МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Західноукраїнський національний університет
Факультет комп'ютерних інформаційних технологій
Кафедра кібербезпеки

ПРАЧКОВСЬКИЙ Ігор Павлович

Моделі виявлення та розслідування інцидентів кіберзлочинності / Models for Cybercrime Incident Detection and Investigation

спеціальність: 125 – Кібербезпека

освітньо-професійна програма –Кібербезпека

Кваліфікаційна робота

Виконав студент групи КБм -21
І.П. Прачковський

Науковий керівник
д.т.н., професор М.М. Касянчук

Кваліфікаційну роботу допущено
до захисту:

«____» _____ ___2023 р.

Завідувач кафедри
_____ В.В.Яцків

ТЕРНОПІЛЬ – 2023

Факультет комп'ютерних інформаційних технологій
Кафедра кібербезпеки
Освітній ступінь «магістр»
спеціальність: 125 – Кібербезпека
освітньо-професійна програма – Кібербезпека

ЗАТВЕРДЖУЮ
Завідувач кафедри

_____ В.В.Яцків
«____» _____ 2022 року

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ
ПРАЧКОВСЬКИЙ ІГОР ПАВЛОВИЧ

1. Тема кваліфікаційної роботи:
Моделі виявлення та розслідування інцидентів кіберзлочинності / Models for Cybercrime Incident Detection and Investigation
керівник роботи д.т.н., професор М.М. Касянчук

затверджені наказом по університету від «__» _____ 2022 року № _____

2. Строк подання студентом закінченої кваліфікаційної роботи 1 грудня 2023 р.

3. Вихідні дані до кваліфікаційної роботи: завдання на кваліфікаційну роботу студента, наукові статті, технічна література.

4. Основні питання, які потрібно розробити:
– огляд та аналіз актуальності та основних проблем у боротьбі з кіберзлочинністю;
– визначити принципи реалізації кібератак та способи підготовки і скоєння кіберзлочинів;
– розробити класифікацію джерел загроз у кіберзлочинності;
– розробити функціональну модель кіберзлочинів;
– встановити основні етапи інформаційного обміну та вчинення кіберзлочинів.

5. Перелік графічного матеріалу у роботі:
– модель реалізації державної інформаційної політики України;
– схема роботи кіберзлочинців;
– еволюція тактики реалізації загроз;
– сучасна схема роботи кіберзлочинців;
– функціональна модель кіберзлочинів;
– схема етапу вчинення кіберзлочину.

6. Консультанти розділів кваліфікаційної роботи

	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7. Дата видачі завдання 8 грудня 2022 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строки виконання етапів кваліфікаційної роботи	Примітка
1	Актуальність та проблеми боротьби з кіберзлочинністю	12.2022 р. – 03.2023 р.	
2	Способи реалізації кібератак	03.2023 р. – 05.2023 р.	
3	Функціональна модель кіберзлочинів	05.2023 р. – 11.2023 р.	

Студент _____ Прачковський І.П.
(підпис)

Керівник роботи _____ д.т.н., професор М.М.Касянчук

АНОТАЦІЯ

Випускна кваліфікаційна робота на тему „Моделі виявлення та розслідування інцидентів кіберзлочинності” на здобуття освітнього ступеня «Магістр» зі спеціальності 125 „Кібербезпека” освітньо-професійної програми «Кібербезпека» написана обсягом 75 сторінок і містить 13 ілюстрацій, 3 таблиці, 1 додаток та 32 джерела за переліком посилань.

Метою випускної кваліфікаційної роботи є розробка моделей для виявлення інцидентів кіберзлочинності та їх розслідування..

Методи дослідження. Математичні методи моделювання та програмування, методи визначення життєвого циклу.

Результати дослідження: Здійснено аналіз основних типів кіберзлочинності, що дозволило встановити основні типи атак на інформаційну систему та способи реагування на такі інциденти. Розроблено математичні моделі кіберзлочинності, що дозволило враховувати їх встановленні процесів інформа. На основі побудованих моделей кіберзлочинності визначено етапи еволюціїї кіберзлочинності, що дозволило розробити схему їх функціональної моделі. Розроблено функціональну схему моделі кіберзлочинів, на основі чого визначено життєвий цикл кіберзлочинності.

Результати роботи можуть успішно застосовуватися для виявлення та розслідування інцидентів кіберзлочинності.

КЛЮЧОВІ СЛОВА: КІБЕРЗЛОЧИННІСТЬ, ІНЦИДЕНТ, РОЗСЛІДУВАННЯ, МОДЕЛЬ КІБЕРЗЛОЧИНЦЯ, ІНФОРМАЦІЙНА СИСТЕМА.

ABSTRACT

The graduate work on the topic „Models for Cybercrime Incident Detection and Investigation” for Master’s degree on speciality 125 "Cybersecurity " is written on 75 pages and contains 13 illustrations, 3 tables, 1 suplement and 32 references.

The aim of graduate work is to develop models for detecting cybercrime incidents and their investigation.

Research methods. Mathematical methods of modeling and programming, methods of determining the life cycle.

Results of the study. An analysis was made of the main types of cybercrime, which made it possible to establish the main types of attacks on the information system and methods of responding to such incidents. Mathematical models of cybercrime were explained, which made it possible to take into account their establishment of information processes. On the basis of the constructed models of cybercrime, the stages of the evolution of cybercrime were determined, which made it possible to develop a diagram of their functional model. A functional scheme of the cybercrime model was developed, based on which the life cycle of cybercrime was determined.

The results of the work can be successfully applied to detect and investigate cybercrime incidents.

Keywords: CYBERCRIME, INCIDENT, INVESTIGATION, CYBERCRIMINAL MODEL, INFORMATION SYSTEM.

ЗМІСТ

ВСТУП

На даний час комп'ютерні та телекомунікаційні технології охоплюють практично всі сфери життя суспільства [1-4]. Більшість людей значну частину свого часу проводять в Інтернеті. Цей віртуальний світ багато в чому відбиває реальний світ: злочинність, що є, на жаль, невід'ємною частиною соціуму, існує і у віртуальному середовищі [5-6]. Зростання обміну інформаційними даними в Інтернеті та електронні платежі – це саме той ласий шматок, який найбільше приваблює зловмисників. Структура сучасної кіберзлочинності практично сформована: вже існують чітко визначені взаємини та бізнес-моделі [7-8].

Кримінальна діяльність завжди була дзеркальним відображенням легального бізнесу [9-10]: образ фінансиста-мафіозі – перше, що спадає на думку. Однак сучасна кіберзлочинність – це не одна-дві мафіозні організації на чолі з ватажком [11-12]. Скоріше, це світ, що складається із взаємодоповнюючих та взаємодіючих один з одним груп.

Сучасна кіберзлочинність розвивається так само, як і будь-який інший бізнес. Прибутковість, управління ризиками, освоєння нових ринків також є важливими складовими цього бізнесу .

Проблема кіберзлочинності переросла у масштаби світової спільноти [13-14]. Для розробки наукового підходу до вирішення цієї проблеми необхідна її формалізація: виділення основних об'єктів і визначення принципових властивостей аналізованого явища.

Результати аналізу характеристик комп'ютерної злочинності вказують на можливість ускладнення боротьби з нею, оскільки методи вчинення комп'ютерних злочинів стають все більш витонченими і важкозрозумілими кожним роком [15-17]. Для вирішення цієї проблеми необхідно вживати комплексний підхід.

Мета роботи. Метою роботи є розробка моделей для виявлення інцидентів кіберзлочинності та їх розслідування.

Для вирішення поставленої мети вирішуються наступні **завдання**:

– огляд та аналіз актуальності та основних проблем у боротьбі з кіберзлочинністю;

– визначити принципи реалізації кібератак та способи підготовки і скоєння кіберзлочинів;

– розробити класифікацію джерел загроз у кіберзлочинності;

– розробити функціональну модель кіберзлочинів;

– встановити основні етапи інформаційного обміну та вчинення кіберзлочинів.

Об’єкт дослідження. Процес протидії інцидентам кіберзлочинності.

Предмет дослідження. Методи і засоби виявлення та розслідування інцидентів кіберзлочинності.

Методи дослідження. Математичні методи моделювання та програмування, методи визначення життєвого циклу.

Наукова новизна одержаних результатів.

1. Здійснено аналіз основних типів кіберзлочинності, що дозволило встановити основні типи атак на інформаційну систему та способи реагування на такі інциденти.

2. Розроблено математичні моделі кіберзлочинності, що дозволило враховувати їх при визначенні методів захисту від основних типів атак на систему.

3. На основі побудованих моделей кіберзлочинності визначено етапи еволюціїї кіберзлочинності, що дозволило розробити схему їх функціональної моделі.

Практичне значення отриманих результатів. Розроблено функціональну схему моделі кіберзлочинів, на основі чого визначено життєвий цикл кіберзлочинності.

Публікації та апробація КР.

1. Прачковський І.П., Черняк В.А. Класифікація кіберзлочинців у сучасному кіберпросторі. Збірник матеріалів науково - практичної конференції молодих вчених, аспірантів та студентів «Кібербезпека та комп’ютерно-інтегровані технології» (КБКІТ-2023), Тернопіль, 2023. С.51-54 [18].

2. Прачковський І.П., Грицьків А.В. Актуальність та проблеми боротьби з кіберзлочинністю. Матеріали науково-практичного симпозіуму «Захист інформації». Тернопіль, 2023. С.145-147 [19].

1 АКТУАЛЬНІСТЬ ТА ПРОБЛЕМИ БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ

1.1 Основні поняття та визначення

Злочинність у віртуальному просторі – порівняно нове явище, але частина злочинів, що скоюються у сфері високих технологій – це знайомі всім крадіжки, шахрайства, вимагання тощо [20-22]. І для дослідження проблеми кіберзлочинності необхідно дати коректні визначення таким явищам, як віртуальний простір, кіберзлочинність, комп'ютерні злочини, кібертероризм, щоб відмежувати їх один від одного та суміжних понять.

Нині немає скільки-небудь узагальнених даних на формування понять основних елементів характеристики кіберзлочинів. Все ще немає чіткого визначення поняття кіберзлочину і дискутуються різні точки зору щодо їх класифікації.

Деякі правознавці вважають, що комп'ютерними злочинами є всі злочини, у якому комп'ютер є зброєю, засобом чи метою їх скоєння [23-24]. Інші об'єднують під цим терміном всі протизаконні дії, які завдають шкоди майну і пов'язані з електронною обробкою інформації. У Німеччині, наприклад, поліція, використовує визначення кіберзлочинності як «всі протизаконні дії, у яких електронна інформація виступала засобом чи об'єктом».

У визначеннях "комп'ютерного злочину", наприклад, автори чітко акцентують увагу на тому, що це суспільно небезпечні дії, передбачені кримінальним законом [25-26].

Кіберзлочинність - це форма злочинності, яка відбувається у віртуальному просторі. Термін "віртуальний простір" означає інформаційний простір, створений за допомогою комп'ютера, в якому містяться дані про особи, об'єкти, факти, події, явища і процеси у математичному, символьному або іншому форматі. Ці дані переміщуються через локальні та глобальні комп'ютерні мережі або зберігаються в пам'яті фізичних або віртуальних пристроїв, спеціально призначених для зберігання, обробки та передачі інформації.

Це визначення відповідає рекомендаціям експертів ООН, які вважають, що термін "кіберзлочинність" охоплює будь-який злочин, що може бути вчинений

за допомогою комп'ютерних систем чи мереж, всередині чи поза ними, або проти них. Таким чином, кіберзлочинами можуть бути визнані будь-які протиправні дії, які відбуваються в електронному середовищі [27].

Злочини, скоєні в кіберпросторі, включають незаконне втручання в роботу комп'ютерів, програм та мереж, несанкціоновану модифікацію комп'ютерних даних, а також інші протиправні та суспільно небезпечні дії, вчинені за допомогою комп'ютерів, мереж та програм [28-29].

Поняття кіберзлочинності включає у собі не тільки дії, скоєні в глобальній мережі Інтернет. Цей вид злочинності охоплює всі категорії правопорушень, які відбуваються у сфері інформаційно-телекомунікаційних технологій [30]. Тут інформація, інформаційні ресурси та техніка можуть бути об'єктом або метою злочинних дій, середовищем, де вони вчиняються, і знаряддям або засобом здійснення злочину.

Згідно з Конвенцією Ради Європи, існує чотири основні типи чистих комп'ютерних злочинів, які визначаються як порушення конфіденційності, цілісності та доступності комп'ютерних даних та систем:

- незаконний доступ - ст. 2 (незаконне навмисне проникнення до комп'ютерної системи або її частини);

- незаконне перехоплення - ст. 3 (протиправне навмисне перехоплення не призначених для громадськості передач комп'ютерних даних у комп'ютерну систему, з неї або в її межах);

- втручання у дані - ст. 4 (протиправне пошкодження, видалення, порушення, зміна або припинення передачі комп'ютерних даних);

- втручання у систему - ст. 5 (серйозне протиправне перешкоджання функціонуванню комп'ютерної системи шляхом введення, передачі, пошкодження, видалення, порушення, зміни чи припинення передачі комп'ютерних даних).

За нашою думкою, саме ці чотири види злочинів є справжніми "комп'ютерними", тоді як інші вважаються пов'язаними з комп'ютером (computer-related) або скоєними за допомогою комп'ютера (computer-facilitated) злочинами. До них відносяться:

- злочини, у яких комп'ютер є знаряддям (електронні розкрадання, шахрайства тощо);

- дії, під час яких комп'ютер є інтелектуальним засобом (наприклад, розміщення на сайтах дитячої порнографії, інформації, що розпалює національну, расову, релігійну ворожнечу і т.д.).

Сам термін «кібертероризм» з'явився в лексиконі приблизно 1997 року. Саме тоді спеціальний агент ФБР Марк Поллітт визначив цей вид тероризму як «навмисні політично мотивовані атаки на інформаційні, комп'ютерні системи, комп'ютерні програми та дані, виражені у застосуванні насильства стосовно цивільних цілей з боку субнаціональних груп чи таємних агентів».

Відомий експерт Д. Деннінг говорить про кібертероризм як про «протиправну атаку або загрозу атаки на комп'ютери, мережі або інформацію, що перебуває в них, здійснену з метою змусити органи влади до сприяння у досягненні політичних чи соціальних цілей».

Дослідники М.Дж. Девост, Б.Х. Х'ютон, Н.А. Поллард визначають інформаційний тероризм (а кібертероризм є його різновидом) як:

1) поєднання злочинного використання інформаційних систем за допомогою шахрайства або зловживань із фізичним насильством, властивим тероризму;

2) свідоме зловживання цифровими інформаційними системами, мережами чи компонентами цих систем чи мереж з метою, що сприяють здійсненню терористичних операцій чи актів.

Узагальнюючи такі різні точки зору, можна дійти невтішного висновку про те, що у теперішній час існує два основних наукових напрямки стосовно цього питання.

Існує два підходи серед дослідників до класифікації комп'ютерних злочинів. Згідно з однією групою дослідників, комп'ютерні злочини включають в себе події, в яких комп'ютер виступає як об'єкт або знаряддя посягань. Інша група дослідників обмежує комп'ютерні злочини лише протизаконними діями в сфері автоматизованої обробки інформації. Як головною класифікуючою

ознакою, що дозволяє віднести ці злочини до відокремленої групи, виділяється спільність методів, знарядь, об'єктів посягань тощо.

Іншими словами, об'єктом зазіхання є інформація, яка оброблюється в комп'ютерній системі, а комп'ютер служить знаряддям зазіхання [31-32].

Підбиваючи деякі підсумки, можна виділити такі характерні особливості кіберзлочину:

1) неоднорідність об'єкта зазіхання;

2) розгляд машинної інформації як об'єкта, так і як засобу злочину;

3) різноманіття предметів та засобів злочинного посягання.

Тому існує проблема, яка знайшла своє відображення в роботах учених, існують різноманітні думки, але відсутня єдність поглядів на поняття зазначеної категорії злочинів.

Зарубіжними колегами, наприклад, використовуються такі поняття як High tech crime або Cyber crime, які перекладаються як «злочини у сфері високих технологій» та «кіберзлочини».

Тому доцільно позначити термін «кіберзлочин» як злочини, вчинені з використанням комп'ютерної мережі як компонента злочину, акцентуючи увагу на способі вчинення.

1.2 Класифікація кіберзлочинності

У 1991 році був розроблений та інтегрований в автоматизовану систему пошуку кодифікатор стосовно кіберзлочинності. На даний час він доступний підрозділам Національних центральних бюро Міжнародної кримінальної поліції "Інтерпол" більш, ніж у 120 країнах світу.

Усі коди, що характеризують комп'ютерні злочини, мають ідентифікатор, що починається з літери Q. Для характеристики злочину можна використовувати до п'яти кодів, розміщених в порядку зменшення значимості здійсненого:

1) QA – несанкціонований доступ або перехоплення;

- QAH – це комп'ютерний абордаж;
- QAI – це перехоплення;

- QA1 – це крадіжка часу;

- QAZ – це деякі інші види несанкціонованого доступу і перехоплення;

2) QD – це зміна комп'ютерних даних;

- QDL – це логічна бомба;

- QDT – це троянський кінь;

- QDV – це комп'ютерний вірус;

- QDW – це комп'ютерний хробак;

- QDZ – це інші якісь види зміни даних;

3) QF – це комп'ютерне шахрайство (computer fraud);

- QFC – це шахрайство із банкоматами;

- QFF – це комп'ютерна підробка;

- QFG – це шахрайство із ігровими автоматами;

- QFM – це маніпуляції із програмами для введення висновку;

- QFP – це шахрайства із платіжними коштами;

- QFT – це телефонне шахрайство;

- QFZ – це якісь інші комп'ютерні шахрайства;

4) QR – це незаконне копіювання (тобто "піратство");

- QRG – це комп'ютерні ігри;

- QRS – це якесь інше ПЗ;

- QRT – це топографія у напівпровідникових виробах;

- QRZ – це якесь інше незаконне копіювання;

5) QS – це комп'ютерний саботаж;

- QSH - із апаратним забезпеченням;

- QSS - із ПЗ;

- QSZ – це якісь інші види саботажу;

6) QZ – це якісь інші комп'ютерні злочини;

- QZB - із використанням комп'ютерних дощок для оголошення;

- QZE – це крадіжка інформації, яка становить комерційну таємницю;

- QZS – це передача інформації конфіденційного характеру;

- QZZ – це деякі інші комп'ютерні злочини.

Несанкціонований доступ – неправомірний доступ до комп'ютерної системи або мережі шляхом порушення охоронних заходів.

Несанкціоноване перехоплення - неправомірне і здійснене за допомогою технічних засобів перехоплення повідомлень, що надходять до комп'ютерної системи чи мережі, що виходять із комп'ютерної системи чи мережі та передаються в рамках комп'ютерної системи чи мережі.

Зміна комп'ютерних даних - неправомірна зміна комп'ютерних даних.

Комп'ютерне шахрайство – це є введення, стирання, зміна чи придушення комп'ютерних даних чи комп'ютерних програм або якесь інше втручання в процес обробки даних, що впливає на результат обробки даних, який завдає економічної шкоди або призводить до втрати власності іншої особи, з наміром отримати незаконним шляхом економічну вигоду для себе або іншої особи.

Комп'ютерний саботаж – це є зміна, введення, стирання чи придушення комп'ютерних даних чи комп'ютерних програм або створення перешкод комп'ютерним системам з наміром перешкодити роботі комп'ютера чи телекомунікаційної системи.

Прокласифікувати комп’ютерні злочини можна за такими критеріями:

1) у сфері обороту комп'ютерної інформації:

а) неправомірний доступ комп'ютерної інформації, що охороняється законом;

б) операції з шкідливими програмами;

в) порушення авторських чи суміжних прав щодо програм, а також інших об'єктів авторського чи суміжного права, що знаходяться у вигляді документів на машинному носії;

г) незаконні виготовлення із метою поширення чи рекламування, поширення, рекламування порнографічних матеріалів на машинних носіях, у системі чи мережі, так само як незаконна торгівля ними;

д) виготовлення та обіг матеріалів з порнографічними зображеннями неповнолітніх;

2) у сфері телекомунікацій:

а) незаконне прослуховування телефонних переговорів та інших повідомлень;

б) незаконне перехоплення та реєстрація інформації із технічних каналів зв'язку;

в) неправомірний контроль електронних поштових повідомлень та відправлень;

3) у сфері інформаційного обладнання:

а) порушення правил експлуатації систем чи мереж;

б) незаконний оборот різних спеціальних технічних засобів, які призначені (пристосованих, розроблених, запрограмованих) для негласного отримання інформації;

в) незаконний оборот спеціальних технічних засобів, призначених (розроблених, пристосованих, запрограмованих) для негласного отримання (знищення, зміни) інформації із технічних засобів для її створення, обробки, передачі та зберігання;

г) незаконне виготовлення із метою збуту або збут підроблених кредитних чи розрахункових карток;

д) порушення авторських прав щодо топологій інтегральних мікросхем;

4) у сфері захисту інформації, що охороняється законом:

а) незаконне збирання або розповсюдження відомостей про особисте життя особи, що становлять її особисту чи сімейну таємницю, у тому числі персональних даних – це будь-яка інформація, що відноситься до певної або визначеної на підставі такої інформації фізичної особи (суб'єкта персональних даних), в тому числі її прізвище, ім'я, по батькові, рік, місяць, дата та місце народження, адреса, сімейне, соціальне, майнове становище, освіта, професія, доходи, інша інформація;

б) розголошення інформації, що охороняється законом: державної таємниці; службової таємниці та професійної таємниці;

в) незаконні збирання, розголошення чи використання відомостей, які становлять податкову, комерційну чи банківську таємницю;

г) незаконні експорт чи передача іноземній організації чи її представнику науково-технічної інформації, що використовувати можна під час створення озброєння і військової техніки і щодо якої встановлено експортний контроль;

5) у сфері інформаційних правовідносин:

а) поширення свідомо неправдивої інформації;

б) неправомірна відмова у наданні або ухилення від надання інформації;

в) приховування чи спотворення інформації;

6) у сфері економіки і комп'ютерної інформації:

а) шахрайство у сфері надання послуг електрозв'язку та доступу до інформаційних ресурсів мережі "Інтернет";

б) шахрайство у сфері електронного переказу коштів;

в) незаконна діяльність у сфері надання послуг електрозв'язку та доступу до інформаційних ресурсів мережі "Інтернет";

г) інші злочини, скоєні у сфері економіки і комп'ютерної інформації.

Спрощена схема класифікації кіберзлочинів за різними критеріями наведена на рисунку 1.1.

1.3 Актуальність та проблеми боротьби з кіберзлочинністю

Зростання обсягів комп'ютерних мереж, інформації та числа користувачів, спрощення доступу їх до інформації, що циркулює по мережах, істотно підвищує ймовірність розкрадання чи руйнування такої інформації.

Нині значимість проблеми для захисту інформаційних ресурсів, зокрема особистих, визначається такими факторами:

- розвитком світових та національних комп'ютерних мереж і нових технологій, які забезпечують доступ до інформаційних ресурсів;

- переведенням на електронні носії інформаційних ресурсів та концентрацією їх у інформаційних системах;

- підвищенням "ціни" створюваної та накопиченої інформації, що є реальним ресурсом соціально-культурного та особистісного розвитку;

- розробкою та удосконаленням інформаційних технологій, що можуть ефективно використовуватись кримінальними структурами.

Рисунок 1.1 – Схема класифікації кіберзлочинів

Комп'ютерна злочинність стає реальним бичем економіки розвинених країн. Так, наприклад, майже 100% фірм та організацій у Великій Британії в різний час ставали об'єктами електронного піратства або перебували під його загрозою.

Найбільшу суспільну небезпеку становлять злочини, що пов'язані із неправомірним доступом до комп'ютерної інформації. Відомо, що такі правопорушення мають дуже високу латентність, яка за різними даними становить 85-90%. Більше того, факти виявлення незаконного доступу до інформаційних ресурсів на 90% мають випадковий характер.

Злочин даного виду, як свідчить світова практика, завдає величезної матеріальної і моральної шкоди. Тобто в сучасних умовах соціально-економічного розвитку комп'ютерна злочинність стала реальністю життя. Підтвердженням зростання таких комп'ютерних злочинів є статистичні дані.

У розвитку комп'ютерної злочинності виділяються основні такі тенденції:

а) високі темпи у зростанні;

б) корислива мотивація у більшості скоєних комп'ютерних злочинів;

в) ускладнення способів під час скоєння комп'ютерних злочинів і поява нових видів у протиправній діяльності в сфері комп'ютерної інформації;

г) зростання кримінального професіоналізму у комп'ютерних злочинців;

д) омолоджування комп'ютерних злочинців та збільшення частки осіб, які раніше не притягувалися до кримінальної відповідальності;

е) зростання матеріальних збитків від комп'ютерних злочинів в загальній частці збитків від інших видів злочинів;

є) перенесення центру тяжкості скоєння комп'ютерних злочинів із допомогою комп'ютерних мереж;

ж) переростання комп'ютерної злочинності до розряду транснаціональної злочинності;

з) високий рівень латентності у комп'ютерних злочинах.

Боротьба із кіберзлочинністю має стати пріоритетною функцією для всіх правоохоронних органів та силових відомств.

Оскільки Інтернет загалом нікому безпосередньо не належить, ніким безпосередньо не регулюється, то немає і відповідальної за Інтернет адміністративної інстанції, яка могла б заборонити практику розміщення на Web-сайтах порнографічних картинок. Положення ускладнюється тим, що інформація може зберігатися на Web-сайтах в іншій країні або іншому континенті, де законодавство не готове встановлювати відповідальність за зберігання і розповсюдження непристойної інформації. Проблема має вирішуватись на міжнародному рівні, можливо в рамках ЮНЕСКО.

Результати при аналізі характеристики комп'ютерної злочинності дають можливість спрогнозувати ускладнення боротьби із нею з огляду, що способи

скоєння комп'ютерних злочинів набувають із кожним роком все більше витонченого і важковизначеного характеру. Для вирішення такої проблеми потрібно комплексно підходити.

Фахівці виділяють такі елементи при організації діяльності правоохоронних органів в інформаційних глобальних мережах:

- вивчення та оцінка обстановки у мережах;

- здійснення оптимального розміщення сил та засобів, забезпечення певної взаємодії;

- планування, управління та контроль; координація дій суб'єктів правоохоронних органів.

Істотним елементом у системі заходів боротьби із комп'ютерною злочинністю є заходи у превентивному характері чи заходи попередження. Більшість зарубіжних фахівців вказують, що попереджувати комп'ютерний злочин набагато легше та простіше, ніж розкрити та розслідувати його.

Зазвичай виділяють основні три групи заходів запобігання комп'ютерним злочинам: організаційно-технічні, правові та криміналістичні, що становлять в сукупності цілісну систему боротьби із цими соціально небезпечними явищами.

Стратегія міжнародного співробітництва у сфері протидії комп'ютерній злочинності та пріоритетні напрямки її реалізації, у тому числі міждержавні угоди, організація міждержавної оперативно-розшукової діяльності, прийняття міждержавного регламенту та вдосконалення інтеграційних процесів у рамках міждержавних організацій, обґрунтування необхідності розробки та прийняття відповідної комплексної міждержавної програми.

1.4 Поняття кіберцифрової зброї

Кібернетична злочинність в основному визначається як будь-яка злочинна діяльність, що реалізується через інтернет. Злочинна діяльність з використанням IT-технологій пов'язана з хактивізмом, шахрайством, шкідливими програмами, вірусами, крадіжкою даних, кіберсталкінгом, тероризмом, шпигунством, кампаніями дезінформації та військовими діями у кіберпросторі. Але

ефективність розкриття зазначених суспільно небезпечних діянь далека від ідеалу, що передбачає подальше дослідження цієї проблематики.

У рамках розробки процесуальних та криміналістичних основ розслідування пригод та злочинів у збройних формуваннях виділяються інноваційні пропозиції щодо доповнення криміналістичного зброєзнавства під галуззю «криміналістичне дослідження кіберцифрової зброї». Слід констатувати, що кібертероризм є елементом гібридних воєн. Тому розробка сутнісних структур, концептуальних положень, методологічних засад у галузі процесуальних, пошуково-пізнавальних, слідчих, тактичних дій при розслідуванні кібератак та кіберзлочинів, а також використання кіберцифрової зброї органами військової юстиції, дізнання та слідства виступає пріоритетним напрямом діяльності щодо запобігання злочинності, загибелі у збройних формуваннях, убивств військовослужбовців тощо.

У кіберцифровій зброї складно виділити лінійні розміри. Вона, зазвичай, застосовується безконтактно, віддалено, індивідуально з урахуванням інформаційно-комп'ютерного забезпечення, обчислювальних потужностей, рівня кібернетичної захищеності. Намір та атрибуція використання такої зброї під час кібернетичних злочинів можуть бути невідомі. Крім того, кібернетичні атаки часто створюють каскадні ефекти, які залишалися поза початковими цілями зловмисників. Кіберцифрова зброя як знаряддя та засіб здійснення кібернетичних атак застосовується у специфічному середовищі існування: комп'ютерних нейронних мережах – кібернетичному, цифровому просторі.

При криміналістичному дослідженні кіберцифрової зброї пропонується виділяти його структуру та елементи з урахуванням використання у злочинних цілях: комп'ютерні технології; програмні засоби; електронно-обчислювальні засоби, мобільні пристрої; носії інформації – знімні, стаціонарні; хмарні технології; технічне рішення; апаратно-програмні комплекси (бот-ферми); шкідливі програми; можливості кібернетичного простору, що включає глобальні, локальні, бездротові, Wi-Fi, інтернет-ресурси, соціальні мережі; ретрансляційне обладнання, у тому числі супутники, повітряні судна, наземні об'єкти, надводні та підводні кораблі, гідротехнічні споруди та предмети. Цей

список, безумовно, нескінченний через сили і засоби, а також професійні навички та тактичні прийоми, що знаходяться в арсеналі хакерів.

Механізм скоєння кіберзалежного злочину полягає в тому, що хакери перехоплюють управління високоточними технологічними системами – супутниками, безпілотниками, бойовими надводними кораблями та підводними човнами, бронетанковою технікою, бойовими знаряддями, авіаційними засобами, ракетами, вносять шкідливі корективи у програму діяльності та перенацілюють їх на завдання ударів по вибраним ними цілям. Це, безперечно, ставить перед правоохоронними органами, органами дізнання та попереднього розслідування, у тому числі військової юстиції, завдання щодо запобігання, своєчасного виявлення та розслідування аналізованих злочинів з використанням кіберцифрової зброї для забезпечення безпеки, запобігання загибелі військовослужбовців.

Особливістю розслідування кіберзлочинів є їх якісно новий рівень. Передбачається використання сучасних тактичних прийомів при плануванні слідчих дій в умовах реальності, що постійно змінюється, і нового масштабу часу в технологічних процесах скоєння таких злочинів. Виклик від кіберзлочинців – хакерів, крекерів, фрікерів, кардерів, вірусописачів, вірмейкерів, крипторів, ботоводів, фродів, скамерів, спамерів – прийнятий науковою спільнотою та правоохоронними органами.

Формування тактичних операцій, направлених на розкриття і розслідування кібернетичних злочинів, безпосередньо пов’язано з слідчими ситуаціями. Результати дослідження дозволили виявити особливості, що впливають на планування розслідування, висування загальних та приватних версій та вироблення рекомендацій при використанні тактичних прийомів. Як характеристики розкриття злочинів цієї категорії слід відзначити анонімність і скритність механізму кібернетичного злочину. Існує кілька методів анонімізації, які використовують кіберзлочинці. Анонімайзери або анонімні проксі-сервери приховують ідентифікаційні дані користувачів, маскуючи їх IP-адресу та замінюючи її іншим. Правопорушники також можуть вдаватися до анонімних мереж для шифрування, блокування трафіку та приховування адреси інтернет-

протоколу або IP-адреси, присвоєного комп'ютеру провайдером при підключенні до мережі. Відомими прикладами анонімних мереж є Tor, Freenet та невидимий інтернет-проект, відомий як I2P. Анонімні мережі не лише маскують користувачів, а й розміщують їх веб-сайти за допомогою можливостей прихованих сервісів. Подібні мережі використовуються для доступу до так званих сайтів Darknet (або Dark Web). При прийнятті тактичного рішення з метою впливу на наслідкову ситуацію необхідно враховувати, що Всесвітню павутину легко уявити за допомогою візуалізації, внаслідок чого її можна характеризувати як видиму павутину чи прозору мережу, доступну громадськості. Тут дані можуть бути знайдені за допомогою традиційних пошукових систем, таких як Google або Bing. Глибока павутина - це та темна частина айсберга, яка знаходиться під поверхнею. Вона включає захищені паролями сайти, неіндексовані пошуковими системами. Темне павутиння вимагає залучення спеціалізованого програмного забезпечення з метою приховування можливостей доступу до сайтів, саме ця область кібернетичного простору використовується крекерами.

Також слід зазначити, що атрибуція є ще однією особливістю розслідування кіберзалежних злочинів. При цьому встановлюється зв'язок між кібератакою та цифровим пристроєм. Застосування засобів підвищення анонімності може ускладнити ідентифікацію апаратури і навіть осіб, відповідальних за злочинні дії. Атрибуція додатково ускладнюється за рахунок використання заражених шкідливими програмами комп'ютерів зомбі (або ботнетів) або цифрового пристрою, контрольованого за допомогою віддаленого доступу. Шкідливі програми забезпечують доступ до систем та дають можливість керувати ними без відома користувача. Для цього створюється ефект несправності алгоритму (бекдора) на інфікованому пристрої.

При провадженні попереднього розслідування кіберзалежного злочину важливою тактичною рекомендацією слід визнати застосування зворотного відстеження (traceback) – способу, що дозволяє простежити незаконні дії у зворотний бік до кіберцифрової зброї. Це можливо після скоєння кіберзлочину або при його виявленні. Тому пропонується оснащувати органи дізнання та

попереднього розслідування черговим апаратним техніко-криміналістичним комплексом, що дає можливість виконувати зворотне відстеження та апаратний пошук – криміналістичний тролінг (forensic trolling). Отримуючи електронні сліди та цифрові докази використання кіберзброї, співробітник відповідного підрозділу на підставі запиту чи постанови органу попереднього розслідування готує звітні документи. Тому доцільно подавати матеріали оперативнорозшукових заходів відповідно до нормативних актів у вигляді довідки з додатками у формі блок-схем з'єднань в інформаційно-технологічних мережах, якими користувався хакер. Водночас відомості, на підставі яких встановлюються обставини, що підлягають доведенню, можуть відображатися і у висновках експерта, які формуються за результатами звітного періоду – чергування фахівця з forensic trolling. Підготовку фахівців із використання криміналістичного тролінгу, програмно-технічного та апаратного комплексу, спрямованого на автоматичне виявлення, фіксацію та документування цифрових слідів злочинів, слід проводити на постійній основі в установах, що пройшли відповідну акредитацію.

Цифрові докази можуть виявлятися органами дізнання, що здійснюють оперативно-розшукові заходи, шляхом вивчення лог-файлів: журналів подій, які є продуктами діяльності файлових систем та розкривають інформацію про дії кіберзлочинців. Прикладами таких журналів є програми, що фіксують «події, реєстровані програмами та додатками», та журнали безпеки, що дозволяють здійснювати «запис усіх спроб входу в систему (як дійсних, так і недійсних) і створення, відкриття або видалення файлів, програм або інших об'єктів користувачем комп'ютера».

За допомогою криміналістичного тролінгу ці інструменти дають змогу виявити як інтернет-провайдера, так і IP-адресу, яку приховують правопорушники. Залежно від механізму злочину відстеження в рамках криміналістичного тролінгу не завжди забезпечується встановлення єдиного джерела, що ідентифікується. Наприклад, це може спостерігатися лише у випадках, коли заражені шкідливими програмами комп'ютери-зомбі використовуються для кіберзлочинів або декілька хакерів одночасно проводять

розподілену атаку "відмови в обслуговуванні" (тобто DDoS-атаку) проти системи або веб-сайту.

Потрібно визнати потужність кіберцифрової зброї як елемента криміналістичної характеристики кіберзлочинів. Досліджені особливості провадження пошуково-пізнавальних дій для виявлення, фіксації та документування цифрових слідів з метою розкриття кібератак та викриття осіб, які їх вчинили, безумовно, впливають на всю систему тактики попереднього розслідування.

Слід наголосити на необхідності вироблення інноваційних підходів та сучасних рекомендацій для слідчої та судової практики при розслідуванні кіберзалежних злочинів. Сформульовані положення як у кримінологічному, так і в криміналістичному аспектах сприяють збільшенню нових знань у галузі, що розглядається, розширенню понятійного апарату в правоохоронних органах.

2 СПОСОБИ РЕАЛІЗАЦІЇ КІБЕРАТАК

2.1 Принципи реалізації атак

Найважливішим критерієм оцінки будь-якого бізнесу є його прибутковість, і кіберзлочинність тут не є винятком. Кіберзлочинність неймовірно прибуткова! Дуже великі суми грошей опиняються у кишенях злочинців в результаті великих окремих афер, не кажучи уже про незначні суми, що просто йдуть потоком.

На рисунку 2.1 наведено приклад схеми легалізації коштів від кіберзлочинів.

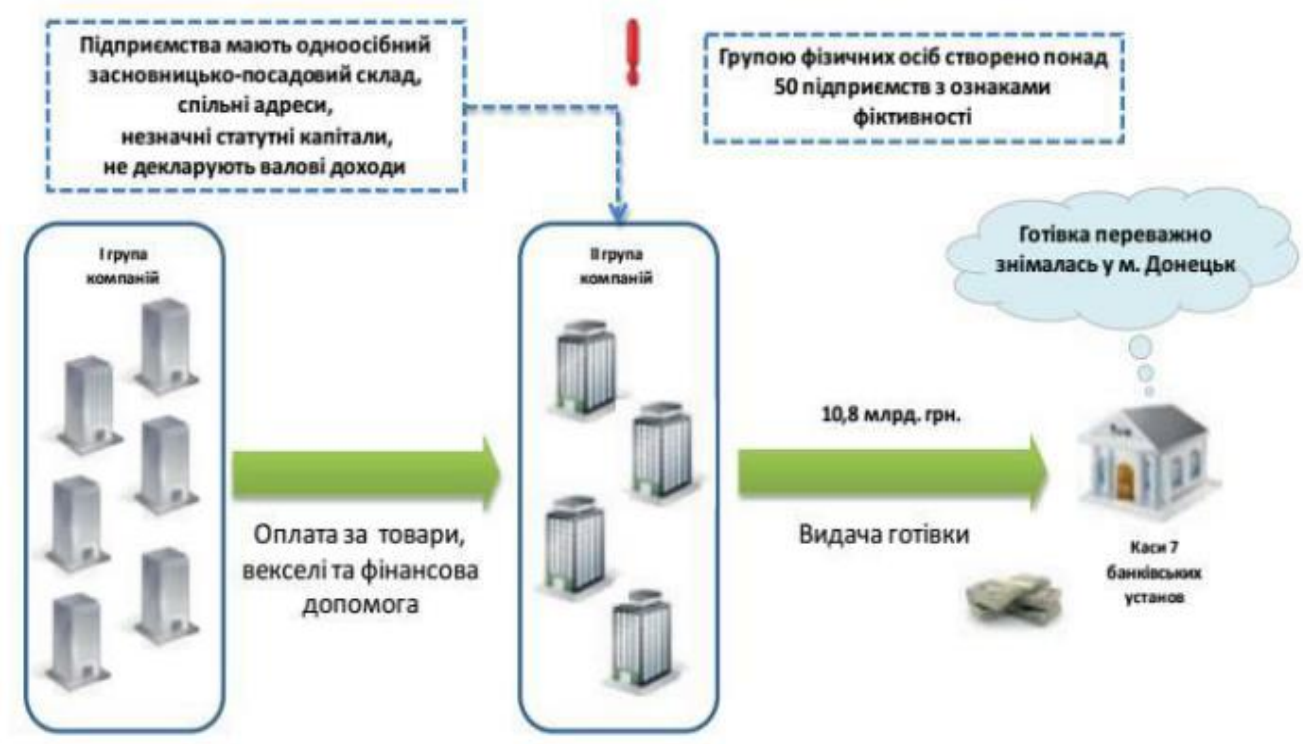

Рисунок 2.1 - Схема легалізації коштів від кіберзлочинів

Як правило, самі потерпілі та правоохоронні органи намагалися привернути до них увагу громадськості. Але найчастіше організації, які зазнали атаки, самі проводять розслідування, або цим займаються правоохоронні органи, – але без розголосу. Результати практично ніколи не оприлюднюються.

Кожне покоління злочинців має свої унікальні інструменти. Сучасні кіберзлочинці переважно обирають зброєю своєю троянські програми. За їх

допомогою вони будують різні ботнети, зокрема, для крадіжки персональних паролів та іншої конфіденційної інформації, проводять відповідні атаки DoS і шифрують дані користувачів, щоби потім можна було шантажувати своїх жертв. Характерною та небезпечною рисою теперішніх шкідливих програм є те, що прагнуть вони зберегти присутність свою на інфікованій машині. Для досягнення такої мети кіберзлочинці використовують різноманітні технології.

В даний час деякі злочинці вважають за краще проводити тільки окремі атаки, які будуть націленими на конкретні організації. Саме собою написання спеціальної програми для однієї цільової атаки – завдання надзвичайно трудомістке, але важливо ще забезпечити цій програмі працездатність на зараженому комп'ютері користувача протягом досить тривалого часу. Однак якщо такі цільові атаки вдається запустити, то успіх їм практично завжди забезпечений: в цьому випадку кіберзлочинці не тільки компенсовують собі всі можливі витрати на розробку та запуск атаки, але і отримують солідний прибуток.

Для прикладу на рисунку 2.2 наведена типова схема виявлення комп’ютерних атак.

Сучасні кіберзлочинці для отримання бажаного результату повинні правильно організувати два важливі моменти: доставку та забезпечення працездатності програми.

Перший крок будь-якого кіберзлочину – доставка та встановлення на комп’ютері користувача шкідливої програми. Злочинці використовують декілька технологій задля досягнення цієї мети. Основні сучасні способи поширення таких шкідливих програм (так звані вектори зараження) - спам-розсилки та заражені веб-сторінки. Ідеальним для злочинців є комп'ютер-жертва, що має вразливість. Вразливість дозволяє злочинцям встановити шкідливу програму, як тільки вона доставлена зі спам-розсилкою, або за допомогою так званих технологій drive by download при відвідуванні інфікованих інтернет-сайтів.

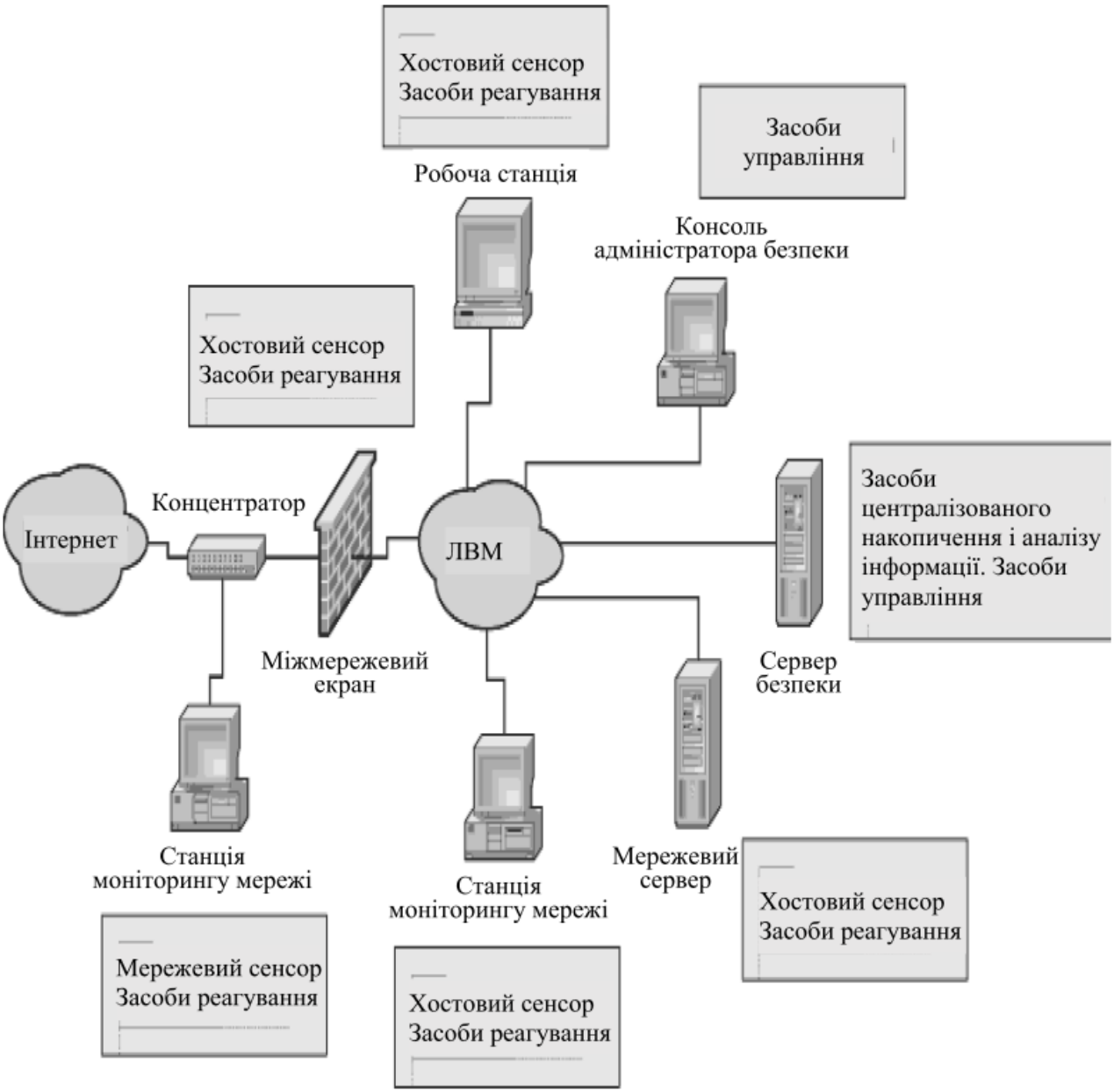

Рисунок 2.2 – Типова схема виявлення комп’ютерних атак

Наступне завдання кіберзлочинців після доставки шкідливої програми – якнайдовше зберегти її невиявленою. Вірусописувачі використовують кілька технологій для того, щоб збільшити термін служби кожної частини шкідливої програми.

Першорядне стратегічне завдання, яке стоїть перед будь-яким вірусописачем, – зробити свою шкідливу програму невидимою не тільки для того, щоб успішно її доставити, а й для того, щоб вона «вижила». Чим менша програма для систем антивірусних радарів раннього оповіщення, тим довше її можна буде використовувати для отримання доступу до заражених комп'ютерів

і збору інформації. Стандартні технології приховування програми на комп'ютері включають застосування руткітів, блокування системи сповіщень про помилки та вікон попереджень, що видаються антивірусом, приховування збільшення розмірів файлів, використання безлічі різноманітних пакувальників.

Щоб уникнути виявлення шкідливих програм, вірусописувачі широко використовують технологію умисного заплутування. Поліморфізм – одна з таких технологій, він був популярним у 90-х роках, але потім фактично зник. Сьогодні вірусописачі повернулися до поліморфізму, але вони рідко роблять спроби змінювати код на комп'ютерах жертв. Натомість застосовується так званий "серверний поліморфізм" - зміна коду на веб-серверах з включенням до нього "порожніх" інструкцій, що змінюються з часом, що суттєво ускладнює виявлення нових шкідливих програм, розміщених на веб-сервері.

2.2 Способи підготовки та скоєння кіберзлочинів

Усі методи підготовки, скоєння та приховування комп'ютерних злочинів володіють своїми індивідуальними, властиві лише їм ознаки, по яких можна їх розпізнати та класифікувати на загальні окремі групи. Тоді як основна класифікуюча ознака виступає метод, при допомозі якого здійснюється злочинцем цілеспрямований вплив на засоби обчислювальної техніки і комп'ютерну інформацію. Вирізняють загальні такі групи:

1) вилучення засобів обчислювальної техніки (ЗОТ);

2) перехоплення інформації;

3) несанкціонований доступ до ЗОТ і комп'ютерної інформації;

4) маніпуляція даними і керуючими командами;

5) різні комплексні способи.

До першої групи відносять традиційні способи скоєння злочинів, де дії злочинця напрямлені на вилучення чужого майна. В даному випадку чужим майном є будь-які ЗОТ. З кримінальної та правової точки зору такі злочинні діяння кваліфікуватимуться за сукупністю відповідними статтями Кримінального кодексу.

До другої групи способів при скоєнні комп'ютерних злочинів належать такі, які грунтуються на отриманні комп'ютерної інформації злочинцем за допомогою використання методів електромагнітного та аудіовізуального перехоплення, які широко практикуються у оперативно-розшуковій роботі. Зокрема, до них, належать:

1) пасивне (безконтактне) перехоплення, що здійснюється шляхом дистанційного перехоплення певних електромагнітних випромінювань, які виділяються при роботі ЗОТ:

- перехоплення відповідних оптичних сигналів (зокрема, зображень) в видимому, інфрачервоному (ІЧ) та ультрафіолетовому (УФ) діапазонах хвиль (це здійснюється злочинцем за допомогою оптикоелектронних, оптичних, лазерних, телевізійних, тепловізійних, фото- чи якихось інших візуальних засобів для знімання інформації);

- перехоплення акустичних сигналів, якіо поширюються у повітряному, водному та твердому середовищах (це здійснюється із використанням гідроакустичних, акустичних, віброакустичних, лазерних і сейсмічних засобів);

- перехоплення електромагнітних сигналів, які поширюються по різних технічних каналах основних та допоміжних засобів і систем в вигляді фізичних паразитних інформативних полів: наприклад, побічних електромагнітних випромінювань та наведень, при паразитних модуляціях ВЧ сигналів, певних паразитних інформативних струмів та напруг в мережах електрозв'язку чи електрофікації, електрогодинфікації, пожежно-охоронної сигналізації, в мережах ЗОТ, у блоках ЗОТ тощо.

2) активне (контактне) перехоплення, що здійснюється шляхом безпосереднього підключення до ЗОТ чи до системи при передачі даних за допомогою штатних різних оперативно-технічних та спеціально розроблених, виготовлених, пристосованих та запрограмованих засобів для негласного отримання інформації, інколи із використанням прихованих (зашифрованих чи замаскованих,) каналів. У такому разі злочинець цілеспрямовано може впливати

на ЗОТ загалом чи на його складові, а також на канали передачі, систему для санкціонування доступу та комп'ютерну інформацію.

До третьої групи відносять способи для скоєння комп'ютерного злочину, які спрямовуються на отримання несанкціонованого доступу до ЗОТ злочинцем, зокрема, з використанням методу для легендування, або шляхом несанкціонованого підключення в систему передачі комп'ютерної інформації із метою для перехоплення управління викликом "на себе" абонента мережі тощо.

Четвертою групою є дії злочинця, що пов'язані із використанням методів маніпуляції із вхідними чи вихідними даними чи керуючими командами у засобах обчислювальної техніки. Дуже часто они використовуються і є досить добре відомі співробітникам у підрозділах боротьби із економічними злочинами, зокрема, здійснення заміни вхідних та вихідних даних у бухгалтерському обліку у процесі автоматизованої обробки певних документів чи внесення умисної зміни до існуючої програми, що свідомо призводить до несанкціонованого блокування, знищення, модифікації чи копіювання інформації, а також порушення роботи ЗОТ, систем ЗОТ або його мережі. Як наочні приклади такі можна навести способи, як «троянська матрьошка», «троянський кінь», «салямі», «повітряний змій», «люк», «тимчасова» або «логічна бомба», «комп'ютерний вірус» тощо.

До п'ятої групи злочинів відносяться вже комплексні способи для скоєння комп'ютерного злочину, які засновані на застосуванні злочинцем двох чи більше способів з різних груп. При цьому один із них використовується завжди як основний, тоді як інші допоміжні функції виконують, зокрема, приховування слідів злочину.

Для слідотворчого впливу характерні такі види слідів:

- програми та текстові файли та (або) їх частини, що не входять до стандартного складу системи, що функціонує в даному пристрої раніше, до скоєння злочину;

- набори команд, окремих знаків, символів і т.д., що містяться в програмах системи, текстових та інших документах, які були навмисно внесені злочинцем до системи для змін її властивостей, можливостей, змісту тощо;

- записи в облікових файлах системи, так звані log-файли, в яких міститься інформація про користувачів (не тільки про злочинців), які коли-небудь використовували цей пристрій і які реєструють особливості роботи користувача в системі, час його роботи і т.д., причому кількість реєстрованих службових параметрів залежить як від системи, що функціонує в даному пристрої, так і від політики безпеки, що проводиться на ньому.

Дані сліди не є традиційними і не можуть бути віднесені до жодної групи слідів, що існують в криміналістиці.

2.3 Класифікація джерел загроз у кіберзлочинності

При поділі джерел за класами можна виходити з його належності певним категоріям осіб, мотивів дій і цілей, характеру методів досягнення поставлених цілей, кваліфікації, технічної оснащеності і знань про інформаційну систему, що атакується.

Типовим комп'ютерним злочинцем може бути як немолодий хакер, що використовує телефон і домашній комп'ютер для отримання доступу до великих комп'ютерів, так і службовець, якому дозволено доступ до системи.

Кіберзлочинці класифікуються на зовнішніх та внутрішніх. Потенційно до внутрішніх належить персонал (інсайдери). Інсайдер - особа, яка має в силу свого службового чи сімейного стану доступ до конфіденційної інформації про справи компанії. До цієї групи включаються особи, які добувають конфіденційну інформацію про діяльність корпорації та використовують її з метою особистого збагачення. Внутрішніх кіберзлочинців можна класифікувати на три основних типи:

- зловмисник (хакер, крекер, фрікер);
- об'єднання хакерів;
- розвідка (конкурентна розвідка, розвідка державна).

Розглянемо докладніше можливі схеми дій зовнішніх зловмисників, які використовують віддалене проникнення в інформаційну систему об'єкта атаки.

Хакер – людина, яка повністю поглинена програмуванням та комп'ютерною технологією, яка любить вивчати коди оперативних систем та інших програм, щоб подивитися, як вони працюють. Потім він використовує свою комп'ютерну ерудицію в незаконних цілях, таких як отримання доступу до комп'ютерних систем без дозволу та псування програм та даних у цих системах. Будучи хакером, людина здатна красти інформацію, займатися промисловим шпигунством і запускати приховані програми, віруси та троянських коней.

Крекер – це людина, яка обходить або руйнує засоби безпеки мережі або окремої комп'ютерної системи, щоб отримати несанкціонований доступ. Класична мета крекера – нелегально отримати інформацію від комп'ютерної системи, щоб потім нелегально використати комп'ютерні ресурси. Як би там не було, головною метою більшості крекерів є руйнування системи.

Фрікер – це людина, яка проникає у телефонні мережі чи інші захищені телекомунікаційні системи.

Даний тип кібезлочинців дуже обмежений в фінансовому плані. Необов'язково він має глибокі знання у галузі комп'ютерних технологій, а використовує найчастіше готові комп'ютерні програми, які доступні із Інтернету, для реалізації загроз через давно відомі вразливості. Малоймовірно, що такий порушник володіє достатніми знаннями щодо побудови інформаційної системи об'єкта атаки. Його дії є експериментальними, і йому не потрібен доступ до конкретної інформації або її модифікація для особистої користі. Його цікавить лише проведення деяких дій з інформаційною системою об'єкта атаки, недоступними для звичайних користувачів Інтернету. Його дії характеризуються як приховані та відповідні його вмінням. Зазвичай вони припиняються після першого успішного втручання.

Наступний рівень загрози представлений об'єднаною групою хакерів. Цей тип зловмисників обмежений фінансово і поки що не має обчислювальної потужності на рівні великого підприємства чи схожого пропускного каналу в Інтернеті. Однак їх знання в галузі комп'ютерних технологій становлять серйозну загрозу. Ці зловмисники використовують різні методи для сканування інформаційних систем з метою виявлення нових вразливостей та

використовують відомі вразливості для реалізації загроз. Вони можуть розробляти програми, які використовують ці вразливості, такі як мережеві черв'яки, віруси, троянські програми та інші шкідливі програми. Для виконання своїх планів вони можуть вбудовувати шкідливі програми в обчислювальні системи своїх жертв. Використовуючи такі програми, вони можуть отримати доступ до великих обчислювальних потужностей мереж великих наукових або військових установ, а також до каналу з високою пропускною здатністю, що з'єднує уражену мережу з Інтернетом.

Описані дії дозволяють виробляти потужні атаки на інформаційні системи в Інтернеті. Зазвичай ці дії є цілеспрямованими, і група робить певні зусилля, щоб зрозуміти принципи функціонування системи захисту банку. Плануючи свої дії, група вживає всіх можливих заходів для приховування факту несанкціонованого доступу. Хакерська група не припиняє діяти, доки не досягне своєї мети або не зіткнеться з непереборними перешкодами щодо подальшого вторгнення.

Наступний тип - розвідка, заснована на конкуренції. Конкурентна розвідка - збір та обробка даних із різних джерел для вироблення управлінських рішень з метою підвищення конкурентоспроможності комерційної організації, що проводяться в рамках закону та з дотриманням етичних норм (на відміну від промислового шпигунства); а також структурний підрозділ підприємства, який виконує ці функції. Конкурентна розвідка - це є постійна, циклічна послідовність деяких дій, результатом якої є інформація для вироблення управлінських рішень [10].

Промислове шпигунство — одна з форм недобросовісної конкуренції, яка застосовується на всіх рівнях економіки, починаючи з невеликих підприємств і до держав. Основне призначення промислового шпигунства - економія коштів і часу, які потрібно витратити, щоб наздогнати конкурента, що займає лідируючу позицію, або не допустити в майбутньому відставання від конкурента, якщо той розробив або розробляє нову перспективну технологію, а також вийти на нові для підприємства ринки. Це справедливо і щодо міждержавної конкуренції, де до питань економічної конкурентної спроможності додаються й питання

національної безпеки. Основна відмінність промислового шпигунства від конкурентної розвідки в тому, що промислове шпигунство порушує норми законодавства, насамперед, кримінального, тоді як конкурентна розвідка цього робити не може.

Ця модель включає: потужні власні обчислювальні мережі та канали для передачі даних із високою пропускною здатністю при виході у Інтернет; значні фінансові можливості; високі знання у комп'ютерних фахівців і самої компанії, і найманих фахівців під замовлення. Можливі також спроби підкупу співробітників у службі безпеки або інші дії в галузі соціальної інженерії. Конкуренти можуть зробити серйозні зусилля для отримання інформації про функціонування системи інформаційного захисту, у тому числі впровадити свого представника в службу безпеки. Серед цілей можуть бути: блокування функціонування інформаційної системи конкурента, завдання підриву в іміджі, деструктивні дії, спрямовані на заподіяння непоправної шкоди конкуренту, аж до його руйнування та банкрутства.

Для досягнення цілей використовуються високо вдосконалені методи проникнення в інформаційні системи та впливу на потоки даних у них. Дії конкурентів можуть приймати форму як прихованого, так і відкритого, демонстративного характеру. У реалізації своїх намірів конкуруюча сторона витримує конфлікт до остаточного успіху.

Найсерйознішими кіберзлочинцями є державні розвідки відомчого рівня та спецслужби різних держав. Вони мають фактично необмежені обчислювальні та фінансові ресурси, самостійно регулюють і контролюють трафік в мережі Інтернет. В їхньому розпорядженні перебувають висококваліфіковані комп'ютерні фахівці. У деяких країнах відомі випадки, коли найманих хакерів замість тюремного ув'язнення або після нього залучають до роботи національних служб безпеки. Ці експерти беруть участь у розробці стандартів безпеки інформації, мережевих протоколів і добре орієнтовані в можливостях та недоліках всіх комп'ютерних технологій. Під час сертифікації обчислювальних систем представники відомчих органів можуть мати вичерпну інформацію про їхню структуру. Цілі, досягнуті такою групою, дуже різноманітні і

непередбачувані. Подібні злочинці можуть не приховувати свої дії, і, як вже було сказано, майже ніщо не здатне їх зупинити. Вони можуть користуватися підтримкою як законодавчих, так і інших правових актів, а також підтримкою владних і судових органів.

У таблиці 2.1 згруповано порівняльну характеристику розглянутих моделей типового кіберзлочинця.

Таблиця 2.1 - Порівняльна характеристика моделей типового кіберзлочинця

Характеристика	Зловмисник	Група зловмисників	Конкурентна розвідка	Державна розвідка
1	2	3	4	5
Обчислювальна потужність	Персональний комп'ютер	ЛОМ, використання чужих обчислювальних мереж	Потужні обчислювальні мережі	Необмежені обчислювальні потужності
Вихід в Інтернет	Модем або виділена лінія	Використання чужих каналів з високою пропускною здатністю	Власні канали з високою пропускною здатністю	Самостійний контроль над маршрутизацією трафіка в Інтернеті
Фінансові можливості	Сильно обмежені	Обмежені	Великі можливості	Практично необмежені
Комп'ютерні знання	Невисокі	Високі	Високі	Високі, розробники стандартів
Використані технології	Готові програми, відомі вразливості	Пошук нових вразливостей, виготовлення шкідливих програм	Сучасні методи проникнення в інформаційні системи і впливи на потоки даних в них	Досконалі знання комп'ютерних технологій, можливих вразливостей і недоліків

Продовження таблиці 2.1

1	2	3	4	5
Цілі, що переслідуються	Експеримент, допитливість	Підробка рахунків, внесення спотворень в роботу системи	Блокування функціонування системи, підрив іміджу, розорення	Непередбачуваний різноманітний характер
Знання про побудову системи безпеки об’єкта	Навряд, чи володіє достатніми знаннями про побудову інформаційної системи	Можуть докладати визначених зусиль для отримання уявлень про принципи функціонування системи захисту.	Можуть докладати серйозні зусилля для отримання відомостей про функціонування системи інформаційного захисту, в тому числі впровадити свого представника в службу безпеки	В процесі сертифікації обчислювальної системи представники відомчих органів можуть отримати достатньо повну інформацію про її побудову
Характер дій	Характер дії – прихований в міру своїх здібностей	Прикладає всі можливі зусилля для приховування факту НСД	Можуть носити як прихований, так і відкритий, демонстративний характер	Можут не затрудняти себе приховуванням своїх дій
Глибина проникнення	Найчастіше зупиняється після проведення першого успішного впливу	До моменту досягнення поставленої мети або настання непереборних перешкод для проведення подальшого вторгнення	При здійсненні своїх намірів конкуруюча сторона буде йти до переможного кінця	Практично ніщо не здатне їх зупинити

2.4 Моделі кіберзлочинності

Для прикладу, на рисунку 2.3 представлена модель реалізації державної інформаційної політики України.

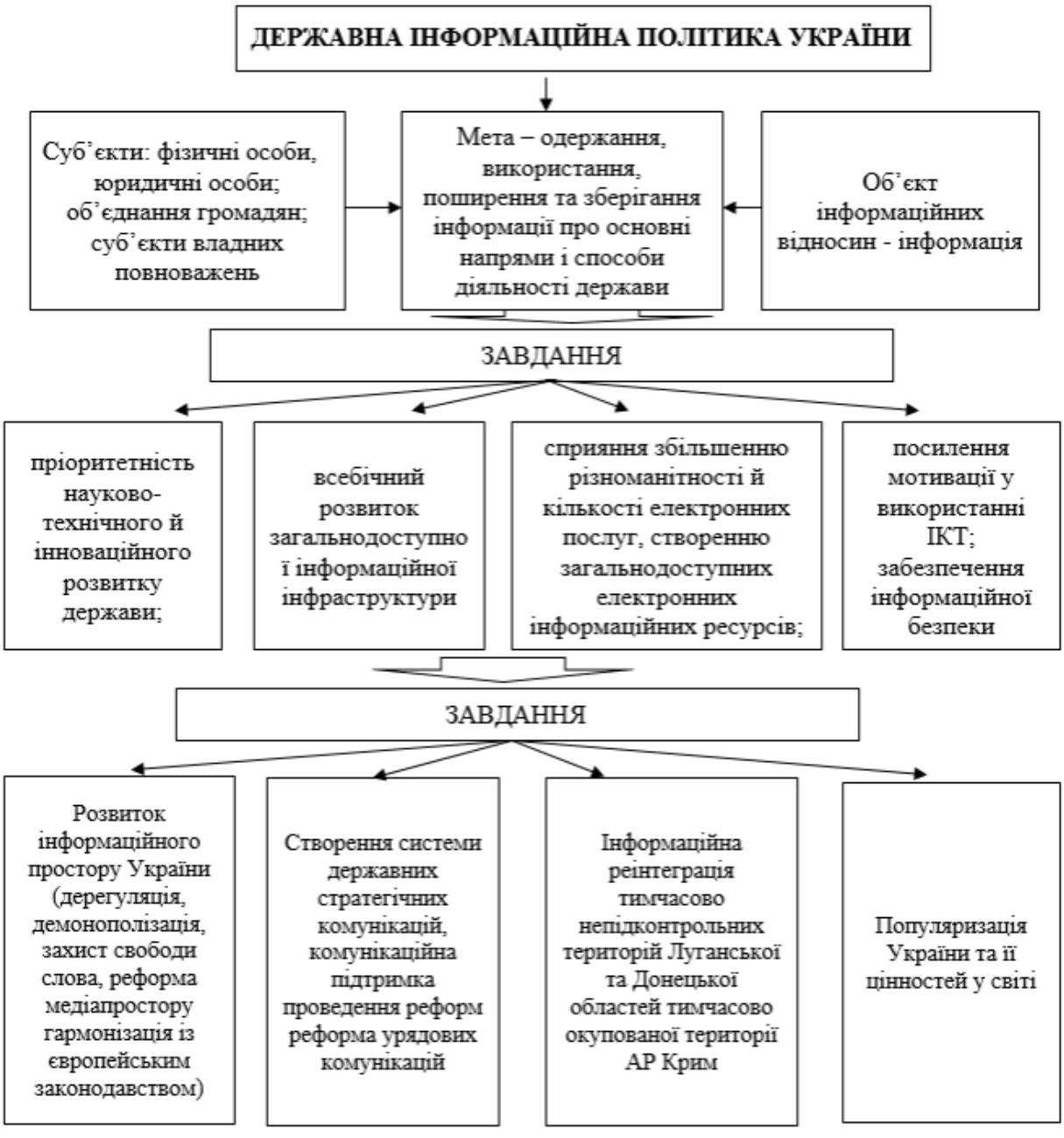

Рисунок 2.3 - Модель реалізації державної інформаційної політики України

Статичні моделі кіберзлочинності включають опис виявлених загроз безпеці інформації, аналіз вихідної захищеності, опис моделей можливих порушників, оцінку реалізованості та небезпеки загроз, перелік актуальних

загроз безпеці інформації. Розробляються експертами власників інформаційних систем з урахуванням призначення, умов та особливостей функціонування.

Статичні моделі загроз безпеці інформації мають такі недоліки:

− недоліки експертних методів (експертних оцінок);

− розробляються на поточний стан системи, у зв'язку з цим виникають складності у постійній актуалізації таких моделей в конкретно визначений момент часу – проблема підтримки моделі в актуальному стані;

− не враховують усі необхідні показники при визначенні переліку актуальних загроз, а саме: зміни в моделі ризиків (негативних наслідків від реалізації загроз); зміна умов експлуатації об'єктів впливу (елементи архітектури, що обробляють інформацію, яка захищається); версійність СПЗ, ППЗ; способи реалізації, тактики і техніки атак, що динамічно розвиваються;

− нераціональне використання багатьох відомих баз даних, уразливостей, тактик та технік атак (MITRE ATT&CK, CVE, CWE, OSVDB, NVD, Secunia і т.д.);

− як наслідок, неякісна оцінка ефективності СЗІ (рівня захищеності).

В даний час існує безліч моделей атак, методів та засобів моделювання атак. Порушник – «будь-яка особа, яка навмисно використовує вразливості технічних і нетехнічних заходів та засобів контролю та управління безпекою з метою захоплення або компрометації інформаційних систем та мереж, або зниження доступності ресурсів інформаційної системи та мережевих ресурсів для законних користувачів».

Основні моделі атак на інформаційні системи представлені на рисунку 2.4.

Переваги та недоліки основних моделей атак представлені в таблиці 2.2. Моделі атак мають ряд спільних недоліків, а саме:

− складність моделювання;

− вимагають обчислювальних ресурсів;

− вимагають залучення висококваліфікованих фахівців в області інформаційної безпеки;

− помилки експертних методів (експертних оцінок).

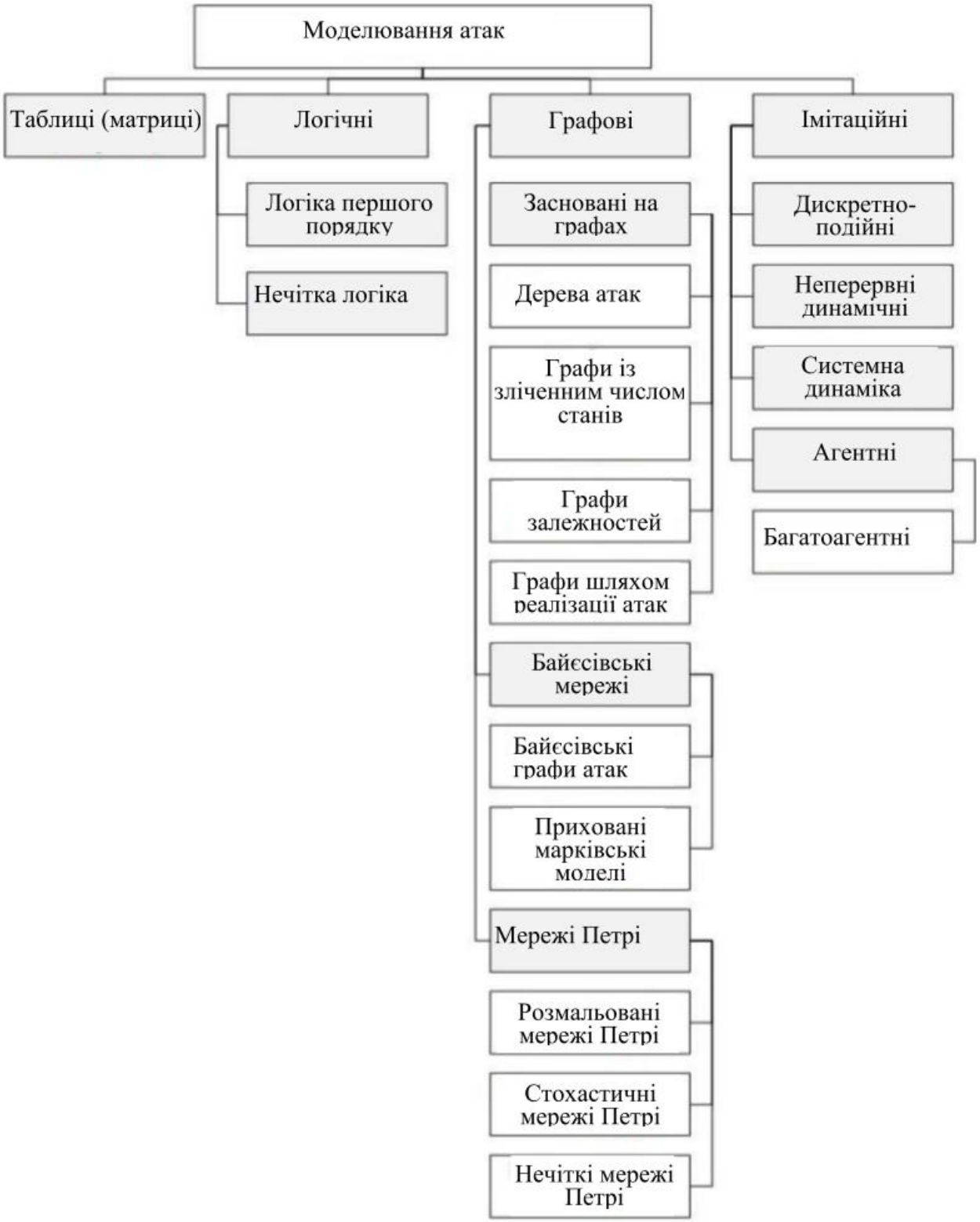

Рисунок 2.4 – Моделі атак на інформаційні системи

Разом з тим, їм властиві і спільні переваги, зокрема, наочність, масштабованість, зручність у використанні, адаптованість до різних конкретних випадків.

Таблиця 2.2 – Переваги і недоліки моделей атак

№	Модель	Переваги	Недоліки
1	2	3	4
1	Табличні (матричні)	Найбільш прості	Складна при моделюванні циклічних атак, великої кількості зв’язків між інцидентами або діями зловмисника.
2	Логічні	Обробка інцидентів і використання мов представлення знань. Враховує випадки невизначеності вхідних даних про модельовані атаки	Використовує професійне ПЗ. Вимагає значних обчислювальних ресурсів.
3	Графові	Призначені для вирішення великого числа задач: аналіз інцидентів, виявлення атак, оцінка ефективності СЗІ тощо.	Масштабованість, пов’язана з формуванням графа з великою кількістю елементів
4	Графові на деревах атак	Наочність, масштабованість, адаптованість, універсальніть.	Складні при моделюванні циклічних атак. Відсутність динамічного моделювання.
5	Байєсівські графи	Наочність, масштабованість, адаптованість, універсальніть, враховує випадки невизначеності вхідних даних про атаки.	Складні при моделюванні циклічних атак. Відсутність динамічного моделювання.

Продовження таблиці 2.2

1	2	3	4
6	Мережі Петрі	Зручність моделювання динамічних і паралельних процесів, здатних відображати ймовірнісні процеси, використання часових параметрів, простота вивчення.	Нездатність описувати поведінку порушника і цілі атаки.
7	Імітаційні	Дозволяє моделювати поведінкові характеристики порушника і цілі атаки. Зручні для моделювання розподілених атак.	Вимагають великих обчислювальних ресурсів.

2.5 Еволюція кіберзлочинності

Порівняно недавно головним результатом кіберзлочинів була слава про зловмисників, а крадіжка інформації і шпіонаж відсувалися на другий план (рисунок 2.5).

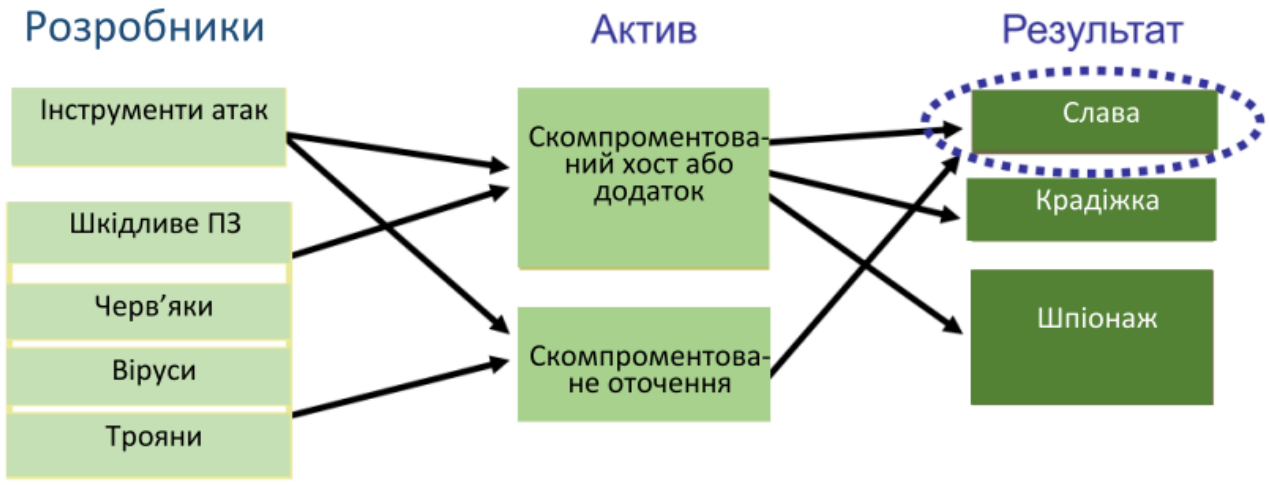

Рисунок 2.5 – Схема роботи кіберзлочинців

Відповідно до цього обираються інструменти атак (наприклад, шкідливе ПЗ, черв'яки, віруси, трояни тощо) та об'єкти атаки (скомпроментований хост або додаток, скомпроментоване зовнішнє оточення). Одночасно з розвитком інструментів зловмисника також відбувалась і еволюція загроз і вразливостей (рисунок 2.6).

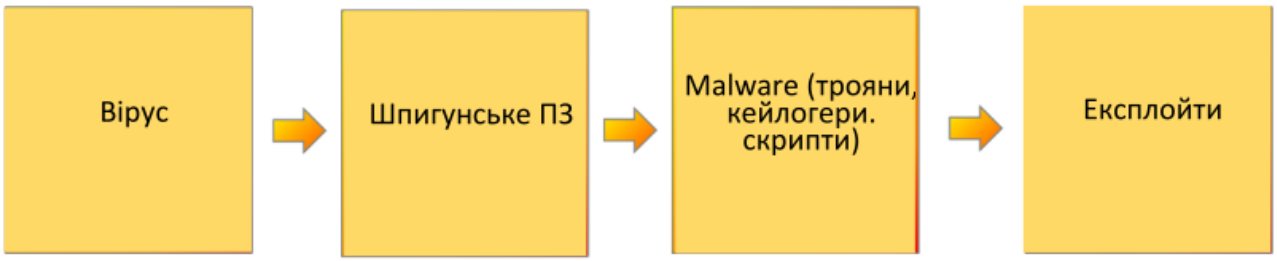

Рисунок 2.6 – Еволюція загроз

Дослідження показують, що навіть найкращі антивіруси і Web-шлюзи не ефективні проти сучасних загроз. Шкідливі програми крадуть уже не посилання на відвідувані вами сайти, а реквізити доступу до них. Web і соціальні мережі все частіше стають розсадником шкідливих програм, а також інструментом розвідки зловмисників. Шкідливі програми використовують для своїх дій невідомі вразливості (0-Day 0-Hour).

Подібним чином відбувалась також і еволюція тактики реалізації загроз (рисунок 2.7).

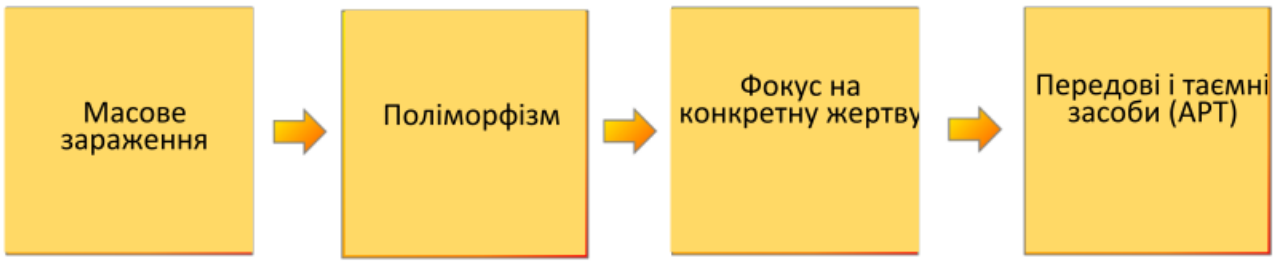

Рисунок 2.7 – Еволюція тактики реалізації загроз

Зловмисників на даний час зовсім не цікавить їх впізнаваність і слава. Їм важливішою є фінансова вигода від реалізації загрози. Сучасні загрози постійно змінюються, щоб засоби захисту їх не змогли відслідкувати – зміна поведінки,

адресів серверів управління тощо. Загрози можуть бути розроблені спеціально під конкретний випадок – враховують інфраструктуру і вбудовуються в неї, що робить неможливим використання стандартних методів аналізу. Загрози стають модульними, вони самовідновлюються і стають стійкими до відмов та виявлення.

3 ФУНКЦІОНАЛЬНА МОДЕЛЬ КІБЕРЗЛОЧИНІВ

3.1 Функціональна модель кіберзлочинів

Цілком очевидно, що всі кіберзлочини відбуваються за якоюсь певною моделлю, що існують певні етапи, через які обов'язково необхідно пройти зловмиснику при скоєнні протиправних дій (наприклад, вивчення об'єкта атаки, отримання доступу до об'єкта, крадіжка інформації та приховування слідів).

Всі моделі скоєння кіберзлочинів у загальній частині містять три етапи: вивчення жертви, атака на жертву та приховування слідів кіберзлочину. Кожен із етапів містить три стадії: рекогносцировка, сканування, складання карти, отримання доступу до системи, розширення повноважень, крадіжка інформації, знищення слідів, створення «чорних ходів» і відмова у обслуговуванні. Однак у всіх наявних моделей кіберзлочинів є безліч недоліків щодо відображення процесів формування зв'язків, управлінь і механізмів, а також середовища їх виникнення.

Оскільки після кожного кроку зловмисника народжуються нові сліди, збитки відповідно стають специфічними. Ретельно досліджуючи збитки та проводячи зворотні дії з об'єктом атаки, можна реконструювати сам кіберзлочин буквально по кроках.

Так, наприклад, якщо в ході аналізу випливає, що зловмисник періодично викрадав конфіденційну інформацію із закритого джерела в мережі, то стає очевидним, що він не міг провернути цього без початкового отримання доступу до мережі об'єкта, без збільшення повноважень у цій мережі, без сканування інформаційних ресурсів і без зомбування об'єкта (виключення становлять інсайдери). Інформація про це неодмінно повинна залишитися у файлових журналах серверів, ретельне вивчення яких цілком може вказати безпосередньо на зловмисника.

Якщо в ході вивчення фактів виявляється, що особливо цінна інформація знищена загальновідомими шкідливими програмами, які не могли проникнути на об'єкт внаслідок наявності на останньому міжмережевого екрану, необхідно приділити особливу увагу відкритим каналам передачі даних (флеш-

накопичувачі, компакт-диски тощо), а також здійснити пошук приватних кодів. Підозри можуть у цьому випадку впасти на упаковані файли, що виконуються в системних папках операційної системи, яких просто там бути не повинно.

Або, наприклад, якщо стає відомим, що зловмисник модифікував дані в певній базі даних, варто приділити увагу модифікованим в цей період записам, в результаті чого можна визначити коло облікових записів, під якими був отриманий несанкціонований доступ. Також варто приділити увагу системним журналам бази даних, у яких може залишитись інформація про те. під яким обліковим записом намагався отримати доступ зловмисник і був пароль зламаний грубим перебором чи вже заздалегідь відомий. З аналізу проведених зловмисником змін можна визначити рівень його знань у галузі цієї бази даних і звузити крутий підозрюваних осіб.

Тільки чітке уявлення проводящего аналіз спеціаліста у тому, що це кибезлочини відбуваються у певній послідовності, і навіть про те, які сліди народжуються у процесі інформаційного взаємодії різних стадіях, дозволять йому поглянути наявні факти отримання несанкціонованого доступу до інформації комплексно і адекватно. Схематично процес моделювання кіберзлочинів наведено на рисунку 3.1.

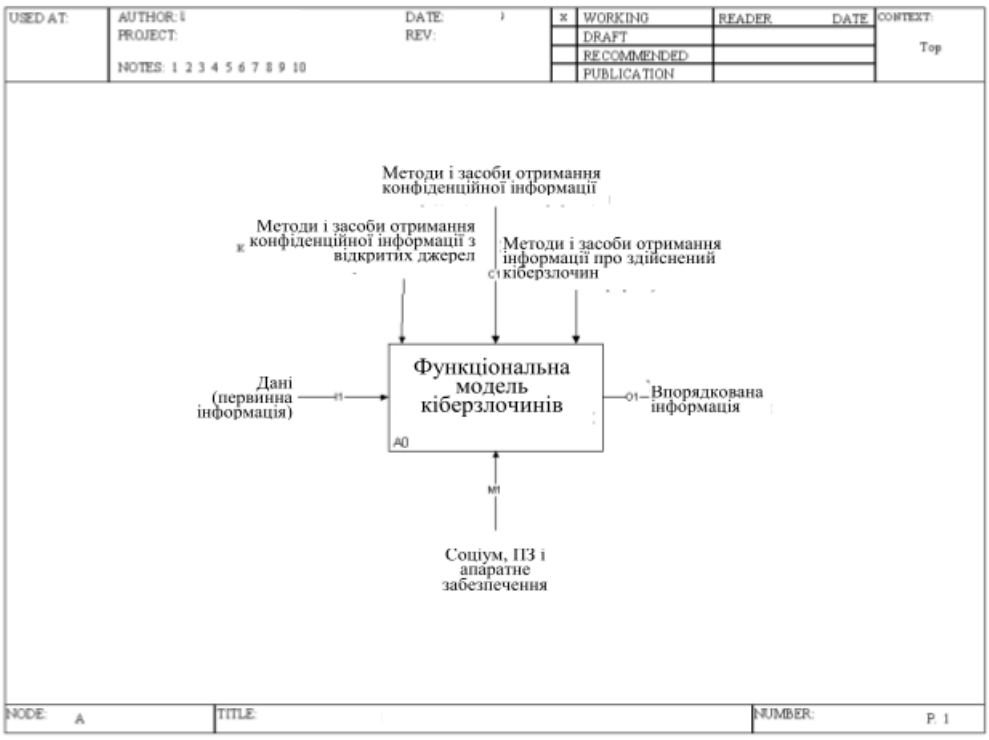

Рисунок 3.1 – Схема процесу моделювання кіберзлочинів

В якості «нульового» наближення (прототипу) для моделювання вибрана схема дії для здійснення кіберзлочинів, запропонована зарубіжними дослідниками Макклуре С., Скембрей Дж., Курті Дж. Поетапно описано функціонування схеми, також розглянуті методи проходження різноманітних стадій.

На рисунку 3.2 представлена функціональна модель кіберзлочинів.

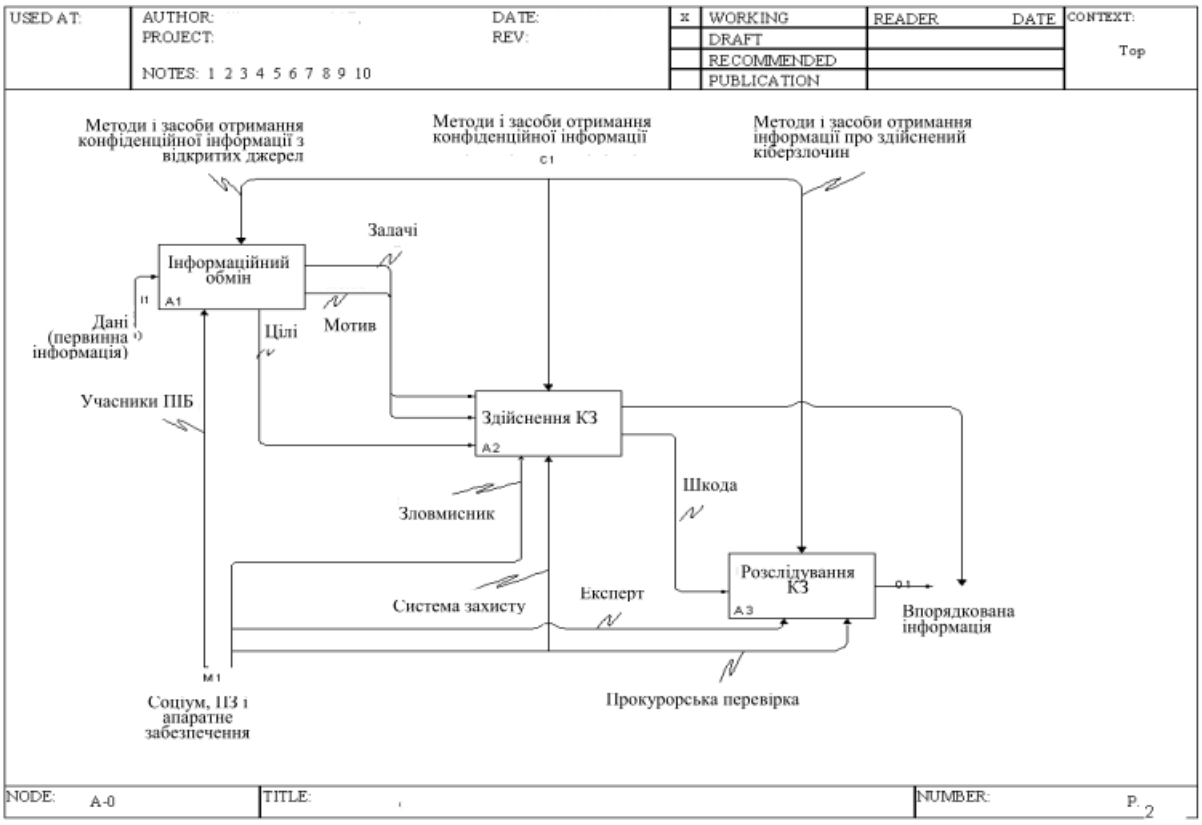

Рисунок 3.2 – Функціональна модель кіберзлочинів

3.2 Інформаційний обмін

Інформаційний обмін є необхідним динамічним компонентом інформаційної системи. Інформаційний обмін складається з декількох стадій: обмін даними, розвідка, сканування, складання карти.

На стадії обміну даними зловмисник дізнається про існування об'єкта атаки, у нього з'являється мотив для скоєння злочину, а також формуються цілі та перелік завдань. Математична залежність інформаційного обміну може бути представлена так:

$$A1=<I1, C1, M1, O1, O2, O3>, \quad (3.1)$$

де A1 - результат інформаційного обміну;

I1 - первинні дані;

C1 - методи та засоби отримання конфіденційної інформації;

M1- соціум, програмне та апаратне забезпечення;

O1 – підсумкова мотивація;

O2 – сформовані завдання;

O3 – кінцеві цілі.

Далі він на стадії рекогносцирування проводить дослідження об'єкта, де з'ясовує, які уразливості існують у системі захисту об'єкта. Потім на стадії сканування він перевіряє, які можливі вразливості у системі захисту доступні. Після цього він переходить на стадію складання карти та проводить графічне чи принципове моделювання об'єкта з метою визначення наступних заходів та відпрацювання ефективної схеми нападу. До цього моменту всі дії зловмисника не порушують законодавство, тому дана частина моделі зустрічається в багатьох видах комп'ютерних злочинів. На рисунку 3.3 докладно описано етап інформаційного обміну.

Перш ніж зловмисник досягне успіху, він повинен пройти всі ці етапи. Розглянемо докладно кожен з них.

Рекогносцирування означає мистецтво збирання інформації про мету. Злочинці не почнуть грабувати банк із того, що просто зайдуть і вимагатимуть гроші. Попередньо злочинці зберуть інформацію про банк: маршрути броньованих інкасаторських машин, час перевезення грошей, розміщення відеокамер, кількість касирів, запасні виходи та інше, що необхідно знати для успішного здійснення злочинної авантюри.

Те саме справедливо для нападників на комп'ютерні системи. Зловмисникам потрібно зібрати безліч інформації, щоб зробити хірургічно точну атаку (ту, яку миттєво не перехоплять). Внаслідок цього атакуючі повинні зібрати максимально можливу кількість інформації про всі аспекти

комп'ютерного захисту організації. Збір відомостей завершується упорядкуванням карти потенційних зон ураження, тобто профілю наявних підсистем Інтернету, віддаленого доступу, інтрамережі та екстрамережі. Дотримуючись структурованої методології, атакуючі можуть систематично отримувати інформацію з багатьох джерел для складання точної карти зон ураження будь-якої організації.

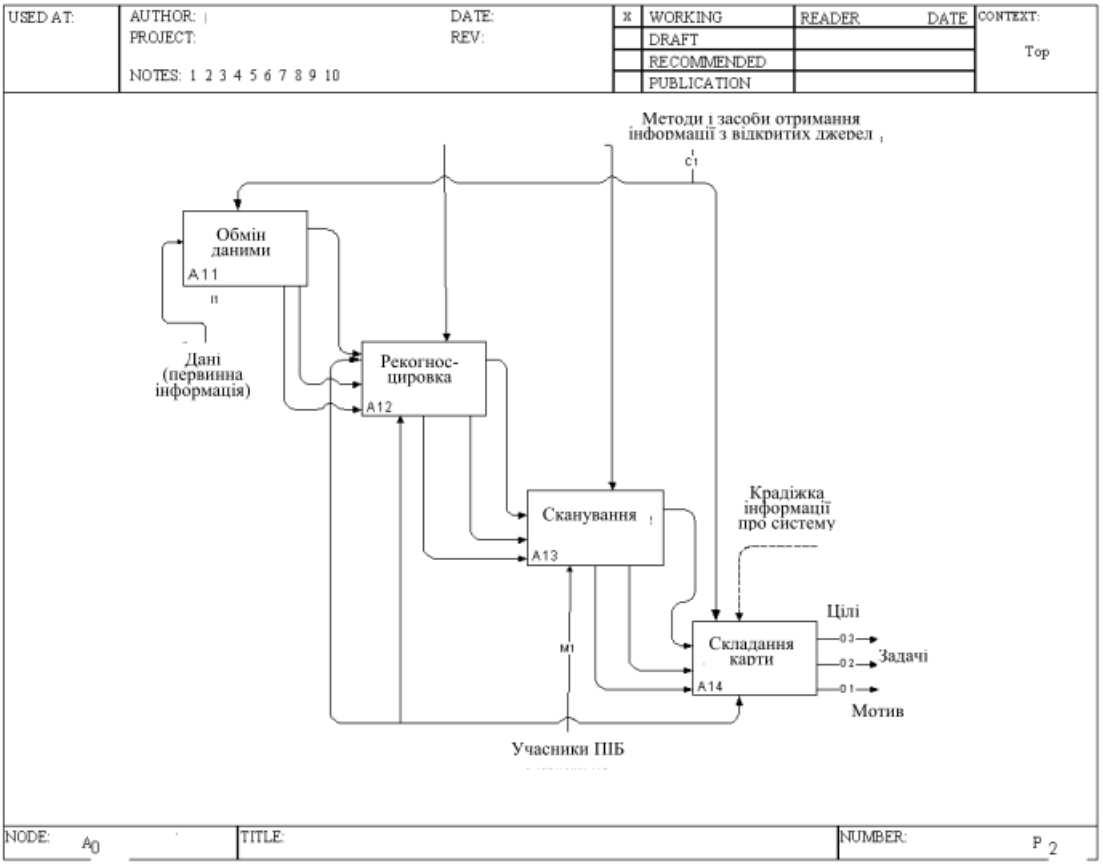

Рисунок 3.3 – Етап інформаційного обміну

Систематичне рекогносцирування організації дозволяє атакуючим створити докладний профіль стану її комп'ютерного захисту. Комбінуючи різні засоби та технології, зловмисники можуть з'ясувати для невідомого об'єкта набір доменних імен, мережевих блоків та індивідуальних IP-адрес систем, безпосередньо підключених до Інтернету. Існує безліч методів розвідки, але всі вони спрямовані переважно на пошук інформації, пов'язаної з такими технологіями: Інтернет, інтрамережа, віддалений доступ та екстрамережа. У

таблиці 3.1 показані технології та інформація, яку намагається знайти будь-який атакуючий.

Таблиця 3.1 - Технології та основні відомості, що виявляються атакуючими

Технологія	Ідентифікуються
Інтернет	Доменні імена Блоки мережевих адрес Конкретні IP адреси систем, доступних з Інтернету Служби TCP та UDP, які працюють на кожній ідентифікованій системі Системна архітектура (наприклад, SPARC або X86) Механізми управління доступом та відповідні списки управління доступом (ACL) Системи виявлення вторгнень (IDS) Перелік характеристик системи (імена користувачів та груп, системні заголовки, таблиці маршрутизації, інформація SNMP)
Інтрамережа	Використані мережеві протоколи (наприклад, IP, IPX, DecNET тощо) Імена внутрішніх доменів Блоки мережевих адрес Конкретні IP-адреси систем, доступні через інтрамережу Служби TCP та UDP, які працюют на кожній ідентифікованій системі Системна архітектура (наприклад, SPARC або X86) Механізми управління доступом та відповідні списки управління доступом (ACL) Системи виявлення вторгнень IDS Перелік характеристик системи (імена користувачів та груп, системні заголовки, таблиці маршрутизації, інформація SNMP)
Віддалений доступ	Аналогові/цифрові телефонні номера Тип віддаленої системи Механізми аутентифікації
Екстрамережа	Джерело і точка призначення з’єднання Тип з’єднання Механізм управління доступом

Рекогносцирування необхідне для систематичного та послідовного підтвердження того, що визначена вся інформація, яка стосується згаданих вище технологій. За відсутності якісної методології такого дослідження можна пропустити ключові елементи інформації, пов'язаної з конкретною технологією чи організацією.

Багато методів розвідки різних технологій (наприклад, Інтернету та інтрамережі) збігаються. Приділимо основну увагу рекогносцируванню підключень організацій до Інтернету. Складно скласти поетапний посібник з рекогносцирування, оскільки воно може проводитися у кількох напрямах. Опишемо базові етапи, що дозволяють виконати ретельний рекогносцирувальний аналіз. Багато із запропонованих методів можуть застосовуватись і для інших технологій:

1) етап 1 - визначення сфери дій. Перший етап полягає у визначенні галузі рекогносцирувальної діяльності. Потрібно провести рекогносцирування всієї організації чи лише окремих зон (наприклад, корпорації чи дочірніх фірм). У деяких випадках непросто визначити всі об'єкти, пов'язані з обраною організацією як з ціллю. На щастя, Інтернет надає широкий набір ресурсів, що дозволяють обмежити сферу дій та з'ясувати типи та обсяги загальнодоступної інформації про організацію та її співробітників. В якості стартової точки зловмисник уважно вивчає web-сторінку організації, якщо така є. Багато web-сторінок надають достатньо інформації атакуючим. До інших цікавих відомостей відносяться:

а) місцезнаходження:

- пов'язані організації або об'єкти;
- новини про злиття або придбання;
- телефонні номери;
- контактні імена та адреси електронної пошти;
- політики розмежування доступу та захисту, що вказують на типи механізмів захисту;

б) посилання на інші web-сервери, пов'язані з цією організацією.

Також використовується перегляд коментарів у HTML-коді. Багато питань, не призначених для спільного доступу, заховані у тегах коментарів HTML.

Після вивчення веб-сторінок проводиться пошук за відкритими джерелами інформації, пов'язаними з цією організацією. Новини, заяви для преси тощо можуть містити додаткові відомості про стан організації та її комп'ютерний захист. Якщо досліджується профіль компанії, яка в основному діє в Інтернеті, то у відповідних публікаціях можна знайти відомості про численні інциденти з порушення комп'ютерного захисту. Для виконання цієї роботи досить звичної системи пошуку у Web. Однак існують і досконаліші засоби пошуку та методи введення критеріїв відбору, які можна використовувати для отримання додаткової інформації (комплект утиліт FerretPRO).

2) етап 2 - перелік мережі. Перший крок у процесі створення переліку (інвентаризації) мережі полягає в ідентифікації доменних імен та пов'язаних з ними мереж, що належать до цієї організації. Доменні імена характеризують присутність в Інтернеті та є мережевими еквівалентами назви компанії. Існує безліч баз даних, які можна опитати для отримання необхідної інформації. Різні запити надають різноманітну інформацію. Основна частина відомостей, які використовуються зловмисниками на початку атаки, змінюється запитами наступних типів:

- організаційним. Виводить всю інформацію, що стосується конкретної організації;

- доменний. Виводить всю інформацію, що стосується конкретного домену;

- мережевий. Виводить всю інформацію, що стосується конкретної мережі або однієї IP-адреси;

- контактний. Виводить всю інформацію, що відноситься до конкретної особи, зазвичай - до відповідального співробітника організації.

3) етап 3 - опитування DNS. Після визначення всіх зв'язаних доменів можна розпочати опитування DNS (Domain Name Service — служба доменних імен). DNS є розподіленою базою даних, що використовується для відображення IP-адрес на імена мережевих комп'ютерів і навпаки. Якщо DNS налаштована без

урахування вимог захисту, то важлива інформація про організацію стає доступною.

Однією з найбільш серйозних помилок конфігурації, яку може зробити системний адміністратор, є дозвіл ненадійним користувачам Інтернету виконувати пересилання зон DNS.

Пересилання файлу зони (zone transfer) дозволяє вторинному керуючому серверу оновлювати свою базу даних про зони та формувати запити до первинного керуючого сервера. Це робиться для підвищення надійності (резервування) DNS у разі відмови первинного сервера імен. Зазвичай пересилання зони DNS достатньо виконувати лише на вторинних керуючих серверах DNS. Однак багато серверів DNS налаштовані неправильно, тому видають копію зони будь-кому, хто її запросить. Це не так погано, якщо виводиться лише інформація про підключені до Інтернету системи та реальні імена мережевих комп'ютерів, хоча пошук потенційних цілей для атаки спрощується. Справжня проблема виникає тоді, коли організація не користується механізмом загальних, особистих DNS для відділення зовнішньої інформації DNS (яка є загальнодоступною) від своєї внутрішньої (особистої, приватної) інформації. У цьому випадку атакуючим розкриваються імена та IP-адреси внутрішніх мережевих комп'ютерів. Надання в Інтернеті інформації про внутрішні IP-адреси ненадійному користувачеві аналогічне наданню повної схеми або дорожньої карти внутрішньої мережі організації.

Відомості про місця обробки електронної пошти (MX, Mail Exchange) є чудовою відправною точкою для виявлення розташування брандмауера мережі досліджуваної організації. Часто в комерційних комп'ютерних середовищах пошта обробляється на тій же системі, де стоїть брандмауер, або принаймні в тій же мережі.

4) етап 4 - розвідка мережі. Після ідентифікації мереж зловмисник намагається визначити їхню топологію, а також потенційні шляхи доступу. Якщо розвідка - це пошук джерел інформації, то сканування виявляє вразливості систем. Під час розвідки атакуючий отримує імена та телефони співробітників, діапазони IP-адрес, сервери DNS та поштові сервери. Тепер він визначає, які

системи живі та досяжні з Інтернету за допомогою утиліт діапазонної перевірки з ping, сканування портів та автоматизованих засобів дослідження.

Одним із базових етапів складання схеми мережі є автоматизоване зондування програмою ping діапазону IP-адрес та блоків мережевих адрес для визначення реально функціонуючих систем. Утиліта ping традиційно застосовується для відправки адресованій системі пакетів ICMP ECHO з метою отримання пакету ICMP ECHO REPLY, що вказує на те, що адресована система дійсно працює. Утиліта ping підходить для мереж малого або середнього розміру і не є ефективною у великих мережах рівня підприємства. Повне сканування великих мереж може в цьому випадку зайняти години, якщо не дні.

Існують методи та засоби визначення функціонуючих систем, проте вони не такі точні та ефективні, як звичайне діапазонне пакетне зондування з ping.

Якщо трафік ICMP блокується, то для визначення функціонуючих мережевих комп'ютерів проводиться сканування портів. Скануючи загальні порти за кожною потенційною IP-адресою, зловмисник визначає, які мережеві комп'ютери дійсно працюють, якщо вдасться ідентифікувати відкриті або слухаючі порти хоста. Цей метод вимагає багато часу і не завжди дає добрі результати. Однією з утиліт сканування портів є nmap.

Застосувавши діапазонне зондування ICMP або TCP, зловмисник знаходить функціонуючі (живі) системи і при цьому збирає деяку корисну інформацію. Потім починає сканування портів кожної системи. Сканування портів є процесом підключення до портів TCP і UDP досліджуваної системи з метою виявлення працюючих служб або стану порту LISTENING (прослуховування).

Ідентифікація слухаючих портів важлива у визначенні типу операційної системи та використовуваних програм. Активні слухачі можуть дозволити неавторизованому користувачеві отримати доступ до систем з неправильною конфігурацією або до версій програмних продуктів з відомими слабкими місцями захисту.

Отже, існує безліч засобів та методів сканування портів. Основна мета при скануванні портів полягає у виявленні слухаючих портів TCP та UDP

досліджуваної системи. Друга мета - визначення типу сканованої операційної системи. Конкретна інформація про операційну систему використовується на етапі побудови картки слабких місць. Потрібна максимальна точність у виявленні вразливих місць досліджуваної системи чи систем. Тому потрібна певна міра впевненості у цьому, що вдасться ідентифікувати операційну систему цільового об'єкта. Застосовують методи захоплення заголовків, які отримують інформацію зі служб FTP, telnet, SMTP, HTTP, POP та ін. Це найпростіший спосіб визначення операційної системи та відповідного номера версії працюючої служби.

Далі зловмисник складає карту (план) своїх наступних дій, де визначає конкретні цілі, завдання та мотиви свого діяння. Після цього зловмисник переходить на стадію скоєння КП, де його дії порушують законодавство різних країн.

3.3 Вчинення кіберзлочину

Етап скоєння кіберзлочину містить шість стадії - отримання доступу, розширення повноважень, крадіжка інформації, зомбування, знищення слідів і відмова в обслуговуванні.

Схематично етап скоєння кіберзлочину детально подано на рисунку 3.4.

Маючи певні цілі, мотиви та завдання кіберзлочинець отримує доступ до об'єкта. На стадії отримання доступу, зловмисник вирішує проблеми обходу систем захисту об'єкта, а також отримання доступу до потрібного інформаційного ресурсу з мінімальними правами.

Отримавши доступ до об'єкта з обмеженими правами, зловмисник за допомогою спеціалізованих утиліт здійснює ескалацію своїх привілеїв, тобто розширює свої повноваження.

Щоб отримати інформацію зі зламаної машини та решти мережі, необхідно розширити привілеї до статусу потужнішого облікового запису. Цей процес називається розширенням привілеїв. Він описує процес розширення можливостей власника поточного облікового запису користувача до

можливостей більш привілейованого облікового запису, такого як обліковий запис адміністратора або запис SYSTEM. З точки зору злочинця, злом облікового запису користувача та наступна атака з розширення привілеїв може бути простішою, ніж пошук на віддаленій системі вразливого місця, яке відразу ж могло надати права рівня суперкористувача. У будь-якому випадку зловмисник, який пройшов автентифікацію, швидше за все, матиме у своєму розпорядженні більше ресурсів, ніж той, хто не пройшов автентифікацію, незалежно від рівня привілеїв.

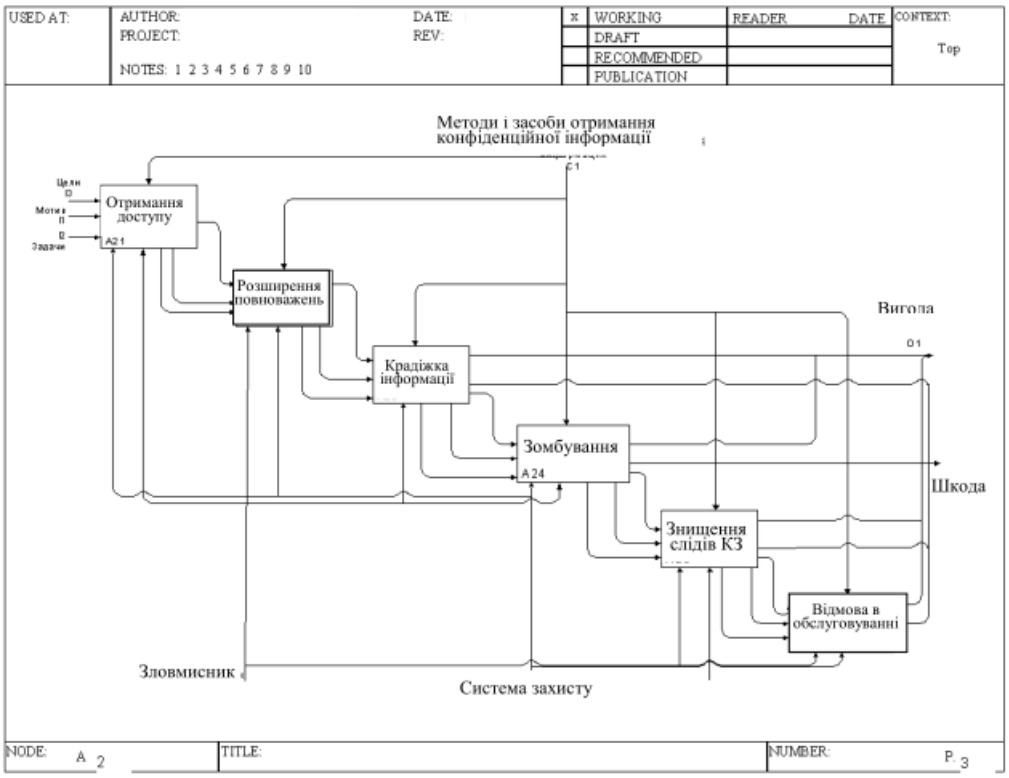

Рисунок 3.4 – Схема етапу вчинення кіберзлочину

У Windows кожен суб'єкт доступу має деякий (можливо, порожній) набор привілеїв. Привілеї є право виконання суб'єктом дій, що стосуються системи загалом, а не окремих її об'єктів.

Розширення привілеїв - це дуже потужний вид атак, які використовуються для підвищення прав облікового запису користувача до рівня адміністратора.

Після розширення повноважень до необхідного зловмиснику рівня він робить крадіжку інформації, яка можлива у двох реалізаціях:

- безпосереднє перенесення інформації на комп'ютер, з якого зловмисник отримав доступ;

- копіювання на загальні ресурси типу файлообмінних серверів, а потім перенесення цих ресурсів на потрібний комп'ютер.

Якщо в першому випадку відстежити комп'ютер, на який відбулося перенесення інформації, не становить якихось великих складнощів, то в другому випадку процедура пошуку може зайти в глухий кут через набагато більшу територіальну віддаленість апаратної частини цього сервера або через його анонімність.

Здійснивши крадіжку інформації, зловмисник оцінює її значущість і вирішує зробити зомбування об'єкта, переходячи тим самим на стадію-зомбування.

Зловмисник негласно для легального користувача переносить на об'єкт необхідні шкідливі програми.

Спочатку переноситься спеціалізована програма класу "Downloader" необхідної версії та призначення, згодом саме ця програма в автоматичному режимі буде проводити усі інші переноси шкідливих кодів від класу "scanner" - для періодичного вивчення змін інформації до "rootkit" - для прихованого віддаленого адміністрування даного об'єкта.

Після перенесення на об'єкт усіх необхідних шкідливих програм, зловмисник періодично проводить аудит ресурсів, експлуатує апаратні та інформаційні ресурси об'єкта тощо. Останнім часом стала актуальною тенденція об'єднання заражених комп'ютерів за допомогою спеціалізованих шкідливих програм у «зомбі - мережі», завдяки яким можна керувати одночасно кількома зараженими комп'ютерами.

Програми, які дозволяють кіберзлочинцям віддалено керувати зараженими машинами (частиною комп'ютерів, кожною окремо, що входять до мережі, або всією мережею повністю) без відома користувача. Такі програми називають ботами.

Ботнети мають потужні обчислювальні ресурси, є грізною кіберзброєю та хорошим способом для заробляння грошей зловмисниками. Зараженими

машинами, які входять до мережі, господар ботнета може керувати будь-звідки: із іншої країни, міста або навіть із іншого континенту. Організація Інтернету робити це дозволяє анонімно.

Керування комп'ютером, зараженим ботом, може як бути прямим, так і опосередкованим. В разі прямого керування може зловмисник встановити зв'язок із інфікованим комп'ютером та ним керувати, використовуючи команди, вбудовані у тіло програми-бота. У випадку опосередкованого керування сам бот з'єднується із центром керування чи іншими машинами у мережі, надсилаючи запит та виконуючи отриману команду.

Комп'ютери, що заражені шкідливою програмою-ботом, які знаходяться під таємним контролем кіберзлочинців, ще називають зомбі-комп'ютерами, а мережу, куди вони входять, – зомбі-мережею.

3.4 Життєвий цикл кіберзлочинності

На рисунку 3.5 представлена сучасна схема роботи кіберзлочинців. В порівнянні з попередньою схемою роботи, крім розробників та результату, тут присутні атаки першої хвилі, посередники та атаки другої хвилі.

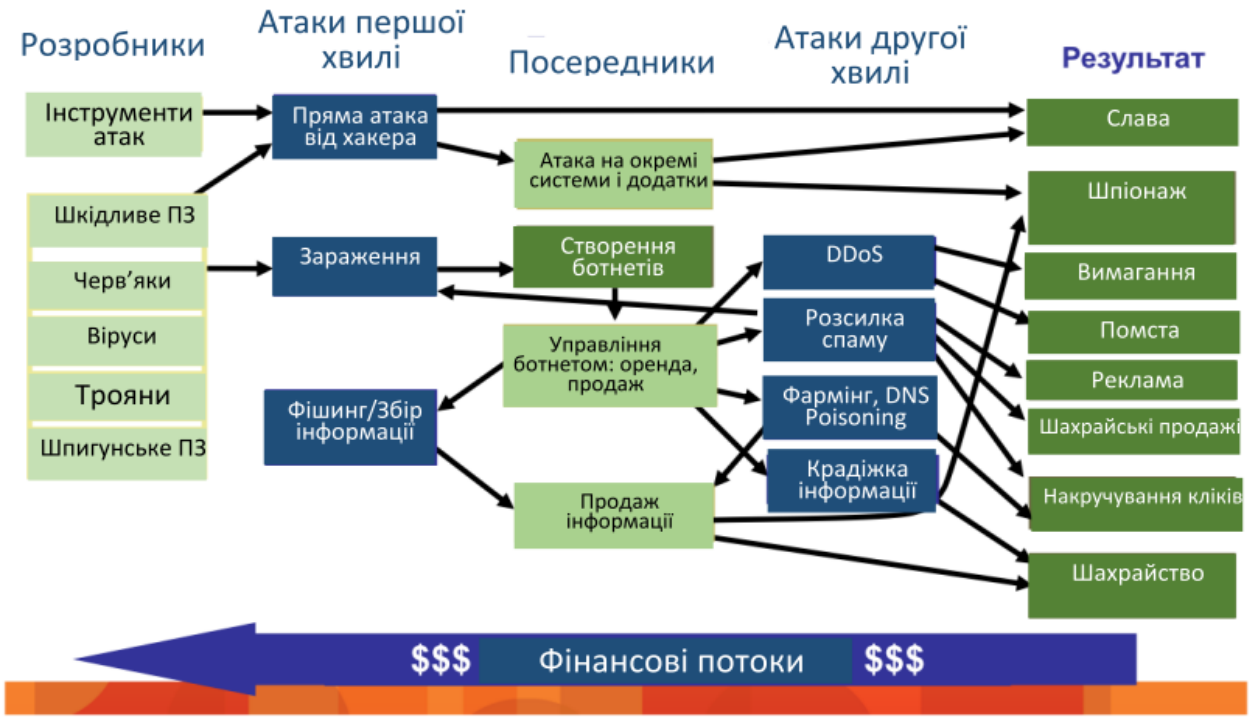

Рисунок 3.5 – Сучасна схема роботи кіберзлочинців

Для кожної схеми кіберзлочинності важливим є поняття його життєвого циклу. Він, як правило, складається з таких елементів:

1) розробка та тестування шкідливого коду;

2) шкідливий код оголошується на продаж;

3) шкідливий код розміщується на різних сайтах. Сайти можуть бути як спеціально підготовлені, так і загальнопопулярні, але зламані;

4) шкідливий код завантажується на комп'ютери користувачів під час відвідування заражених сайтів. У разі спеціально підготовлених сайтів використовуються партнерські схеми pay-per-install;

5) шкідливий код збирає інформацію для продажу (облікові записи, персональні дані, ключі електронного підпису тощо);

6) зібрана інформація використовується або продається.

ВИСНОВКИ

1. Здійснено аналіз основних типів кіберзлочинності, що дозволило встановити основні типи атак на інформаційну систему та способи реагування на такі інциденти.

2. Розроблено математичні моделі кіберзлочинності, що дозволило враховувати їх встановленні процесів інформа.

3. На основі побудованих моделей кіберзлочинності визначено етапи еволюціїї кіберзлочинності, що дозволило розробити схему їх функціональної моделі.

4. Розроблено функціональну схему моделі кіберзлочинів, на основі чого визначено життєвий цикл кіберзлочинності.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Волокітін А.В., Маношкин А.П., Солдатенков А.В., Савченко С.А., Петров Ю.А. Інформаційна безпека державних організацій і комерційних фірм. К.: Юніор, 2012. 303 с.

2. Козловський А.В., Паночишин Ю.М., Погрішук Б.В. Комп'ютерна техніка та інформаційні технології: навч. посіб. К.: Знання, 2014. 463 с.

3. Гринчук А.М., Пилипів С.І., Войтенко О.О., Черняк В.А. Структура центру управління інформаційною безпекою для протидії загрозам. Збірник матеріалів проблемної наукової міжгалузевої конференції «Автоматизація та комп'ютерно-інтегровані технології» (АКІТ-2022). Тернопіль, 2022. С.88-90.

4. Teslyuk V.M., Beregovskyi V.V., Pukach A.I. Development of smart house system model based on colored Petri nets, Proc. of the XVIII-th International Seminar. // Workshop On Direct And Inverse Problems Of Electromagnetic And Acoustic Wave Theory (DIPED – 2013), Lviv, Ukraine, 2013. P. 205-208.

5. Азаров Д.С. Злочини у сфері комп'ютерної інформації (кримінально-правове дослідження): моногр. К.: Атіка, 2007. 304 с.

6. Бурячок В.Л. Кібернетична безпека – головний фактор сталого розвитку сучасного інформаційного суспільства. Сучас. спец. техніка. 2011. № 3 (26). С. 104–114.

7. Бельський Ю. Щодо визначення поняття кіберзлочину. Юридичний вісник. 2014. № 6. С. 414–418.

8. Бутузов В. Протидія комп'ютерній злочинності в Україні (системно-структурний аналіз): моногр. / В. Бутузов. К.: КИТ, 2010. 148 с.

9. Арістова І.В. Державна інформаційна політика: організаційно-правові аспекти: монографія; за загальною редакцією д-ра юрид. наук, проф. Бандурки О. М.. Харків: Вид-во Ун-ту внутр. Справ, 2015. 368 с.

10. Богуцький П. Нелінійна раціональність системи права// Право України. 2018. № 6. С. 182-195.

11. Лісовська Ю. Кібербезпека. Ризики та заходи. К.: Кондор, 2019. 272 с.

12. Бурячок В.Л., Гулак Г.М., Толубко В.Б. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби: Підручник. К.: ДУТ, 2015. 449 с.

13. Дубов Д.В. Кіберпростір як новий вимір геополітичного суперництва: монографія. К.: НІСД, 2014. С. 36.

14. Картунов О.В., Маруховський О.О. Інформаційне суспільство: аналіз політичних аспектів зарубіжних концепцій: монографія. За заг. ред. Картунова О.В.; Ун-т економіки та права "КРОК". К.: Ун-т економіки та права "КРОК", 2012. 343 с.

15. Грищук Р.В., Даник Ю.Г. Основи кібернетичної безпеки: Монографія. Житомир: ЖНАЕУ, 2016. 636 с.

16. Бурячок В.Л., Толубко В.Б., Хорошко В. О., Толюпа С.В. Інформаційна і кібербезпека: соціотехнічний аспект: Підручник. К.: ДУТ, 2015. 288 с.

17. Пількевич І.А., Лобанчикова Н.М., Молодецька К.В. Захист інформації в автоматизованих системах управління: посібник. Житомир: Вид-во ЖДУ ім. І. Франка, 2015. 226 с.

18. Прачковський І.П., Черняк В.А. Класифікація кіберзлочинців у сучасному кіберпросторі. Збірник матеріалів науково - практичної конференції молодих вчених, аспірантів та студентів «Кібербезпека та комп'ютерно-інтегровані технології» (КБКІТ-2023), Тернопіль, 2023. С.51-54.

19. Прачковський І.П., Грицьків А.В. Актуальність та проблеми боротьби з кіберзлочинністю. Матеріали науково-практичного симпозіуму «Захист інформації». Тернопіль, 2023. С.145-147.

20. Леонов А.П. Комп'ютерна злочинність і інформаційна безпека.; під заг. ред. А. П.Леонова. Запоріжжя: АРІЛ, 2000. 552 с.

21. Москаленко А., Губерський Л., Іванов В. Основи масово-інформаційної діяльності. К., 2014. 71 с.

22. Нестеряк Ю.В. Нормативно-правові основи державної інформаційної політики України в умовах розвитку інформаційного суспільства. Теорія та практика державного управління. 2016. Вип. 4 (39). С. 111–119.

23. Коваленко Л.П. Теоретичні проблеми розвитку інформаційного права України: монографія. Х.: Право, 2012. 248 с.

24. Окінавська хартія глобального інформаційного суспільства. [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/998_163.

25. Погорецький М. Кіберзлочини: до визначення поняття. Вісник прокуратури. 2012. № 8. С. 89–96.

26. Пожуєв В.І. Формування державної інформаційної політики в умовах глобалізації. Гуманітарний вісник Запорізької державної інженерної академії. 2016. Вип. 43. С. 4–12.

27. Петров В.В. Щодо формування національної системи кібербезпеки України. Стратегічні пріоритети: [наук.-аналіт. щокварт. зб.]. Нац. ін-т стратег. дослідж. К.: НІСД, 2013. № 4 (29). С. 127–130.

28. Бєляков К.І. Інформатизація в Україні: проблеми організаційного, правового та наукового забезпечення: моногр. К.: КВІЦ, 2014. 576 с.

29. Березовська І. Державна інформаційна політика України та основні напрями її вдосконалення. Міжнародні відносини. Серія «Економічні науки». 2019. № 4. С.10-18.

30. Богуш В.М., Кривуца В.Г., Кудін А.М. Інформаційна безпека: Термінологічний навчальний довідник. Київ: ООО «Д.В.К.», 2014. 508 с.

31. Довгань О.Д. Система інформаційної безпеки України: онтологічні виміри. Інформація і право. 2018. № 1 (24). С. 89-103.

32. Лужецький В.А. Інформаційна безпека: навч. посіб. Вінниця: УНІВЕРСУМ-Вінниця, 2009. 240 с.

ДОДАТОК А

Копії публікацій