}$, утиліт $u^{*|D}$ і стратегій $\Theta^{*/D}$.

У поданій гіпергеймовій моделі ігрове дерево відрізняється в залежності від мети захисника. Це має значення як для гіпергри, так і для окремих підігор. Зокрема, значення виграшу можуть істотно відрізнятися в контексті різних цілей. Наприклад, виграш від мети пов'язаний з ймовірністю того, що зловмисник успішно знайде реальні системи або інформацію, і може грунтуватися виключно на тому, як така інформація прихована. Ймовірність того, що зловмисник випадково взаємодіє з реалістичними системами виглядає приманкою і є нею.

Роблячи приманки більш привабливими, ніж реальні системи, можна збільшити цю ймовірність і ймовірність отримання відповідного виграшу.

Однак одна і та ж гра може мати різні виграші для різних цілей. Мета гіпергейму - затримати атакуючих, поки в системі завершується якась критична діяльність, тоді виграш може бути заснований на кількості часу, який атакуючий витрачає на взаємодію з окремими приманками. Хоча набір стратегій може бути ідентичним, відмінності в цілі гри можуть призвести до різних виграшів, здатних вплинути на вибір абсолютно різних стратегій [61].

Оскільки кібер-ігри масово повторюються, онлайн-навчання є необхідним компонентом адаптивної системи кібер-обману. Захисник повинен спробувати визначити переконання нападника з плином часу і застосувати їх до свого майбутнього прийняття рішень. Оскільки захисник спостерігає, як зловмисник взаємодіє з мережею через інформацію, зібрану його датчиками, захиснику необхідно буде використовувати цю інформацію для моделювання стану атакуючого і оцінки передбачуваних виграшів атакуючого.

Знаючи поточне ігрове дерево і оцінюючи сприйняття атакуючого, захисник тепер може динамічно маніпулювати ігровим полем, щоб змінити виграші, пов'язані з наступними можливими діями. Це ітеративний процес, в якому захисник повинен продовжувати вивчати атакуючого за допомогою спостереження і відповідним чином оновлювати моделі. Прийняті рішення і дії захисника одночасно маніпулюють виграшами, які може отримати атакуючий, і обмежують стратегії, доступні атакуючому на наступному часовому кроці [61].

Висновки до розділу 2

В другому розділі дипломної роботи було:

1. Охарактеризовано принципи управління ризиками. Управління ризиками - це процес прийняття та виконання управлінських рішень, спрямованих на зниження ймовірності виникнення несприятливого результату і мінімізації можливих втрат, викликаних його реалізацією. В рамках управління ризиками здійснюється кількісна та якісна оцінка ймовірності досягнення

передбачуваного результату, невдачі і відхилення від мети. Дотримання основних принципів управління ризиками дозволяє підприємцю ефективніше використовувати ресурси і розподіляти відповідальність, покращувати результати роботи підприємства і забезпечувати його безпеку від дії ризиків. Процес управління ризиком складається із таких етапів: ідентифікація ризику, оцінка ризику, вибір методу та засобів управління ризиком, запобігання ризику, контролювання ризику, фінансування ризику, оцінка остаточних результатів.

2. Проаналізовано процес оцінки ризиків. Оцінка ризиків — це один із процесів в методології управління ризиками. Організації використовують оцінку ризиків для визначення ступеня потенційної загрози та ризику, пов'язаного з IT-системою протягом усього її життєвого циклу. Основним завданням оцінювання ризиків є виявлення можливих видів ризиків, а також властивостей, які впливають на рівень ризику під час проведення підприємницької діяльності. Важливе місце в процесі оцінювання ризику займає визначення усіх обставин і детальний опис усіх видів ризику. Щоб визначити ймовірність майбутньої несприятливої події, загрози для AIC повинні бути проаналізовані в поєднанні з потенційними вразливостями і засобами контролю, що діють для IT-системи.

3. Досліджено використання методології теорії ігор для захисту AIC за допомогою ігрових ризик-моделей. Теорія ігор вивчає проблеми прийняття рішень серед групи гравців і застосовується до ситуацій, коли два або більше гравців мають суперечливі цілі. Теорія ігор може дати уявлення про те, коли і як стратегії повинні бути прийняті кібер-захисником або, в нашому випадку, адаптивною системою кібер-захисту з використанням автоматизованих методів обману. Гра складається з гравців, дій, виплат і стратегій. У послідовних іграх гравці чергують ходи, вибираючи з набору доступних дій в кожній точці. Основна модель, розроблена в кожній з цих робіт, - це модель захисника, що розгортає пастки для виявлення атакуючого і отримання інформації про наміри атакуючого.

4. Охарактеризовано застосування методів теорії ігор для здійснення адаптивного кібер-захисту. Кібер-обман також є новою областю досліджень в

області кібер-захисту. Адаптивний захисний кібер-обман поєднує в собі ці дві концепції для стратегічного представлення дезінформації, яка автоматично змінюється в міру спостереження за змінами в мережі або поведінці зловмисника. Існує безліч методів кібер-обману, обговорюваних в дослідженнях кібер-безпеки, включаючи медові горщики і медові токени, атаки відтворення, Створення пакетів і змінені корисні навантаження, смоляні ями, фальшиві документи, системи приманки та інші. Реалізація адаптивної стратегії кібер-обману в реальному кібер-середовищі вимагає можливостей, які не можуть бути розгорнуті в звичайній мережі. Методи кібер-обману можуть бути використані не тільки для того, щоб затримати, заплутати і здивувати зловмисника. Кібер-обман може бути використаний для більш прямого впливу на атаку. Ігрові моделі кібер-обману вимагають додаткової складності, оскільки вони найкраще моделюються як гібридні ігри з недосконалою і неповною інформацією

РОЗДІЛ 3
МОДЕЛЮВАННЯ ЕФЕКТИВНОСТІ ВИКОРИСТАННЯ ПОМИЛКОВИХ ІНФОРМАЦІНИХ СИСТЕМ

3.1. Аналіз ефективності використання ПІС для захисту АІС

Ефективність помилкової інформаційної системи - це величина, яка виражається у ступені відволікання порушника від об'єкта, який захищається при умові, що ПІС не буде впливати якимось чином на функціонування АІС, що захищається.

Імовірність можливостей запобігання атаки на захищену інформацію за розрахунок використання ПІС, при умові відсутності перевищення затрат обчислювальних ресурсів АІС встановленого рівня, в загальному випадку залежить від часу і може бути оцінена наступним чином [65]:

$$p(t) = \begin{cases} 1 - p_a(t), \text{если } R < R_{доп} \\ 0, \text{если } R > R_{доп} \end{cases}, \quad (3.1)$$

Де $p_a(t)$ - це ймовірність вдалої реалізації атаки на захищену інформацію;

$R_{доп}$ - допустимий рівень затримки обчислювальних ресурсів АІС.

В такому випадку ефективність ПІС, як засобу захисту можна розрахувати з використанням показника [95]:

$$L(t) = p_{лис}(t) - p(t) \quad (3.2)$$

де $p_{лис}(t)$ - це ймовірність запобігти атаці на захищену за допомогою ПІС інформацію.

Відповідно до ігрової моделі прийняття рішень розроблено певний підхід до управління ефективністю ПІС. У зв'язку з тим, що найбільш важливою проблемою ефективної роботи ПІС є невизначеність у частині необхідності створення емульованих об'єктів та витрат ресурсів АІС, за основу методики взято модель захисту ПІС, в якій створення емульованного об'єкт гарантує захист

власного об'єкта, а ефективність роботи повністю залежить від правильності розподілу ресурсів та вчасності створення помилкового об'єкта [67].

Нехай y(t) - це функція, яка описує число емульованих об'єктів ПІС у момент часу t,t > 0. Тоді відсутність помилкових об'єктів не допускається, тобто $y(t) \geq 0$ при всіх t.

Помилкова інформаційна система в будь-який момент часу аналізує трафік з використанням різних засобів, який направлений в АІС. Зловмисник з певною інтенсивністю посилює пакети даних λ_a, які обробляються ПІС [68].

В процесі роботи ПІС зафіксовує виявлені порушення безпеки і емулює помилкові об'єкти з певною інтенсивністю λ_{em}, яка першочергово залежить від інтенсивності аналізу трафіку, тобто за інтервал часу Δt ПІС емулює $\lambda_{em}\ \Delta t$ об'єкти.

У моменти часу $t_0 = 0$, t_1 , … , t_n ПІС аналізує ситуацію та змінює інтенсивність створення помилкових об'єктів у залежності від стратегій зловмисника, що збільшує продуктивність системи величиною Q_0 , Q_1 , … , Q_n відповідно. Таким чином, зміна в час продуктивності y(t) , полягає в можливості емуляція помилкових об'єктів та зображується зубчастою ламаною лінією (рисунок 3.1), що складається з похилих і вертикальних ланок ланцюжка.

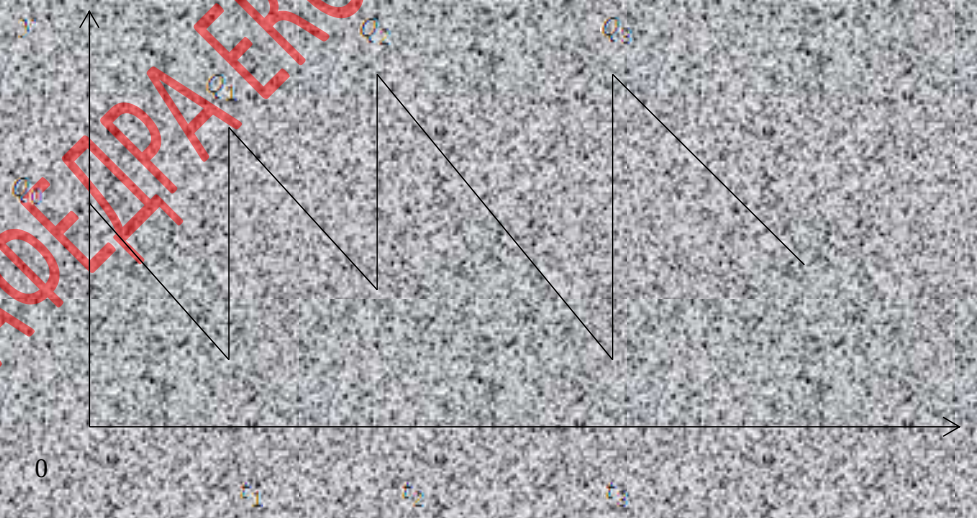

Рисунок 3.1 - Змінення продуктивності ПІС в частині запасу для створення емульованих об'єктів

У момент t_i продуктивність ПІС у частині створення помилкових об'єктів y(t) збільшується на Q_i. Таким чином, функція y(t) має розриви в точках t_1 , … , t_n . У рамках дослідження оптимальності стратегії розвитку АІС враховується те, що ця функція невідривна справа.

Нехай S - плата за обслуговування одиничного помилкового об'єкта протягом одиниці часу. Оскільки можна вважати, що величина запасу об'єктів до емуляції y(t) не змінюється протягом малого інтервалу часу (dt диференціал, тобто є нескінченно мала), то витрати за виділені ресурси протягом інтервалу часу [0:T) , де T - інтервал планування, пропорційні (з коефіцієнтом пропорційності S) площі під графіком y(t) і рівні формулі:

$$Z = S \cdot \int_0^T y(t)dt. \qquad (3.3)$$

Нехай g - плата за збільшення продуктивності ПІС. У рамках дослідження враховується, що g є розробленою системою зміни ресурсів ПІС і не залежить від розміру змін продуктивності.

Нехай n(T) - число змін продуктивності, які надійшли в інтервалі [0:T). При цьому початкова продуктивність включена в момент $t_0 = 0$, але відсутні зміни в момент t = T (якщо такі відбувалися). Тоді сумарні витрати на зміну продуктивності протягом дослідження рівні g * n(T) . Отже, загальна вартість зміни стратегій захисту ПІС і витрат на утримання помилкових об'єктів за час T рівна:

$$F(T;y) = F(y(t), 0 \le t < T) = gn(T) + S\int_0^T y(t)dt. \qquad (3.4)$$

Оскільки емуляція об'єктів відбувається з постійною інтенсивністю і дефіцит не допускається, то користь від роботи ПІС пропорційна прогнозуванню, а середня користь постійна. Отже, максимізація користі еквівалентна мінімізації витрат або середніх витрат на підтримання ефективної роботи ПІС.

Якщо задати моменти зростання продуктивності ПІС і величини числа емульованих об'єктів, то буде повністю визначена функція y = y(t) при всіх 0 ≤ t ≤ T . Тоді правильним буде зворотне - фіксація функції y = y(t), 0 ≤ t ≤ T повністю визначає моменти збільшення продуктивності ПІС і кількість емулюючих об'єктів. І те, і інше називається планом роботи управління ресурсами ПІС. Для його оптимізації необхідно вибрати моменти часу:

$t_0 = 0$, t_1 , … , t_0 , тоді, зростання продуктивності і збільшення числа емулюючих об'єктів буде Q_0 , Q_1 , … , Q_n .

Таким чином, модель роботи ПІС в рамках теорії ігор описується чотирма параметрами:

λ_{em} - (інтенсивність емуляції помилкових об'єктів);

S - (плата за обслуговування одиничного помилкового об'єкта протягом одиниці часу);

g - (плата за збільшення продуктивності ПІС);

T - (горизонт планування).

З метою оптимізації ефективності ПІС необхідно вибрати значення параметрів так, щоб мінімізувати середні витрати роботи ПІС при фіксованому T.

У зв'язку з тим, що власник АІС зацікавлений в мінімізації витрат на надлишкову продуктивність, оптимальний план потрібно обирати серед тих, у яких всі зубці доходять до осі абсцис, тобто збільшення продуктивності необхідно проводити в момент, коли запас об'єктів до емуляції дорівнює 0.

План, для якого запас продуктивності для емуляції дорівнює 0 (тобто, y = = y(t) = 0 називається напруженим.

Зазвичай від довільного плану завжди можна перейти до напруженого, зменшивши при цьому витрати. Нехай з плином часу при наближенні до моменту t_1 збільшення продуктивності Q_1 рівень ресурсів не прагне до 0, а лише зменшується до $y(t_1 - 0) > 0$. Тоді розглянемо новий план збільшення продуктивності з тими ж моментами збільшення і їх величинами, за винятком величин в моменти $t_0 = 0$ і $t = t_1$.

Тепер замінимо:

Q_0 на $Q_{01} = Q_0 - y(t_1 - 0)$

Q_1 на $Q_{11} = Q_1 - y(t_1 - 0)$

Тоді графік рівня ресурсів ПІС паралельно зрушиться вниз на інтервалі (0,t), досягнувши 0 в t, і не зміниться правіше точки t (рисунок 3.2).

Рисунок 3.2 - Графічне представлення напруженого плану

Таким чином, витрати по збільшенню продуктивності не зміняться, а витрати по зайвому виділенню ресурсів зменшаться на величину g, пропорційну з коефіцієнтом пропорційності площі паралелограма, утвореного колишнім і новим положеннями графіка рівня ресурсів на інтервалі (0,t).

В результаті першого кроку отримано план, в якому крайній зліва зубець досягає осі абсцис. Наступний крок проводиться аналогічно, тільки момент часу $t_0 = 0$ замінюється на $t = t_1$.

Якщо є така можливість, друге похиле ланка графіка рівня ресурсів ПІС паралельно зсувається вниз, досягаючи в крайній правій точці t_2 осі абсцис. Аналогічно робимо з усіма іншими зубцями, рухаючись зліва направо. В результаті отримуємо напружений план.

На кожному кроці витрати по зайвому виділенню ресурсів або скорочувалися, або залишалися попередніми (якщо відповідна ланка графіка не знижувалась). Отже, для отриманого в результаті описаного перетворення напруженого плану витрати по зайвому виділенню ресурсів є меншими, ніж для вихідного плану, або рівні (якщо вихідний план вже був напруженим).

Наступним кроком необхідно оптимізувати інтервали між збільшенням продуктивності.

При фіксованому числі поставок витрати на збільшення ресурсів не змінюються. Отже, буде достатньо мінімізувати витрати на обслуговування помилкових об'єктів.

Для напружених планів збільшення продуктивності визначається за допомогою інтервалів між збільшенням продуктивності:

$$Q_{i-1} = \lambda_{em}(t_i - t_{i-1}), i = 1,2,\dots,n(T) - 1, \tag{3.5}$$

$$Q_{n(T)-1} = \lambda_{em}(T - t_{n(T)-1}). \tag{3.6}$$

Зазвичай чергове збільшення продуктивності Q_{i-1} є однаковим з розміром ресурсів в момент t_{i-1}, та витрачається з інтенсивністю λ_{em} одиниць емулюючих об'єктів в одну одиницю часу і повністю вичерпується до моменту t_1.

Отже, для мінімізації обслуговування помилкових об'єктів серед напружених планів з фіксованим числом поставок досить вирішити завдання оптимізації:

$$\begin{cases} \Delta_1^2 + \Delta_2^2 + \dots + \Delta_n^2 \to \min, \\ \Delta_1 + \Delta_2 + \dots + \Delta_n = T, \\ \Delta_i \geq 0, i = 1,2,\dots,n. \end{cases} \tag{3.7}$$

Введемо нові змінні:

$$\alpha_i = \Delta - \frac{T}{n}, \tag{3.8}$$

Тоді:

$$\sum_{i=1}^{n} \alpha_i = \sum_{i=1}^{n} \left(\Delta_i - \frac{T}{n}\right) = \sum_{i=1}^{n} \Delta_i - T = T - T = 0. \tag{3.9}$$

Сума квадратів є завжди додатною. Вона досягає мінімуму, рівного 0, коли всі змінні рівні 0, тобто при:

$$\alpha_1 = \alpha_2 = \cdots = \alpha_n = 0.$$

Тоді:

$$\Delta_i = \frac{T}{n}, i = 1,2,\ldots,n.$$

При таких значеннях Δ_i виконані всі обмеження оптимізаційної задачі по зниженню витрачених ресурсів. Таким чином, витрати на обслуговування емулюючих помилкових об'єктів рівні:

$$S\int_0^T y(t)dt = \frac{S\lambda_{эм}}{2}\sum_{i=1}^{n(T)}\Delta_i^2 = \frac{S\lambda_{эм}T^2}{2n(T)}, \quad (3.10)$$

Середні витрати (на одиницю часу) такі:

$$f(T;y) = \frac{1}{T}\left\{gn(T) + \frac{S\lambda_{эм}T^2}{2n(T)}\right\} = \frac{gn(T)}{T} + \frac{S\lambda_{эм}T}{2n(T)}. \quad (3.11)$$

Завдання полягає в мінімізації по Q. При цьому можлива величина поставки приймає дискретні значення, так як:

$$Q \in \left\{\frac{nT}{n}, n = 1,2\ldots\right\} \quad (3.12)$$

Вивчимо функцію $f_1(Q)$, визначену при $Q > 0$. При наближенні до 0 вона веде себе як гіпербола, а при зростанні аргументу, як лінійна функція. Похідна має вигляд:

$$\frac{df_1(Q)}{dQ} = -\frac{\lambda_{эм}g}{Q^2} + \frac{S}{2}. \quad (3.13)$$

Похідна монотонно зростає, тому розглянута функція має єдиний мінімум:

$$Q_0 = \sqrt{\frac{2\lambda_{эм}g}{S}}, \quad (3.14)$$

Де Q_0 - функція, що описує запас ресурсів ПІС;

λ_{em} - інтенсивність емуляції помилкових об'єктів;

g - плата за збільшення продуктивності ПІС;

S - плата за обслуговування одиничного помилкового об'єкта протягом одиниці часу.

Таким чином, дослідивши функцію, яка описує витрати на підтримку продуктивності ПІС з метою своєчасного створення емулюючих об'єктів, було розроблено формулу з управління оптимальністю запасу ресурсів, необхідного ПІС для підтримки успішного протистояння зловмисникові.

3.2. Оптимізація ресурсів, які використовує ПІС в процесі роботи

Розглянемо проблему оптимізації ресурсів ПІС із заданими параметрами та з подальшим управлінням. Нехай ПІС з ціллю підтримки захищеності АІС протягом 80 секунд від реалізації атаки зловмисника з інтенсивністю необхідно емулювати 30 одиниць помилкових об'єктів за 1 секунду. Вартість підтримки одного емулюваного об'єкта в працездатному стані протягом 1 секунди складає 100 грн. Періодична плата за збільшення продуктивності ПІС становить 25.000 грн. Сформуємо оптимальний план підтримки ПІС в стані постійної захищеності протягом 80 секунд і дослідимо оптимальність при зміні параметрів.

В такому випадку λ = 20 (од / sec), S = 100 (грн. / од. sec), g = 26000 (грн. / Ресурси),

T = 30 (sec). За формулою (3.17) розраховуємо

$$Q_0 = \sqrt{\frac{2\lambda g}{S}} = \sqrt{\frac{2 * 20 * 26000}{100}} = 101$$

Множина допустимих значень для Q має вигляд:

$$\left\{\frac{\lambda T}{n}, n = 1, 2, \dots\right\} = \{600, 300, 200, 150, 120, 100, \dots\}$$

Таким чином, Q_1 = 100 , а , Q_2 = 120. Перше значення визначає напружений план з шістьма зубцями, друге - з п'ятьма.

$$f_1(Q) = \frac{20 * 26000}{Q} + \frac{100 * Q}{2} = \frac{52000}{Q} + 50 * Q$$

В такому випадку:

$f_1(Q_1) = f_1(100) = 52000/100 + 5000 = 5520,$

$f_1(Q_2) = f_1(120) = 52000/120 + 6000 = 6433.$

Так як $f_1(Q_1) < f_1(Q_2)$ то $Q_{opt} = Q_1 = 100$

Таким чином, можна зробити висновок про те, що оптимальним є напружений план з шістьма зубцями.

Рисунок 3.4 - Оптимальне управління ресурсами ЛИС

Оцінимо зайві витрати на ресурси в порівнянні з планом Q_0. Для плану з $Q = Q_0$ інтервал між поставками складає:

$$\frac{Q_0}{\lambda} = \frac{101}{20} = 5{,}05\ sec$$

Таким чином поповнення ресурсів ЛИС з метою емуляції об'єктів відбудуться в моменти:

$t_0 = 0$ sec

$t_1 = 5{,}05$ sec

$t_2 = 10{,}1$ sec

$t_3 = 15{,}15$ sec

$t_4 = 20{,}2$ sec

t_5 = 25,25 sec

Наступний етап поповнення ресурсів мав би відбутися за межами планованого проміжку захищеності T = 30 sec., В момент t_6 = 30,3 sec

Таким чином, оптимальний рівень ресурсів складався б з 5 повних циклів збільшення продуктивності і одного неповного. До моменту T = 30 sec. пройде 30 – 25,25 = 4,75 sec, з моменту останнього збільшення ресурсів. Таким чином до моменту T будуть міститися ресурси, що дають можливість емулювання додаткову кількість помилкових об'єктів.

План $Q = Q_0$ не є напруженим, а тому не є оптимальним в рамках даного завдання. Оскільки залишилася можливість емулювати ще помилкові об'єктів, за обслуговування необхідно платити.

Загальні витрати на емулювання помилкових об'єктів за оптимальним планом складуть:

u = 25.25 * 100 = 2525 грн

Таким чином, через дискретність більшість допустимих значень, витрати зросли, при цьому оптимальний розмір партії Q = 100 одиниць/sec відрізняється від Q0 = 101 одиниць/sec на 1 одиницю, таким чином відмінність становить 1%.

3.3. Оцінка проведення організаційно-економічного дослідження ефективності використання ПІС на підприємстві

Проведемо розрахунок витрат для розробки математичних моделей, оцінки ризиків та аналізу ефективності роботи помилковою інформаційної системи при реалізації атак з урахуванням роботи ПІС.

В ході дослідження наявні наступні етапи:

- вивчення помилкових інформаційних систем;
- аналіз сучасних неправдивих інформаційних систем;
- оцінка ризиків кібератак на інформаційні системи;
- складається сценаріїв ігор для адаптивного оборонного кібер-обману;
- аналіз знайдених вразливостей і можливих напрямків атак.

Вартість аналізу визначається за фактичними витратами. В основі визначення вартості лежить перелік виконаних робіт та її трудомісткість.

Трудомісткість – показник, що характеризує витрати робочого часу на виробництво певної споживної вартості або на виконання конкретної операції.

Для визначення трудомісткості виконання робіт визначимо перелік основних етапів та видів робіт. По кожному виду робіт визначається також кваліфікаційний рівень виконавців.

Трудомісткість виконання аналізу визначимо за сумою трудомісткості етапів і видів робіт, оцінюваних в людях на день. Розподіл робіт за видами і кваліфікаційним рівнем виконавців, та величини трудомісткості для проведеного проекту наведені в таблиці 4.1.

Таблиця 4.1

Розрахунок трудомісткості

№	Етапи виконуваних робіт	Трудомісткість, люд./дні	
		Головний інженер	Інженер
1.	Розробка та уточнення технічного завдання	2	2
2.	Вивчення оцінки ризиків	4	4
3.	Вивчення підсистеми	1	1
4.	Аналіз можливих атак	3	3
5.	Аналіз сучасних засобів захисту	2	2
6.	Побудова моделі захисту АІС за допомогою ПІС	4	3
7.	Оформлення звіту	0	2
8.	Здача аналізу	1	1
9.	Підсумок	17	18

На основі трудомісткості виконання робіт буде розраховані витрати на оплату праці її виконавців.

Основна заробітна плата – це винагорода за виконання роботи відповідно до встановлення норм праці (годину, виробітку, обслуговування, посадових обов'язків) [41].

Основна заробітна плата виконавців аналізу розраховується на підставі наступних даних:

- трудомісткість виконання робіт $T_{гол.\ інж}$ та $T_{інж}$;
- оклад керівника проекту, головного інженера, за місяць (двадцять два робочих дня) складає 25 000 грн., денна ставка восьми часового робочого дня керівника проекту складає $C_{гол.інж.} = 1136,36$ грн.;
- оклад інженера за місяць (двадцять два робочих дня) складає 15 300 грн., денна ставка восьми часового робочого дня інженера складає $C_{інж.} = 681,82$ грн;
- єдиний соціальний внесок ЄСВ = 22%;
- відсоток додаткової заробітної плати = 15%;
- накладні витрати = 40 %.

Основна заробітна плата виконавців ($З_{осн\ з/пл}$) розраховується за такою формулою:

$$З_{осн.з/пл} = T_{гол.інж.} * C_{гол.інж.} + T_{інж.} * C_{інж.} \quad (4.1)$$

$$З_{осн.з/пл} = 17 * 1136,36 + 18 * 681,82 = 31590,88 \text{ грн}.$$

Додаткова заробітна плата — це винагорода за понаднормативну працю, трудові успіхи та винахідливість і за особливі умови праці. Вона включає доплати, надбавки, гарантії та компенсації, передбачені чинним законодавством, премії, пов'язані з виконанням виробничих завдань та функцій [41].

Додаткова заробітна плата виконавців (Здодат з/пл) розраховується за формулою:

$$З_{додат.з/п} = З_{осн.з/пл*15/100} \quad (4.2)$$

$$З_{додат.з/пл} = 31590,88 * 0,15 = 4738 \text{ грн}.$$

Єдиний соціальний внесок - обов'язковий платіж до системи загальнообов'язкового державного соціального страхування, що справляється в

Україні з метою забезпечення страхових виплат за поточними видами загальнообов'язкового державного соціального страхування [42].

Внески розраховуються за формулою:

$$В_{соц.} = (З_{осн.з/пл} + З_{додат.з/пл}) * ЄСВ/100 \quad (4.3)$$

$$В_{соц.} = (31590 + 4738)*0,22 = 7992 \text{ грн}$$

Накладні витрати – це витрати не пов'язані безпосередньо з технологічним процесом на виготовлення продукції, а утворюються під впливом певних умов роботи з організації, управління та обслуговування виробництва [43].

Накладні витрати розраховуються за формулою:

$$НВ= (З_{осн.з/пл} + З_{додат.з/пл}) *40/100 \quad (4.4)$$

$$НВ = 31590 + 4738 *0,4 = 14531 \text{ грн.}$$

Вартість витратних матеріалів, необхідних для виконання роботи, визначається виходячи з величини їх витрат, діючих цін і транспортних витрат. В даному розрахунку відносяться використані при виконанні аналізу матеріалів - таблиця 4.2.

Таблиця 4.2

Калькуляція витрат

Матеріал	Од. виміру	Кількість	Ціна, грн.	Сума, грн.
Папір для принтера	пачка	2	150	300
Картридж для принтера	штука	2	429	858
Транспортні витрати			20	
Загалом				1158

Для розробки ризик-моделі використовувалась стороння організація: «Aidstest».

$С_{інтер.}$ = 120 грн /місяц.

Податок на додану вартість (ПДВ) - це непрямий податок, який входить в ціну товарів (робіт, послуг) і сплачується покупцем, але його облік і перерахування до державного бюджету здійснює продавець (податковий агент). ПДВ складає 20 %.

Для розрахунку витрат ($В_{інтер}$), скористаємося формулою:

$В_{інтер} = Т_{інтер} х С_{інтер}$. (4.5)

$В_{інтер.} = 1*(1500*1,2)= 1800$ грн

Витрати, пов'язані з утриманням техніки, є складовою всіх витрат підприємства. Усі витрати на утримання техніки поділяють на постійні і змінні. Постійні витрати - це витрати, які не залежать від інтенсивності використання техніки - кількості годин роботи або виконаного обсягу робіт [44].

Змінні витрати на техніку безпосередньо пов'язані з її експлуатацією. До них відносять витрати на паливо і мастила, ремонт техніки, оплату праці робітників, які її обслуговують, інші витрати [44].

При розробці методики використовувалося обладнання у вигляді двох комп'ютерів з первісною вартістю 15 000 грн. кожен. Для них необхідно прорахувати витрати на електроенергію і амортизаційні відрахування.

Так само буде враховуватися освітлення, необхідне для роботи. Всі ці витрати розраховуються на підставі наступних даних:

- розмір тарифу споживання електроенергії $С_{ел} = 0,5$ грн кВт * ч;
- розмір споживання комп'ютером за 8 годин роботи $К_{ел.} = 1,70$ кВт;
- розмір споживання освітленням за 8 годин роботи $О_{ел.} = 2,50$ кВт;
- первісна вартість комп'ютера $В_{комп.} = 15\ 000$ грн.;
- час використання основного засобу інженером Твик інж =2 місяці;
- час використання основного засобу головним інженером $Т_{вик.гол.інж.} = 2$ місяці;
- термін амортизації комп'ютера = 36 місяців, норма амортизації комп'ютера за 3 місяці На = 8 %;
- коефіцієнт для розрахунку коштів не враховуючи 20 % ПДВ = 1,2.

Для розрахунку витрат на електроенергію на комп'ютери (Зелкомп), скористаємося формулою:

$В_{ел.комп} = (Т_{гол.інж} + Т_{інж.}) * К_{ел} * (С_{ел.}/1,2)*8$ (4.6)

$В_{ел.комп.} = (8 + 15) * 1,70 * 0,4 * 8 = 125,12$ грн.

Для розрахунку витрат на

($В_{ел.осв.}$), скористаємося формулою:

$В_{ел.осв} = (Т_{гол.інж} + Т_{інж.}) * О_{ел.} * (С_{ел.}/1,2) * 8$ (4.7)

$В_{ел.осв.} = (8 + 15)$ X 2,50 X 0,4 X 8 = 184 грн .

Загальні витрати на електроенергію ($В_{заг.ел}$) є сумою витрат електроенергії, що пішла на комп'ютери ($В_{ел.комп}$) і освітлення ($В_{ел. осв}$) скористаємося формулою:

$В_{заг.ел.} = В_{ел.комп.} + В_{ел.осв.}$ (4. 8)

$В_{заг.ел}$= 125,12 + 184 = 309,12 грн.

Амортизаційні відрахування – процес поступового перенесення вартості основних засобів на продукт, що виготовляється з їх допомогою. Для заміщення зношеної частини основних засобів виробництва підприємства роблять амортизаційні відрахування, тобто відрахування певних грошових сум відповідно до розмірів фізичного і морального зносу засобів виробництва [45].

Розрахуємо амортизаційні відрахування по основному засобу за 3 місяці:

$А_{комп.} = В_{комп.} * (Н_а/100)$ (4.9)

$А_{комп.} = 15\,000 \times 0,08 = 1200$ грн.

Обчислимо амортизаційні відрахування по основному засобу для кожного з виконавця щодо часу його використання:

$А_{інж} = А_{комп} * (Т_{вик\ інж}/12)$ (4.10)

$А_{інж.} = 1200$ X — = 192 грн.

$А_{інж.} = 1200 \times 2/12 = 192$ грн.

Загальна амортизація є сумою амортизації інженера і головного інженера:

$А = А_{гол.інж.} + А_{інж.}$ (4.11)

А = 78 + 156 = 270 грн.

Кошторис витрат являє собою зведений план усіх витрат підприємства виробничо-фінансової діяльності за певний календарний період. До кошторису включаються витрати основного і допоміжного виробництва, пов'язані з виготовленням та продажем продукції, товарів і послуг, а також на утримання адміністративно-управлінського персоналу, виконання різних робіт і послуг, у тому числі і не входять в основну виробничу діяльність підприємства [11].

Таблиця 4.3

Загальний кошторис витрат

№	Найменування статті	Сума, грн.
1.	Витрати на оплату праці	31590,88
2.	Єдиний соціальний внесок	7992
3.	Витрати на матеріали	1158
4.	Витрати на послуги сторонніх організацій	1800
5.	Витрати на утримання, експлуатацію та амортизацію обладнання	309,12
6.	Амортизаційні відрахування	270
7.	Накладні витрати	14531
Загалом витрат		57651

Таким чином, загальні витрати на оцінку ефективності впровадження ПІС в АІС на підприємстві будуть становити 57 651 грн.

Висновки до розділу 3

В 3 розділі було:

1. Розроблено модель ефективності використання ПІС для захисту АІС. Побудова помилкових інформаційних систем відбувається так, щоб привернути увагу порушника особливо на помилкові об'єкти. В якості причин, за якими порушник може звернути на них увагу, може бути найменш захищена частина системи. Таким чином, дослідивши функцію, яка описує витрати на підтримку продуктивності ПІС з метою своєчасного створення емулюючих об'єктів, було розроблено формулу з управління оптимальністю запасу ресурсів, необхідного ПІС для підтримки успішного протистояння зловмисникові.

2. Здійснено оптимізацію ресурсів, які використовує ПІС в процесі роботи. Отже, розроблений підхід до управління роботою ПІС базується на оптимізації продуктивності, яку виділяє ПІС для емулювання нових помилкових об’єктів.

Крім цього, алгоритм управління ефективністю ПІС забезпечує оптимальність отриманого значення ресурсів для ефективного і практичного застосування методики. На основі розрахунків план $Q = Q_0$ не є напруженим, а тому не є оптимальним в рамках даного завдання. Оскільки залишилася можливість емулювати ще помилкові об'єктів. Загальні витрати на емулювання помилкових об’єктів за оптимальним планом складуть: 2525 грн. Таким чином, через дискретність більшість допустимих значень, витрати зросли, при цьому оптимальний розмір партії Q = 100 одиниць/sec відрізняється від Q0 = 101 одиниць/sec на 1 одиницю, таким чином відмінність становить 1%.

3. Оцінено проведення організаційно-економічного дослідження ефективності використання ПІС на підприємстві. Витрати на дослідження ефективності впровадження ПІС в АІС на підприємство є доцільними, оскільки в майбутньому це допоможе доповнювати засоби захисту інформаційних систем за допомогою помилкових інформаційних систем та збільшиться рівень забезпечення безпеки, що дозволить уникнути підприємству великих фінансових втрат. Загальні витрати на оцінку ефективності впровадження ПІС в АІС на підприємстві будуть становити 57 651 грн.

ВИСНОВКИ

В результаті проведеного наукового дослідження були отримані наступні висновки;

1. Охарактеризовано помилкові інформаційні системи їх види та причини використання. Помилкові інформаційні системи використовують для реалізації механізму введення порушника в оману. Такий принцип застосовують для нав'язування порушнику певним спеціальним способом зарання підготовленої помилкової інформації чи помилкових об'єктів щоб чим більше обтяжити й ускладнити атаки на інформаційні системи, що захищаються. Помилкові інформаційні системи використовують як ресурс безпеки, призначення якого – це дослідження атак з сторони порушників. Таким чином, непрямий вплив ПІС на підвищення безпеки інформаційних систем, що захищаються проявляється у виявленні стратегії, методів і засобів порушника, а отримана інформація використовується для наступних підсилень захисних алгоритмів.

2. Досліджено автоматизовані інформатизовані системи. Автоматизовані інформаційні системи – це ІС до яких належить сукупність інформації, економіко-математичних методів і моделей, технічних і програмних засобів, організованих на базі інформаційної технології. У стадії формування вимог до АІС включається комплекс науково - дослідних і організаційно-технічних заходів з обстеження, що дозволяють визначити виробничі можливості підприємства щодо підвищення прибутку, зниження витрат в результаті створення ІС. Проводиться техніко-економічне обстеження, що включає системний опис конкретного об'єкта, діагностичний аналіз в системах управління і дослідження інформаційних потоків.

3. Проаналізовано принципи управління ризиками та методологію їх оцінки. В основному, якісна оцінка ризиків це оцінка середовища за якого виникає ризик та визначення його впливу на діяльність суб'єкта стандартними методами і засобами. Визначення ризику для ІТ-системи вимагає глибокого розуміння середовища обробки системи. Аналіз і управління інформаційними ризиками – це один з основних процесів, які визначають ефективність системи

забезпечувати інформаційну безпеку. При розробці системи безпеки, яка має варіативні заходи і методи забезпечення інформаційної безпеки, саме аналіз інформаційних ризиків визначає якість і практичність роботи усієї системи. Для якісного забезпечення процесу управління ризиком для АІС необхідно розробити стратегію управління ним, яку будуть застосовувати в моменти невизначеності та яка буде грунтуватися на оцінці ймовірності ризику і методах його мінімізації. Мінімізація негативного впливу на організацію та необхідність надійної основи для прийняття рішень є фундаментальними причинами, за якими організації впроваджують процес управління ризиками для своїх ІТ-систем. Ефективне управління ризиками має бути повністю інтегровано в життєвий цикл розробки системи

4. Охарактеризовано методологію теорії ігор для здійснення адаптивного кібер-захисту АІС. Теорію ігор застосовують для вирішення ситуацій, в яких результат рішень гравців залежить не від того, як вони їх вибирають, а і від вибору рішень інших гравців, з якими вони взаємодіють в даній грі. Основною задачею теорії ігор є виявлення оптимальних стратегій інших гравців. Базове припущення, застосовуючи яке знаходять найефективніші стратегії, полягає в тому, що противник такий ж розумний, як і сам гравець, і робить все щоб досягти своєї цілі. Тому теоретико-ігровий підхід повинен допомогти розробити таку стратегію створення ЛІС, яка б забезпечила найкращий підхід. Реалізація адаптивної стратегії кібер-обману в реальному кібер-середовищі вимагає можливостей, які не можуть бути розгорнуті в звичайній мережі. Методи кібер-обману можуть бути використані не тільки для того, щоб затримати, заплутати і здивувати зловмисника. Кібер-обман може бути використаний для більш прямого впливу на атаку. Ігрові моделі кібер-обману вимагають додаткової складності, оскільки вони найкраще моделюються як гібридні ігри з недосконалою і неповною інформацією. Проте адаптивні системи кібер-захисту АІС все ще перебувають у зародковому стані, і кібер-обман - це лише невелика частина системи кібер-захисту. Зосередження на адаптивних системах кібер-обману та використання теорії ігор є досить важливим для створення автономних

систем кібер-обману, які можуть вирішувати, коли, де і як найкраще використовувати обман на основі поведінки атакуючого.

5. Розроблено модель аналізу ефективності використання помилкових ІС для захисту автоматизованих ІС. На практичному прикладі було обчислено та доведено практичність підходу управління ПІС для функцій захисту, який заснований на оптимізації продуктивності, яка виділяється на емулювання помилкових об'єктів. Дана методика дозволить здійснити перехід від кількісних до якісних принципів аналізу функціонування ПІС.

6. Проведено оптимізацію ефективності використання ресурсів помилковою інформаційною системою для здійснення захисту АІС. Алгоритм управління ефективністю ПІС забезпечує оптимальність отриманого значення ресурсів для ефективного і практичного застосування розглянутої методики. Розрахунки проведені згідно з даною методикою, дозволили визначити оптимальний план поповнення ресурсів ПІС на рівні 100 одиниць емульованих помилкових об'єктів і довести оптимальність отриманого значення, оцінив додаткові витрати у сумі 2525 грн.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Александров Д. В. Інструментальні засоби інформаційного менеджменту. CASE-технології та розподілені інформаційні системи: Навчальний посібник / Д.В. Александров. - М.: ФІС, 2011. - 224 с.

2. Алієв В. С. Інформаційні технології та системи фінансового менеджменту: Навчальний посібник / В. С. ОГЛИ Алієв. - М.: Форум, Інфра-М, 2011. - 320 с.

3. Балдін К. В. Інформаційні системи в економіці: Навчальний посібник(ГРИФ) / К. В. Балдін. - М.: Інфра-М, 2012. - 218 с.

4. Бліновська Я. Ю. Введення в геоінформаційні системи: Навчальний посібник / Я. Ю. Бліновська, Д. С. Задоя. - М.: Форум, НДЦ Інфра-М, 2013. - 112 с.

5. Бодров О. А. Предметно-орієнтовані економічні інформаційні системи / О.А Бодров. - М.: ГЛТ, 2013. - 244 с.

6. Бородакій Ю.В. Інформаційні технології. Методи, процеси, системи / Ю.В. Бородакій, Ю. Г. Лободинський. - М.: ГЛТ, 2004. - 456 с.

7. Брусакова І.А. Інформаційні системи і технології в економіці / і. А. Брусакова, В. Д. Чертовски. - М.: Фінанси і статистика, 2007. - 352 с.

8. Буреш, О.В. Інтелектуальні інформаційні системи управління соціально-економічними об'єктами / о. в. Буреш, М. А. Жук. - М.: Красанд, 2012. - 192 с.

9. Варфоломєєва, А.О. Інформаційні системи підприємства: Навчальний посібник / А. О. Варфоломєєва, а. в. Коряковський, в. п. Романов. - М.: ніц Інфра-М, 2013. - 283 с.

10. Вдовін, В.М. Предметно-орієнтовані економічні інформаційні системи: Навчальний посібник / В. М. Вдовін, л. є. Суркова, А. а. Шурупов. - М.: Дашков і К, 2016. - 388 с.

11. Гвоздьова, В.А. Інформатика, автоматизовані інформаційні технології та системи: Підручник / В. А. Гвоздьова. - М.: ІД ФОРУМ, ніц Інфра-М, 2013. - 544 с.

12. Гришин, А.В. Промислові інформаційні системи та мережі: практичне керівництво / а. в. Гришин. - М.: радіо і зв'язок, 2010. - 176 с.

13. Данелян, Т.Я. Економічні інформаційні системи (ЕІС) підприємств і організацій: Монографія. / Т.Я. Данелян . - М.: юніті, 2015. - 284 с.

14. Дворкович, В.П. Цифрові відеоінформаційні системи (Теорія і практика) / В. П. Дворкович, А. В. Дворкович. - М.: Техносфера, 2012. - 1008 с.

15. 33. Ємельянов, С.В. Інформаційні технології та обчислювальні системи / С. в. Ємельянов. - М.: Ленанд, 2011. - 84 с.

16. Єрмолін, Н. П. Інформаційні системи в економіці. Практикум / Н.П. Єрмолін. - М.: КноРус, 2012. - 256 с.

17. Заварина, Є. С. Інструментальні засоби інформаційного менеджменту. CASE-технології та розподілені інформаційні системи: Навч. посібник / Є.С. Заварина. - М.: Фінанси і статистика, 2011. - 224 с.

18. Золотова, Є.В. Основи кадастру: територіальні інформаційні системи / Є. В. Золотова. - М.: академічний проект, 2012. - 416 с.

19. Іванкін, Е.Ф. Інформаційні системи з апостеріорною обробкою результатів спостережень / Е. Ф. Іванкін. - М.: ГЛТ, 2008. - 168 с.

20. Іванкін, Е. Ф. Інформаційні системи з апостеріорною обробкою результатів спостережень. / Е. Ф. Иванкин. - М.: ГЛТ, 2009. - 168 с.

21. Ісаєв, Г. Н. Інформаційні системи в економіці: Підручник для студентів вузів / Г. н. Ісаєв. - М.: Омега-Л, 2013. - 462 с.

22. Калашян, А. Н. Інформаційні системи в економіці: в 2-х ч. ч. 2. Практика використання: Навчальний посібник / А. Н. Калашян. - М.: Фінанси і статистика, 2006. - 240 с.

23. Кармінський, А.М. Інформаційні системи в економіці: в 2-х ч. ч. 2. Практика використання / А.М. Кармінський, Б. В. Черніков. - М.: Фінанси і статистика, 2006. - 240 с.

24. Кармінський, А.М. Інформаційні системи в економіці: в 2-х ч. ч. 1. Методологія створення / А.М. Кармінський, Б. В. Черніков. - М.: Фінанси і статистика, 2006. - 336 с.

25. Косиненко, Н.С. Інформаційні системи і технології в економіці: Навчальний посібник / Н.С. Косиненко, і. Г. Фризен. - М.: Дашков і к, 2015. - 304 с.

26. Косиненко, Н. С. Інформаційні системи і технології в економіці: Навчальний посібник для бакалаврів / Н. С.Косиненко, і. Г. Фризен. - М.: Дашков і к, 2015. - 304 с.

27. Кувшинов, М. С. Інформаційні системи в економіці. Управління ефективністю банківського бізнесу / м.с. Кувшинов. - М.: КноРус, 2013. - 176 с.

28. Ліхтенштейн, В. Є. Інформаційні технології в бізнесі. Практикум: застосування системи Decision в мікро - і макроекономіці: Навчальний посібник / В.Є. Ліхтенштейн. - М.: ФІС, 2008. - 512 с.

29. Авчаров І. В. Боротьба з кіберзлочинністю / і. в. Авчаров. // Інформатизація та інформаційна безпека правоохоронних органів. XI міжн. конф. - М., 2012. - С. 191-194.

30. Айков Д. В. Комп'ютерні злочини. Керівництво по боротьбі з комп'ютернимй злочинами / Д.Айков, К. Сейгер, у. Фонсторх. - М.: Світ, 2014.- 351 с.

31. Биков В. С. Удосконалення кримінальної відповідальності за злочини, пов'язані з комп'ютерними технологіями / в. Биков, а. нехороше, в. Черкасов. // Кримінальне право. 2013. - № 3. - С. 9-11.

32. Вехов В.Б. Комп'ютерні злочини: способи вчинення і розкриття / в. Б. Вехов; під ред. акад. Б. П. Смагоринського. - М.: Право і закон, 2014.- 182 с.

33. Лукацький, Олексій виявлення атак / Олексій Лукацький . - М.: BHV-Санкт-Петербург, 2016. - 596 с.

34. Митник, К. Привид в мережі. Мемуари найбільшого хакера / К.Митник, В. Л. Саймон. - М.: Видавництво "Ексмо" ТОВ, 2016. - 416 с.

35. Новак Дж. Як виявити вторгнення в мережу. Настільна книга фахівця з системного аналізу / Джуді Новак, Стівен Норткатт, Дональд Маклахен. - М.: Лорі, 2012. - 384 с.

36. Керівництво для програміста на Java. 75 рекомендацій з написання надійних і захищених програм. - М.: Вільямс, 2014. - 256 с.

37. Скляров, Д. Мистецтво захисту і злому інформації / Д.Скляров . - М.: БХВ-Петербург, 2012. - 288 с.

38. Скляров, ІВАН Скляров (+CD-ROM) / Іван Скляров . -М.: БХВ-Петербург, 2011. - 320 с.

39. Скляров, ІВАН хакерські фішки / Іван Скляров . - М.: Лорі, 2010. - 384 с.

40. Соколов, А. В. Захист від комп'ютерного тероризму. Довідковий посібник / А.В. Соколов, О. М. Степанюк. -М.: БХВ-Петербург, 2012. - 496 с.

41. Фленов, М. Web-сервер очима хакера / м.Фленов . -М.: БХВ-Петербург, 2013. - 320 с.

42. Фленов, М. Комп'ютер очима хакера / м.Фленов . -М.: БХВ-Петербург, 2012. - 272 с.

43. Фленов, Михайло Linux очима хакера (+CD-ROM) / Михайло Фленов. -М.: БХВ-Петербург, 2010. - 480 с.

44. Фленов, Михайло Комп'ютер очима хакера (+CD-ROM) / Михайло Фленов. -М.: БХВ-Петербург, 2016. - 336 с.

45. . Харріс, Шейн Кібервойн@. П'ятий театр військових дій / Шейн Харріс. - М.: Альпіна нон-фікшн, 2016. - 392 с.

46. Холмогоров, Валентин Pro Віруси/Валентин Холмогоров . - М.: Страта, 2015. - 142 с.

47. Еріксон, Джон Хакінг. Мистецтво експлойта / Джон Еріксон. - М.: Символ-плюс, 2010. - 512 с.

48. Leman Akoglu, Rishi Chandy, and Christos Faloutsos. Opinion fraud detection in online reviews by network effects. Proceedings of the 7th International AAAI Conference on Web and Social Media, 2013.

49. Leman Akoglu, Mary McGlohon, and Christos Faloutsos. Oddball: Spotting anomalies in weighted graphs. In Advances in Knowledge Discovery and Data Mining. Springer, 2010.

50. Jonathan Albright. Data is the real post-truth, so here's the truth about post-election2016 propaganda. https://medium.com/@d1gi/ data-is-the-real-post-truth-so-heres-the-truth-about-post-\election2016-propaganda-2bff5ae1dd7.

51. Jonathan Albright. The election2016 micro-propaganda machine. https://medium.com/@d1gi/ the-election2016-micro-propaganda-machine-383449cc1fba.

52. Hunt Allcott and Matthew Gentzkow. Social media and fake news in the 2016 election. Technical report, National Bureau of Economic Research, 2017.

53. Solomon E Asch and H Guetzkow. Effects of group pressure upon the modification and distortion of judgments. Groups, leadership, and men, pages 222–236, 1951.

54. Eytan Bakshy, Jake M Hofman, Winter A Mason, and Duncan J Watts. Everyone's an influencer: quantifying influence on twitter. In Proceedings of the 4th ACM International Conference on Web Search and Data Mining, 2011.

55. Tim Berners-Lee, Robert Cailliau, Jean-François Groff, and Bernd Pollermann. World-wide web: The information universe. Internet Research, 20(4):461–471, 2010.

56. Alessandro Bessi and Emilio Ferrara. Social bots distort the 2016 us presidential election online discussion. First Monday, 2016.

57. Alex Beutel. User behavior modeling with large-scale graph analysis. 2016.

58. Alex Beutel, Kenton Murray, Christos Faloutsos, and Alexander J Smola. CoBaFi: collaborative bayesian filtering. In Proceedings of the 23rd International Conference on World Wide Web. ACM, 2014.

59. Alex Beutel, Wanhong Xu, Venkatesan Guruswami, Christopher Palow, and Christos Faloutsos. Copycatch: stopping group attacks by spotting lockstep behavior in social networks. In Proceedings of the 22rd International Conference on World Wide Web. ACM, 2013.

60. Johan Bollen, Huina Mao, and Xiaojun Zeng. Twitter mood predicts the stock market. Journal of computational science, 2(1):1–8, 2011.

61. Ceren Budak, Divyakant Agrawal, and Amr El Abbadi. Limiting the spread of misinformation in social networks. In Proceedings of the 20th International Conference on World Wide Web. ACM, 2011.

62. Justin Cheng, Lada Adamic, P Alex Dow, Jon Michael Kleinberg, and Jure Leskovec. Can cascades be predicted? In Proceedings of the 23rd International Conference on World Wide Web. ACM, 2014.

63. Justin Cheng, Cristian Danescu-Niculescu-Mizil, and Jure Leskovec. Antisocial behavior in online discussion communities. In Proceedings of the 9th International AAAI Conference on Web and Social Media, 2015.

64. Clayton Allen Davis, Onur Varol, Emilio Ferrara, Alessandro Flammini, and Filippo Menczer. Botornot: A system to evaluate social bots. In Proceedings of the 25th International Conference Companion on World Wide Web, 2016.

65. Michela Del Vicario, Alessandro Bessi, Fabiana Zollo, Fabio Petroni, Antonio Scala, Guido Caldarelli, H Eugene Stanley, and Walter Quattrociocchi. The spreading of misinformation online. Proceedings of the National Academy of Sciences, 113(3):554–559, 2016.

67. Остапенко А. Г. Перспективы развития методологии риск-анализа систем / А.Г. Остапенко, Д.О. Карпеев, Д.Г. Плотников // Информация и безопасность. - 2009. - Т.12. - №3. - С.419-424.

68. Остапенко А. Г. Предупреждение и минимизация последствий компьютерных атак на элементы критической информационной инфраструктуры и автоматизированные информационные системы критически важных объектов: риск-анализ и оценка эффективности защиты / А. Г. Остапенко, Е. В. Ермилов, А.Н. Шершень, Е.С. Соколова, И.В. Шевченко // Информация и безопасность. - 2013. - Т.16. - №2. - С.167-178.

69. Остапенко А. Г. Риски ущербности, шансы полезности и жизнестойкость компонент автоматизированных систем в условиях воздействия на них информационных угроз / А. Г. Остапенко, Е.В. Ермилов, А.О. Калашников // Информация и безопасность. - 2013. - Т.16. - №2. - С.215-218.

70. Протасов И.Д. Теория игр и исследование операций // Учебное пособие. М.: Гелиос АРВ. - 2003. - 368 с.

71. Кравченко ВА. Світовий досвід управління підприємницькими ризиками: історія та здобутки 20-го сторіччя / Володимир Кравченко // Актуальні проблеми міжнародних відносин : [збірник наукових праць]. - В. 70. - Ч. II (у двох частинах). - К.: Київський національний університет імені Тараса Шевченка. Інститут міжнародних відносин. - 2007. - 316 с. - С. 260 -263.

72. Сулим М. В. Економічний ризик та методи його вимірювання: навч. посіб. / М.В. Сулим. - Л.: вид-во Львів. комерц. акад., 2003. -196 с.

73. Тарасова К. І. Суб'єктивна точка зору підприємців на проблему ризиків / К. І. Тарасова // Спецпроект: аналіз наукових досліджень: матеріали VII Міжнар. наук.-практ. конф., 14-15 черв. 2012 р. : у 7 т. – Дніпропетровськ : Біла К.О., 2012. – С. 92–95.

74. Старостіна А. О. Ризик-менеджмент : теорія та практика : Навчальний посібник / А. О. Старостіна, В. А. Кравченко. – К. : ІВЦ «Видавництво «Політехніка», 2004. – 200 с.