МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ
ІННОВАЦІЙНИХ ОСВІТНІХ ТЕХНОЛОГІЙ
КАФЕДРА БЕЗПЕКИ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач випускової кафедри
_____ О.Г. Корченко
«_____»_____ 2020 р.

На правах рукопису
УДК 004.056.5

ДИПЛОМНА РОБОТА
ЗДОБУВАЧА ОСВІТНЬОГО СТУПЕНЯ «МАГІСТР»

Тема: Метод побудови захищеного кіберпростору

Виконавець: Ю.М.Ткач

Науковий керівник: д.т.н., доцент С.В.Казмірчук

Нормоконтролер: О.О. Бурбела

Київ 2020

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Навчально-науковий інститут: інноваційних освітніх технологій
Кафедра: Безпеки інформаційних технологій
Освітній ступінь: Магістр
Спеціальність: 125 «Кібербезпека»
ОПП: «Адміністративний менеджмент у сфері захисту інформації»

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ О.Г. Корченко
«___» _____ 2020 р.

ЗАВДАННЯ
на виконання дипломної роботи
студента Ткач Юлії Миколаївни

1. Тема: *Метод побудови захищеного кіберпростору*.

Затверджена наказом ректора від «19» 10 2020 р. № 2067/ст

2. Термін виконання: з «05» жовтня 2020 р. по «23» грудня 2020 р.

3. Вихідні дані: *проаналізувати сучасні тенденції розвитку кіберпростору, дослідити існуючі моделі й методи забезпечення захищеності кіберпростору; розробити метод, який дасть можливість забезпечувати оптимізацію вибору стандартного функціонального профілю захищеності будь-якої системи захисту інформації; провести експериментальне дослідження розробленого методу.*

4. Зміст пояснювальної записки (перелік питань, що підлягають розробці):

1. Аналіз сучасні тенденції розвитку кіберпростору.
2. Основні етапи проведення дослідження та розробки методу.
3. Експериментальне дослідження розробленого методу.

КАЛЕНДАРНИЙ ПЛАН

виконання дипломної роботи

№ п/п	Етапи виконання бакалаврської атестаційної роботи	Термін виконання етапів	Примітка
1.	*Уточнення завдання*	05.10.20	Виконано
2.	*Аналіз літературних джерел*	12.10.20	Виконано
3.	*Обґрунтування вибору рішення*	19.10.20	Виконано
4.	*Збір інформації*	26.10.20	Виконано
5.	*Проаналізувати сучасні тенденції розвитку кіберпростору*	02.11.20	Виконано
6.	*Дослідити існуючі моделі й методи забезпечення захищеності кіберпростору*	09.11.20	Виконано
7.	*Розробити метод, який дасть можливість забезпечувати оптимізацію вибору стандартного функціонального профілю захищеності будь-якої системи захисту інформації*	16.11.20	Виконано
8.	*Провести експериментальне дослідження розробленого методу*	23.11.20	Виконано
9.	*Оформлення презентації*	30.11.20	Виконано
10.	*Отримання рецензій від опонентів*	02.12.20	Виконано
11.	*Захист в ЕК*	23.12	Виконано

Дипломник Ю.М.Ткач

(підпис, дата)

Науковий керівник С.В.Казмірчук

(підпис, дата)

РЕФЕРАТ

Дипломна робота складається зі вступу, трьох розділів, висновку, списку використаних джерел, додатків, загальним обсягом робота складає 98 сторінок, має 8 рисунків, 4 таблиці, 24 сторінки додатків. Список використаних джерел має 68 найменувань і займає 6 сторінок.

Метою дипломної роботи є забезпечення захищеності кіберпростору шляхом вибору оптимального стандартного функціонального профілю захищеності.

В дипломній роботі проаналізовано сучасні тенденції розвитку кіберпростору, досліджено існуючі моделі й методи забезпечення захищеності кіберпростору.

Розроблено метод вибору стандартного функціонального профілю захищеності системи захисту інформації та проведено експериментальне дослідження розробленого методу.

ТЕНДЕНЦІЇ РОЗВИТКУ КІБЕРПРОСТОРУ, ЗАХИЩЕНИЙ КІБЕРПРОСТІР, СТАНДАРНИЙ ФУНКЦІОНАЛЬНИЙ ПРОФІЛЬ ЗАХИЩЕНОСТІ.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

КБ – кіберпростір;

СЗІ - системи захисту інформації

ОЗ - об'єкту захисту

СФПЗ - стандартний функціональний профіль захищеності

АС - автоматизована система

КЗЗ - комплекс засобів захисту

НСД — несанкціонований доступ

КСЗІ — комплексна система захисту інформації

К - конфіденційність

Ц - цілісність

Д - достовірність

НД ТЗІ - нормативний документ технічного захисту інформації

ВОФПЗ - вибір оптимального функціонального профілю захищеності

ВСТУП

Актуальність. Стрімкий розвиток інформаційних технологій та створення глобального інформаційного простору сформували принципово нові субстанції – кіберпростір, інформаційний простір та інформаційне суспільство, які мають необмежений потенціал та починають відігравати все більшу роль в економічному та соціальному розвитку країн. Однак, створення інформаційного суспільства призвело до виникнення нового типу загрози – кіберзагроз.

Проблеми кібербезпеки, захисту інформації, інформаційної безпеки є актуальними та набувають статус ключових в поточному сторіччі. Насамперед це пов’язано, з одного боку, з поширенням використання сучасних інформаційних технологій в усіх сферах життєдіяльності людини, а, з іншого, суттєвим ускладненням організації їх побудови та забезпеченням їх захисту. Темпи впровадження інформаційних технологій в значному ступені залежать від рівня захищеності, який вони зможуть забезпечити для ресурсів, що обробляються і зберігаються. У цьому аспекті кіберзахист може розглядатися як цілеспрямована діяльність із забезпечення безпеки кіберпростору.

Ефективність вирішення завдань із кіберзахисту безпосередньо пов’язано з формуванням сучасних системних поглядів на основи, стан та напрямки розвитку теорії побудови захищеного кіберпростору.

Загрози кібернетичного характеру є сьогодні надзвичайно актуальними також і для України. Це пов’язане зі спробами іноземних держав та організацій досягти своїх інтересів по відношенню до нашої держави через встановлення контролю над національним інформаційним простором. Тому серед основних завдань, визначених Указом Президента України № 96/2016 від 27.01.2016 року у "Стратегії кібербезпеки України", є створення в Україні національної системи кібербезпеки.

Метою дипломної роботи є забезпечення захищеності кіберпростору шляхом вибору оптимального стандартного функціонального профілю захищеності.

Досягнення мети потребує розв’язання таких **завдань**:

- аналіз сучасних тенденції розвитку кіберпростору, основних складових інфраструктури захисту кіберпростору та існуючих моделі й методи забезпечення кіберзахисту;
- розробка методу вибору оптимального стандартного функціонального профілю захищеності з метою побудови захищеного кіберпростору;
- експериментальне дослідження методу вибору оптимального стандартного функціонального профілю захищеності.

Під ефективністю будемо розуміти, що здійснюється не тільки загальний захист кіберпростору (КБ), а також окремих частин, які є складовими КБ.

Об’єкт дослідження: процес побудови захищеного кіберпростору.

Предмет дослідження: моделі та методи захисту кіберпростору.

Оцінка сучасного стану проблеми на основі вітчизняної та зарубіжної літератури. Інтеграція України у світовий інформаційний простір, розвиток суспільства нашої країни, як суспільства знань, призвели до появи нових загроз її національним інтересам, пов’язаних з кібербезпекою. За даними РНБО України тільки в першому півріччі 2020 року за злочини в кіберпросторі проти державності було засуджено більш ніж 20 чоловік.

Згідно з дослідження "Глобальний індекс кібербезпеки" (Global Cybersecurity Index), яке щорічно проводить Міжнародний союз електрозв’язку (ITU), у 2018 році Україна зайняла "почесне" 59 місце у рейтингу з 193 можливих. При цьому ряд пострадянських країн — Латвія, Білорусь та Азербайджан суттєво випередили нас у рейтингу, а Росія (10 місце), Грузія (8 місце) і Естонія (5 місце) увійшли у десятку світових лідерів у даній області.

В останнє десятиліття істотно зросла кількість досліджень, присвячених проблемам кіберпростору та його безпеки. На особливу увагу заслуговують праці К.Александера, Г.Раттрея, Д.Шелдона, К.Демчака, П.Домбровського, Дж.Ная-мол., С.Старра, Лі Джанга, А.Клімбурга. Дослідженню сутності кіберпростору як нового явища глобального безпекового середовища та

термінологічні дослідження з кібербезпекової проблематики знайшли належне відображення у працях Дж.Ліпмана, Д.Фахренкурга, Ф.Крамера, Л.Вентца, Дж.Льюїса, Дж.Ліпмана, М.Лібіцкі, Д.Куела, С.Бейделмана, Л.Жанчевскі, А.Коларіка, М.Каветлі.

Різні аспекти забезпечення кібернетичної безпеки досліджувалися у працях вітчизняних науковців, зокрема С.Бондаренка, О.Довганя, О.Дзьобаня, Д.Дубова, О.Климчука, О.Корченка, О.Мандзюка, О.Манжая, В.Панченко, М.Присяжнюка, В.Фурашева, В.Шеломенцева, В.Хорошка, В.Бурячка, С.Гнатюка, І.Храбана [22-25]. Методологічне та організаційне забезпечення створення Національної системи кібернетичної безпеки досліджено в працях В.Горбуліна, В.Бутузова, М.Ожевана, В.Пилипчука, В.Петрова [19-20] та інших.

У працях зазначених авторів недостатня увага приділялася вирішенню теоретичних, організаційних, технічних та практичних проблем забезпечення безпеки саме кіберпростору держави, зокрема питанням:

- вирішення проблем, пов’язаних із розбудови національного сегменту кіберпростору та його безпеки, централізованій координації зусиль щодо ефективної взаємодії усіх учасників процесу забезпечення кібербезпеки, у тому числі й приватного сектору;

- моніторингу ефективності захисту шляхом формування та використання чітких метрик оцінки станів кіберпростору та його безпеки;

- вдосконаленню методів, механізмів і процедур кіберзахисту, управління змінами в реалізації політики безпеки, вдосконаленню операційної дисципліни підприємств за рахунок збільшення уваги інформаційним технологіям захисту (коригування існуючого й розробки нового програмного забезпечення відповідних інформаційних систем забезпечення кібербезпеки, точок контролю доступу для мережевих систем, застосунків, функцій, даних, веб-контенту, спільних мережевих інформаційних середовищ тощо);

- системному підходу до кіберзахисту, який забезпечує контроль, вдосконалює сумісність компонентів складових забезпечення кібербезпеки,

підтримує точний реєстр апаратно-програмного обладнання складових кіберпростору;

- вдосконалення методів, механізмів і процедур скорочення часу, потрібного для запобігання кібератак (тобто часу, що витрачається на виявлення та припинення кібератак, та часу, що витрачається на знешкодження наслідків кібератак).

Галузь застосування. Запропонований метод може бути корисними для керівників ІТ-підрозділів та організацій для підтримки необхідного рівня безпеки установи.

Новизна. Вперше розроблено метод вибору стандартного функціонального профілю захищеності кіберпростору, який дозволяє здійснити оптимальний вибір при виконанні умови максимізації відверненого збитку та неперевищення допустимих витрат за рахунок ймовірно-вартісної оцінки показників кількості й частоти появи загрози, ймовірних збитків від реалізації визначених загроз й вартості послуги захисту.

Практична цінність полягає у тому, що запропонований метод може використовуватись аналітиками з питань ІБ, для проведення вибору оптимального функціонального профілю захищеності. Також надається можливість проведення аналізу, лише окремих частин системи захисту підприємства, наприклад, обчислення показника вірогідності та показника відвернення появи i-ої загрози, обчислення показника вірогідності використання j-ої вразливості. Результат аналізу надається у кількісному вигляді з необхідністю, на основі отриманих даних, подальшого прийняття рішення керівництвом або експертами.

РОЗДІЛ 1
АНАЛІЗ ТЕНДЕНЦІЇ РОЗВИТКУ КІБЕРПРОСТОРУ

1.1. Основні поняття кіберпростір, інформаційний простір, кібербезпека

Сучасні інформаційні технології глибоко проникли у різні сфери життєдіяльності та радикально змінили відношення людини зі своїм середовищем проживання та друг з другом. Сформувалась нова сутність кіберпростір (*cyberspace*). Кіберпростір став головною ознакою сьогодення. Повсякденною стала цифровізація усіх сфер діяльності держави, суспільства, бізнесу, науки, освіти та окремої людини (електронний уряд, електронні послуги, електронні документи, електронні гроші, електронний підпис, звичайним стало дистанційне навчання, наради, робота тощо). Однак така цифровізація призводить до більшої вразливості як державної інфраструктури, так і життєвого простору людини. Розвиток інформаційних технологій спровокував розростання методів та технологій кібератак, кібертероризму, кібердиверсій тощо.

Список кіберзагроз становиться все довше з кожним днем, а професійні кіберзлочинці піддають кіберпростір постійним цифровим нападам. Кібератаки, поряд з стихійними лихами, стають одними з головних загроз майбутнього: вони мають високу ймовірність виникнення, а потенційний збиток від них - величезний. За статистикою, у 2018 році зафіксовано більш ніж п’ять млрд випадків крадіжки даних у приватних структурах (більш ніж разом за два попередніх роки). Однак найбільш часті та агресивні кібератаки направлені на урядові структури та збройні сили, які знаходяться практично під постійними атаками, тому що зберігають конфіденційну інформацію, що потенційно відноситься не тільки до кіберсуверенітету країни, але й до особистого життя її громадян.

Найбільш вразливими точками інфраструктури є енергетика, телекомунікації, авіаційні диспетчерські системи, фінансові електроні системи,

державні інформаційні системи, а також автоматизовані системи управління військами і зброєю. Ієрархія кібернетичних загроз за важливістю має наступний вигляд: кібервійна, кібертероризм, кібершпигунство, кіберзлочинність.

Інтеграція України у світовий інформаційний простір, розвиток суспільства нашої країни, як суспільства знань, призвели до появи нових загроз її національним інтересам, пов'язаних з кібербезпекою. За даними РНБО України тільки в першому півріччі 2020 року за злочини в кіберпросторі проти державності було засуджено більш ніж 20 чоловік. Згідно з дослідження "Глобальний індекс кібербезпеки" (Global Cybersecurity Index), яке щорічно проводить Міжнародний союз електрозв'язку (ITU), у 2018 році Україна зайняла "почесне" 59 місце у рейтингу з 193 можливих [60]. При цьому ряд пострадянських країн - Латвія, Білорусь та Азербайджан суттєво випередили нас у рейтингу, а Росія (10 місце), Грузія (8 місце) і Естонія (5 місце) увійшли у десятку світових лідерів у даній області.

В останнє десятиріччя істотно зросла кількість досліджень, присвячених проблемам кіберпростору та його безпеки. На особливу увагу заслуговують праці К. Александера, Г. Раттрея, Д. Шелдона, К. Демчака, П. Домбровського, Дж. Ная-мол., С. Старра, Лі Джанга, А. Клімбурга. Дослідженню сутності кіберпростору як нового явища глобального безпекового середовища та термінологічні дослідження з кібербезпекової проблематики знайшли належне відображення у працях Дж. Ліпмана, Д. Фахренкурга, Ф. Крамера, Л. Вентца, Дж. Льюїса, Дж. Ліпмана, М. Лібіцкі, Д. Куела, С. Бейделмана, Л. Жанчевскі, А. Коларіка, М. Каветлі.

Різні аспекти забезпечення кібернетичної безпеки досліджувалися у працях вітчизняних науковців, зокрема С. Бондаренка, О. Довганя, О. Дзьобаня, Д. Дубова, О. Климчука, О. Корченка, О. Мандзюка, О. Манжая, В. Панченко, М. Присяжнюка, В. Фурашева, В. Шеломенцева, В. Хорошка, В. Бурячка, С. Гнатюка, І. Храбана [22-25]. Методологічне та організаційне забезпечення створення Національної системи кібернетичної безпеки досліджено в працях В.

Горбуліна, В. Бутузова, М. Ожевана, В. Пилипчука, В. Петрова [19-20] та інших.

У працях зазначених авторів недостатня увага приділялася вирішенню теоретичних, організаційних, технічних та практичних проблем забезпечення безпеки саме кіберпростору держави, зокрема питанням:

- вирішення проблем, пов'язаних із розбудови національного сегменту кіберпростору та його безпеки, централізованій координації зусиль щодо ефективної взаємодії усіх учасників процесу забезпечення кібербезпеки, у тому числі й приватного сектору;

- моніторингу ефективності захисту шляхом формування та використання чітких метрик оцінки станів кіберпростору та його безпеки;

- вдосконаленню методів, механізмів і процедур кіберзахисту, управління змінами в реалізації політики безпеки, вдосконаленню операційної дисципліни підприємств за рахунок збільшення уваги інформаційним технологіям захисту (коригування існуючого й розробки нового програмного забезпечення відповідних інформаційних систем забезпечення кібербезпеки, точок контролю доступу для мережевих систем, застосунків, функцій, даних, веб-контенту, спільних мережевих інформаційних середовищ тощо);

- системному підходу до кіберзахисту, який забезпечує контроль, вдосконалює сумісність компонентів складових забезпечення кібербезпеки, підтримує точний реєстр апаратно-програмного обладнання складових кіберпростору;

- вдосконалення методів, механізмів і процедур скорочення часу, потрібного для запобігання кібератак (тобто часу, що витрачається на виявлення та припинення кібератак, та часу, що витрачається на знешкодження наслідків кібератак).

Тому не викликає сумніву актуальність дослідження проблем щодо розбудови кіберпростору держави та розробки сучасних інформаційних технологій й інформаційних систем забезпечення безпеки кіберпростору України.

Аналіз наукових публікацій В.Гібсона, М.Камчатого, М.Присяжнюка, Л.Бурячка, В.Хорошка, С.Гнатюка та інших щодо розкриття суті та значення поняття «кіберпростір» показав, що вони тлумачать це по різному. Такі концептуальні відмінності у визначенні «кіберпростору» заважають розробці міжнародних угод та координації дій.

Розглянемо як на даний час співвідносяться між собою поняття інформаційний простір, кіберпростір та кібербезпека.

У західній науковій літературі, а також публіцистиці й дипломатичній риториці використовується термін «кіберпростір», у той же час використання терміну «інформаційний простір» характерно для Росії та пострадянських країн. Як правило, інформаційний простір визначає більш широку сферу по відношенню до кіберпростору, який обмежується комп'ютерними електронними мережами та інформацією, яка в них знаходиться. У той же час інформаційний простір охоплює більш широку область, що об'єднує усю інформацію та данні, які існують як у віртуальному, так і у реальному вимірах (рис.1.1).

Рис.1.1. Співвідношення «кіберпростру» та «інформаційного простору».

Інформаційний простір розглядають як область ведення інформаційної війни, дії в якому можуть розгортатися як в технічній сфері, так і в сфері психологічній (рис.1.2).

Рис.1.2. Декомпозиція інформаційного простору.

Технічна сфера - це область інформаційного простору, в якій створюється, обробляється та накопичується інформація. Крім того, це область, в якій функціонують системи управління, зв'язку та розвідки [13]. В подальшому в ряді керівних документів розвиток та уточнення поняття технічної сфери інформаційного простору призвело до створення понятійного апарату кіберпростору.

Вперше загальне визначення кіберпростору було надано дослідницькою службою конгресу США для того, щоб через термінологічний базис "кіберпонять" визначати сутності, які відносяться до протиборства в технічній сфері інформаційного простору (іншими словами, області ведення інформаційної війни) [1-3]. Основи цієї термінології надані в керівних документах ЗС США [4-8] та міжнародних стандартах ITU-T та ISO [9-11].

Кіберпростір – це всеохоплююча множина зв'язків між людьми, яка створена на основі комп'ютерів та телекомунікацій незалежно від фізичного чи географічного положення [6].

У Єдиному статуті комітету начальників штабів Збройних сил США [6] кіберпростір визначено наступним чином: «кіберпростір - це сфера (область), в якій застосовуються різні РЕЗ (зв'язку, радіолокації, розвідки, навігації, автоматизації, управління та наведення) для прийому, передачі, обробки, зберігання, трансформації інформації та пов’язана з ними інформаційна інфраструктура ЗС».

У міжнародному стандарті ISO/IEC 27032:2012 [9] кіберпростір визначено з урахуванням тенденцій розвитку глобальної мережі Інтернету: «кіберпростір - це середовище, яке не існує у будь-якій фізичній формі, та являє собою наслідок результату взаємодії людей, програмного забезпечення та послуг в Інтернеті за допомоги технологій, засобів та мереж».

Таким чином, основу кіберпростору складають сукупність розподілених у просторі взаємопов'язаних електронних засобів (комп'ютерів, серверів, мережевих маршрутизаторів, сховищ даних, шифраторів тощо) з відповідним програмним забезпеченням, за допомогою яких створюється та циркулює інформація (обробляється, передається, запам’ятовується та зберігається). З інфраструктурної точки зору глобальний кіберпростір можна розглядати як адресний простір, що складається з національних та регіональних сегментів Інтернету. Суб'єктами кіберпростору є людина, суспільство, держава, а також жива істота, яка спроможна сприйняти, запам'ятати та переробити інформацію, а також обмінятися нею [13].

У цих же стандартах [9], через поняття кіберпростір визначено також термін кібербезпека: «кібербезпека - це безпека в кіберпросторі».

У рекомендації X.1205 МСЭ-Т [10] кібербезпека визначена через поняття кіберпростору та систему управління рисками: «кібербезпека — це набір засобів, стратегій, принципів забезпечення безпеки, мір з забезпечення безпеки, керівних принципів, підходів к керівництву рисками, дій, професійної

підготовки, практичному досвіду, страхуванню та технологій, які можуть бути використані для захисту кіберпростору, ресурсів організації та користувача».

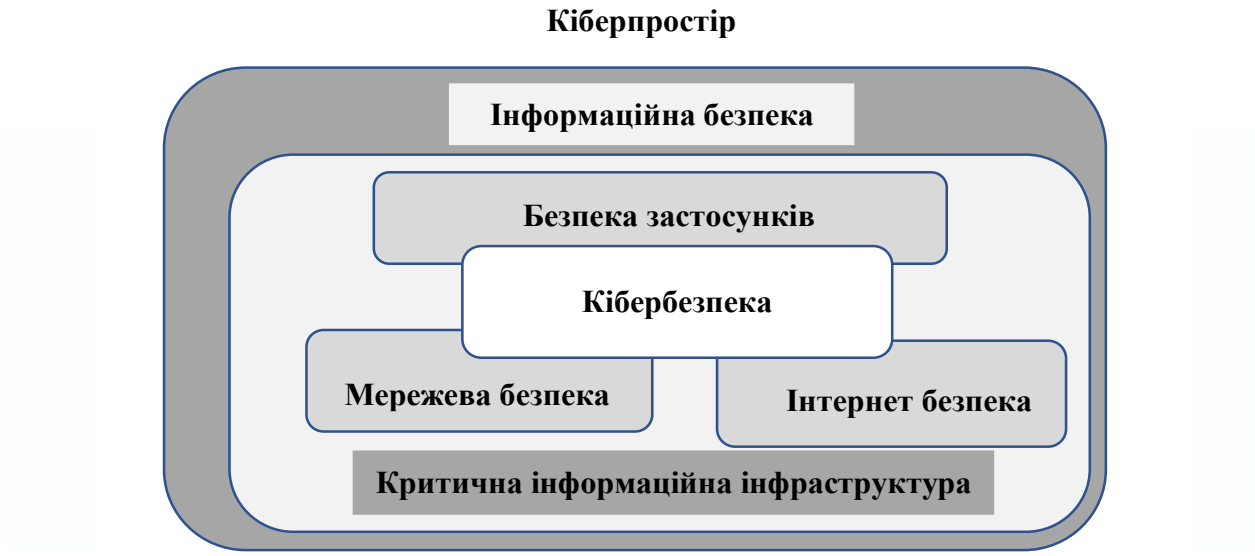


Рис.1.3. Зв’язок терміну «кібербезпека» с термінологічним базисом стандарту ISO/IEC 27032:2012 [9].

Стандарт ISO/IEC 27032:2012 [9] визначає зв'язок термінів кібербезпека, мережева безпека, прикладна безпека, Інтернет безпека та безпека критичних інформаційних інфраструктур. В стандарті надана візуалізація зв'язку цих термінів (рис.1.3). З точки зору міжнародних експертів усі ці терміни об'єднує поняття інформаційна безпека.

У подальшому в даній роботі будемо використовувати термінологічний базис “кіберпонять”, який наведено у Додатку А.

1.2. Сучасні тенденції розвитку кіберпростору

Визнавши суттєве значення кіберпростору у функціонуванні держави в прийдешності, для успішної його розбудови в Україні та побудови відповідної системи кібербезпеки проаналізуємо основні тенденції розвитку сучасного кіберпростору, які вже враховують країни-лідери при забезпеченні функціонування та безпеки своїх сегментів кіберпростору.

Аналізуючи процес розвитку глобального кіберпростору можна виділити декілька цікавих тенденцій, які в найближчому майбутньому суттєво вплинуть на його функціювання.

Тенденція перша: *кіберпростір поступово перетворюється у п'ятий театр військових дій*.

Кібервійни з фантастичних романів перейшли у реальність. Кіберпростір поряд з традиційними наземним, морським, повітряним та космічним стає новим театром військових дій, де разом з військами планується участь спец-служб, хакерів та усіх тих, хто може створювати та використовувати інформаційні технології для нанесення ударів по ворогу.

Ряд країн (в першу чергу, США, Росія, Китай) вже проводять державну політику, яка розглядає кіберпростір як поле боя, внаслідок чого направляє свої зусилля на встановлення повного контролю в цій сфері, створюючи засоби та можливості на здійснення такого контролю. Такі прецеденти численні - інформаційна зброя використовувалася в усіх військових конфліктах на протязі останніх двадцяти років, вона стала важливою частиною озброєння збройних сил Китаю, Росії, США та їх союзників. Є дані, що роботи щодо розвитку потенціалу інформаційного протиборства проводять більш ніж 120 країн світу (для прикладу, розробки в області ядерної зброї ведуть не більше 20 країн).

Війни майбутнього будуть вестися в режимі онлайн, коли противник, окрім застосування сил на полі бою, буде використовувати вразливості комп'ютерних систем озброєння, інформаційних систем керування державних структур та об'єктів критичної інфраструктури для їх руйнування та знищення, а також соціальні мережі для створення паніки серед населення в масштабі цілої країни для зниження його здатності к супротиву агресії.

Вже відбувається трансформація усієї військової інформаційної архітектури, спостерігається "інформатизація" традиційних збройних сил і "інтелектуалізація" озброєнь. Активно розвивається концепція ексцентричного ведення бойових дій, мається на увазі досягнення переваги над ворогом шляхом ефективної організації збору, обробки і використання інформації.

Сьогодні можна вже говорити про те, що інформаційна зброя в деяких розвинених країнах перейшла в розряд тактичної. Повідомляється про розробки високочастотної електромагнітної імпульсної зброї, здатної виводити з ладу електроніку в радіусі сотень кілометрів. Експерти відмічають, що низка країн вже нині має в розпорядженні такі можливості. Ведуться розробки мікрохвильової зброї великої потужності, здатної змінювати траєкторію ракет у польоті, викликати перевантаження або виведення із ладу мереж зв'язку, телеметричного устаткування та електроніки систем озброєння. Є можливість вражати екрановані приміщення, захищені від радіоактивного випромінювання, та завдавати збитку здоров'ю й життю осіб, що знаходяться в радіусі дії такої зброї.

Тенденція друга: *інформаційна безпека напряму залежить від кібербезпеки, тобто політики безпеки, що реалізується у кіберпросторі країни чи коаліції країн*.

Фактор наявності кіберпростору починає істотно впливати на інформаційну безпеку будь-якої держави. З точки зору інтересів країни, кіберпростір треба розглядати як частину національної інфраструктури, яка має окреслені межі та потребує певної системи безпеки, як й інші елементи державної інфраструктури. Основна проблема кіберпростору - це забезпечення безпеки інформації, яка там циркулює, та стійкість його національного сегменту к кібератакам.

Кібербезпека – це стратегічна проблема державної важливості. Держав-на політика кібербезпеки (National Cyber Security Strategy - NCSS) служить засобом посилення безпеки та надійності інформаційних систем країни. Першими така політика була впроваджена у США. Слідом за США, стратегії кібербезпеки були прийняті в Канаді, Японії, Індії, Австралії, Новій Зеландії, Колумбії тощо. У країнах-членів Євросоюзу такі ж прийняли: Швеція (2008 г.), Естонія (2008 г.), Фінляндія (2008 г.), Словакія (2008 г.), Чехія (2011 г.), Франція (2011 г.), Німеччина (2011 г.), Литва (2011 г.), Люксембург (2011 г.),

Нідерланди (2011 г.), Великобританія (2011 г.) та інші. Список країн наглядно показує, що проблема кібербезпеки рахується важливою у всьому світі.

В Україні для створення умов безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави також прийнята відповідна Стратегія кібербезпеки України [61], у якій передбачено:

- створення національної системи кібербезпеки;
- посилення спроможностей суб'єктів сектору безпеки та оборони для забезпечення ефективної боротьби із кіберзагрозами воєнного характеру, кібершпигунством, кібертероризмом та кіберзлочинністю, поглиблення міжнародного співробітництва у цій сфері;
- забезпечення кіберзахисту державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, а також інформаційної інфраструктури, яка знаходиться під юрисдикцією України та порушення сталого функціонування якої матиме негативний вплив на стан національної безпеки і оборони України (критична інформаційна інфраструктура).

Для реалізації Стратегія кібербезпеки Кабінет Міністрів України щорічно повинен затверджувати план заходів з її реалізації (нажаль, останній такий план на 2018 рік був прийнятий розпорядженням Кабміну від 11 липня 2018 р. № 481-р).

Тенденція третя: *для захисту держави від кіберзагроз створюються національні органи кібербезпеки*.

Наприклад, у жовтні 2016 року уряд Великобританії створив новий Національний центр комп’ютерної безпеки (NCSC), що є частиною британського агентства з розвідки, інформації та кібербезпеки GCHQ (аналога АНБ США). Головною його задачею є своєчасне виявлення кібератак та їх швидке усунення. NCSC вже активно проводить пошук вразливостей на сайтах державного сектору, виявляє та виводить з роботи десятки тисяч фішингових сайтів, виявляє спуфінг електронної пошти. Наприклад, середній строк життя

фішингового сайту, що знаходиться у Великобританії, вже скоротився з 27 годин до часу.

По зразку процесів, що пройшли в багатьох країнах, у 2020 році в Україні почав функціонувати оновлений Національний координаційний центр кібербезпеки (НКЦК), який став сучасним хабом - «генеральним штабом» захисту держави від кіберзагроз, де виявляють, запобігають, вчасно реагують на кіберінциденти як у державному, так і у приватному секторі [14]. Оновлений і значно підсилений НКЦК координує та контролює діяльність суб'єктів сектору безпеки і оборони, які забезпечують кібербезпеку у відповідних сферах – Держспецзв'язку, СБУ, Національної поліції, Національного банку, Генерального штабу ЗСУ.

Тенденція четверта: *для боротьби з кіберзагрозами починають формуватися міжнародні коаліції.*

Кібербезпека не є проблемою кожної окремої держави. У разі виявлення загрози, що вона може зачепити не одну окремо взяту країну.

Неможливо забезпечити безпеку кіберпростору тільки в межах однієї країни, тому виникає необхідність розробки міжнародних правил і регулювання, які визначають умови забезпечення безпеки у кіберпросторі.Спільними зусиллями боротися з такими загрозами набагато ефективніше.

Тому нині розпочалася міжнародна кооперація щодо налагодження механізмів співпраці у питанні захисту від кіберзагроз. Наприклад, шість європейських країн - Литва, Естонія, Хорватія, Польща, Нідерланди та Румунія - об'єднали зусилля щодо боротьби з кіберзагрозами у створенні спільних міжнародних можливостей швидкого реагування. Статус спостерігача отримали також такі країни як Бельгія, Греція, Іспанія, Італія, Франція, Словенія і Фінляндія. Відтепер міжнародна команда швидко-го реагування CRRT (Cyber Rapid Response Team) перебуває у режимі очікування на декількох фізичних сайтах і готова негайно відреагувати на кібератаки та інциденти в країнах, які

підписали угоду, в країнах-спостерігачах, а в майбутньому - і в структурах ЄС [15].

З ініціативою створення таких сил у 2017 році виступила Литва, минулого року відбулися перші навчання, а з початку цього року вже несе чергування міжнародна команда з литовців, голландців, поляків та румунів. У під-писаному Меморандумі про взаєморозуміння юридично визначено механізм роботи CRRT, його правовий статус, ролі та процедури. Створені цивільними і військовими експертами, CRRT приєднаються до нейтралізації і розслідування небезпечних кіберінцидентів практично або, за необхідності, фізично.

Це конкретний приклад того, як країни ЄС невійськовими засобами можуть сприяти підвищенню безпеки Європи, підтримувати зусилля в справі оборони і стримування.

Відбувається також зближення точок зору щодо безпеки кіберпростору між США та ЄС: налагоджується комплексна взаємодія та координація їх політики в сфері управління кіберпростором з широкого спектру завдань, в тому числі, з захисту персональної інформації, свободи слова і самовираження, управління потоками даних, управління Інтернетом, електронної комерції, забезпечення кібербезпеки та ведення кібервійн. Метою усього того є управління кіберпростором, створення правил поведінки, що відображають інтереси трансантлантичних партнерів, та закріплення лідерства у даній сфері.

Тенденція п’ята: *для забезпечення переваги у кіберпросторі провідні країни світу почали формувати військово-мережевий комплекс*.

В часи “холодної війни”, коли за відсутності активних воєнних дій роз-горнулася безпрецедентна "гонка озброєнь", в США та СРСР уперше виникли так звані військово-промислові комплекси (ВПК). Основною задачею ВПК на першому плані виступив такий чинник могутності, як спроможність розробляти й виготовляти озброєння та військову техніку (ОВТ) на сучасному рівні і в належній кількості.

Під військово-промисловим комплексом розуміють сукупність підприємств і організацій тієї чи іншої країни, що виготовляють ОВТ для потреб збройних сил своєї держави та на експорт (рис.1.4). В офіційних документах України (а також Росії) зараз замість ВПК, як правило, вживається термін оборонно-промисловий комплекс [16].

Військово-промисловий комплекс – це суспільний феномен, у підґрунті якого лежить збіг інтересів керівництва воєнних корпорацій, вищого командного складу ЗС і високих посадових осіб держави, а одним з головних проявів є лобіювання бізнес-інтересів воєнної промисловості на вищому державному рівні та посилення її впливу на суспільні процеси. До нього звичайно зараховують ракетно-космічну, авіабудівну, суднобудівну, бронетанкову, радіоелектронну та артилерійсько-стрілецьку галузі.

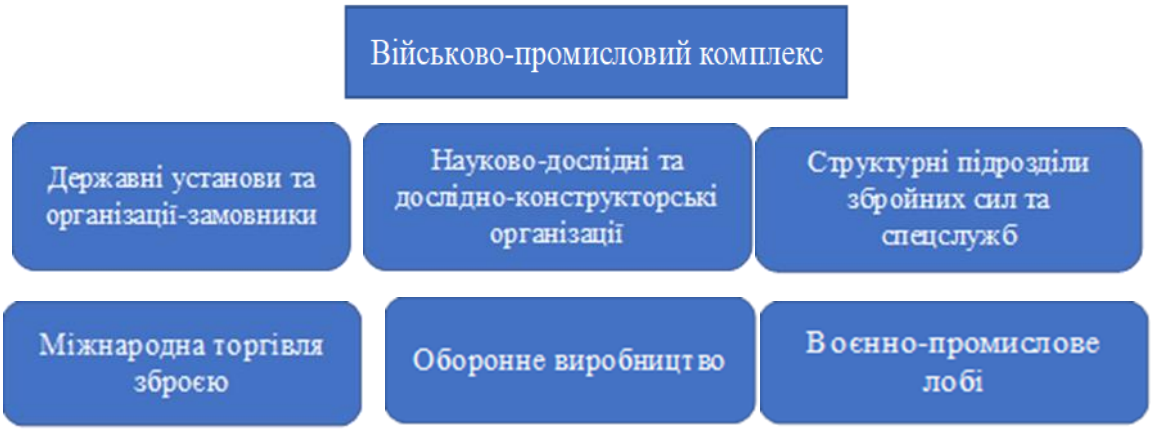


Рис.1.4. Структура військово-промислового комплексу.

Процеси, які зараз проходять в сфері інформаційного протиборства, подібні процесам часів створення ВПК. Ми є свідками формування *військово-мережевого комплексу*, коли інтереси та можливості спецслужб і воєнного сектору країни переплітаються з інтересами та можливостями приватних структур, що разюче змінює як сам кіберпростір, так і характер воєнних дій в ньому.

Військово-мережевий комплекс подібний до свого попередника у тому, що стосується делегування деяких питань національної безпеки: збройні сили не займаються створенням озброєнь та засобів оборони - вони платять

стороннім виробникам за таку діяльність, а держава залишає за собою монополію на застосування сили. На цьому схожість завершується, військово-мережевий комплекс круто сходить з дороги історії: можливості корпорацій щодо збору інформації не поступаються можливостям держави, компанії розробляють засоби виявлення загроз, шукають так звані вразливості «нульового дня», а потім використовують їх у своїх інтересах.

Без сумніву, держава бере участь в цьому процесі та дечим може підтримувати компанії: надавати більше конкретної та корисної інформації про те, звідки виходять загрози; чинити тиск на провайдерів, щоб вони зачиняли доступ до відомих ворожих джерел; зрештою, вжити дії щодо попередження атаки, якщо вона була виявлена своєчасно. Однак, енергетичні компанії, банки, транспорт, зв'язок тощо, як й раніше можуть покладатись тільки на свої сили при відбитті атак хакерів. Держава не в силах захистити усі мережі, число яких стало досить великим, а географічне поширення – занадто широким.

Відбувається наочна колоборація державних структур (в першу чергу, США, Китаю та Росії) з техноіндустрією Інтернету - крупними виробниками мікроелектроніки, обчислювальної та телекомунікаційної техніки щодо збору інформації о користувачах. В засобах масової інформації неодноразово з'являлися дані щодо співпраці зі спецслужбами таких відомих потужних виробники засобів телекомунікації (Cisco, Huaway), шифраторів (Crypto AG, Omnisec, Mils Electronic), програмного забезпечення (Microsoft), соціальних мереж (Facebook, Вконтакте, Одноклассники), антивірусних систем (Касперский, Radware, McAfee), постачальників послуг електронної пошти, мережевих та Інтернет-гігантів (Google, Yahoo, AT&T, CenturyLink, Verizon).

Така співпраця включає навіть вбудовування необхідних закладок (бекдорів) та передачі спецслужбам таємні вразливості в апаратному та програмному забезпеченні операційних систем, систем захисту, криптографічних систем (у тому числі діючі ключі шифрування) [18]. Теоретичне обґрунтування надійності таких закладок вивчається новим

науковим напрямком *клептографією*, що стрімко розвивається в останнє десятиріччя.

Тенденція шоста: *проблеми інформаційної безпеки у кіберпросторі та формування військово-мережевого комплексу приводять до перерозподілу повноважень існуючих гравців в сфері захисту інформації*.

Поки в Україні тільки починає налагоджуватися державно-приватне партнерство у сфері кібербезпеки, а у розвинутих країнах вже давно відстежується перерозподіл повноважень серед існуючих гравців у сфері захисту інформації.

Існуючі проблеми інформаційної безпеки кіберпростору показують, що державні органи не завжди будуть основними гравцями у цій сфері, в усякому разі, її постійними лідерами. Вони будуть виробляти стратегію, встановлювати закони і контролювати стандарти безпеки кіберпростору, а ключові об'єкти інфраструктури повинні будуть їх виконувати. Але повсякденна робота по захисту ключових промислових об'єктів стане турботою корпорацій, які впораються з цією задачею не гірше держави. Вони будуть створювати новий вид послуг зі сканування, аналізу трафіка та застосування власних методів виявлення шкідливих програм та хакерської активності - методів, які будуть основані на тих даних, які компанії будуть збирати в режимі реального часу в своїх інформаційних мережах, а також в мережах своїх клієнтів. Це виходить свого роду краудсорсінг, коли залучають до вирішення тих чи інших проблем інноваційної діяльності широке коле осіб для використання їх творчих здібностей, знань та досвіду для субпідрядної роботи із застосування інформаційних технологій.

Ці ж організації будуть створювати кібервійська та навчати їх воювати в мережі, що зрештою приведе до їх інтеграції з арсеналом збройних сил країни.

Тенденція сьома: *Надання послуг із захисту інформації у кіберпросторі стає новим видом бізнесу*.

Більш того, ці ж самі організації будуть не просто розслідувати вже здійсненні вторгнення, а й пропонувати свої послуги по захисту мереж клієнтів

від потенційних загроз, подібно тому, як охоронні фірми пропонують убезпечити наші дома і офіси від грабіжників.

Для того, щоб захиститись від повсякденних кіберзагроз будуть створюватися безпечні зони Інтернету, тобто повноцінні кібернетичні інфраструктури, у яких безпека буде поставлена на чільне місце, а трафік аналізуватися більш активно та ретельно, ніж у загальнодоступному Інтернеті. Це буде свого роду "екозона безпеки", онлайн аналог особливо охоронної території.

Підвищена кібербезпека стане привабливою споживчою якістю, той особливістю, яка буде залучати клієнтів. Кампанії, що візьмуться за створення та обслугу таких захищених кіберзон (інтернет-провайдери, банки та інші, що мають діло з персональними даними), будуть залучати найбільш досвідчених і кваліфікованих співробітників, оскільки рівень зарплат у них буде значно більший ніж у державному чи воєнному секторі.

Як і в любій приватній організації, власники такої інфраструктури зможуть обмежувати її користування, встановлювати правила й вимоги їх виконання, а також пропонувати особливі переваги, насамперед безпеку. В межах таких мереж буде ретельно проводитись аналіз трафіку щодо шкідливих про-грам, надсилатися попередження о потенційній загрозі особовим даним, про-водиться контроль тих, хто намагається війти в мережу, та не допускати в неї будь-яких підозрілих користувачів.

Тенденція восьма: *фундаментальна залежність інформаційної інфраструктури сегментів кіберпростору більшості країн від іноземних виробників апаратних та програмних засобів*.

Слід відзначити ще той факт, що у державному та військовому секторах багатьох країн використовуються комерційні програмні продукти, які майже завжди мають вади в захисті, що робить обороноздатність країни потенційно уразливою для нападів кібернетичних сил противника (його військових формувань, спецслужб, хакерів та терористів).

Розвідслужби Литви торік оголосили, що в кіберпросторі ЄС простежується шкідницька діяльність кібернетичних потужностей Росії і Китаю. У традиційній оцінці загроз нацбезпеці зазначається, що найбільшу загрозу для безпеки інформаційних систем і інформації, що зберігається в них, є кібершпіонаж розвідслужб Росії, а новим фактором ризику може стати розвиток технологій 5G, якщо не буде приділятися належна увага надійності постачальника послуг або продуктів інформаційних технологій.

Наприклад, в Україні майже 90% об'ємів продажів телекомунікаційного устаткування на внутрішньому ринку (його місткість нараховується мільярдами доларів) припадає на зарубіжні устаткування, запасні частини або комплектуючі, що використовуються при ремонті та обслуговуванні. Така залежність небезпечна не лише з точки зору економічної безпеки країни, але й без-пеки в ширшому контексті, особливо враховуючи, що зарубіжне програмне забезпечення широко використовується на стратегічних об'єктах українського оборонного комплексу. Відомі непоодинокі реальні прецеденти щодо закладок недокументованих програмних модулів для здійснення втручання в робо-ту програмного забезпечення.

В Україні планується співпраця на постійній основі на платформі Національного координаційного центру кібербезпеки (НКЦК - робочого органу РНБО України) з представниками американських компаній-виробників технологій та обладнання для кібербезпеки та захисту: Cisco, Fortinet, IBM, MicroFocus, Microsoft та ізраїльської Radware. Однак, дивним є останнє рішення Держспецзв’язку щодо стратегічної співпраці з китайською фірмою Хуавей з питань кібербезпеки, кіберзахисту та телекомунікацій у той час коли більшість країн Європи, США, Канада та інші на законодавчому рівні забороняють роботу державних органів на виробах фірми Хуавей.

У той же час, про підтримку національних розробок, хоча б софтових рішень з кібербезпеки, мови майже не йдеться. А такі рішення українських розробників існують, взяти, наприклад, розробки операційних систем на базі BSDI чи LINUX, або антивірусної системи наступного покоління ROMAD, що

запатентована навіть у США та реалізує цілковито новий підхід до знаходження вірусів на базі аналізу характеристик їх поведінки у реальному часі.

Виходячи з вище викладеного, принципове значення має підтримка розробки і виробництва в Україні конкурентних засобів інформатизації, телекомунікацій та зв’язку (у тому числі, з використанням вітчизняної мікроелектроніки, яку потрібно відновити та розвивати) та програмного забезпечення в інтересах українських користувачів, а також застосування таких засобів в Україні, і передусім, в оборонному комплексі і на об'єктах критичної цивільної інфраструктури.

Буде проаналізовано основні складові кіберпростору, сформовано вимоги до них та методику побудови так званого «захищеного кіберпростору», як вагомої складової інформаційної безпеки держави, корпорації, підприємства тощо.

Висновки до першого розділу

Сьогодні перелік кіберзагроз щодня становиться все довше. Щохвилини кіберпростір піддається цифровим нападам з боку професійних кіберзлочинців. Таким чином, проблема створення безпечного кіберпростору актуальна та нагальна.

У ході дослідження з'ясовано, що найбільш вразливими точками інфраструктури є енергетика, телекомунікації, авіаційні диспетчерські системи, фінансові електроні системи, державні інформаційні системи, а також автоматизовані системи управління військами і зброєю. Ієрархія кібернетичних загроз за важливістю має наступний вигляд: кібервійна, кібертероризм, кібершпигунство, кіберзлочинність. Недостатня увага приділялася вирішенню теоретичних, організаційних, технічних та практичних проблем забезпечення безпеки саме кіберпростору держави, зокрема питанням, вирішення проблем, пов'язаних із розбудовою національного сегменту кіберпростору та його безпеки; моніторингу ефективності захисту шляхом формування та використання чітких метрик оцінки станів кіберпростору та його безпеки; вдосконаленню методів, механізмів і процедур кіберзахисту; - системному підходу до кіберзахисту, який забезпечує контроль, вдосконалює сумісність компонентів складових забезпечення кібербезпеки, підтримує точний реєстр апаратно-програмного обладнання складових кіберпростору; вдосконаленню методів, механізмів і процедур скорочення часу, потрібного для запобігання кібератак.

Встановлено співвідношення та потрактовано поняття інформаційний простір, кіберпростір та кібербезпека. Отже, інформаційний простір визначає більш широку сферу по відношенню до кіберпростору, який обмежується комп'ютерними електронними мережами та інформацією, яка в них знаходиться. У той же час інформаційний простір охоплює більш широку область, що об'єднує усю інформацію та данні, які існують як у віртуальному, так і у реальному вимірах. Поняття кіберпростору увійшло у вжиток в ряді керівних документів, як підміна поняття технічна сфера (область інформаційного простору, в якій створюється, обробляється та накопичується

інформація). *Кіберпростір* – це всеохоплююча множина зв'язків між людьми, яка створена на основі комп'ютерів та телекомунікацій незалежно від фізичного чи географічного положення. Кібербезпека — це набір засобів, стратегій, принципів забезпечення безпеки, мір з забезпечення безпеки, керівних принципів, підходів к керівництву рисками, дій, професійної підготовки, практичному досвіду, страхуванню та технологій, які можуть бути використані для захисту кіберпростору, ресурсів організації та користувача. Таким чином, кібербезпека включається в кіберпростір, а кіберпросторі в свою чергу входить до складу інформаційного простору.

Виділено тенденції, які в найближчому майбутньому суттєво вплинуть на його функціювання кіберпростору: 1) кіберпростір поступово перетворюється у п'ятий театр військових дій; 2) інформаційна безпека напряму залежить від кібербезпеки, тобто політики безпеки, що реалізується у кіберпросторі країни чи коаліції країн; 3) для захисту держави від кіберзагроз створюються національні органи кібербезпеки; 4) для боротьби з кіберзагрозами починають форму-ватися міжнародні коаліції; 5) забезпечення переваги у кіберпросторі провідні країни світу почали формувати військово-мережевий комплекс; 6) проблеми інформаційної безпеки у кіберпросторі та формування військово-мережевого комплексу приводять до перерозподілу повноважень існуючих гравців в сфері захисту інформації; 7) Надання послуг із захисту інформації у кіберпросторі стає новим видом бізнесу; 8) фундаментальна залежність інформаційної інфраструктури сегментів кіберпростору більшості країн від іноземних виробників апаратних та програмних засобів.

РОЗДІЛ 2

ДОСЛІДЖЕННЯ СУЧАСНИХ МОДЕЛЕЙ Й МЕТОДІВ ЗАБЕЗПЕЧЕННЯ ЗАХИЩЕНОСТІ КІБЕРПРОСТОРУ

2.1. Аналіз моделей захисту кіберпростору

Розглянемо найбільш відомі підходи до моделювання систем захисту кіберпростору:

1. *Моделі стримування атак на кіберпростір*, у яких виділяється декілька рівнів стримування кібератак: національний рівень несе відповідальність за кіберрозвідку та контроль над кіберзброєю, а корпоративні та індивідуальні рівні – за захист корпоративних і приватних даних відповідно [29].

2. *Моделі захисту персональних даних,* які в основному базуються на регуляторних процесах і являють собою юридичний інструмент для регулювання обробки персональних даних [30-31]. В цих моделях йдеться, з одного боку, про регламент щодо захисту персональних даних в кіберпросторі, а, з іншого, про етику і відповідальність при їх обробці. Недоліки регуляторної моделі полягають у тому, що виконання регламентів мають на увазі підтримання самоконтролю за їх виконанням. Штрафні санкції вводяться тільки у разі, коли витік персональних даних став надбанням громадськості.

3. *В моделях управління доступом* розглядаються права доступу користувача або в рамках одного домену (корпорації) [32-33] або у мультидоменному середовищі [34-36]. У випадку мультидоменної організації доступу можлива ситуація, коли різним акаунтам користувача у різних доменах прописуються різні ролі та права доступу до різних об'єктів інформаційної інфраструктури (мережевих ресурсів різних обчислювальних кластерів, процесів, файлів тощо). Таким чином, дані моделі не можуть бути використані в рамках кіберпростору, де у користувача існують різні уявлення, певні в різних доменах, і немає єдиного провайдера аутентифікації для всіх доменів і типів об'єктів.

4. *Моделі реагування на кіберінциденти* є найбільш розробленим та вживаним класом моделей систем захисту кіберпростору. Традиційні моделі реагування на інциденти представлено в NIST 800-61 [37], в ISO 27035 [38], SANS's Incident Handler's Handbook [39] та інших [40]. У моделях даного класу містяться описи процесів, пов'язаних з виявленням, стримуванням, розслідуванням, аналізом, відновленням та запобіганням інцидентів безпеки в класичній інформаційній інфраструктурі. Однак всі вони не беруть до уваги такі притаманні кіберпростору особливості як хмарні інфраструктури, масштабованість, відмовостійкість, віртуальний характер середовища тощо.

5. *Моделі кіберзагроз*. Існує декілька відомих моделей даного класу. Найбільш популярною є модель загроз STRIDE від компанії Microsoft для розробників програмних додатків [41]. Використовуються також моделі CAPEC та ATT&CK від компанії MITRE. У першій моделі будується периметр захисту корпорації на основі типових сценаріїв атак [42], а у другій – будується та підтримується база знань ATT&CK, яка заснована на зборі та аналізі реальних кіберінцидентів. Ця база знань використовується як основа для розробки конкретних тактик і методик супротиву загрозам в урядовому секторі, у приватному секторі та у сфері надання послуг кібербезпеки [43]. Але найбільш успішною виявилася модель кіберзагроз, що була розроблена у 2011 році Еріком Хатчинсом, аналітиком корпорації Lockheed Martin (США), та має назву ***Cyber Kill Chain*** (CKC) [18]. Більшість фахівців вважають цю модель поворотним моментом в еволюції кібероборони.

Ерік Хатчинс проаналізував дії кібернападників і розділив процес їх вторгнення на наступні етапи дій: «Кіберрозвідка» → «Проникнення й фіксація у системі жертви» → «Комунікація з центром керування нападом» → «Експлуатація вразливостей для отримання доступу до ресурсів жертви» → «Пошук серверів з цінною конфіденційною інформацією» → «Ексфільтрація/вигрузка конфіденційної інформації» → «Завершення атаки, самоліквідація або звернення в центр керування для отримання нових команд». Це дало йому можливість описати мотиви, цілі та дії системи кіберзахисту для

блокування дій нападників на кожному етапі. Опишемо коротко метод Cyber kill chain.

Все починається із спостереження та розвідки. СКС відстежує ключові слова, які приводять на сайт компанії-жертви при пошуку у Google чи інших пошукових машинах. Хакери шукають у прес-релізах та веб-сторінках компанії імена співробітників, щоб провести фішингову атаку. Вони також встановлюють дані щодо програмного забезпечення, яким користуються співробітники. Навіть відслідковуються вислови та інтерв'ю керівників, щоб у фішинговому листі можна було послатися на запланований захід.

На другому етапі, який називається «озброєння», аналітики шукають явні кіберкриміналістичні докази присутності шкідливого ПЗ. Для більш ефективного забезпечення кіберзахисту своїх клієнтів ведеться база даних всіх інфікованих pdf-файлів, які коли-небудь потрапляли до фахівців компанії. Ці дані використовуються у програмах-сканерах для виявлення підозрілих файлів, автоматично аналізуються усі електроні листи, що отримують співробітники компанії, та відправляють у карантин підозрілі з них, які можуть бути інфіковані зловмисним ПЗ.

Наступними етапами Cyber kill chain є «доставка» (тобто відправка шкідливого ПЗ на електронну пошту або на USB-накопичував), «експлойт» (коли аналітики приділяють особливу увагу пошуку вразливостей нульового дня), «встановлення» на комп'ютер, «управління та контроль» (комунікація з керуючим центором нападу) та «цільові дії» (викрадення файлів, видалення даних або нищення елементів фізичного обладнання). На всі ці дії розробляються відповідні протидії, які підтримуються у актуальному стані.

Виявлений на ранніх етапах (скажімо на другому чи третьому) нападник є менш небезпечний, бо йому ще треба зробити низку кроків до того, як з'явиться можливість нанести свій удар. На останньому же етапі хакер є максимально небезпечним. Якщо фахівці СКС виявляють активність хакерів, то вони негайно повідомляють керівництво про атаку та вживають протидіючі заході. Описана концептуальна схема багаторівневої системи захисту дає можливість блокувати

кібернападників ще до того, як вони наблизяться до мети свого нападу. Таким чином, кіберзахист може більш ефективно використовувати свої ресурси, оскільки не потрібно реагувати на кожне попередження, як на екстрену ситуацію.

2.2 Аналіз методів захисту кіберпростору

Захист кіберпростору потребує не тільки безпечних захисних бар'єрів, але й більш інтенсивного моніторингу систем безпеки та раннього виявлення атак. Автоматичний безперервний моніторинг у реальному часі необхідний для збору та зіставлення даних, а також для ініціювання відповіді на атаки, що є ключовим фактором у запобігання кібератак. Моніторинг виявляє підозрілі шаблони у потоках даних та виявляє атаки на ранніх стадіях. У цьому контексті виявлення має першорядне значення. Система виявлення та попередження вторгнень є системою активного захисту від кібератак, вона може бути встановлена на кінцевій точці, у мережі або на контролері безпеки хмари, який збирає інформацію з хостів та мереж.

На сьогоднішній день системи активного захисту від кібератак поєднують з системами аудиту та моніторингу стану безпеки кіберпростору з метою виявлення аномалій в агрегованих даних та під час їх обробки, які можуть свідчити про наявність активної кіберзагрози.

Інтелектуальна система ІТ-безпеки може задіяти не тільки захисні заходи, але й превентивні й наступальні можливості. Вона виявляє атаки на ранішніх стадіях, відслідковує та знищує шкідливе ПЗ в системі та приваблює нападника у так звані «приманки»: такі фейкові ІТ-інфрастуктури заманюють кібервзлочинців легкою на вигляд добичею, а потім збирає інформацію про них, у той час як реальна ІТ-структура залишається захищеною.

У даний час інфраструктура захисту кіберпростору представлена *комплексною системою захисту інформації* та *комплексною системою антивірусного захисту*. Методи захисту, які там застосовуються, можна умовно розділити на детерміністичний підхід та ймовірнісний підхід в залежності того, як реалізує детектування кіберзагроз.

Детерміністичний підхід можна поділити: на методи на основі відстеження поведінок, які можна пов'язати з відомими кібератаками [44-45]; методи на основі специфікації, які виявляють атаки згідно з політиками, визначеними експертами [22, 23]; методи на основі сигнатурних вердиктів, що використовують послідовності байт, які унікально ідентифікують кібератаку. Сигнатури зазвичай представлені у вигляді правил, що створюються експертами або спеціальними роботами і використовуються кіберспільнотою. У більшості випадків такі сигнатури можуть ефективно виявляти певну групу відомих атак. Однак ці підписи сприйнятливі лише до незначної модифікації коду і майже на працюють при використанні механізмів заплутування чи шифрування шкідливого коду.

Ймовірнісний підхід переважно використовує алгоритми машинного навчання, тому його слід розглядати в контексті методів і моделей, побудованих на основі алгоритмів машинного навчання. Продуктивність таких методів багато в чому залежить від вихідного набору даних. Машинне навчання – наука, що дозволяє комп'ютерам вчитися без явно запрограмованого на це. Машинне навчання застосовує статистику і алгоритми масштабування на великих обсягах даних. Одна з цілей машинного навчання – це досягнення штучного інтелекту. Штучний інтелект – це наука, що дозволяє комп'ютеру автоматизувати те, що потрібно людині: інтелект, аналіз і прийняття рішень.

Тому нині є актуальною задача створення концептуально нових методів інформаційно-аналітичної підтримки прийняття рішень щодо забезпечення інформаційної безпеки кіберпростору. Потреби у розробці новітніх та вдосконаленні наявних методів використання національних інформаційних ресурсів обумовлені вимогами поліпшення та автоматизації робочих інструментів експертів відповідної галузі.

Розглянемо деякі приклади реалізацій методів на основі алгоритмів машинного навчання, що активно застосовуються у кібербезпеці.

1. *Методи виявлення аномалій* відслідковує рідкісні події, які викликають підозри та істотно відрізняючись від більшості даних. Згідно з [48] алгоритми виявлення аномалій існують трьох типів:

- методи виявлення аномалій без вчителя, які працюють на пошук аномалій в наборах даних, тобто шукають такі дані, які найменш схожі на більшість інших нормальних даних;

- методи виявлення аномалій із вчителем, які вимагають набір даних з позначкою як "нормальні" чи "ненормальні" і передбачають підготовку класифікатора;

- методи виявлення аномалій із напівнаглядом, які конструюють модель, що являє собою звичайну поведінку з даного нормального набору даних навчання, а потім перевіряють ймовірність того, що досліджувана модель буде згенерована досліджуваним екземпляром.

2. *Метод зіставлення зі зразком* (pattern matching) проводить аналіз та обробку структур даних на базі виконання певних умов залежно від збігу досліджуваного значення з тим чи іншим зразком (шаблоном), яким може бути частина шкідливого коду чи мережевого трафіка.

3. *Метод асоціативних правил*, використаний у роботі [49], вирішує проблему великої кількості помилкових позитивних сигналів тривоги, які генеруються у системі захисту кіберпростору для виявлення вторгнень, ускладнює розділення помилкових оповіщень від реальних атак. Одним із засобів зменшення цієї проблеми є використання метасигналів або правил, які ідентифікують відомі шаблони атак у потоках сигналів тривоги. Очевидний ризик при такому підході полягає в тому, що база правил не може бути повною стосовно кожного профілю справжньої атаки, особливо тих, які є новими. Зараз нові правила відкриваються вручну, процес, який є дорогим і схильним до помилок. Дослідники представляють новий підхід, що використовує видобуток правил асоціації, щоб скоротити час, що минув від появи нового профілю атаки в даних до його визначення, як правило, в інфраструктурі моніторингу організації. Недоліком методу є обмежений обсяг проведених експериментів та

необхідність апріорних знань про атаку задля виявлення асоціацій, побудови ланцюга атаки та генерації правил.

Таким чином, моделі машинного навчання, що побудовані з урахуванням моделей загроз, являють собою ефективні інструменти для автоматизації виявлення кібератак на кіберпростір, підвищуючи його обороноспроможність. При виборі моделі необхідно керуватися не тільки показниками її ефективності, але і типом навчання моделі (з вчителем чи без нього), прозорістю моделі та інтерпретації результатів.

2.3. Підходи до оцінювання ефективності методів виявлення кібератак

Метою функціонування будь-якої системи кіберзахисту є, в першу чергу, мінімізація проміжку часу $T_{\text{компр}}$ від початку атаки на кіберпростір $t_{\text{атаки}}$ до моменту виявлення та блокування атаки$t_{\text{блок}}$. Крім того, важливим параметром є також фінансові витрати на відновлення працездатності функціонування інфраструктури кіберпростору $\boldsymbol{S}$ та втрати від їх простою $\boldsymbol{V}$, які, звісно, бажано теж мінімізувати. У більшості випадків така мінімізація досягається за рахунок введення певної обчислювальної надмірності у інфраструктуру діагностування кіберпростору $\boldsymbol{D}$, що дозволяє одночасно покращити якість сервісу на час атаки шляхом забезпечення доступності, цілісності та конфіденційності інформації.

Тому у загальному вигляді цільову функцію мети функціонування системи кіберзахисту можна представити у вигляді:

$$\boldsymbol{Z} = min\ \boldsymbol{F}\ (T_{\text{компр}}, S, V, D) = min\ \boldsymbol{F}\ (t_{\text{блок}} - t_{\text{атаки}}, S, V, D). \qquad (1.1)$$

Найбільш адекватними критеріями для оцінювання виявлення системою кібератак можуть бути такі показники як точність та повнота. *Точність* (*Precision*) – це міра того, наскільки точним є робота системи з виявлення кібератак: більша точність відповідає меншій кількості помилкових виявлених атак $\boldsymbol{FP}$ (False Positives). У той же час, *повнота* (*Recall*) показує скільки фактично атак виявила система. Більш високе значення повноти відповідає меншій кількості пропущених атак $\boldsymbol{FN}$ (False Negative). В ідеалі ми хочемо мати

класифікатор з високою точністю і повнотою, оскільки це відповідає низьким значенням ***FP*** і ***FN***. Точність та повнота обчислюються за формулами [46]:

$$\textbf{\textit{Precision}} = TP / (TP + FP), \quad \textbf{\textit{Recall}} = TN / (TN + FN), \tag{1.2}$$

де ***TP*** – кількість кібератак, що вірно виявлені системою;

TN – кількість подій, яких система правильно не визнала кібератакою;

FP – кількість подій помилково виявлених системою, як кібератака;

FN – кількість невиявлених системою кібератак.

Якщо система кіберзахисту функціонує по багатокластерному сценарії, то точність і повнота розраховуються окремо для кожного кластеру. Щоб розрахувати ці метрики для певного кластеру, інші кластери розглядаються як один (такий підхід називається “одним проти всіх”). Нарешті, точність і повнота для всіх кластерів об'єднуються разом з використанням середньозваженої величини [47].

2.4. Інфраструктура системи захисту кіберпростору

CERT-UA, який функціонує в рамках Держспецзв'язку України, при побудові надійної системи кібербезпеки об'єкту рекомендує, в першу чергу, використання наступних елементів [64]:

- ліцензійних операційних систем й інших програмних продуктів, які потрібно своєчасно та систематично оновлювати;
- антивірусного програмного забезпечення з технологією евристичного аналізу;
- мережевих екранів (брандмауерів) та штатних засобів захисту від шкідливого програмного забезпечення;
- систем зберігання та резервного копіювання даних;
- надійних систем криптографічного захисту інформації та автентифікації.

Компоненти інфраструктури системи захисту кіберпростору, як правило, повинні реалізовувати наступні функції:

- розмежування доступу до інформації;
- ідентифікацію та автентифікацію;
- аудиту, моніторингу та керування політикою безпеки;

- виявлення та попередження вторгнень;
- криптографічний захист інформації.

Більшість з наведених функцій реалізуються у рамках захищених операційних систем різного призначення (загального користування та спеціалізованих для обчислювальних систем, технологічних для засобів телекомунікацій тощо). Окремо відокремлюють антивірусні системи, що реалізують функції виявлення і попередження вторгнень в кіберпростір, а також системи криптографічного захисту, які повинні мати свої особливості для кіберпростору. Розглянемо більш детально кожну з названих систем.

2.5. Захищені операційні системи

До захищених операційних систем будемо відносити такі, у яких є спеціально розроблений комплекс систем захисту, що, принаймні, забезпечує захист від наступних загроз: сканування файлової системи, викрадення ключової інформації, підбор паролів, програмних закладок, перевищення повноважень, збирання сміття тощо.

При розробці захищених операційних систем на етапі проектування закладаються усі функціональні можливості захисту (визначення вимог безпеки, розробка моделі безпеки, визначення об’єктів взаємодії, вибір правил і механізмів керування доступом, вибір методів ідентифікації й автентифікації користувачів, визначення множини подій для аудиту), які потім гарантовано реалізуються.

В останній час проходять значні зміни у сфері безпеки операційних систем. Все почалось з того моменту, коли у розробників ОС поступово впевнились щодо неможливості виправлення усіх помилок у програмному коді. Незважаючи на зусилля у код операційних систем, який стає усе складнішим, нові похибки добавляються скоріше ніж виправляються старі. Частина з цих помилок приводить до вразливостей кібербезпеки, що є проблемою. Для її вирішення з’явилося два взаємодоповнюючі підходи, які поліпшили ситуацію з безпекою ОС:

- *перший підхід*, коли у ядро операційної системи добавляють засоби самозахисту. Тобто, у випадку помилки чи атаки система повинна безпечно

обробити цю ситуацію. Наприклад, в минулому році Microsoft Security Response Center надав детальний огляд типів вразливостей і способів боротьби з ними у ядрі Windows. Є також відповідна розроблена карти засобів захисту ядра Linux, яка відображає взаємозв'язки між типами вразливостей, методами їх експлуатації та існуючими механізмами захисту. Однак на практиці впровадження засобів самозахисту ядра операційної системи не буває безкоштовним. За більшу безпеку приходиться платити падінням продуктивності та додатковою складністю для розробників системи.

- *другий підхід* до вирішення проблеми помилок в операційних системах - це безперервне використання автоматичних засобів динамічного та статичного аналізу. Більшість операційних систем написані на мовах програмування низького рівня. Такі мови дають розробнику більше можливостей, але потребує більшої уваги та професіоналізму. Тому на допомогу приходять автоматизовані засоби перевірки – різні методи статичного аналізу (у тому числі пошук помилок по паттернам) та технології динамічного аналізу (наприклад, фаззінг - методика тестування ПЗ випадковими даними). Прикладом проекту, що дав значний вклад в безпеку багатьох операційних систем, є фаззер syzkaller. При цьому у автоматизованих засобів пошуку вразливостей є важливий побічний ефект: вони доступні також атакуючим.

Основними підсистемами, що забезпечують захист операційних систем, є наступні:

- *підсистема розмежування доступу*, яка безпосередньо реалізовує політику безпеки. Вона надає доступ кожному користувачеві лише до тих захищених об'єктів, доступ до яких йому дозволений політикою безпеки;

- *підсистема ідентифікації та автентифікації*, яка забезпечує доступ в систему тільки тих користувачів, які надають свій ідентифікатор та підтверджують його справжність за допомоги додаткової інформації;

- *підсистема аудиту*, яка здійснює реєстрацію усіх подій, що є потенційно небезпечними. Підсистема аудиту здійснює захист журналів, в яких

відбувається реєстрація НСД, а також проводить аналіз журналів та відстеження джерел тих чи інших подій;

- *підсистема керування політикою безпеки* надає інтерфейси, які дозволяють адміністраторам ефективно вирішувати завдання з підтримання адекватної політики безпеки, для чого їм надаються інтерфейси для настроювання підсистем розмежування доступу, ідентифікації, автентифікації та аудиту;

- *підсистема забезпечення цілісності* надає додаткові засоби для захисту цілісності даних не лише від НСД, але й від випадкових помилок та від аварій і збоїв системи. В першу чергу це стосується даних файлових систем, де реалізуються можливості відкату, створення резервних копій і відновлення з них.

2.6. Антивірусні системи

Під системою антивірусного захисту розуміють сукупність програм, які надають можливість виявляти і знешкоджувати відомі шкідливі програми, які відносяться як до вірусів (наприклад, троянські коні, мережеві хробаки, шпигунські програми тощо), так і до засобів здійснення атак. Як правило, антивірусні засоби не входять до складу ОС, а постачаються окремо.

Відомо декілька типів антивірусних систем.

Сигнатурні антивіруси найбільш розповсюджені, вони першими почали розвиватися. Спочатку для успішного детектування вистачало просто ґеш-функції зразка штаму типу CRC або MD5. Але технологія написання вірусів швидко змінюється, при їх створенні використовують різного типу стиск та шифрування (до 80% сучасних вірусів упакована). Більшість сигнатурних антивірусів будується на статичному аналізі з використанням інтелектуальних алгоритмів. Статичний аналіз передбачає вилучення необхідної інформації без запуску на виконання файлів з подальшим застосуванням алгоритмів дискретної математики, теорії компіляторів, штучного інтелекту, статистики тощо, з метою отримання певної сигнатури, достатньо стабільної до метаморфних змін. Інколи використовується динамічний аналіз, коли код, що аналізується, виконується або на емуляторі, або під керівництвом

трасировщика [50] чи інструментуючого фреймворка [51], або за допомоги прямої трансляції [52].

Для того, щоб антивірус запрацював необхідно вірус виловити, згенерувати необхідний набір інструкцій для отримання сигнатури та відновити усі клієнтські бази антивірусних даних. Таким чином, час, який минув від появи штаму вірусу до початку його знаходження, був відданий вірусу для зараження комп'ютерів. Крупні антивірусні компанії генерують сигнатури на нові зразки вірусів за 6-8 годин з моменту появи зразка у VirusTotal, а деякі штами вірусів виявляються більш ніж за добу. А за тиждень з'являються більше 110 нових штамів, що належать тільки до двох розповсюджений класів вірусів Zeus та TDSS.

Сигнатури на регулярних виразах є тільки частиною сучасного движка антивірусу. Любий сучасний антивірус має HIPS-компонент (Host-based Sntrusion Prevention) *проактивної антивірусної системи*, що аналізує поведінку програм. Фундаментальна складність проактивної системи полягає у тому, що поза контекстом неможливо вказати є та чи інша конкретна дія шкідливою. Цю проблему можна вирішити або запитом до користувача, або враховувати історію дій програми та мати список правил поведінки у тому чи іншому форматі. Оскільки запитувати користувача про кожну дію програми нераціонально, то використовують проактивну систему на базі HIPS-компонент, яка веде списки правил, типові приклади та різні виключення. Відомо декілька підходів подолання проактивних систем, а проти *0-day* HIPS не захистить за визначенням.

Хмарні антивіруси [53] будуються за принципом тонкого клієнта та грубого серверу, коли тонкий клієнт передає той чи інший підозрілий зміст для детального антивірусного аналізу у хмару. Для роботи хмарної антивірусної системи необхідний постійно діючий інтернет-канал та необхідно мати критерій відбору інформації для відправки у хмару. Тому усім файлам приписується певна «репутація» і файли з низькою репутацією відправляються

на аналіз у хмару. Хмари на основі репутації файлів страждають хибними спрацюваннями.

У більшості сучасних антивірусних методів є суттєві недоліки. Методи статичного аналізу не забезпечують надійне виявлення зашифрованого чи упакованого шкідливого програмного забезпечення. Хмарні системи неефективні з точки зору роботи на упередження або страдають хибними спрацьовуваннями. Проактивні системи потребують втручання користувача, що у більшості випадків приводить до неусвідомлених його дій і відключення захисту.

У зв'язку з цим, бачиться перспективним новий підхід до виявлення шкідливого ПЗ на базі динамічних структур [54], які будуються на основі аналізу послідовності системних викликів (syscalls), тому що такі послідовності є одною з найбільш стабільних характеристик програми. Фактично люба дія будь-якої програми (наприклад, створення файлу, мережева або міжпроцесорна взаємодія) обов'язково потребує викликів API операційної системи. Вірусне ПЗ також використовує необхідні виклики Native API або навіть безпосередньо syscall. Таким чином, даний підхід має наступні переваги:

- обійти механізм системних викликів з програми користувача практично неможливо;

- сигнатура від системних викликів, по суті, виступає максимально інтелектуальною проактивною системою, яка абсолютно точно знає, яка послідовність дій конкретного вірусного ПЗ наносить шкоду;

- у зв'язку з тим, що сигнатура системних викликів може бути знята з довільної точки будь-якої програми, то існує можливість створювати сигнатури робочих тіл троянців;

- мінімальною кількістю сигнатур від системних викликів можна покрити ціле сімейство шкідливих програм.

2.7. Криптографічне забезпечення безпеки кіберпростору

Використання криптографічного захисту розглядається як важливий елемент забезпечення безпеки кіберпростору. Використання апаратного

шифрування з приватним алгоритмом може зірвати особливо віроломні кібератаки, пов’язані з такими діями, як проникнення і шпіонаж в комп’ютерних мережах шляхом маскування, маніпулювання та підслуховування секретних даних і розміщення зловмисного програмного забезпечення.

Для ефективного криптографічного захисту від кібератак поєднання програмних та апаратних засобів має вирішальне значення. Слід відмітити, що програмна реалізація криптографічного захисту не може надавати достатню інформаційну безпеку. Надійне шифрування повинно базуватися на швидкісних апаратних компонентах. Вони являють собою статичну міру безпеки в рамках загальної стратегії кібербезпеки. Навіть, якщо нападники можуть проникнути в програмні застосунки, то ключі та криптографічні параметри, а також обчислювання залишаються повністю захищеними в межах апаратури.

Системи криптографічного захисту застосовуються для захисту конфіденційності і цілісності інформації, для автентифікації і забезпечення неможливості відмовлення від авторства. Криптографічні функції можуть використовуватись у якості самостійних засобів захисту, або в якості допоміжних механізмів в інших засобах захисту (наприклад, автентифікація разом з ідентифікацією).

Сучасна інфраструктура кіберпростору з чисельними користувачами та розвинутими комунікаціями ставить нові вимоги до криптографічної системи криптозахисту, деякі з яких можуть вирішити алгоритми автентифікованого шифрування (authenticated encryption - одночасного шифрування та імітозахисту). Алгоритми автентифікованого шифрування забезпечують конфіденційність, контроль цілісності й автентичність даних. Абоненти, у яких є загальний ключ, можуть організувати конфіденційний обмін повідомленнями, а також організувати контроль цілісності при обміні повідомленнями шляхом додавання до них імітовставок при відправці та перевірки їх при отриманні. Перевірка імітовставок дозволяє одержувачу переконатися в тому, що сторона-відправник знає ключ, а прийняте повідомлення є достовірне.

Автентифіковане шифрування забезпечує певну гнучкість у функціональності: ключі можуть оновлюватися в процесі обробки даних; можливо шифрувати тільки окремі частини повідомлення; можливо чергувати шифровані та відкриті повідомлення; імітовставки можуть бути відсутні або, навпаки, зустрічатися кілька разів.

Існує декілька підходів побудови алгоритмів автентифікованого шифрування. Класичний підхід використовує композиції з алгоритму шифрування та алгоритму імітозахисту, наприклад композицію типу «Encrypt-then-MAC» (зашифрувати, а потім обчислити імітовставку) [55]. Незважаючи, що дана композиція є надійною, вона не забезпечує необхідної швидкості обробки даних та потребує використання двох різних ключів, один з яких застосовується для шифрування, а іншій — для імітозахисту.

Більш ефективним підходом до побудови алгоритмів автентифікованого шифрування є розробка спеціальних алгоритмів. В останні роки у симметрічній криптографії виник новий напрямок PBC- криптография (permutation-based cryptography) на базі sponge-функцій [58]. Sponge-функції відносяться до *LRX*-класу криптографічних перетворень і можуть ефективно реалізуватися на програмованих логічних інтегральних схемах, тому що в них задіяні тільки логічні операції (*L*), циклічні зсуви (*R*) та виключне АБО (*X*). Це дає їм певні переваги у створенні високопродуктивних засобів криптографічного захисту інформації різноманітного призначення, у тому числі алгоритмів автентифікованого шифрування [59].

Конструкції sponge є ітераційними. Їх основою є sponge-функція, яка визначає складне бієктивне перетворення над внутрішнім станом $S \in \{0,1\}^b$ конструкції. У стані S виділяють підстани $S_r \in \{0,1\}^r$ та $S_c \in \{0,1\}^c$, такі що $r+c=b$ та $S=S_r||S_c$. Підстан S_r може видаватися назовні, а підстан S_c - не видається та зберігається в секреті. Різні значення r та c визначають компроміс між швидкістю обробки даних та стійкістю sponge-конструкції: збільшення r з одночасним зменшенням c призводить до збільшення швидкості та до зниження стійкості.

Для конструкцій sponge виділяють дві фази функціонування: “вбирання” (the absorbing phase) та “вичавлення” (the squeezing phase). При цьому вхідні дані обробляються в першій фазі, а вихідні дані видаються в другій. На вхід sponge-алгоритму шифрування $\boldsymbol{E}$ подається секретний ключ $\boldsymbol{K}$, відкриті дані (заголовок) $\boldsymbol{A}$ та відкритий текст $\boldsymbol{M}$, при цьому $\boldsymbol{A}$ чи $\boldsymbol{M}$ можуть бути пустими. Виходом алгоритму $\boldsymbol{E}$ є шифртекст $\boldsymbol{C}$, де $|\boldsymbol{C}| = |\boldsymbol{M}|$, і імітовставка $\boldsymbol{T}$, яка контролює цілісність и автентичність $\boldsymbol{A}$ і $\boldsymbol{M}$: $\boldsymbol{E}(\boldsymbol{K}, \boldsymbol{A}, \boldsymbol{M}) = (\boldsymbol{C}, \boldsymbol{T})$.

Sponge-алгоритм розшифрування $\boldsymbol{D}$ приймає на вході ключ $\boldsymbol{K}$, відкриті дані $\boldsymbol{A}$, шифртекст $\boldsymbol{C}$ та імітовставку $\boldsymbol{T}$. Виходом алгоритму є відкритий текст $\boldsymbol{M}$ та , якщо перевірка імітовставки була успішною, символ «1», у іншому випадку — «0»: $\boldsymbol{D}(\boldsymbol{K}, \boldsymbol{A}, \boldsymbol{C}, \boldsymbol{T}) \in \{\boldsymbol{M}, 1\}$.

Алгоритми $\boldsymbol{E}$ і $\boldsymbol{D}$ можуть також залежить ще від наступних параметрів: довжини ключа, довжини імітовставки, довжини внутрішнього стану.

В деяких sponge-алгоритмах імітовставки можуть бути проміжними, що дозволяє отримувачу раніше визначити порушення цілісності, ще до завершення обробки всього повідомлення. Ця властивість алгоритму є важливим при обробці повідомлень великої довжини.

В роботі [58] для sponge-алгоритмів (у припущенні, що $\boldsymbol{K} \in \{0,1\}^{K\vee}$ зберігається таємно та обирається випадково та рівномірно) визначають наступні признаки безпеки:

1. *Неможливість відновлення ключа* (the key recovery infeasibility): ймовірність знаходження супротивником ключа $\boldsymbol{K}$ при будь-яких атаках, де він може перевірити n ключів, не перевищує $n \cdot 2^{K\vee}$.

2. *Неможливість підробки імітовставки* (the tag forgery infeasibility): навіть якщо супротивнику відомий шифртекст $\boldsymbol{C}$, що відповідає $(\boldsymbol{A},\boldsymbol{M})$, та виходи (C_i, T_i) для обраних їм входів (A_i, M_i), де $(A_i, M_i) \neq (\boldsymbol{A},\boldsymbol{M})$, ймовірність успішного визначення імітовставки для будь-якої пари $(\boldsymbol{A},\boldsymbol{M})$ дорівнює $2^{-T\vee}$.

3. *Неможливість відновлення відкритого тексту* (the plain text recovery infeasibility): найбільш ефективним методом отримати супротивнику будь-яку інформацію щодо $\boldsymbol{M}$ (за винятком довжини) по виходу $(\boldsymbol{C},\boldsymbol{T})$, що відповідає

входу (***A***,***M***), де ***M*** невідомо, а ***A*** вибирається супротивником, є лише відновлення ключа, навіть якщо йому відомі виходи (C_i, T_i) для обраних їм входів (A_i, M_i), де $A_i \neq \boldsymbol{A}$.

На базі одної sponge-функції можна побудувати ціле сімейство криптографічних алгоритмів та протоколів різного призначення: класичне ґешування, древовидне ґешування, поточного шифрування, імітозахисту, протоколів автентифікації, генерації псевдовипадкових чисел, організації захищених з'єднань тощо.

Висновки до другого розділу

У розділі проведено дослідження сучасних методів та моделей захищеності кіберпростору.

Розглянуто найбільш відомі підходи до моделювання систем захисту кіберпростору, а саме м*оделі стримування атак на кіберпростір; моделі захисту персональних даних; моделі управління доступом; моделі реагування на кіберінциденти; моделі кіберзагроз.*

Методи захисту умовно розділено на детерміністичний підхід та ймовірнісний підхід в залежності того, як реалізує детектування кіберзагроз. *Детерміністичний підхід* поділено на методи на основі відстеження поведінок, які можна пов'язати з відомими кібератаками; методи на основі специфікації, які виявляють атаки згідно з політиками, визначеними експертами; методи на основі сигнатурних вердиктів, що використовують послідовності байт, які унікально ідентифікують кібератаку. *Ймовірнісний підхід* переважно використовує алгоритми машинного навчання, тому його слід розглядати в контексті методів і моделей, побудованих на основі алгоритмів машинного навчання. До методів на основі алгоритмів машинного навчання, що активно застосовуються у кібербезпеці, віднесено: м*етоди виявлення аномалій, метод зіставлення зі зразком; метод асоціативних правил. Зроблено висновок, що* моделі машинного навчання, що побудовані з урахуванням моделей загроз, являють собою ефективні інструменти для автоматизації виявлення кібератак на кіберпростір, підвищуючи його обороноспроможність, а при виборі моделі необхідно керуватися не тільки показниками її ефективності, але і типом навчання моделі (з вчителем чи без нього), прозорістю моделі та інтерпретації результатів.

Запропоновано підходи до оцінювання ефективності методів виявлення кібератак. Зокрема, якщо система кіберзахисту функціонує по багатокластерному сценарії, то точність і повнота розраховуються окремо для кожного кластеру. Щоб розрахувати ці метрики для певного кластеру, інші кластери розглядаються як один (такий підхід називається “одним проти всіх”).

Нарешті, точність і повнота для всіх кластерів об'єднуються разом з використанням середньозваженої величини

З’ясовано, що при побудові надійної системи кібербезпеки об'єкту необхідно використовувати в першу чергу: ліцензійні операційних систем й інших програмних продуктів, які потрібно своєчасно та систематично оновлювати; антивірусне програмне забезпечення з технологією евристичного аналізу; мережеві екрани (брандмауери) та штатні засоби захисту від шкідливого програмного забезпечення; систем зберігання та резервного копіювання даних; надійних систем криптографічного захисту інформації та автентифікації.

Підходи до уникнення помилок ОС, що призводить до вразливостей кібербезпеки: *перший підхід*, коли у ядро операційної системи добавляють засоби самозахисту; *другий підхід* до вирішення проблеми помилок в операційних системах - це безперервне використання автоматичних засобів динамічного та статичного аналізу.

Виокремлено основні підсистеми, що забезпечують захист операційних систем: *підсистема розмежування доступу*; *підсистема ідентифікації та автентифікації*; *підсистема аудиту*; *підсистема керування політикою безпеки*; *підсистема забезпечення цілісності*.

Найбільш широко вживаними у контексті забезпечення кібербезпеки антивірусними системами виявились с*игнатурні антивіруси* найбільш розповсюджені, вони першими почали розвиватися; х*марні антивіруси*, які будуються за принципом тонкого клієнта та грубого серверу, коли тонкий клієнт передає той чи інший підозрілий зміст для детального антивірусного аналізу у хмару.

Криптографічного захисту розглянуто як важливий елемент забезпечення безпеки кіберпростору. Зроблено висновок, що для ефективного криптографічного захисту від кібератак необхідно поєднувати програмні та апаратні засоби криптозахисту.

РОЗДІЛ 3

РОЗРОБКА МЕТОДУ ТА ЙОГО ЕКСПЕРИМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ

3.1. Побудова методу вибору оптимального стандартного функціонального профілю захищеності

Згідно із НД ТЗІ 2.5-005-99 [1] метою введення класифікації АС і стандартних функціональних профілів захищеності є полегшення задачі співставлення вимог до комплексу засобів захисту (КЗЗ) обчислювальної системи автоматизованої системи (АС) з характеристиками самої АС. Стандартний функціональний профіль захищеності являє собою перелік мінімально необхідних рівнів послуг, які повинен реалізовувати КЗЗ обчислювальної системи АС, щоб задовольняти певні вимоги щодо захищеності інформації, яка обробляється в даній АС. Стандартні функціональні профілі будуються на підставі існуючих вимог щодо захисту певної інформації від певних загроз і відомих на сьогоднішній день функціональних послуг, що дозволяють протистояти даним загрозам і забезпечувати виконання пред'явлених вимог.

Загально відомо, що інформація з точки зору безпеки характеризується такими властивостями: конфіденційністю, цілісністю і доступністю. У кожному класі АС виділяються відповідні підкласи у їх різних комбінаціях (К, Ц, Д, КЦ, КД, ЦД, КЦД тощо) [1]. При чому кожний підклас деякого класу складається з певної кількості ієрархічних стандартних функціональних профілів. Ця кількість може бути різною від профілю до профілю. Стандартні функціональні профілі є ієрархічними, оскільки їх реалізація забезпечує наростаючу захищеність.

Під час створення нових функціональних профілів необхідно дотримуватись описаних в НД ТЗІ 2.5-004-99 [2] умов для кожної із послуг, що включаються до профілю. Послуги можуть містити декілька рівнів захисту (1 – мінімальний, 2 – базовий, 3 – повний, 4 – абсолютний). Рівні розпочинаються з

першого і зростають до рівня n, де n - визначене для кожного виду послуг число. Чим вище рівень послуги, тим більш складно забезпечується захист від різного типу загроз. Отже, послуга є набором функцій, що дозволяють забезпечити захист від певної сукупності загроз.

Розглянувши загальні питання формування стандартного функціонального профілю захищеності (СФПЗ), перейдімо до його вибору та оптимізації цього рішення.

У НД ТЗІ 2.5-005 -99 налічується 22 послуги, які забезпечують захист від чотирьох основних типів загроз (конфіденційності, цілісності, доступності та їх всі можливі комбінації) [1].

СФПЗ є мінімальним набором необхідних послуг для визначеного рівня та для забезпечення обраного рівня захищеності, але вибір способів їх реалізації залишається за розробником (експертом). За рахунок реалізації обраного СФПЗ забезпечується зменшення збитку, який може бути нанесений ОЗ.

Формалізуємо завдання вибору оптимального СФПЗ. Для цього побудуємо математичну модель СФПЗ.

Нехай $\overline{F}$ – множина усіх можливих СФПЗ заданих рівнів, які визначаються вимогами до захищеності інформації, F–вектор розмірності 22 (нормативно визначена кількість). Компонентами вектора F є булеві змінні$f_i \in \{0,1\}$. Розмірність вектора F введена для зручності і уніфікації опису СФПЗ, оскільки відомо, що до складу багатьох СФПЗ входять не усі послуги. У разі відсутності якої-небудь послуги відповідна компонента дорівнює нулю. *S(F)* - загальний відвернений збиток.

Тоді формальна постановка задачі має вигляд:

$$S(F_0) = \max_{F \in \overline{F}} S(F) \qquad (3.1)$$

при обмеженні

$$C(F) \le C_r, \qquad (3.2)$$

де F– деякий вектор, що описує СФПЗ, $\overline{F}$ –сукупність усіх допустимих профілів,F_0- оптимальне значення вектора F,аC_r- допустимі витрати на СФПЗ.

Таким чином, нас перш за все буде цікавити значенняF_0, який визначає оптимальний при даній постановці задачі набір послуг, що будуть влючені до СФПЗ.

Відмітимо, що допустима інша постановка задачі, а саме:

$$C(F_0) = \min_{F \in \overline{F}} C(F), \qquad (3.3)$$

$$S(F) \geq C_r. \qquad (3.4)$$

У даному випадку знаходимо F_0, при якому витрати на СФПЗ будуть мінімальними, і при цьому відвернений можливий збиток складатиме не менше C_r.

Припустимо, що може бути реалізований деякий набір вразливостей ***t***, внаслідок чого може виникнути ряд загроз i, $i = \overline{1, \dots n}$. При цьому кожну i –у загрозу характеризує ймовірність її появиP_{t_i} та можливий збиток інформаційного середовища, S_i. Позначимо P_i- ймовірність відвернення *i*-ої загрози, а ймовірний відвернений збиток за рахунок запобігання *i*-ої загрози через$r_i, r_i = P_i P_{it} S_i$.

Загрози нейтралізуються за рахунок реалізації функціональних послуг, тобто відповідними засобами і механізмами СЗІ. Тоді P_i - вірогідність нейтралізації кожної *i*-ої загрози буде основною характеристикою СЗІ. Очевидно, що ймовірність нейтралізації *i*-ої загрози:$P_i = g_i(F) = g_i(f_{1,} f_{2,\dots,} f_m)$, де *m*=22.

Позначимоp_{ij} – ймовірність відвернення *i*-ої загрози за рахунок включення до СФПЗ компонентиf_j, маємо:

$$P_i = \sum_{j=1}^{m} p_{ij} f_j - \sum_{j,l=1, l>j}^{m} p_{ij} p_{il} f_j f_l + \dots + (-1)^{m-1} \prod_{j=1}^{m} p_{ij} f_j \qquad (3.5)$$

Значення ймовірностей p_{ij} можна знайти за допомогою експертів. Тоді загальний відвернений збиток виражається співвідношенням:

$$S(F) = \sum_{i=1}^{n} r_i = \sum_{i=1}^{n} P_i P_{it} S_i \qquad (3.6)$$

Таким чином, (6) визначає явний вид цільової функції $S(F)$ задачі математичного програмування (1) - (2). Однак функція $S(F)$ визначена на булевій множині, що суттєво ускладнює проблему пошуку оптимального розв’язку.

З метою спрощення задачі можна розглянути дещо інший підхід до побудови цільової функції. Цілком природньо серед усіх можливих послуг $f_{j,}$ які дозволяють усунути *i*-ту загрозу вибрати таку, для якої ймовірність p_{ij} є максимальною, тоді

$$S(F) = \sum_{i=1}^{n} P_{it} S_i \max_{f_j} \{p_{ij} f_j\} \qquad (3.7)$$

Вірогідність появи *i*-ої загрози P_{it} визначається таким чином. Як було вказано раніше, кожна загроза залежить від вірогідності використання деякої множини вразливостей$V_{ij} = \{v_{ij}, i = 1, \dots, n\}$, тобто $P_{it} = f_i(v_{ij}, \dots, v\ )$. Даний показник також можна визначити на основі експертного методу.

Вірогідність використання *j*-ої вразливостіv_{ij}можна визначити за допомогою обчислення відносної частоти їх появи. А саме,

$$v_{ij} = \frac{\lambda_{ij}}{\sum_{k=1}^{n} \lambda_{ik}}, \qquad (3.8)$$

деλ_{ij} - частота виникнення *j*-ої вразливості, а *i* - відповідний номер загрози.

Отже, запропоновано метод вибору оптимального функціонального профілю захищеності (ВОФПЗ), який складається з наступних кроків:

- відбір експертів для визначення та оцінки показників відповідних ймовірностей;
- збір інформації та її обробка;
- обчислення показника вірогідності появи *i*-ої загрози;
- обчислення показника вірогідності відвернення *i*-ої загрози,
- обчислення показника вірогідності використання *j*-ої вразливостіv_{ij};
- обчислення показника відверненого збитку;
- оцінка оптимальності СФПЗ за умови виконання $S(F_0) = \max_{F \in \overline{F}} S(F)$при обмеженні $C(F) \le C_r$

На рис. 3.1 представлено схему методу метод вибору оптимального функціонального профілю захищеності об'єкту захисту (ВОФПЗ).

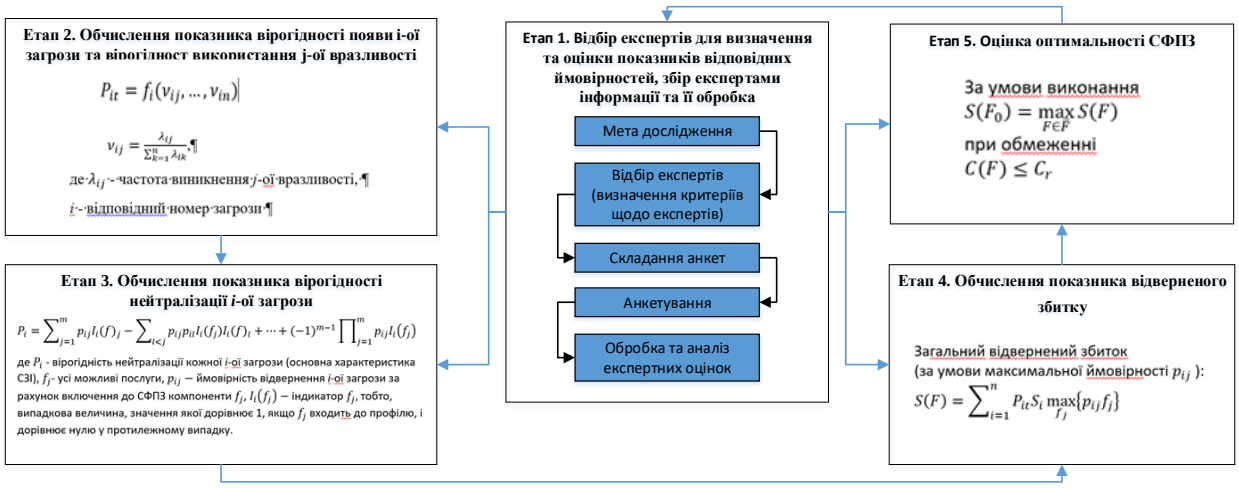


Рис.3.1. Схематичне представлення методу вибору оптимального Функціонального профілю захищеності об'єкту захисту (ВОФПЗ)

3.2. Застосування розробленого методу до вибору функціонального профілю захищеності

Проілюструємо застосування запропонованого методу на прикладі. Нехай відомо (встановлено на основі статистичних даних), що з ймовірностями 0,2; 0,2; 0,4; 0,6 можуть бути реалізовані наступні типові загрози НСД:

1. Шахрайське копіювання ПЗ.
2. Використання підроблених або скопійованих ПЗ.
3. Спотворення даних.
4. Незаконна обробка даних.

що, в свою чергу, може привести до втрати конфеденціальності та/або цілісності інформації. Для відвернення названих загроз можна обрати функціональні послуги $f_{k_1}, f_{k_2}, f_{k_3}, f_{k_4}, f_{k_5}, f_{k_6}, f_{k_7}, f_{k_8}, f_{k_9}$, із них $f_{k_1}, f_{k_2}, f_{k_3}$ – для відвернення першої загрози, f_{k_4}, f_{k_5} – для відвернення другої загрози, відповідно f_{k_6}, f_{k_7} і f_{k_8}, f_{k_9} – для відвернення третьої та четвертої загроз. Експертним методом встановлюємо значення ймовірностей p_{ij} (табл. 3.1).

Таблиця 3.1

Значення ймовірностей p_{ij}

f_j	f_{k_1}	f_{k_2}	f_{k_3}	f_{k_4}	f_{k_5}	f_{k_6}	f_{k_7}	f_{k_8}	f_{k_9}

p_{ij}	p_{1k_1} $= 0{,}6$	p_{1k_2} $= 0{,}6$	p_{1k_3} $= 0{,}5$	p_{2k_4} $= 0{,}7$	p_{2k_5} $= 0{,}5$	p_{3k_6} $= 0{,}7$	p_{3k_7} $= 0{,}6$	p_{4k_8} $= 0{,}8$	p_{4k_9} $= 0{,}8$

За формулою (3.5) розрахуємо ймовірність відбиття загроз, маємо:

$$P_1 = 0{,}92; P_2 = 0{,}85; P_3 = 0{,}88; P_4 = 0{,}96.$$

Відомо, що можливі збитки від реалізації загроз складають відповідно

$$S_1 = 10; S_2 = 6; S_3 = 12; S_4 = 20$$

тисяч гривень. Розрахуємо ймовірні відвернуті збитки: $r_1 = 1{,}84; r_2 = 1{,}02;\ r_3 = 4{,}224; r_4 = 11{,}52.$ Нехай, крім того, відома вартість функціональних послуг, яка відповідно складає 1,5; 0,5; 2 і 3 тис. грн.; $C_r = 5{,}5$ тис. грн. Пошук оптимального розв'язку задачі (3.1)-(3.2) можна інтерпретувати як задачу про пакування рюкзака, яку розв'яжемо методом динамічного програмування. Таким чином, маємо чотири СЗІ для відвернення загроз, кожна з яких характеризується двома значеннями $C_i, r_i,$ відповідно, витратами на придбання послуги (C_i), та ймовірним відверненим збитком (r_i) (табл. 3.2).

Таблиця 3.2

Значення витрат на придбання послуги (C_i)
та ймовірного відверненого збитку (r_i)

Номер ЗСІ	1	2	3	4
C_i	1,5	0,5	2	3
r_i	1,84	1,02	4,224	11,52

У даній задачі зручно провести індукцію по можливим витратам на придбання послуг з кроком 0,5. Результати реалізації алгоритму наведені в таблиці 2. Значеня кожної клітинки таблиці, $a_{c_i j,}$ дорівнює максимальному ймовірному відверненому збитку за умови, що в наявності є $k \le j$ послуг ЗІ, а допустимі витрати на їх придбаня складають c_i. Наприклад, значеня першого стобпчика дорівнюють максимальному ймовірному відверненому збитку, якщо маємо тільки ЗСІ для відбиття першої загрози. Розрахунки значень комірок таблиці виконані за формулою:

$$a_{[c_i][j]} = max\begin{cases} a_{[c_i - c_j][j-1]} + r_j \\ a_{[c_i][j-1]} \end{cases} \qquad (3.9)$$

Проілюструємо алгоритм заповнення таблиці на прикладі третього стовпчика, $C_3 = 2, r_3 = 4{,}224$. Поки $c_i < 2$, ми не можемо придбати третю послугу ЗІ, тому у нулевий , перший , другий та третій рядки третього стовпчика переносимо відповідні значення другого. На четвертій ітерації

$$a_{[c|\ \ |5][3]} = max\{a_{[c_1][2]} + r_3, a_{[c_5][2]}\} = max\{1{,}02 + 4{,}224; 2{,}86\} = 5{,}244;$$

Далі $a_{[c|\ \ |4][3]} = max\{a_{[c_0][2]} + r_3, a_{[c_4][2]}\} = max\{4{,}224; 2{,}86\} = 4{,}224;$

$$a_{[c|\ \ |5][3]} = max\{a_{[c_1][2]} + r_3, a_{[c_5][2]}\} = max\{1{,}02 + 4{,}224; 2{,}86\} = 5{,}244;$$

$$a_{[c|\ \ |6][3]} = max\{a_{[c_2][2]} + r_3, a_{[c_6][2]}\} = max\{1{,}02 + 4{,}224; 2{,}86\} = 5{,}244;$$

$$a_{[c|\ \ |7][3]} = max\{a_{[c_3][2]} + r_3, a_{[c_7][2]}\} = max\{1{,}84 + 4{,}224; 2{,}86\} = 6{,}064;$$

$$a_{[c|\ \ |8][3]} = max\{a_{[c_4][2]} + r_3, a_{[c_8][2]}\} = max\{2{,}86 + 4{,}224; 2{,}86\} = 7{,}084;$$

Аналогічно знаходимо $a_{[c|\ \ |8][3]}; a_{[c|\ \ |10][3]}, a_{[c|\ \ |11][3]}$ знаходимо.

Результати реалізації алгоритму наведені в таблиці 3.3.

Таблиця 3.3

Результати реалізації алгоритму

	1	2	3	3
0	0	0	0	0
0,5	0	1,02	1,02	1,02
1,0	0	1,02	1,02	1,02
1,5	1,84	1,84	1,84	1,84
2,0	1,84	2,86	4,224	4,224
2,5	1,84	2,86	5,244	5,244
3,0	1,84	2,86	5,244	11,52
3,5	1,84	2,86	6,064	12,54
4,0	1,84	2,86	7,084	12,54
4,5	1,84	2,86	7,084	13,36
5,0	1,84	2,86	7,084	15,744
5,5	1,84	2,86	7,084	16,764

Таким чином, при заданих фінансових обмеження на реалізацію захисту максимальний відвернутий збиток складатиме 16,764 тис. грн.

Далі експерт має визначити, виходячи з моделі загроз, яка з властивостей К, Ц, Д або їх комбінація потребують захисту (Додаток Б).

Зазначимо, що загрози кіберпростору за впливом на базові характеристики безпеки інформаційних ресурсів (конфіденційність, цілісність, доступність) у відповідності з джерелом [65] поділяють на:

- К-тип (загроза конфіденційності);
- Ц-тип (загроза цілісності);
- Д-тип (загроза доступності);
- КЦ-тип;
- КД-тип;
- ЦД-тип;
- КЦД-тип.

Природа джерела загроз та стан джерела загроз розділяють на:

- об'єктивна (загроза, виникнення якої не залежить від прямої діяльності людини і пов'язана з різними стихійними природними явищами, такими, як пожежі, блискавки, землетрусу, радіоактивне випромінювання, нападу гризунів і т.п.);
- суб'єктивна (загроза, виникнення якої залежить від діяльності людини).

Суб’єктивну загрозу за мотивом поділяють на активну, таку що пов’язана з діями людини, які направленні на отримання певної вигоди та пасивну, тобто ту, яка виключає вказану складову і пов’язана з помилками людини [66]. Пасивні загрози - це помилки системи (пошкодження окремих компонентів обладнання, тобто апаратного забезпечення підприємства) та катастрофи [67]. Також зазначають, що пасивна загроза - несанкціонований доступ до інформації без зміни стану самої системи, активна - несанкціонована зміна системи, яка вносить певні зміни в стан самої системи [68].

Для прикладу, представимо в табл. 3.4 множину профілів та послуг, якими характеризується АС класу 1.

Таблиця 3.4

Стандартні функціональні профілі захищеності

Послуги		Типи загроз та рівні захисту																					
		К		Ц		Д				КЦ		КД				ЦД				КЦД			
		1	2	1	2	1	2	3	4	1	2	1	2	3	4	1	2	3	4	1	2	3	4
Конфіденційність	КА	0	1	0	0	0	0	0	0	0	1	1	1	1	1	0	0	0	0	1	1	1	1
	КО	0	1	0	0	0	0	0	0	0	1	1	1	1	1	0	0	0	0	1	1	1	1
	КК	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Цілісність	ЦА	0	0	0	2	0	0	0	0	0	2	0	0	0	0	1	1	1	1	1	1	1	1
	ЦО	0	0	0	1	0	0	0	0	0	1	0	0	0	0	1	1	1	1	1	1	1	1
Достовірність	ДР	0	0	0	0	1	2	2	2	0	0	1	2	2	2	1	2	2	2	1	2	2	2
	ДС	0	0	0	0	0	1	2	3	0	0	0	1	2	2	0	1	2	3	0	1	2	3
	ДЗ	0	0	0	0	0	1	2	3	0	0	0	1	2	3	0	1	2	3	0	1	2	3
	ДВ	0	0	0	0	1	2	2	3	0	0	1	2	2	3	1	2	2	3	1	2	2	3

Примітка: 0 – ставився у випадку, якщо певна послуга в профілі взагалі відсутня, 1,2,3 – рівні захисту у відповідному СФПЗ.

З табл. 3.4 видно, що до всіх профілів включені послуги НР, НИ,НК, НО, НЦ, НТ, проте відсутні НВ, НА та НП, в сукупності всі вони характеризують у СФПЗ спостереженість. Також жодного разу не зустрічались деякі характеристики і інших властивостей інформації (конфіденційність, цілісність), зокрема, КД, КК, КВ, ЦД, ЦВ.

Зауважимо, що наявність спостереженості у всіх СФПЗ обумовлюється тим, що спостереженість є властивістю системи, яка стосується її керованості, а тому має бути притаманна всім системам, що реалізуються функції захисту інформації (ЗІ). Аналогічне явище щодо спостереженості присутнє і в СФПЗ АС класу 2 та АС класу 3 (Додаток В).

Оскільки максимальний відвернутий збиток складатиме 16,764 тис. грн., це незначна сума, то експерту варто зупинитись на стандартних функціональних профілях захищеності для автоматизованих систем класу 1. СФПЗ, який за заданих умов буде забезпечувати максимальний захист (рис. 3.2):

1.КЦД.2 = { КА-1, КО-1, ЦА-1, ЦО-1, ДР-2, ДС-1, ДЗ-1, ДВ-2, НР-2, НИ-2, НК-1, НО-1, НЦ-1, НТ-2 }

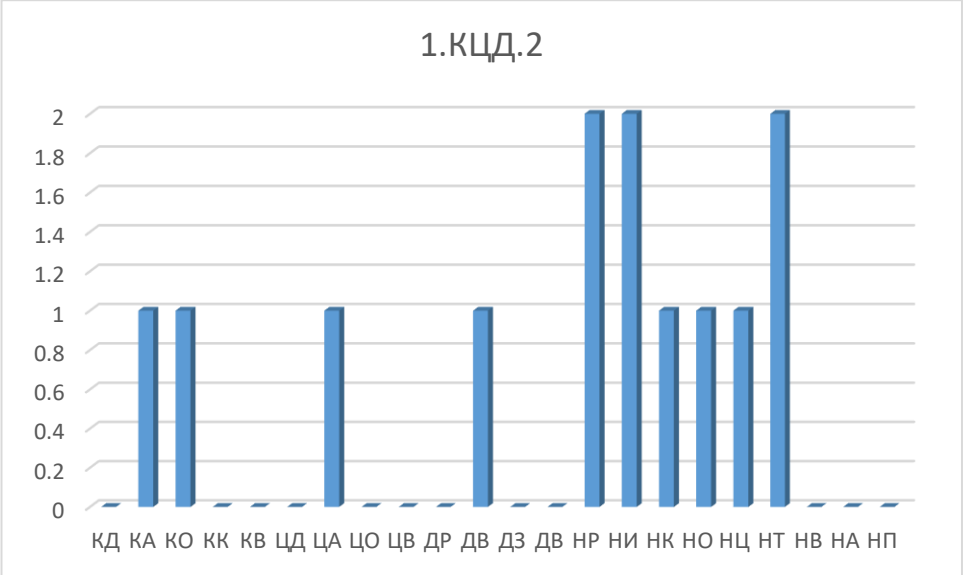


Рис. 3.2. Графічне представлення СФПЗ 1.КЦД.2

Застосунок 2.

Номер загрози	1	2	3	4
p_1 (ймовірність появи загрози)	0.5	0,4	0,3	0,6
S_i (можливі збитки від реалізації загроз)	20	25	30	50

	Відвернення загрози 1		Відвернення загрози 2		Відвернення загрози 3		Відвернення загрози 4		
f_j (послуги)	f_{k_1}	f_{k_2}	f_{k_3}	f_{k_4}	f_{k_5}	f_{k_6}	f_{k_7}	f_{k_8}	f_{k_9}
p_{ij} (ймовірність відбиття загрози певною послугою)	$p_{1k_1} = 0,6$	$p_{1k_2} = 0,6$	$p_{1k_3} = 0,5$	$p_{2k_4} = 0,7$	$p_{2k_5} = 0,5$	$p_{3k_6} = 0,7$	$p_{3k_7} = 0,6$	$p_{4k_8} = 0,8$	$p_{4k_9} = 0,8$
Ймовірність відбиття загроз	$P_1 = 0,88$		$P_2 = 0,9$		$P_3 = 0,91$		$P_4 = 0,974$		
r_i (ймовірні відвернуті збитки)	8,8		9		8,19		29,22		

c_i (допустимі витрати)	2,0	1,5	2,5	4

$C_r = 8{,}5$

	1	2	3	4
0	0	0	0	0
0,5	0	0	0	0
1,0	0	0	0	0
1,5	0	9	9	9
2,0	8,8	9	9	9
2,5	8,8	9	9	9
3,0	8,8	9	9	9
3,5	8,8	17,9	17,9	17,9
4,0	8,8	17,9	17,9	29,22
4,5	8,8	17,9	17,9	29,22
5,0	8,8	17,9	17,9	29,22
5,5	8,8	17,9	17,9	38,22
6,0	8.8	17,9	26,09	38,22
6,5	8,8	17,9	26,09	38,22
7,0	8.8	17,9	26,09	38,22
7,5	8,8	17,9	26,09	38,22
8,0	8,8	17,9	26,09	55,31
8,5	8,8	17,9	26,09	55,31

Таким чином, при заданих фінансових обмеження на реалізацію захисту максимальний відвернутий збиток складатиме 55,31 тис. грн.

Експерт визначив, що за заданих умов оптимальним СФПЗ буде (рис. 3.3):

1.КЦД.3 = { КА-1, КО-1, ЦА-1, ЦО-1, ДР-2, ДС-2, ДЗ-2, ДВ-2, НР-3, НИ-2, НК-1, НО-1, НЦ-2, НТ-2 }

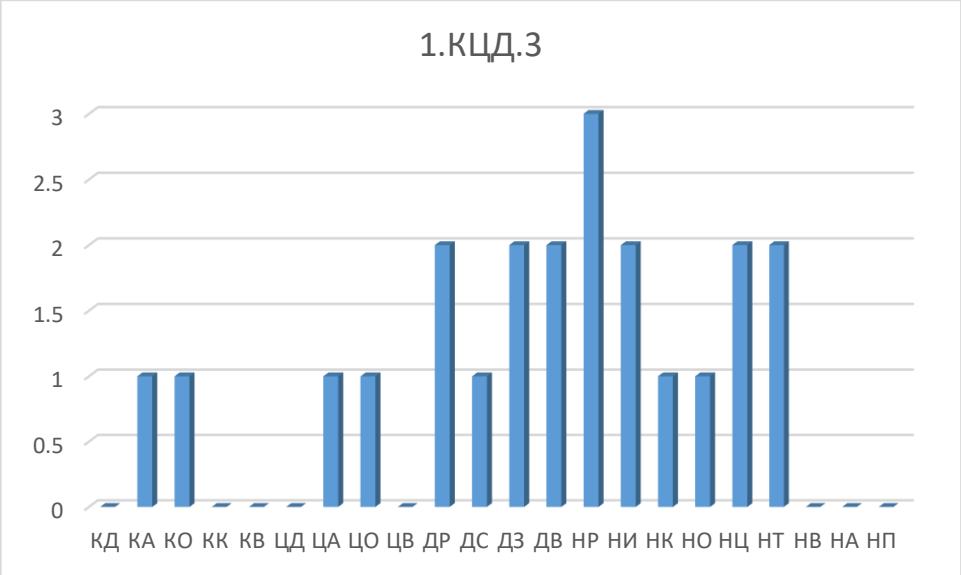


Рис. 3.3. Графічне представлення СФПЗ 1.КЦД.3

Застосунок 3.

Номер загрози	1	2	3	4
p_1 (ймовірність появи загрози)	0.2	0,4	0,5	0,6
S_i	60	25	40	50

	Відвернення загрози 1		Відвернення загрози 2		Відвернення загрози 3		Відвернення загрози 4		
f_j	f_{k_1}	f_{k_2}	f_{k_3}	f_{k_4}	f_{k_5}	f_{k_6}	f_{k_7}	f_{k_8}	f_{k_9}
p_{ij}	$p_{1k_1} = 0,7$	$p_{1k_2} = 0,8$	$p_{1k_3} = 0,5$	$p_{2k_4} = 0,8$	$p_{2k_5} = 0,8$	$p_{3k_6} = 0,8$	$p_{3k_7} = 0,7$	$p_{4k_8} = 0,8$	$p_{4k_9} = 0,7$
	$P_1 = 0,94$		$P_2 = 0,9$		$P_3 = 0,96$		$P_4 = 0,982$		
r_i	11,28		9		19,2		29,46		
c_i	2,5		1,5		2,5		4,5		

$C_r = 10$

	1	2	3	4
0	0	0	0	0
0,5	0	0	0	0

1,0	0	0	0	0
1,5	0	9	9	9
2,0	0	9	9	9
2,5	11,28	11,28	19,2	19,2
3,0	11,28	11,28	19,2	19,2
3,5	11,28	11,28	19,2	19,2
4,0	11,28	20,28	28,2	28,2
4,5	11,28	20,28	28,2	29,46
5,0	11,28	20,28	30,48	29,46
5,5	11,28	20,28	30,48	29,46
6,0	11,28	20,28	30,48	38,46
6,5	11,28	20,28	30,48	38,46
7,0	11,28	20,28	30,48	48,66
7,5	11,28	20,28	30,48	48,66
8,0	11,28	20,28	30,48	48,66
8,5	11,28	20,28	30,48	48,66
9,0	11,28	20,28	30,48	48,66
9,5	11,28	20,28	30,48	59,95
10,0	11,28	20,28	30,48	59,95

Таким чином, при заданих фінансових обмеження на реалізацію захисту максимальний відвернутий збиток складатиме 59,95 тис. грн.

Експерт визначив, що за заданих умов оптимальним СФПЗ буде (рис. 3.4):

2.КЦД.2 = { КД-2, КА-2, КО-1, ЦД-1, ЦА-2, ЦО-1, ДР-1, ДВ-1, НР-2, НИ-2, НК-1, НО-2, НЦ-2, НТ-2 }

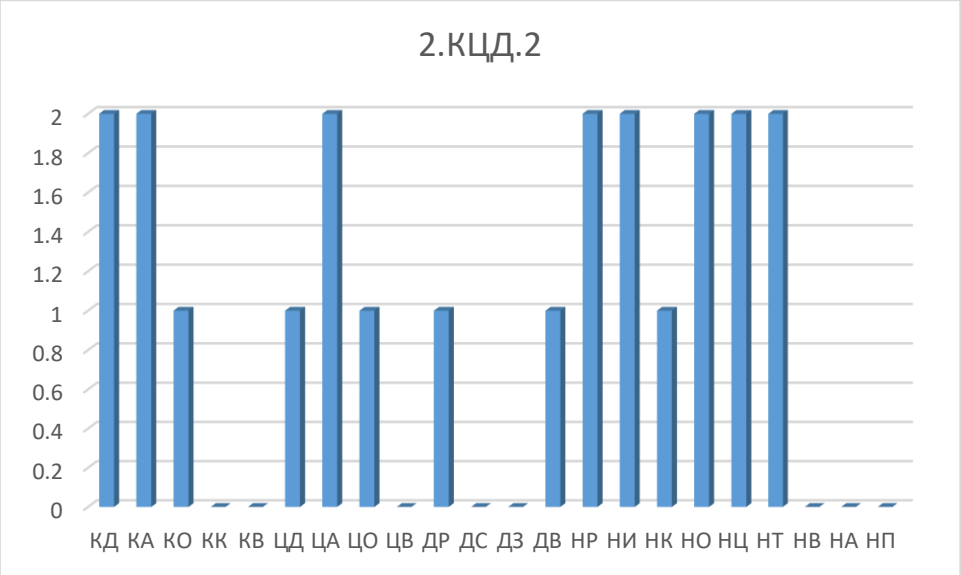


Рис. 3.4. Графічне представлення СФПЗ 2.КЦД.2

Висновки до третього розділу

У розділі запропоновано метод вибору оптимального стандартного функціонального профілю захищеності.

Метод складається з таких кроків:

- відбір експертів для визначення та оцінки показників відповідних ймовірностей;
- збір інформації та її обробка;
- обчислення показника вірогідності появи *i*-ої загрози;
- обчислення показника вірогідності відвернення *i*-ої загрози,
- обчислення показника вірогідності використання *j*-ої вразливостіv_{ij};
- обчислення показника відверненого збитку;
- оцінка оптимальності СФПЗ за умови виконання $S(F_0) = \underset{F \in F}{max} S(F)$при обмеженні $C(F) \leq C_r$

Розроблений метод може бути використаним при створенні системи захисту інформації в кіберпросторі та передбачає виконання умови максимізації відверненого збитку та не перевищення допустимих витрат.

Проведене застосування методу продемонструвало його дієвість та дозволило зробити висновки про доцільність його використання для вибору оптимального стандартного функціонального профілю захищеності.

ВИСНОВКИ

Проаналізувавши існуючі підходи до моделювання та побудови методів захисту кіберпростору, можна дійти такого висновку, що усі запропоновані методи та моделі мають, як свої переваги так і недоліки. Для того щоб побудувати безпечний сегмент національного кіберпростору необхідно ретельно дослідити основні його властивості, динаміку розвитку в різних мірилах часу (від миттєвих до багаторічних) та методи керування цією динамікою. Потребує також визначення та наукового обґрунтування основних показників та критеріїв кібербезпеки, розробка відповідних моделей та методів їх оцінювання, системний аналіз та отримання оцінок застосування тих чи інших заходів безпеки. Окрім того, бажано, щоб більшість технічних рішень захисту кіберпростору (в першу чергу програмних) базувалася на національних розробках.

Під час виконання роботи було:

1. Проведено аналіз сучасних тенденції розвитку кіберпростору. Виділено вісім актуальних тенденцій: *кіберпростір поступово перетворюється у п'ятий театр військових дій*; *інформаційна безпека напряму залежить від кібербезпеки, тобто політики безпеки, що реалізується у кіберпросторі країни чи коаліції країн*; *для захисту держави від кіберзагроз створюються національні органи кібербезпеки*; *для боротьби з кіберзагрозами починають форму-ватися міжнародні коаліції*; *для забезпечення переваги у кіберпросторі провідні країни світу почали формувати військово-мережевий комплекс*; *проблеми інформаційної безпеки у кіберпросторі та формування військово-мережевого комплексу приводять до перерозподілу повноважень існуючих гравців в сфері захисту інформації*; н*адання послуг із захисту інформації у кіберпросторі стає новим видом бізнесу*; *фундаментальна залежність інформаційної інфраструктури сегментів кіберпростору більшості країн від іноземних виробників апаратних та програмних засобів*.

Розкрито підходи до оцінювання ефективності методів виявлення кібератак, описано інфраструктуру системи захисту кіберпростору, розглянуто

захищені операційні системи, антивірусні системи та криптографічне забезпечення безпеки кіберпростору.

Аналіз дозволив виділити напрями дослідження проблем безпеки кіберпростору:

а) Розробка моделей кіберпростору та основних факторів, що впливають на його функціонування. Безумовно, необхідна ретельна продумана модель загроз. Одним з важливіших напрямків є створення математичних моделей, що дозволяють отримати чисельні характеристики інформаційної безпеки (ступень загроз інформаційної безпеки, аналізу інформаційних ризиків, оцінки ефективності заходів захисту).

б) Розробка комплексної системи показників, що охоплюють усі сторони функціонування кіберпростору та забезпечення його захисту від можливих загроз.

в) Створення спеціальних методів забезпечення стійкості кіберпростору або його фрагментів під впливом загроз, для чого, зокрема необхідно:

- провести аналіз топологічної структури кіберпростору та виробити рекомендації щодо її зміни, способів та конкретних алгоритмів реалізації;
- розробити методи криптографічного захисту, основані не тільки на чисто обчислювальних механізмах реалізації стійкості, но й на використанні переваг багатозв’язної архітектури зв’язків та великого числа користувачів;
- створити методи інформаційної безпеки на основі соціальних сервісів для протидії кібератакам з використанням спеціальних процедур аналізу групової поведінки тощо.

г) Розробка інтелектуальних методів забезпечення безпеки кіберпростору, зокрема:

- методів інтелектуальної ідентифікації користувачів;
- інтелектуальних методів запобігання вірусних чи інших атак;
- інтелектуальних методів виявлення кібератак та проникнень;
- методів ситуаційного аналізу станів інформаційної безпеки;

- нових методів криптографічного захисту, базованих на нейромережевих технологіях, технологіях автентичного шифрування тощо.

2. Розроблено метод, який дозволяє здійснити оптимальний вибір фукціонального профілю захищеності при виконанні умови максимізації відверненого збитку та неперевищення допустимих витрат за рахунок ймовірно-вартісної оцінки показників кількості й частоти появи загрози, ймовірних збитків від реалізації визначених загроз й вартості послуги захисту.

3. Проведено застосування запропоновано методу у трьох різних ситуаціях. Експеримент показав дієвість методу та дозволив зробити висновки про доцільність його використання для вибору оптимального стандартного функціонального профілю захищеності.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. JP 3-13.1. Electronic Warfare. - US Joint Chiefs of Staff, 2007. - 115 p.

2. Cyber Space Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure. - Washington D.C.: The White House, 2009.

3. Informational Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World. - Washington D.C.: The White House, 2011.

4. Department of Defense Strategy for Operating in Cyberspace. - Washington D.C.: U.S. Department of Defense, 2011.

5. AFDD 3-12. Cyberspace Operations. - USAF, 2010. - 60 p.

6. AFDD 3-13. Information Operations. - USAF, 2011. - 65 p.

7. AFPD 10-7. Information Operations. - USAF, 2006. - 29 p.

8. DoDD 3600.1. Information Operations. - US DoD, 2013. - 12 p.

9. Стандарт ISO/IEC 27032:2012. Інформаційні технології. Методи забезпечення безпеки. Керівні вказівки по забезпеченню кібербезпеки. 2012.

10. Стандарт ITU-T X.1205:2008. Огляд кібербезпеки. 2008. - Женева: МСЭ-Т, 2008. - 162 с. - URL: www.itu.int/ITU-T.

11. Безпека в електрозв'язку та інформаційних технологіях. Огляд змісту та застосування діючих Рекомендацій МСЭ-Т для забезпечення захищеного електрозв'язку. - Женева: МСЭ-Т, 2009. - 162 с. - URL: www.itu.int/ITU-T.

12. JP 3-13. Information Operations. - US Joint Chiefs of Staff, 2012. - 69 p.

13. Фурашев В.М. Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності / Інформація і право, №2(5), 2012, с.162-169.

14. При РНБО створили хаб з кіберзахисту держави https://www.ukrinform.ua/rubric-polytics/3063682-pri-rnbo-stvorili-hab-z-kiberzahistu-derzavi.html 15.07.2020 18:04.

15. У ЄС з'явиться спецпідрозділ, що відповідатиме за кібербезпеку https://www.ukrinform.ua/rubric-technology/2890304-u-es-zavitsa-specpidrozdil-so-vidpovidatime-za-kiberbezpeku.html.

16. Воєнно-промисловий комплекс // https://uk.wikipedia.org/wiki/Воєнно-промисловий комплекс.

17. Интернет как оружие. Что скрывает Google, Tor и ЦРУ / Левин Яша; Пер.с англ. - М.: Индивидуум, 2019. - 360 с.

18. Кибервойн@: Пятый театр военных действий / Шейн Харис; Пер.с англ. - М.: Альпина нонфикшин, 2020. - 390 с.

19. Петров В.В. Щодо формування національної системи кібербезпеки України // Стратегічні пріоритети, №4 (29), 2013 р. – с.12-130.

20. Петров В.В. Співробітництво України з НАТО щодо забезпечення кібербезпеки // Міжнародні відносини. Серія" Політичні науки". - 2018, вип.18-19.

21. Ф. Шрайер, Б. Викс, Т. Винклер. Кибербезопасность: дорога, которую предстоит пройти. – Женева, 2013. – 52 стр.

22. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. [Підручник]. / В. Л. Бурячок, Г.М.Гулак, В.Б. Толубко. – К. : ТОВ «СІК ГРУП УКРАЇНА», 2015. – 449 с.

23. Ткаченко О.А., Ткаченко К.О. Кіберпростір і кібербезпека: проблеми, перспективи, технології // Цифрова платформа: інформаційні технології в соціокультурній сфері 2018, №177, стор.75-84.

24. Баранов, О.А. Про тлумачення та визначення поняття «кібербезпека», Правова інформатика, 2014., 2 (42), с. 54-62.

25. Толубка, В.Б. ред. Інформаційна та кібербезпека: соціотехнічний аспект. - Київ: ДУІКТ, 2015.

26. Информационное противоборство в современных условиях: [монография] / Л.Г. Пирцхалава, В.А. Хорошко, Ю.Е. Хохлачова, М.Е. Шелест / Под ред. профессора В.А. Хорошко. - К.: ЦП "Компринт", 2019. - 226 с.

27. Адамов О.С. Моделі і методи захисту кіберпростору.

28. Макаренко С.И. Информационное противоборство и радиоэлектронная борьба в сетецентрических войнах начала XXI века. Монография. - СПб.: Наукоемкие технологии, 2017. — 546 с.

29. Cybersecurity Dilemmas: Technology, Policy, and Incentives: Summary of Discussions at the 2014 Raymond and Beverly Sackler U.S.-U.K. Scientific Forum, National Academy of Science, 2014.

30. P De Hert, V. Papakonstantinou The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals, Computer Law & Security Review, Elsevier, 2012.

31. E. Lachaud The General Data Protection Regulation and the rise of certification as a regulatory instrument, Computer Law & Security Review, Vol. 34, Issue 2. April 2018. p.244-256.

32. Bokefode J.D, Ubale S. A, Apte Sulabha S, Modani D. G. Analysis of DAC MAC RBAC Access Control based Models for Security, International Journal of Computer Applications, Vol. 104–No. 5, October 2014.

33. Luo L., He H., Zhu J. Defect Analysis and Risk Assessment of Mainstream File Access Control Policies. In: Wang G., Ray I., Alcaraz Calero J., Thampi S. (eds) Security, Privacy, and Anonymity in Computation, Communication, and Storage. SpaCCS. Springer. 2016. Lecture Notes in Computer Science. Vol. 10066.

34. Elsayed W., Gaber T., Zhang N., Ibrahim Moussa M. (2016) Access Control Models for Pervasive Environments: A Survey. In: Gaber T., Hassanien A., El-Bendary N., Dey N.(eds) The 1st International Conference on Advanced Intelligent System and Informatics (AISI2015), Springer. November 28-30, 2015, Beni Suef, Egypt. Advances in Intelligent Systems and Computing. Vol. 407.

35. Li, B., Tian, M., Zhang, Y., Lv, S.: Strategy of domain and cross-domain access control based on trust in cloud computing environment // Computer Engineering and Networking. Springer. 2014. p.791–798.

36. Cha, B., Seo, J., Kim, J.: Design of attribute-based access control in cloud computing environment // Proc. of the International Conference on IT Convergence and Security 2011. p.41–50.

37. Computer Security Incident Handling Guide, NIST 800-61, Sep 2016, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST .SP.800-61r2.pdf 9.

38. Information security incident management (ISO/IEC 27035-1:2016), Sep 2016 // https://www.iso.org/obp/ui/#iso:std:iso-iec:27035:-1:ed1:v1:en.

39. Incident Handler's Handbook, SANS Institute, Sep 2016,https://www.sans.org/readingroom/whitepapers/incident/incident-handlers-handbook33901.

40. Felix C. Freiling, Bastian Schwittay A Common Process Model for Incident Response and Digital Forensics, IMF 2007, Stuttgart, September 2007, http://www.imfconference.org/imf2007/2%20Freiling%20common_model.pdf 13. Grispos G., Glisson W. B., Storer T., Rethinking Security Incident Response: The Integration of Agile Principles, Sep 2016, https://arxiv.org/ftp/arxiv/papers/1408/1408.2431.pdf.

41. Shostack A. Threat Modeling: Designing for Security, Wiley, 2014, p. 626

42. CAPEC: Common Attack Pattern Enumeration and Classification. https://capec.mitre.org/index.html, 2019.

43. Adversary Tactics and Techniques and Common Knowledge, MITRE, https://attack.mitre.org/, 2019.

44. Phillip A Porras and Richard A Kemmerer. Penetration state transition analysis: A rule-based intrusion detection approach // Proc. IEEE Eighth Annual Computer Security Applications Conference, 1992. P. 220–229.

45. Calvin Ko, Manfred Ruschitzka, and Karl Levitt. Execution monitoring of security-critical programs in distributed systems: A specification-based approach // IEEE S&P. 1997.

46 . Powers, David M W. Evaluation: From Precision, Recall and F-Measure to ROC, Informedness, Markedness & Correlation. Journal of Machine Learning Technologies. 2 (1), P. 37–63, 2011

47. K.N. Junejo, J. Goh, Behaviour-Based Attack Detection and Classification in Cyber Physical Systems Using Machine Learning, CPSS '16: Proceedings of the 2nd ACM International Workshop on Cyber-Physical System Security, May 2016.

48. Chandola, V.; Banerjee, A.; Kumar, V. Anomaly detection: A survey. ACM Computing Surveys. 2009. 41 (3). P. 1–58

49. Treinen J.J., Thurimella R. A Framework for the Application of Association Rule Mining in Large Intrusion Detection Infrastructures. In: Zamboni D., Kruegel C. (eds) Recent Advances in Intrusion Detection. RAID 2006. Lecture Notes in Computer Science, vol 4219. Springer, Berlin, Heidelberg.

50. Joan Calvet. Tripoux: Reverse-Engineering Of Malware Packers For Dummies.

51. Domagoj Babic, Daniel Reynaud, Dawn Song. Malware Analysis with Tree Automata Inference.

52. Adrian E. Stepan. Defeating Polymorfism: Beyond Emulation.

53. http://blog.zeltser.com/post/1256199682/what-is-cloud-ants-virus.

54. Vladimir Grytsan ROMAD TrueProactive™ Threat Defense. Введение в Malware Genetics™ Platform - Сентябрь 28, 2017 - http://www.steeldrum.org.ua/content/sd13/ROMAD_Malware_Genetics_Technical.pdf.

55. Bellare M., Namprempre Ch. Authenticated Encryption: Relations among notions and analysis of the generic composition paradigm // ASIACRYPT 2000, LNCS 1976, 2000, pp 531–545.

56. Dworkin M. Special Publication 800-38C: Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality // National Institute of Standards and Technology, U.S. Department of Commerce, May 2005.

57. Gligor V., Donescu P. Fast Encryption and Authentication: XCBC Encryption and XECB Authentication Modes // Matsui M. (eds) Fast Software Encryption. FSE 2001. LNCS 2355. Springer, Berlin, Heidelberg, 2001, pp. 92–108.

58. Bertoni G., Daemen J., Peeters M., Van Assche G. Cryptographic sponge functions, 2011. Avail. at http://sponge.noekeon.org/CSF-0.1.pdf.

59. Agievich S., Marchuk V., Maslau A., Semenov V. Bash-f: another LRX sponge function. In: Pre-proceedings of the 5th Workshop on Current Trends in Cryptology (CTCrypt2016, Yaroslavl, Russia, June 6–8, 2016), 2016, p. 184–205. Extended abstract avail. at: http://eprint.iacr.org/2016/587.

60. https://delo.ua/special/sostojanie-kiberbezopasnosti-v-ukraine-nezavisi maja-vneshnjaja-o-346292, 15 вересня 2018.

61. Указ Президента України від 15 березня 2016 року № 96/2016 «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України"».

62. https://m.facebook.com/story.php?story_fbid=1572205399646181&id= 243701472496587 – 19.11.2020.

63. https://bit.ly/3pLxNif/Організаційно-технічна модель кіберзахисту.

64. https://cert.gov.ua/recommendations/21#.

65. Джулій В. М. Оцінка стану безпеки інформації в комп'ютерних системах на основі логіко-лінгвістичного підходу / В.М. Джулій, Г.О. Буркун // Вимірювальна та обчислювальна техніка в технологічних процесах. — 2009 р. — № 2.

66. Наконечна Н. В. Безпека автоматизованих облікових систем у системі економічної безпеки підприємства / Наконечна Н. В. // Вісник Хмельницького національного університету. — 2009 — №3.

67. Информационные технологии защиты персональных данных в вузе [Электронный ресурс] / С.У. Увайсов, И.В. Аютова. – Режим доступа к статье: http://www.hse.ru/pubs/lib/data/access/ticket/136906043843f57233fbadc4e1256f887bc7e39bc5/text5.pdf

68. Любченко Н. Л. Сканування загроз як складова управління стабільністю підприємства / Вісник Хмельницького національного університету. — 2009. — № 4, Т. 2 — С. 227-232.

Додаток А

Словник

Кіберпростір (англ. cyberspace) – середовище, створене організованою сукупністю інформаційних процесів на підставі об'єднаних загальними принципами та правилами інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем незалежно від форми власності.

Кібератака (кібернапад) – цілеспрямовані дії, що реалізуються в кіберпросторі (або за допомогою його технічних можливостей), які призводять (можуть призвести) до досягнення несанкціонованих цілей (порушення конфіденційності, цілісності, авторства, спостережності й доступності інформації, деструктивних інформаційно-психологічних впливів на свідомість, психічний стан громадян).

Кіберзагрози – наявні та потенційно можливі явища й чинники, що створюють небезпеку інтересам людини, суспільства та держави через порушення доступності, повноти, цілісності, достовірності, автентичності режиму доступу до інформації, яка циркулює в критичних об'єктах національної інформаційної інфраструктури.

Кіберінцидент – подія, яка фактично або потенційно призводить до негативних наслідків роботи інформаційної системи або порушує цілісність інформації, яка в цій системі обробляється, зберігається, передається, і яка може викликати необхідність зворотних дій для пом'якшення наслідків.

Кіберзлочин – суспільно небезпечне винне діяння, що полягає в протиправному використанні інформаційних і комунікаційних технологій, відповідальність за вчинення якого встановлена кримінальним законодавством.

Кібертероризм – суспільно небезпечна діяльність, що здійснюється в кіберпросторі (або з використанням його технічних можливостей) з терористичною метою і полягає у свідомому, цілеспрямованому залякуванні населення та органів влади або вчиненні інших посягань на життя і здоров'я людей.

Кібердиверсія – це суспільно небезпечні діяння в кіберпросторі, наслідки яких можуть призвести до масового знищення людей, заподіяння тілесних ушкоджень чи іншої шкоди їхньому здоров'ю, зруйнування або пошкодження стратегічних об'єктів у спосіб втручання в роботу інформаційно-телекомунікаційних систем.

Кібершпигунство – передача або збирання з метою передачі іноземній державі, іноземній організації або їх представникам відомостей з обмеженим доступом, яке здійснюється в кіберпросторі.

Кіберозброєння – спеціально створені для протиправних цілей програмні чи/та апаратні комплекси, спрямовані на несанкціоноване отримання інформації з інформаційно-телекомунікаційних мереж, а також використання таких мереж для контролю над об'єктами, в яких вони використовуються та/чи завдання шкоди таким об'єктам.

Кібервійська – спеціальні підрозділи збройних сил держави, діяльність яких спрямована на централізоване здійснення кібервоєнних операцій (кібервійни), управління й захист військових комп'ютерних мереж.

Кібервійна – використання державою чи групою держав спеціальних засобів (кіберозброєнь) проти країни (групи країн) в кіберпросторі, спрямоване на порушення стабільної роботи інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем і мереж об'єктів критичної інфраструктури.

Кібермогутність – здатність до використання кіберпростору для створення переваг і справляння впливу в усіх інших операційних просторах через інструменти могутності.

Кібернетичний (цифровий) суверенітет – здатність держави самостійно й незалежно забезпечувати національні інтереси в кіберсфері, самостійно розпоряджатися власними інформаційними ресурсами та інфраструктурою національного інформаційного простору, а відтак, гарантувати кібернетичну й інформаційну безпеку державі, суспільству та громадянам.

DDoS-атаки – кібератака на обчислювальну систему з метою доведення її до відмови в роботі, тобто створення умов, за яких легальні користувачі системи не можуть отримати доступ до системних ресурсів (сервісів) або цей доступ ускладнений.

Фішинг (англ. fishing) – вид злочинної діяльності, метою якого є отримання доступу до персональних даних користувачів за допомогою використання сайтів і масових поштових розсилок начебто від імені відомих брендів, знайомих або інших джерел, що можуть викликати в отримувача довіру до змісту сайту (листа).

Соціальна інженерія – використання маніпулятивних заходів (передусім у процесі спілкування зловмисника з жертвою) з метою вивідування даних.

SCADA – програмний комплекс, призначений для розроблення чи забезпечення роботи в режимі реального часу систем збору, оброблення, відображення та архівування інформації про об'єкт моніторингу чи управління. Використовується на системах моніторингу та управління промисловими, інфраструктурними та сервісними процесами на нафтопроводах, електростанціях, потужних системах зв'язку, аеропортах, судах і військових об'єктах.

0day (zeroday)-уразливість – нові уразливості програмного продукту, які до цього часу не були виявлені жодним із дослідників безпеки.

Бекдор (англ. back door) – програма, яка забезпечує зловмиснику можливість повторного доступу до системи «зламаного» комп'ютера.

Хактивізм – використання інформаційно-комунікаційних технологій з метою просування політичних лозунгів і закликів. Найчастіше виражається у формі «зламу» титульної сторінки сайту-цілі з подальшим розміщенням на ній політичних закликів.

Фаєрвол (англ. firewall) – пристрій або набір пристроїв (іноді програм), сконфігурованих так, щоб допускати, відмовляти, шифрувати, пропускати через спеціальний елемент (проксі) весь комп'ютерний трафік з набором певних

правил та інших критеріїв. Використовується для додаткової захищеності мереж і комп'ютерів від шкідливої інформації чи кібератак.

Операції в комп'ютерних мережах – використання комп'ютерних мереж для атаки на інформацію, розміщену на комп'ютерах і в комп'ютерних мережах, або на самі комп'ютери та мережі.

Закладки (англ. beetle) – таємно (несанкціоновано) встановлені в комп'ютерні програми чи апаратну частину елементи, які дозволяють зловмисникам отримати несанкціонований доступ до ресурсів системи.

Клептографія – науковий напрям, який вивчає принципи, методи, технології та засоби організації прихованого від санкціонованого користувача каналу передачі чутливої інформацій щодо діючої системи захисту.

Додаток Б

БАЗОВІ ХАРАКТЕРИСТИКИ БЕЗПЕКИ ІНФОРМАЦІЙНИХ РЕСУРСІВ

К-тип (загроза конфіденційності)

Випромінювання і наводки. Виявити зняття інформації з каналів побічних електромагнітних випромінювань і наведень майже неможливо, Частота такого доступу невідома, запобігти це явище досить складно (для цього потрібно застосовувати спеціальні засоби захисту), наслідки потенційно великі. Такі загрози є одним із слабких місць у комп'ютерному захисті, оскільки кабелі, з'єднання та устаткування (відеотермінали, принтери, модеми, клавіатура, конектори, заземлення тощо), випромінюють певні сигнали, які навіть при незначному рівні можуть бути перехоплені чутливою антеною.

Неправильна маршрутизація. Запобігти цій загрозі досить складно, виявити непросто, частота появи можливо висока, але точно не відома, а наслідки потенційно великі. Порушення конфіденційності здійснюються через пересилку повідомлень, файлів та іншої інформації за неправильною адресою, сформованому здебільшого внаслідок ненавмисної помилки.

Перехоплення. Залежно від дії, суб'єктивна чи активна загроза, запобігти якій майже неможливо, виявити досить складно або навіть неможливо. Частоту такої загрози не встановлено, а наслідки потенційно великі. Перехоплення інформації здійснюється переважно через несанкціоноване підключення додаткового терміналу або, наприклад, через спостереження за ПЕМВН. Для захисту від зазначеної загрози використовують криптографічні методи, стеганографію, екранування, фільтри, генератори шумів і т.п.

Програми розкриття паролів. Запобігання і виявлення цієї загрози може бути дуже складним, частота появи невідома, а наслідки потенційно дуже великі. Такі програми, як правило, призначені для вгадування паролів через перебір варіантів, можливих для використання символів або проникнення в систему за допомогою словників. Програми, які засновані на останньому методі, здійснюють злом системи парольного захисту через перебір елементів одного або декількох словникових файлів, складених спеціально або взятих із серверів або жорстких дисків локальних станцій.

Збір сміття. Загроза К-типу, запобігти і виявити яку вельми складно, частота появи невідома, а наслідки потенційно дуже великі. Під збором сміття мається на увазі спосіб отримання інформації через відновлення і перегляд віддалених файлів, використаних дисків, стрічок, лістингів, копірок та інших відходів інформаційної діяльності.

Мережеві аналізатори. Запобігти і виявити загрозу майже неможливе або дуже складно, частота появи невідома і прогресує, а наслідки потенційно дуже великі. Зазначені аналізатори будують на базі програмно-апаратних засобів (в окремих випадках у вигляді програмних), призначених для зчитування будь-яких параметрів потоку даних.

Соціальний інжиніринг. Запобігти і виявити загрозу досить складно, частота появи невідома, а наслідки потенційно дуже великі. Пов'язана з отриманням певних даних (наприклад, імен користувачів, паролів, номерів телефонів та ін.) від різних людей, атакованих за допомогою інформаційного обміну.

Фішинг. Виявити і запобігти цій загрозі складно, частота появи невідома, а наслідки потенційно великі. Фішинг - вид інтернет-шахрайства, метою якого є отримання доступу до конфіденційних даних користувачів - логінів і паролів. Це досягається шляхом проведення масових розсилок електронних листів від імені популярних брендів, а також особистих повідомлень всередині різних сервісів або всередині соціальних мереж (Facebook, Вконтакте, Одноклассники).

Клікджекінг. Запобігання і виявлення загрози може бути дуже складним, частота появи невідома, а наслідки потенційно дуже великі. При цьому зловмисник може отримати доступ до конфіденційної інформації або навіть отримати доступ до комп'ютера користувача, заманивши його на зовні нешкідливу сторінку або запровадивши шкідливий код на безпечну сторінку.

Тайпсквоттінг. Пасивна загроза, запобігти якій досить складно, виявити просто, частота появи можливо висока, але точно не відома, а наслідки потенційно великі. Тайпсквоттінг – реєстрація доменних імен, близьких за написанням з адресами популярних сайтів у розрахунку на помилку частини користувачів.

Spyware. Запобігти і виявити цю загрозу досить складно, частота появи невідома, а наслідки потенційно дуже великі. Spyware – програмне забезпечення, яке здійснює діяльність по збору інформації про конфігурації комп'ютера, діяльності користувача і будь-якій іншій конфіденційній інформації без згоди самого користувача.

Ц-тип (загроза цілісності)

Крекери. Запобігти як досить складно; виявити вплив дуже просто або складно; частота появи невідома, але швидкість досить висока; наслідки потенційно великі. За допомогою крекерів здійснюється злом різних систем захисту через модифікацію захисного механізму в самому ПЗ. Крекери - вузьконаправлені програми, внаслідок впливу яких з'являється можливість не тільки безперешкодно входити в систему, а й вільно використовувати різні комерційні (захищені) версії програм. Після дії крекеру, як правило, відкривається доступ іншим загрозам.

Шахрайство. Виявити і запобігти цій загрозі скрутно, частота появи невідома, а наслідки потенційно великі. При даній загрозі проводиться будь-яке використання РІС для отримання потрібних ресурсів або, наприклад, обману організації з метою певної вигоди.

Неточна / застаріла інформація. Запобігання і виявлення може бути важким, трапляється досить часто, а наслідки потенційно дуже великі. Повідомлення, записи, файли та інша інформація може стати недоброякісною, через її

випадкове спотворення, неповноту або старіння, обумовлене одержанням нових даних.

Підробка (фальсифікація). Запобігання і виявлення може бути важким, частота поява невідома, а наслідки потенційно дуже великі. Підробка пов'язана з навмисним перекручуванням РІС, спрямованим, наприклад, на протизаконне виготовлення документів, файлів і т.п. з метою використати їх замість справжніх.

Умисне пошкодження даних або програм. Запобігання і виявлення цієї загрози вельми складне, частота появи невідома, але швидкість невисока, а наслідки потенційно дуже великі. Вона супроводжується зловмисним руйнуванням суб'єктом таких ресурсів інформаційної системи, як файли, різні дані і т.п.

Різні версії. Загроза запобігти і виявити яку складно, виникає досить часто, а наслідки потенційно великі. Використання різних версій, наприклад, однієї і тієї ж програми, часто призводить до різних непорозумінь, які пов'язані з тим, що нові версії можуть інакше редагувати або створювати файли, а також містити помилки, які не дозволяють нормально її експлуатувати. Досить часто виникають випадки, коли файл з однаковим ім'ям зберігається в різних частинах диска або дискового простору і нерідко помилково використовується інформація не самою останній редакції. Після її зміни вона подається як останній варіант, при цьому попередня модифікація не враховується. Таким чином, жодна версія не буде достовірною, що порушить цілісність даних і може призвести до серйозних наслідків.

Д-тип (загроза доступності)

Імітація та моделювання. Тип загрози варіюється, запобігти їй практично неможливо, частота появи невідома, складність виявлення – різна. За допомогою комп'ютера можна імітувати різні дії, наприклад, пересилку платежів, передачу повідомлень, моделювати процеси та ін.

Неможливість використання. Залежно від мотиву, суб'єктивна активна або пасивна загроза, яка пов'язана з падінням продуктивності функціонування систем внаслідок невикористання з будь-якої причини наявних програмних і апаратних засобів. Запобігти загрозі важко, виникає з невідомою частотою, виявити іноді буває досить складно, а наслідки потенційно великі.

Перевантаження. Залежно від мотиву суб'єктивна активна або пасивна загроза, виявити яку просто, запобігти складно, виникає з невідомою частотою (як правило висока в нових рідко використовуваних системах), а наслідки потенційно дуже великі. Будь-яке програмне або апаратне забезпечення, яке дає збої під час його тестування в критичних режимах, як правило, показує подібні результати і в разі його перевантаження.

Перешкоджання використанню. Запобігти цій загрозі досить важко, виявити легко. Частота появи невідома, а наслідки потенційно дуже великі. Ця загроза пов'язана з уповільненням роботи в системі, наприклад, за рахунок вилучення важливих ключових файлів, несанкціонованого захоплення ресурсів тощо.

Реплікатори. Запобігання виникненню загрози при нових формах може бути складним, вплив зазвичай очевидний, частота народження відносно невисока, наслідки потенційно великі, але на практиці менш небезпечні. Реплікатор являє собою програму, що створює кілька своїх копій в ІС, а в випадку, коли він створює тільки одну і після цього виконує її, то пам'ять системи швидко переповнюється, що обмежує доступ до певних компонентів системи.

fork-бомба. Залежно від мотиву, суб'єктивна активна або пасивна загроза, запобігти і виявити яку досить складно, частота появи невідома, а наслідки потенційно великі. fork-бомба - шкідлива чи помилково написана програма, нескінченно створює свої копії, які зазвичай також починають створювати свої копії і т.д. fork-бомба породжує велику кількість власних копій і тим самим намагається заповнити вільне місце в списку активних процесів операційної системи [61]. Після заповнення списку процесів стає неможливим старт корисної програми. Навіть якщо який-небудь інший процес припинить роботу, і місце в списку процесів звільниться, старт корисної програми малоймовірний, оскільки безліч інших копій fork-бомби вже чекають можливості запустити свою чергову копію. Крім заповнення списку процесів, можливі також стратегії заповнення віртуальної пам'яті, процесорного часу, сокетів та інших системних ресурсів. Результатом вичерпання цих ресурсів стає уповільнення роботи або практично зупинка операційної системи та / або корисних програм (зависання комп'ютера).

КЦД-типу

Апаратні збої і відмови. Запобігти виникненню майже неможливо, частота її появи висока, для оцінки використовується показник напрацювання на відмову, виявити в окремих випадках нескладно, але іноді необхідна спеціальна апаратура, можливі потенційно великі наслідки. Для інформації, оброблюваної в ІС, особливо небезпечні збої (відмови) жорсткого диска, внаслідок яких можуть бути пошкоджені записи, що впливає на цілісність; неможливість виконати завантаження є загрозою доступності; в фірмі з обслуговування дисків може виникнути витік даних, що порушить конфіденційність.

Крадіжки. Запобігти і виявити досить складно; частота появи невідома, а наслідки потенційно дуже великі. Під вплив загрози може підпадати, наприклад, як апаратура, так і файли, при цьому крадіжка останніх, як правило, залишається непоміченою.

Логічні бомби. Запобігти і часто виявити цю загрозу досить складно; частота появи точно невідома (швидше невисока), наслідки потенційно великі. Логічні бомби ініціюються з виникненням різних подій (наприклад, відкриття якого-небудь файлу, інших дій) з метою знищення, спотворення чи модифікування даних.

Недбалість. Запобігти виникненню важко, різна складність виявлення, з'являється часто, наслідки потенційно високі. Така загроза, як правило, пов'язана з різними помилками людини, випадковостями, проявами

некомпетентності і, за оцінками експертів, 50-60% втрат здійснюється саме через неї.

Помилки програмування. Загроза КЦД-типу, запобігти якій майже неможливо, виникає постійно, виявлення буває досить складним, а наслідки потенційно дуже великі. У процесі створення програм в початковому тексті, як правило, на 50 рядків, зустрічається не менше однієї помилки. Під час налагодження більшість з них виправляється, проте певна частина залишається і виявляється, як правило, в позаштатних ситуаціях.

Піггібекінг. Запобігти і виявити загрозу досить важко, частота появи, швидше за все висока, а наслідки потенційно великі. За допомогою піггібекінга здійснюється несанкціоноване проникнення в систему через отримання доступу в результаті тимчасової відсутності або некоректного завершення сеансу роботи легального користувача. Запобігти загрозі можна за допомогою охоронних систем, спеціальних програм зберігачів екрану і т.п. Електронний піггібекінг - це отримання нелегального доступу після того, як легальний користувач, ввівши пароль і підключившись до системи, некоректно завершив сеанс роботи або завершив сеанс роботи, але не відключився від системи [54]. Фізичний піггібекінг – це безпосереднє проникнення в закриту зону після особи, яка має до неї доступ [54].

Самозванство. Запобігти і виявити досить складно, частота появи невідома, а наслідки потенційно великі. Самозванство, як правило, пов'язано з використанням чужого ідентифікатора для проникнення в систему з метою вивчення та копіювання даних, використання робочих станцій і серверів, ініціалізації програм, заміни імен і т.п.

Суперзаппінг. Запобігти і виявити досить складно, частота появи невідома, а наслідки потенційно дуже великі. Фактично, ця загроза пов'язана з несанкціонованим застосуванням утиліт для модифікації, знищення, копіювання, розкриття, вставки, використання або заборони використання комп'ютерних даних.

Таємні ходи (лазівки). Залежно від мотиву, суб'єктивна активна або пасивна загроза, запобігти і виявити яку дуже складно, частота появи невідома, а наслідки потенційно великі. Таємний хід, спеціально створений розробником або виник випадково, фактично є додатковим способом проникнення в систему.

Троянські програми. Запобігти її виникненню майже неможливо або дуже складно, виявити досить важко, частота появи невідома, а наслідки потенційно дуже великі. Фактично троянський кінь – це спеціальна програма, яка дозволяє дії, відмінні від визначених у специфікації, використовуваного ПЗ.

ARP-spoofing. Запобігти і виявити її досить складно, частота появи невідома, а наслідки потенційно дуже великі. Перехопивши на атакуючому хості всередині даного сегменту мережі широкомовний ARP-запит, можна надіслати помилкову ARP-відповідь, в якому оголосити себе шуканим хостом

(наприклад, маршрутизатором), і надалі активно контролювати мережевий трафік дезінформували хоста.

Бекдор, backdoor. Запобігти і виявити цю загрозу досить складно, частота поява досить висока, а наслідки потенційно дуже великі. Основне призначення Backdoor – потайне управління комп'ютером. Як правило, Backdoor дозволяє копіювати файли з ураженого комп'ютера і навпаки, передавати на уражену комп'ютер файли і програми. Крім того, зазвичай Backdoor дозволяє отримати віддалений доступ до реєстру, виробляти системні операції (перезавантаження ПК, модифікацію паролів і т.п.). Також вони дозволяють використовувати комп'ютер користувача для сканування мережі, проведення мережевих атак, злому мереж і т.д.

За допомогою бекдор здійснюється крадіжка конфіденційної інформації з персональних компьтеров, такий як крадіжка паролів від пошти, FTP, адміністративних панелі управління сайтом і т.д. Небезпека Backdoor збільшилася останнім часом у зв'язку з тим, що багато сучасних мережевих черв'яків або містять в собі Backdoor-компоненту, або встановлюють її після зараження ПК [60].

IP-спуфинг. Запобігти і виявити досить складно, частота появи невідома, а наслідки потенційно дуже великі. Метод, який використовується в деяких атаках. Полягає в проставленні у полі зворотної адреси IP-пакета невірного адреси. Застосовується з метою приховування істинного адреси атакуючого, з метою викликати у відповідь пакет на потрібну адресу і з іншими цілями. Протокол транспортного рівня TCP має вбудований механізм для запобігання спуфінга – так звані номера послідовності і підтвердження. Протокол UDP не має такого механізму, отже, побудовані на його основі програми більш уразливі для спуфинга. Гарантованим методом захисту від підміни IP-адреси є зіставлення MAC-адреси і IP-адреси відправника.

ЦД-типу

Диверсії. З'являється не дуже часто, запобігти їй дуже важко, складність виявлення - різна, наслідки потенційно дуже великі. Найчастіше проявляється у фізичному (підпал, пробій тощо) або логічному (зміна імен файлів, підміна програм тощо) пошкодженні.

Комп'ютерні віруси. Запобігання її виникненню при нових формах може бути складним, вплив як правило очевидно, частота появи відносно висока, наслідки потенційно дуже великі, але на практиці менш загрозливі. Віруси по різному впливають на PIC, наприклад, знищують файли, змінюють таблицю розподілення файлів і т.п.

Стихійні лиха. Об'єктивна загроза, запобігти якій досить складно, вплив, як правило, очевидно, зустрічається з невідомою частотою, а наслідки потенційно дуже великі. До цієї загрози можна віднести пожежі, що призводять до значних фінансових втрат, а також землетруси, повені, урагани, затоплення, нашестя гризунів, комах і т.п.

Додаток В

Розподіл рівнів захисту за типами загроз та послуга згідно з стандартними функціональними профілями захищеності

Послуги		Клас	Типи загроз та рівні захисту						
			К	Ц	Д	КЦ	КД	ЦД	КЦД
Конфіденційності	КД	1							
		2	222234			222234	2234		22234
		3	222234			22223	2234		22234
	КА	1	01			01	1111		1111
		2	002234			002234	2234		02234
		3				00223	2234		02234
	КО	1	01			01	1111		1111
		2	011111			011111	1111	0011	11111
		3	011111			01111	1111		11111
	КК	1							
		2				0000112	0112		00112
		3	000112			00011	0112		00112
	КВ	1							
		2							
		3	112344			11233	2344		12334
Цілісності	ЦД	1							
		2		11114		111114		1114	11114
		3		11114		11111		1114	11114
	ЦА	1		02		02		1111	1111
		2		00234		002234		0234	02334
		3		00234		00223		0234	02334
	ЦО	1		01		01		1111	1111
		2		01122		011122		1122	11222
		3		01122		01112		1122	11222
	ЦВ	1							
		2							
		3		11223		11222		1223	12223
Д	ДР	1			1222		1222	1222	1222

		2			1233		1233	1233	11233
		3			1233		1233	1233	11233
	ДС	1			0123		0123	0123	0123
		2			0123		0123	0123	00123
		3			0123		0123	0123	00123
	ДЗ	1			0123		0123	0123	0123
		2			0123		0123	0123	00123
		3			0123		0123	0123	00123
	ДВ	1			1223		1223	0223	1223
		2			1223		1223	0223	11223
		3			1223		1223	1223	11223
Спостереженості	НР	1	12	12	2234	12	2234	2234	2234
		2	222345	22234	2234	222345	2345	2234	22345
		3	222345	22234	2234	22234	2345	2234	22345
	НИ	1	12	12	2222	12	2222	2222	2222
		2	222222	22222	2222	222222	2222	2222	22222
		3	222222	22222	2222	22222	2222	2222	22222
	НК	1	11	11	1111	11	1111	1111	1111
		2	111112	11111	1111	111112	1112	1111	11112
		3	111112	11111	1111	11111	1112	1111	11112
	НО	1	11	11	1111	11	1111	1111	1111
		2	112233	11223	1111	112233	2233	1223	22233
		3	112233	11223	1111	11223	2233	1223	22233
	НЦ	1	11	11	1122	11	1122	1122	1122
		2	122333	12233	1122	122333	2333	2233	22333
		3	122333	12233	1122	12233	2333	2233	22333
	НТ	1	11	11	1222	11	1222	1222	1222
		2	012222	01222	1222	012222	2222	1222	22222
		3	012222	01222	1222	01222	2222	1222	22222
	НВ	1							
		2							
		3	111222	11223	1111	11122	1222	1223	11222
	НА	1							
		2							

		3	000001	00112		00001	0001	0112	00011
	НП	1							
		2							
		3							00011

Додаток Г

Слайди

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІННОВАЦІЙНИХ ОСВІТНІХ ТЕХНОЛОГІЙ
КАФЕДРА БЕЗПЕКИ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

ДИПЛОМНА РОБОТА
ЗДОБУВАЧА ОСВІТНЬОГО СТУПЕНЯ «МАГІСТР»

Тема: Метод побудови захищеного кіберпростору

Автор: Ю.М.Ткач

Науковий керівник: д.т.н., доцент С.В.Казмірчук

1

Актуальність

- Проблеми кібербезпеки, захисту інформації, інформаційної безпеки є актуальними та набувають статус ключових в поточному сторіччі. Насамперед це пов’язано, з одного боку, з поширенням використання сучасних інформаційних технологій в усіх сферах життєдіяльності людини, а, з іншого, суттєвим ускладненням організації їх побудови та забезпеченням їх захисту. Темпи впровадження інформаційних технологій в значному ступені залежать від рівня захищеності, який вони зможуть забезпечити для ресурсів, що обробляються і зберігаються. У цьому аспекті кіберзахист може розглядатися як цілеспрямована діяльність із забезпечення безпеки кіберпростору.

2

Мета та задачі роботи

- **Метою дипломної роботи** є забезпечення захищеності кіберпростору шляхом вибору оптимального стандартного функціонального профілю захищеності.

Досягнення мети потребує розв'язання таких **завдань**:

- аналіз сучасних тенденції розвитку кіберпростору, основних складових інфраструктури захисту кіберпростору та існуючих моделі й методи забезпечення кіберзахисту;
- розробка методу вибору оптимального стандартного функціонального профілю захищеності з метою побудови захищеного кіберпростору;
- експериментальне дослідження методу вибору оптимального стандартного функціонального профілю захищеності.

3

Новизна

- Вперше розроблено метод вибору стандартного функціонального профілю захищеності кіберпростору, який дозволяє здійснити оптимальний вибір при виконанні умови максимізації відверненого збитку та неперевищення допустимих витрат за рахунок ймовірно-вартісної оцінки показників кількості й частоти появи загрози, ймовірних збитків від реалізації визначених загроз й вартості послуги захисту.

4

Практична цінність

- Полягає у тому, що запропонований метод може використовуватись аналітиками з питань ІБ, для проведення вибору оптимального функціонального профілю захищеності. Також надається можливість проведення аналізу, лише окремих частин системи захисту підприємства, наприклад, обчислення показника вірогідності та показника відвернення появи i -ої загрози, обчислення показника вірогідності використання j-ої вразливості. Результат аналізу надається у кількісному вигляді з необхідністю, на основі отриманих даних, подальшого прийняття рішення керівництвом або експертами.

5

Об’єкт та предмет дослідження

- **Об’єкт дослідження:** процес побудови захищеного кіберпростору.
- **Предмет дослідження:** моделі та методи захисту кіберпростору.

6

Сучасні тенденції розвитку кіберпростору

- Тенденція перша: *кіберпростір поступово перетворюється у п'ятий театр військових дій.*
- Тенденція друга: *інформаційна безпека напряму залежить від кібербезпеки, тобто політики безпеки, що реалізується у кіберпросторі країни чи коаліції країн.*
- Тенденція третя: *для захисту держави від кіберзагроз створюються національні органи кібербезпеки.*
- Тенденція четверта: *для боротьби з кіберзагрозами починають форму-ватися міжнародні коаліції.*

7

Сучасні тенденції розвитку кіберпростору

- Тенденція п’ята: *для забезпечення переваги у кіберпросторі провідні країни світу почали формувати військово-мережевий комплекс.*
- Тенденція шоста: *проблеми інформаційної безпеки у кіберпросторі та формування військово-мережевого комплексу приводять до перерозподілу повноважень існуючих гравців в сфері захисту інформації.*
- Тенденція сьома: *Надання послуг із захисту інформації у кіберпросторі стає новим видом бізнесу.*
- Тенденція восьма: *фундаментальна залежність інформаційної інфраструктури сегментів кіберпростору більшості країн від іноземних виробників апаратних та програмних засобів.*

8

Існуючі моделі захисту інформаційних систем

- 1. *Моделі стримування атак на кіберпростір*
- 2. *Моделі захисту персональних даних*
- 3. М*оделі управління доступом*
- 4. *Моделі реагування на кіберінциденти*
- 5. *Моделі кіберзагроз*

9

Існуючі методи захисту інформаційних систем

- 1. *Методи виявлення аномалій*
- 2. *Метод зіставлення зі зразком*
- 3. *Метод асоціативних правил*

10

Формалізуємо завдання вибору оптимального СФПЗ. Для цього побудуємо математичну модель СФПЗ.

- Нехай $\overline{F}$ множина усіх можливих СФПЗ заданих рівнів, які визначаються вимогами до захищеності інформації, F — вектор розмірності 22 (нормативно визначена кількість). Компонентами вектору F є булеві змінні $f_i \in \{0,1\}$. Розмірність вектора F введена для зручності та уніфікації опису СФПЗ, оскільки відомо, що до складу багатьох СФПЗ входять не усі послуги. У разі відсутності якої-небудь послуги відповідна компонента дорівнює нулю.

11

Формальна постановка задачі має вигляд:

- $S(F_0) = \max_{F \in \overline{F}} S(F)$
- при обмеженні
- $C(F) \leq C_r$,
- де *S(F)* - загальний відвернений збиток, F — деякий вектор, що описує СФПЗ, $\overline{F}$ сукупність усіх допустимих профілів, F_0 - оптимальне значення вектору *F,* а C_r - допустимі витрати на СФПЗ, $C(F)$ – функція, що описує вартість застосованих послуг.

12

Припустимо, що може бути реалізований деякий набір вразливостей ***t***, внаслідок чого може виникнути ряд загроз t_i, *i*=1,...,*n* (*n*=4).

При цьому, кожну *i*-у загрозу характеризуватиме ймовірність її *появи* P_{t_i}, можливий збиток інформаційного середовища - S_i, тоді P_i - ймовірність *відвернення i*-ої загрози, а відвернений збиток за рахунок *запобігання i*-ої загрози через $r_i = P_i P_{t_i} S_i$.

13

- Позначимо p_{ij} — ймовірність відвернення *i*-ої загрози за рахунок включення до СФПЗ компоненти f_j, $I_i(f_j)$ — індикатор f_j, тобто, випадкова величина, значення якої дорівнює 1, якщо f_j входить до профілю, і дорівнює нулю у протилежному випадку. Уважаючи випадкові величини $I_i(f_j)$ незалежними, маємо:
- $P_i = \sum_{j=1}^{m} p_{ij} f_j - \sum_{j,l=1,l>j}^{m} p_{ij} p_{il} f_j f_l + \cdots + (-1)^{m-1} \prod_{j=1}^{m} p_{ij} f_j$

14

- *Вірогідність появи i*-ої загрози P_{t_i} визначається таким чином. Як було вказано раніше, кожна загроза залежить від *вірогідності використання деякої множини вразливостей* $V_{ij} = \{v_{ij}, i = 1, \dots, n\}$, тобто $P_{t_i} = f_i(v_{ij}, \dots, v_{in})$. Даний показник також можна визначити на основі експертного методу.
- *Вірогідність використання j-ої вразливості* v_{ij} можна визначити, за допомогою обчислення відносної частоти їх появи. А саме,
- $v_{ij} = \frac{\lambda_{ij}}{\sum_{k=1}^{n} \lambda_{ik}}$, де λ_{ij} - частота виникнення *j*-ої вразливості, а *i* - відповідний номер загрози

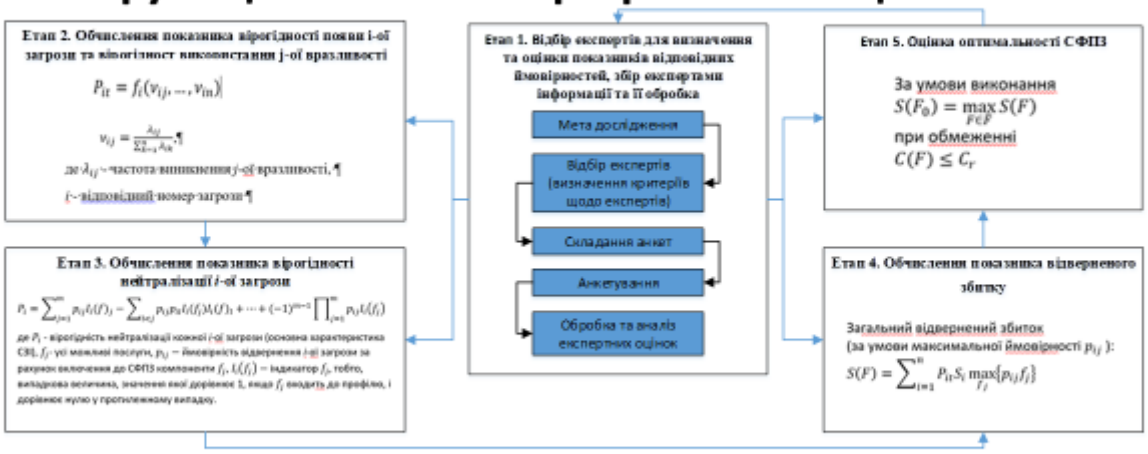
15

Таким чином, метод вибору оптимального функціонального профілю захищеності об'єкту захисту (ВОФПЗ), який складається з наступних кроків:

- Відбір експертів для визначення та оцінки показників відповідних ймовірностей, збір експертами інформації та її обробка.
- Обчислення показника вірогідності *появи i*-ої загрози та вірогідності використання *j*-ої вразливості v_{ij}.
- Обчислення показника вірогідності відвернення *i*-ої загрози.
- Обчислення показника відверненого збитку.
- Оцінка оптимальності СФПЗ за умови виконання $S(F_0) = \max_{F \in \bar{F}} S(F)$ при обмеженні $C(F) \leq C_r$.

16

Метод вибору оптимального стандартного функціонального профілю захищеності



17

Застосування розробленого методу до вибору функціонального профілю захищеності

- Нехай відомо (встановлено на основі статистичних даних), що з ймовірностями 0,2; 0,2; 0,4; 0,6 можуть бути реалізовані наступні загрози:
- загроза несанкціонованого видалення інформації, що захищається;
- загроза перевищення привілеїв;
- загроза використання слабкості протоколу сітьового обміну даними;
- загроза проникнення через контент шкідливого коду,

18

Для відвернення названих загроз можна обрати функціональні послуги $f_{k_1}, f_{k_2}, f_{k_3}, f_{k_4}, f_{k_5}, f_{k_6}, f_{k_7}, f_{k_8}, f_{k_9}$, із них $f_{k_1}, f_{k_2}, f_{k_3}$ – для відвернення першої загрози, f_{k_4}, f_{k_5} – для відвернення другої загрози, відповідно f_{k_6}, f_{k_7} і f_{k_8}, f_{k_9} – для відвернення третьої та четвертої загроз.

- Експертним методом встановлюємо значення ймовірностей рij.

f_j	f_{k_1}	f_{k_2}	f_{k_3}	f_{k_4}	f_{k_5}	f_{k_6}	f_{k_7}	f_{k_8}	f_{k_9}
p_{ij}	$p_{1k_1} = 0,6$	$p_{1k_2} = 0,6$	$p_{1k_3} = 0,5$	$p_{2k_4} = 0,7$	$p_{2k_5} = 0,5$	$p_{3k_6} = 0,7$	$p_{3k_7} = 0,6$	$p_{4k_8} = 0,8$	$p_{4k_9} = 0,8$

19

- Розрахуємо ймовірність відбиття загроз:
- $P_1 = 0,92;\ P_2 = 0,85;\ P_3 = 0,88;\ P_4 = 0,96.$
- Відомо, що можливі збитки від реалізації загроз складають відповідно
- $S_1 = 10;\ S_2 = 6;\ S_3 = 12;\ S_4 = 20$ тисяч гривень.
  Розрахуємо ймовірні відвернуті збитки:
- $r_1 = 1,84;\ r_2 = 1,02;\ r_3 = 4,224;\ r_4 = 11,52.$

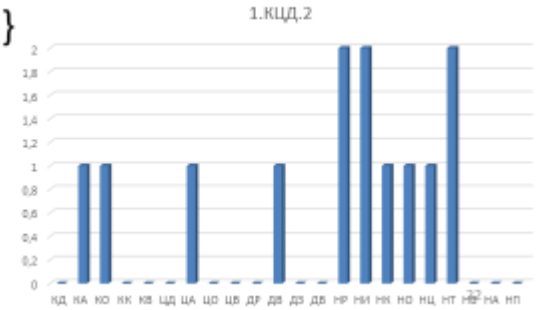
20

Результати реалізації алгоритму наведені в таблиці.
Розрахунки значень комірок таблиці виконані за формулою:
ac[j]=maxac-cjj-1+rjac[j-1]
Таким чином, при заданих фінансових обмеження на реалізацію захисту максимальний відвернутий збиток складатиме 16,764 тис. грн.

	1	2	3	3
0	0	0	0	0
0,5	0	1,02	1,02	1,02
1,0	0	1,02	1,02	1,02
1,5	1,84	1,84	1,84	1,84
2,0	1,84	2,86	4,224	4,224
2,5	1,84	2,86	5,244	5,244
3,0	1,84	2,86	5,244	11,52
3,5	1,84	2,86	6,064	12,54
4,0	1,84	2,86	7,084	12,54
4,5	1,84	2,86	7,084	13,36
5,0	1,84	2,86	7,084	15,744
5,5	1,84	2,86	7,084	16,764

21

- Оскільки максимальний відвернутий збиток складатиме 16,764 тис. грн., це незначна сума, то експерту варто зупинитись на стандартних функціональних профілях захищеності для автоматизованих систем класу 1. СФПЗ, який за заданих умов буде забезпечувати максимальний захист:
  1.КЦД.2 = { КА-1, КО-1, ЦА-1, ЦО-1, ДР-2, ДС-1, ДЗ-1, ДВ-2, НР-2, НИ-2, НК-1, НО-1, НЦ-1, НТ-2 }



22

Застосування методу ВОСФПЗ під час побудови кіберполігону у ЗВО

№ загрози	Загрози	Ймовірності загроз	Збитки від реалізації загроз, тис. грн.	Функціональні послуги для відвернення загроз КЗЗ ОС OpenBSD	Функціональні послуги для відвернення загроз КЗЗПЗ ОС Ubuntu*Pack	Функціональні послуги для відвернення загроз Windows
1	Загроза конфідеційності 1	0,4	55	КД-2, КА-2	КД-2, КА-2	КД-2
2	Загроза конфідеційності 2	0,5	75	КО-1, КВ-2	КО-1, КВ-2	КО-1, КВ-1
3	Загроза цілісності	0,6	90	ЦА-1, ЦД-1, ЦВ-1	ЦА-2, ЦД-1, ЦВ-2	ЦД-1, ЦВ-1
4	Загроза доступності	0,4	95	ДС-2, ДЗ-2, ДВ-2, ДР-2	ДС-1, ДЗ-1, ДВ-1, ДР-1	ДС-1, ДЗ-1, ДВ-1,

23

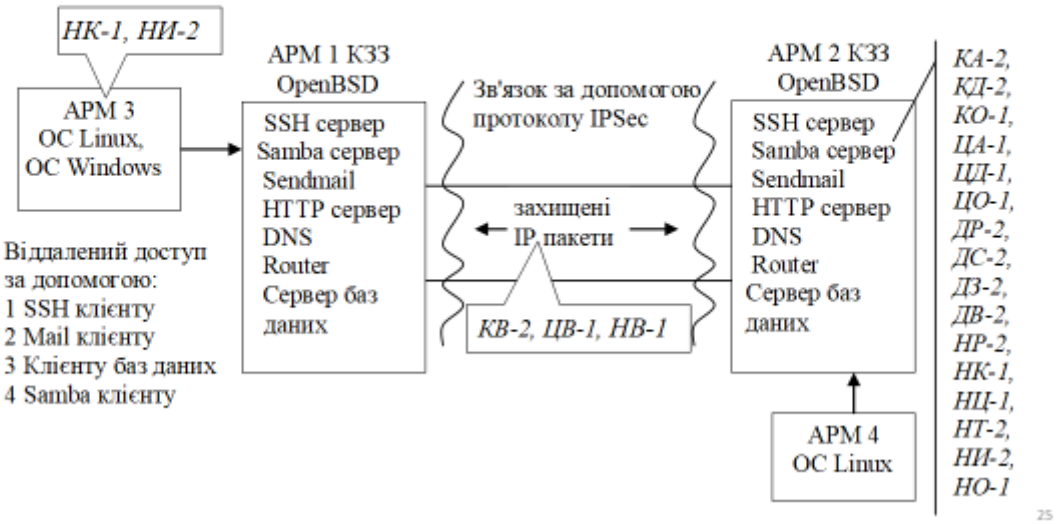
Підсумки розрахунків за методом ВОФСПЗ

Отже, при однакових початкових умовах (загрозах, можливих втратах, в наслідок їх реалізації та фінансових обмеженнях на впровадження профілів захищеності) застосування функціонального профілю, побудованого на основі КЗЗ ОС OpenBSD___виявилось оптимальним, порівняно з іншими наборами функціональних профілів захищеності, оскільки, саме він, при однакових вхідних даних забезпечує більший або такий самий максимальний відвернений збиток, за умови, що відвернення всіх визначених експертами загроз, а саме 1,2,3 та 4.

	Фінансове обмеженнях C_r, тис. грн.	Максимальний відвернутий збиток	Відвернені загрози
Функціональні послуги для відвернення загроз КЗЗ ОС OpenBSD	45	110,523	1,2,3,4
	65	126,8558	1,2,3,4
Функціональні послуги для відвернення загроз КЗЗ ПЗ ОС Ubuntu*Pack	45	93,4965	1, 2, 4
	65	126,1895	2, 3, 4
Функціональні послуги для відвернення загроз КЗЗ Windows	45	81,39	2, 3
	65	116,35	2, 3, 4

24

Структурна схема підключення КЗЗ з ОС OpenBSD



25

Висновки

- Результатом виконаної роботи являється розробка методу, який сприятиме побудові захищеного кіберпростору, за рахунок оптимізації вибору стандартного функціонального профілю захищеності для приватної або державної установи.

Під час виконання роботи було:

- Проведено аналіз методів та моделей захисту кіберпростору, розкрито підходи до оцінювання ефективності методів виявлення кібератак, описано інфраструктуру системи захисту кіберпростору, розглянуто захищені операційні системи, антивірусні системи та криптографічне забезпечення безпеки кіберпростору.
- Розроблено метод, який дозволяє здійснити оптимальний вибір фукціонального профілю захищеності при виконанні умови максимізації відверненого збитку та неперевищення допустимих витрат за рахунок ймовірно-вартісної оцінки показників кількості й частоти появи загрози, ймовірних збитків від реалізації визначених загроз й вартості послуги захисту.
- Проведено застосування запропонованого методу у трьох різних ситуаціях. Експеримент показав дієвість методу та дозволив зробити висновки про доцільність його використання для вибору оптимального стандартного функціонального профілю захищеності.

26