Міністерство освіти і науки України

Харківський національний університет імені В. Н. Каразіна

Факультет комп'ютерних наук

Спеціальність 125 «Кібербезпека»

Освітня програма «Кібербезпека»

«Допущено до захисту»

В.о. завідувача кафедри БІСТ

Мелкозьорова О.М.

_____

«_____» _____ 2024 р.

Пояснювальна записка

до кваліфікаційної роботи бакалавра

на тему: «Дослідження та аналіз впливу різних типів кібератак на рівень інформаційної безпеки користувачів та методи захисту від них»

Оцінка «_____»

Голова ЕК

Лемешко О.В. _____

Керівник к.т.н. Єсіна М.В.

Рецензент к.т.н. Бобух В.А.

Виконавець: студент групи КБ-42

Осадчий Є.М.

Харків – 2024

РЕФЕРАТ

Кваліфікаційна робота бакалавра, 49 сторінок, 6 рисунків, 23 джерел.

Робота складається з вступу, 3 розділів, висновків, переліку використаних джерел.

Об’єкт дослідження – різні типи кібератак на методи захисту від них.

Предмет досліджень – вплив різних типів кібератак на рівень інформаційної безпеки користувачів та методи захисту від них.

Метою дипломної роботи є детальний аналіз різних типів кібератак та їх впливу на рівень інформаційної безпеки користувача. Основним завданням є розуміння та оцінка загроз, які можуть виникнути у віртуальному просторі, а також розробка ефективних засобів захисту від цих кібератак. Завдання полягає у вивченні потенційних ризиків для користувачів внаслідок кібератак та розробці практичних рекомендацій і стратегій захисту, спрямованих на убезпечення інформаційного середовища. Досягнення цієї мети вимагає документування результатів дослідження, підготовки коментаря з висновками та рекомендаціями, а також проведення необхідних оглядів для перевірки обґрунтованості та достовірності отриманих результатів.

Ключові слова: КІБЕРАТАКИ, ІНФОРМАЦІЙНА БЕЗПЕКА, ЗАХИСТ, КІБЕРБЕЗПЕКА, ЗАГРОЗИ, ВРАЗЛИВОСТІ, ПОРІВНЯЛЬНИЙ АНАЛІЗ, РЕКОМЕНДАЦІЇ, ФІШИНГ, DDOS.

ABSTRACT

Qualifying work of a bachelor in volume of 49 pages contains: 6 figures, 23 references.

The work consists of the introduction, 3 sections, conclusion, list of references.

The object of the research is various types of cyberattacks on methods of protection against them.

The subject of the research is the the impact of different types of cyberattacks on the level of user information security and methods of protection against them.

The purpose of the work is a detailed analysis of various types of cyberattacks and their impact on user information security. The main task is to understand and assess the threats that may arise in the virtual space, as well as develop effective means of protection against these cyberattacks. The objective is to study potential risks for users due to cyberattacks and develop practical recommendations and protection strategies aimed at securing the information environment. Achieving this goal requires documenting research results, preparing a commentary with conclusions and recommendations, and conducting necessary reviews to verify the validity and reliability of the obtained results.

Keywords: CYBERATTACKS, INFORMATION SECURITY, PROTECTION, CYBERSECURITY, THREATS, VULNERABILITIES, COMPARATIVE ANALYSIS, RECOMMENDATIONS, PHISHING, DDOS.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

DNS – Domain Name System (система доменних імен)

DNS-тунелювання – це метод злочинців, за допомогою якого вони використовують DNS-протокол для передачі даних між комп’ютерами у мережі

DoS – denial of service (відмова в обслуговуванні)

DDos – Distributed Denial of Service (розподілена відмова в обслуговуванні)

fishing – форма соціальної інженерії та шахрайства, при якій атакуючі обманюють людей, щоб вони розкрили чутливу інформацію або встановили шкідливе програмне забезпечення

MITD – man in the middle («людина посередині»)

SQL – Structured Query Language (мова структурованих запитів)

SQL-ін’єкція – вразливість веб-застосунків, при якій зловмисники використовують некоректно оброблені SQL-запити для введення або видалення даних з бази даних або отримання несанкціонованого доступу до системи

ОС – операційна система

ПЗ – програмне забезпечення

ВСТУП

У сучасному інформаційному суспільстві питання кібербезпеки стають надзвичайно актуальними, оскільки з кожним днем зростає обсяг цифрової активності та залежність від інформаційних технологій. Разом із швидким розвитком технологій зростає і рівень кіберзагроз, які стають важливим аспектом забезпечення безпеки в Інтернет-просторі. Ці загрози викликають серйозні проблеми, а також стають причиною порушення конфіденційності, цілісності та доступності інформації. У цій роботі розглядаються різноманітні форми кіберзагроз і їхній вплив на інформаційні системи, а також можливі заходи для захисту від них в умовах постійно зростаючого цифрового середовища.

Актуальність теми зростає відразу з кількох ключових аспектів. По-перше, інформаційні технології стали не тільки необхідною частиною повсякденного життя, але і критично важливим ресурсом для функціонування великої кількості суспільних, комерційних та господарських процесів. По-друге, зростання залежності від цих технологій відкриває нові можливості для кіберзлочинців, які використовують різноманітні та вдосконалені методи для атак на інформаційні системи.

Забезпечення надійності і безпеки цих систем стає надзвичайно важливим завданням, оскільки кіберзагрози, такі як атаки на мережеві структури, витоки конфіденційної інформації та шкідливі програми, можуть мати серйозні наслідки для економіки, політики та суспільної безпеки. У цьому контексті розуміння різних форм кіберзагроз та їхнього впливу стає стратегічно важливим для розробки ефективних заходів захисту, що відповідають викликам сучасного інформаційного простору.

Зростання кількості та складності кіберзагроз у сучасному світі стає серйозним викликом для сфери кібербезпеки. Різноманітність атак, включаючи

витончені техніки фішингу, атаки з використанням шкідливого програмного забезпечення та атаки на інфраструктуру, показує, що кіберзлочинці постійно вдосконалюють свої методи, адаптуючись до новітніх технологій та змін у сфері кібербезпеки.

Цей постійний розвиток кіберзагроз вимагає не лише реактивних, але й проактивних стратегій захисту. Організації та індивіди, що прагнуть залишатися попереду, повинні не лише оновлювати свої системи та програмне забезпечення, але й розвивати нові методи виявлення та запобігання кібератак. Важливість цього завдання зумовлена тим, що відповідальність за захист інформаційних систем стає не тільки завданням технічних спеціалістів, але й ключовою складовою стратегічного управління будь-якою організацією чи державною установою. У цьому контексті огляд різних форм кіберзагроз та їхнього впливу стає невід'ємною частиною ефективного управління кібербезпекою, спрямованого на забезпечення стабільності та надійності інформаційних систем.

Проведення аналізу впливу кіберзагроз на стійкість інформаційних систем є невід'ємною частиною вдосконалення стратегій кібербезпеки в умовах постійного еволюційного середовища. З урахуванням стрімкого розвитку технологій та збільшення кількості цифрових аспектів нашого життя, зростає і сфера кіберзагроз, що накладає серйозний вплив на інформаційні системи.

Ця робота має на меті розглянути проблему кібербезпеки в контексті сучасних реалій та запропонувати детальний аналіз різноманітних форм кіберзагроз, який охоплює їх вплив на конфіденційність, цілісність та доступність інформації. Зокрема, надаючи огляд найновіших тенденцій у сфері кібербезпеки, виокремити ключові аспекти, що піддаються ризику внаслідок кібератак.

Важливим етапом у нашому аналізі буде визначення ефективних стратегій захисту, які спроможні відповідати викликам сучасного кіберпростору. Запропоновані стратегії враховують як технічні, так і стратегічні аспекти,

спрямовані на удосконалення стійкості інформаційних систем та забезпечення їхньої надійної функціональності в умовах постійної загрози кібербезпеки.

1 ІСТОРІЯ РОЗВИТКУ КІБЕРАТАК ТА КІБЕРБЕЗПЕКИ

1.1 Історія розвитку кібербезпеки та кібератак від початку до сучасності

Кібератаки стали складнішими з моменту створення першого цифрового комп'ютера у 1943 році. Напрямок розвитку цих атак історично пов'язаний з початком взлому телефонних автоматів і мереж у 1950-х роках, коли спеціалісти відкривали протоколи телефонних мереж для безкоштовних дзвінків. Цей етап відзначився допитливістю та прагненням розуміти технічні можливості.

З 1960-х років, коли більшість комп'ютерів були мейнфреймами з обмеженим доступом, почалася ера незаконного або несанкціонованого отримання доступу до комп'ютерних систем, мереж або електронних пристроїв з метою виконання різних дій, таких як отримання конфіденційної інформації, завдання шкоди або зміна функціонування системи. Хакери, які раніше займалися залізничними макетами, почали досліджувати комп'ютерні системи. Наслідком цього стала ідея впровадження заходів безпеки на комп'ютерах для запобігання атак.

Важливим моментом в історії кібербезпеки став 1967 рік, коли студенти, запрошені IBM для огляду комп'ютера, виявили слабкі місця системи. Це призвело до усвідомлення необхідності захисту даних. Подібні випадки відкрили шлях до етичного хакінгу, який сьогодні вважається важливою галуззю кібербезпеки.

Дослідження впливу кібератак на рівень безпеки та розвиток методів захисту стали основою подальшого розвитку цієї галузі. У наступні роки попит на комп'ютери зріс, вони стали доступнішими та компактнішими, що призвело до їх широкого використання у бізнесі та зберіганні даних.

На той час використання паролів було широкою практикою, оскільки закривати комп'ютери в кімнаті було незручно.

1970-ті роки були важливими у розвитку кібербезпеки, з мережею ARPANET як однією з перших спроб у цьому напрямку. У той час була створена програма “Кріпер”, що вважається першим вірусом в історії комп’ютерних загроз.

1980-ті роки були періодом народження комерційних антивірусів та зростання високопрофільних атак. У цей період також виникли терміни "Троянський кінь" та "Комп’ютерний вірус", а загрози кібершпигунства зросли у зв’язку з Холодною війною.

1990-ті роки відзначились розвитком Інтернету та зростанням кіберзагроз, з першим поліморфним вірусом і появою комерційних антивірусів. Також було створено протокол безпеки SSL для захисту онлайн-транзакцій та даних.

2000-ті роки відзначились ростом різноманітності та складності кіберзагроз. Поява нових типів інфікування та атак на основні системи підкреслюють необхідність постійного розвитку заходів з кібербезпеки.

Сучасні кіберзагрози стають все більш витонченими та масштабними. Атаки на бізнес, уряди, інфраструктуру та навіть окремих користувачів стають звичним явищем. Кіберзлочинці використовують новітні технології та методи, щоб обійти заходи безпеки та поширювати шкідливе програмне забезпечення.

У той же час, експерти з кібербезпеки намагаються не відставати. Вони також постійно розробляють інноваційні методи та рішення для боротьби з кіберзагрозами та підвищення надійності захисту інформації [3].

1.2 Поняття кібератака та основні їх види

Кібератака – це спроба несанкціонованого доступу до комп’ютерів, обчислювальних систем або комп’ютерних мереж з метою завдання шкоди.

Ці атаки спрямовані на вимкнення, руйнування, знищення або контроль над системами, а також зміну, блокування, видалення, маніпулювання або крадіжку даних, що містяться в цих системах (рис. 1.1) [7].

Рисунок 1.1 – Типи кібератак

Люди, які здійснюють такі атаки, зазвичай вважаються кіберзлочинцями. Їх часто називають "поганими діячами", "загрозовими діячами" або "хакерами". Вони можуть діяти самостійно, використовуючи свої навички у сфері комп’ютерів для розробки та виконання зловмисних атак. Також вони можуть бути членами кримінального угрупування, співпрацюючи з іншими загрозливими діячами для пошуку слабкостей чи проблем у комп’ютерних системах, які називаються вразливостями, які вони можуть використовувати для злочинних цілей. До таких атак можуть долучатися і групи експертів з комп’ютерів, які спонсоруються державою. Їх визнають як атаки від держави і вони були звинувачені в атаках на ІТ-інфраструктуру інших урядів, а також негромадських суб’єктів, таких як бізнес, неприбуткові організації та комунальні служби.

Кібератаки мають кримінальні або політичні мотиви. Деякі хакери знаходять задоволення у тому, що здатні зробити вимкнення комп’ютерних систем, отримуючи від цього захват або почуття досягнення. Політично мотивовані кібератаки можуть бути спрямовані на пропаганду, шкоду іміджу конкретної держави чи уряду в очах громадськості. Це також може мати більш підступні цілі, такі як розголошення конфіденційної інформації, особистих

комунікацій або компрометуючих даних. Кібератаки можуть піти ще далі: наприклад, хакери, які мають підтримку від держави, теоретично можуть створити програмне забезпечення для порушення та знищення програм зброї чи іншої критичної інфраструктури.

Кібератаки також можуть спричиняти порушення даних, коли великі обсяги інформації витікають онлайн і потім використовуються злочинцями для фінансового шахрайства. Дані, такі як номери кредитних карт, історії покупок, імена та адреси, можуть бути всім, що потрібно деяким шахраям для вчинення крадіжки особистості. Дослідження показують, що злочинці також можуть накопичувати особисті дані з часом, збільшуючи свою можливість використовувати їх для отримання фінансової вигоди. Наприклад, вони можуть зібрати ім’я та адресу з одної атаки та номер кредитної картки з іншої, поєднуючи обидва для вчинення крадіжки особистості [7].

1.2.1 Атаки на основі шкідливих програм

Шкідлива програма, скорочено від "зловмисне програмне забезпечення", відноситься до будь-якої програми, яка вторгається у системи звичайних користувачів, розробленої кіберзлочинцями (часто їх називають "хакерами"), щоб красти дані та завдавати шкоди або знищувати комп’ютери та комп’ютерні системи. Прикладами загально відомих шкідливих програм є віруси, черв’яки, троянські віруси, шпигунське програмне забезпечення, рекламне програмне забезпечення та програмне забезпечення вимагач. Останні шкідливі програми великими масивами виносять інформацію.

Зазвичай бізнеси акцентуються на превентивних інструментах для запобігання порушень. Забезпечуючи безпеку периметра, бізнеси вважають, що вони в безпеці. Однак деякі відомі шкідливі програми врешті-решт знайдуть шлях у вашу мережу. Отже, важливо впроваджувати технології, які постійно моніторять та виявляють шкідливі програми, які обійшли оборону периметра. Ефективний захист від шкідливих програм вимагає кількох рівнів захисту разом

з високорівневою видимістю мережі та інтелектом.

Шкідливі програми незабаром проникнуть у вашу мережу. Ви повинні мати оборонні засоби, які надають значну видимість та виявлення порушень. Щоб видалити шкідливу програму, ви повинні швидко ідентифікувати зловмисних діячів. Це вимагає постійного сканування мережі. Після виявлення загрози вам потрібно видалити шкідливу програму з вашої мережі. Сучасні антивірусні продукти не завжди досить ефективні для захисту від складних кіберзагроз [7].

1.2.2 Фішинг

Фішинг починається з оманливого електронного листа або іншого засобу зв'язку, який призначений зловити жертву. Повідомлення робиться таким, що воно здається від надійного відправника. Якщо це вводить жертву в оману, він або вона намагається надати конфіденційну інформацію, часто на обманному веб-сайті. Часом також завантажується шкідлива програма на комп'ютер жертви.

Іноді фішингові листи надсилаються для отримання інформації для входу співробітників або інших деталей для використання у складній атаці проти конкретної компанії. Кіберзлочинні атаки часто починаються з фішингу.

Одним зі способів захисту вашої організації від фішингу є навчання користувачів. Навчання повинне охоплювати всіх співробітників. Високопоставлені керівники часто є метою атак. Навчіть їх розпізнавати фішингові листи та діяти, якщо вони отримають такі листи. Симуляційні вправи також є ключовими для оцінки реакції ваших співробітників на сценарії фішингових атак [7].

1.2.3 MITM-атаки

Атака Man-in-the-middle (MITM), також відома як атака "людина посередині" або підслуховування, відбувається, коли зловмисник втручається в транзакцію між двома сторонами. Коли зловмисник порушує трафік, дані можуть бути відфільтровані та викрадені. Дві поширені точки входу для

MITM-атак:

- Незахищений публічний Wi-Fi дозволяє зловмисникам потрапити між пристроєм відвідувача та мережею. Відвідувач передає всю інформацію через зловмисника без будь-якого введення.
- Якщо на пристрій потрапляє шкідливе програмне забезпечення, зловмисник може встановити програмне забезпечення для обробки всієї інформації жертви.

Запобігання MitM-атакам:

- Переконайтеся, що веб-сайти, які ви відвідуєте, використовують протокол HTTPS; веб-сайти HTTPS використовують шифрування SSL/TLS, щоб зловмисники не могли викрасти або інтерпретувати дані, якими ви ділитеся. Ви також можете встановити плагіни для браузера, щоб забезпечити дотримання правил лише HTTPS.
- Використовуйте комунікаційні програми та сервіси з шифруванням, такі як WhatsApp, Telegram і Google Messages.
- Оновлюйте програмне забезпечення, включаючи операційні системи, браузери, антивірусні та антишпигунські програми. Cyber Ghost також пропонує преміум-пакет безпеки, який захищає пристрої з Windows від мережевих атак, таких як MitM-атаки.
- Оновлювач безпеки Cyber Ghost автоматично виявляє та оновлює вразливі програми, щоб зловмисники не змогли використати їх для створення лазівки на пристрої [7].

1.2.4 DoS-атаки (відмова в обслуговуванні)

Атака «відмова в обслуговуванні» (DoS) – це тип кібератаки, в якій зловмисник намагається перешкодити цільовому користувачеві використовувати комп’ютер або інший пристрій, втручаючись у нормальне функціонування пристрою.

DoS-атаки зазвичай працюють шляхом перевантаження цільового пристрою або завалення його запитами до тих пір, поки він не зможе обробляти нормальний трафік, що призводить до відмови в обслуговуванні іншим користувачам. Для DoS-атак характерне використання одного комп'ютера для запуску атаки.

Найбільш очевидними ознаками DDoS-атаки є раптове збільшення часу відгуку або недоступність веб-сайту чи сервісу.

Однак різні причини, такі як законні сплески трафіку, можуть викликати подібні проблеми з продуктивністю і часто вимагають подальшого розслідування. Інструменти аналізу трафіку можуть допомогти виявити деякі ознаки DDoS-атаки:

- Підозрілі обсяги трафіку, що надходять з однієї IP-адреси або діапазону IP-адрес.
- Трафік від користувачів зі спільними поведінковими профілями, такими як тип пристрою, географічне розташування, версія браузера тощо.
- Необґрунтований потік запитів до однієї сторінки або кінцевої точки.
- Незвичайні патерни трафіку, такі як сплески в певний час доби або патерни, які не виглядають природними (наприклад, сплески кожні 10 хвилин).

Існують також більш специфічні симптоми DDoS-атаки, які залежать від типу атаки [7].

1.2.5 SQL-ін'єкція

SQL-ін'єкція (SQLi) – це кібератака, при якій шкідливий SQL-код вводиться у застосунок, щоб дозволити зловмиснику переглядати або модифікувати базу даних. Згідно з даними проєкту Web Application Security Project, атаки на SQL-ін'єкції, включаючи ін'єкційні атаки, були третім найбільш серйозним ризиком для безпеки веб-застосунків у 2021 році. 274000 ін'єкцій було виявлено в протестованих ними застосунках.

Для захисту від атак SQL-ін’єкцій важливо розуміти їхній вплив і те, як вони відбуваються, щоб ви могли слідувати найкращим практикам, перевіряти наявність вразливостей і розглянути можливість інвестування в програмне забезпечення, яке проактивно запобігає атакам.

Більшість сучасних веб-сайтів і застосунків залежать від баз даних, а бази даних програмуються за допомогою мови структурованих запитів (SQL). Вразливості SQL-ін’єкцій виникають, коли запити з веб-сайтів не фільтруються, не перевіряються та не контролюються належним чином, що дозволяє зловмисникам намагатися вставити фрагменти SQL-коду в запити до бази даних.

Щоб запобігти атакам SQL-ін’єкцій, програмісти веб-застосунків і баз даних повинні фільтрувати вхідні дані, обмежувати код бази даних, обмежувати доступ до бази даних, а також підтримувати і контролювати застосунок і базу даних. Ці п’ять методів ефективні, але в основному застосовуються до коду на етапі розробки. Це пов’язано з тим, що існуючий код часто занадто великий, щоб його можна було проаналізувати рядок за рядком. На щастя, різні відкриті та комерційні інструменти можуть допомогти виявити вразливості SQL-ін’єкцій, а спеціалізовані постачальники надають готову до використання допомогу [7].

1.2.6 DNS-тунелювання

DNS-тунелювання – це широкий термін, що описує нещодавно виявлені вразливості, які хакери можуть використовувати для атак на системи. Термін "нульовий день" походить від того, що постачальники та розробники тільки дізналися про вразливість і "не мали днів", щоб її виправити. Атаки нульового дня відбуваються, коли хакери використовують вразливості до того, як розробники встигають їх виправити. "Нульовий день" часто визначають як "день 0". Терміни "вразливість", "експлойт" і "атака" часто використовуються разом з "нульовим днем", але корисно знати різницю між ними.

Вразливість нульового дня – це вразливість програмного забезпечення, яку зловмисник виявляє до того, як про неї дізнається розробник. Оскільки розробник не знає про це, для вразливостей "нульового дня" не існує виправлень, і ймовірність атаки є високою.

Експлойти нульового дня – це техніка, яку використовують хакери для атаки на системи з раніше виявленими вразливостями.

Атака нульового дня – це використання експлойту нульового дня для пошкодження або викрадення даних з вразливої системи.

DNS є критично важливим сервісом, і тому проблематично, якщо він буде заблокований. Тому захист від атак на DNS-тунелювання включає в себе різні заходи, які можуть допомогти запобігти таким атакам.

Потрібно бути більш обережними з підозрілими IP-адресами та доменними іменами з невідомих джерел.

Всі внутрішні клієнти можуть бути налаштовані на перенаправлення DNS-запитів (DNS-пошуку) на внутрішній DNS-сервер. Таким чином можна відфільтрувати потенційно шкідливі домени.

Важливо знати про підозрілі домени і постійно відстежувати DNS-трафік. Це зменшить ймовірність атак DNS-тунелювання.

Встановіть брандмауер DNS, щоб виявити і зупинити хакерів.

Рішення DNS в режимі реального часу, яке може виявляти аномальні DNS-запити і незвичайні шаблони трафіку на DNS-серверах, також є чудовим варіантом [7].

1.2.7 Атаки нульового дня

Система доменних імен (DNS) [7] – це протокол, який переводить людські URL-адреси, такі як paloaltonetworks.com, в машинні IP-адреси, такі як 199.167.52.137. Кіберзлочинці знають, що DNS широко використовується і користується довірою. Крім того, оскільки DNS не призначена для передачі даних, багато організацій не відстежують трафік DNS на предмет зловмисної

активності. Як наслідок, існує кілька атак на основі DNS, які можуть бути ефективними проти корпоративних мереж. DNS-тунелювання є однією з таких атак [7].

1.3 Кібератака як одна із форм кібертероризму

Кібертероризм – це комплексне явище, яке виникає через недостатню увагу до безпеки в мережі та активність терористичних організацій у кіберпросторі.

Одним із основних напрямів їх діяльності є використання Інтернету та сучасних технологій для реалізації різних завдань:

- Налагодження конфіденційного зв’язку через онлайн-ігри або кодовані повідомлення.
- Планування атак за допомогою геолокаційних сервісів, наприклад, Google Maps.
- Координація атак із забезпеченням анонімності через VoIP-телефонію та інші технології.
- Визначення потенційних цілей через соціальні мережі.
- Підвищення обізнаності у військовій тактиці та створення вибухових пристроїв.
- Фінансування діяльності через анонімні онлайн-пожертвування та інші електронні платіжні системи.
- Залучення нових членів та поширення ідеології через медіа-ресурси та соціальні мережі.

Також важливо розрізняти різні рівні кібертерору за їх можливостями, від простих неструктурованих атак до комплексно-координованих, спрямованих на масове руйнування інформаційних систем.

Сьогодні кібертерористам особливо цікаві державні інформаційні системи та важливі елементи державної інфраструктури, які можна атакувати через кіберпростір. Проведення кібератак є однією з форм кібертероризму. Наприклад,

в Україні лише за листопад і грудень 2016 року було 6500 кібератак. У результаті цих атак навіть електропостачання в Києві тимчасово вимкнулося. Однак такі атаки часто мають цілі лише для демонстрації можливостей. Так, в червні 2017 року українські системи постраждали від вірусу "Petya.A", який призвів до збоїв у роботі різних організацій та підприємств. Важливою є реакція на такі атаки, яка включає в себе розслідування та усунення наслідків кібератак. На рисунку 1.2 зображені основні джерела кіберзагроз [6]:

Рисунок 1.2 – Джерела кіберзагроз

У разі компрометації об’єкта атаки можливі такі етапи:

- Керування й контроль: Віддалене керування атакованим об’єктом через командний сервер або канал.
- Виконання дій: Зловмисник здійснює різні шкідливі дії, такі як викрадання інформації, шифрування файлів, перехоплення управління, виконання підміни даних, виведення пристроїв з ладу тощо, а також можливі

додаткові атаки на інші пристрої в мережі.

Щоб захиститися від цього, Lockheed Martin рекомендує відповідати на такі питання:

- Які індикатори атаки на кожному етапі "убивчого ланцюжка"?
- Які інструменти безпеки необхідні для виявлення цих індикаторів?
- Чи є проблеми з виявленням атак в системі кібербезпеки організації?

Додатково, є DoS-атака, яка спрямована на переривання мережевого сервісу шляхом перевантаження мережі. Це може бути одним комп'ютером або розподіленою атакою на відмову в обслуговуванні (DDoS), де багато комп'ютерів працюють разом для атаки. Атаки можуть бути прямими, віддзеркаленими або прихованими залежно від того, яким шляхом трафік доставляється до цільової мережі.

Дослідники розглядають такі класифікаційні ознаки кібератак:

- за метою впливу на об'єкт атаки: класифікуються на спрямовані на цілісність/конфіденційність інформації, захист від несанкціонованого доступу, порушення живучості системи та її функціонування;
- за принципом впливу на об'єкт атаки: розрізняються використанням прихованих каналів, застосуванням прав суб'єкта системи до об'єкта;
- за характером впливу на об'єкт атаки: поділяються на активний (виконання дій, які порушують політику безпеки) та пасивний (прослуховування ліній зв'язку);
- за способом впливу на об'єкт атаки: включають захоплення привілеїв, безпосередній доступ до даних/програм/служб з використанням привілеїв;
- за засобами впливу на об'єкт атаки: використанням стандартного ПЗ або спеціально розроблених програм;
- за об'єктом атаки: можуть бути направлені на систему загалом, дані/програми на зовнішніх/внутрішніх пристроях, канали передавання даних, процеси з участю користувачів;

- за станом об’єкта: інформація може зберігатися, передаватися або оброблятися під час атаки;

Щодо DDoS-атак, вони орієнтовані на перевантаження мережі або Інтернет-каналу. Організуються як ботнет або флешмоб, а також можуть використовувати HTTP-flood або SSL-шифровані атаки для обходу захисту. Ідентифікація пристрою, що здійснив атаку, може бути ускладнена через використання проксі-серверів або комутованих з’єднань.

Кібератаки на державні установи, організації та об’єкти критичної інфраструктури становлять серйозну загрозу як для міжнародної, так і для національної кібербезпеки України, особливо в умовах повномасштабної війни з Росією. Ці атаки завдають непоправної шкоди суспільству, оскільки кібертерористи використовують сучасні засоби інформаційного суспільства для поширення ідей та досягнення своїх цілей через кіберпростір.

Рекомендації для виявлення слідів кібератак та заходів протидії включають:

- контроль цілісності програм, файлів даних та інших інформаційних ресурсів;
- аналіз діяльності користувачів, процесів та мережевого трафіку;
- контроль фізичних форм атаки на елементи інформаційної системи;
- аналіз дій адміністраторів з попередніх інцидентів.

Хоча жодні заходи не гарантують 100% захисту, їх впровадження до системи кіберзахисту може зменшити нанесену шкоду від кібератак [5].

2 ОГЛЯД ТА АНАЛІЗ ВПЛИВУ РІЗНИХ ТИПІВ КІБЕРАТАК НА РІВЕНЬ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ КОРИСТУВАЧІВ

2.1 Комп’ютерні віруси

Комп’ютерні віруси – це вид комп’ютерних програм, які можуть змінювати роботу комп’ютера без дозволу або відома користувача і намагаються приховатися в інших файлах. Ці програми зазвичай вбудовуються в інші програми на комп’ютері, спрямовуючи на вкладання в інші файли після успішного запуску. Для активації вірусів їх необхідно запустити. Важливо відзначити, що комп’ютер не заражається автоматично при вставці зараженого носія даних, такого як CD, дискета або флеш-накопичувач, якщо відсутній файл автоматичного запуску. Заражений файл має бути запущений операційною системою або вручну, щоб вірус став активним. Раніше заражені файли зазвичай мали розширення .exe, .com або .pif, але з розвитком технологій збільшився спектр "виконуваних" файлів, включаючи .doc і .gif, які раніше вважалися безпечними [22].

2.2 Комп’ютерні черв’яки

Комп’ютерні черв’яки – це шкідливе програмне забезпечення, яке має складну структуру. Вони зазвичай поширюються через електронну пошту із застосунками, веб-сайтами та файлами, що розділяються в мережі. Коли черв’яки захоплюють систему, вони намагаються швидко передати свої вихідні файли іншим користувачам, використовуючи джерела даних користувачів, такі як список електронної пошти, без необхідності будь-яких додаткових дій від користувача. Це дозволяє їм масово розмножуватися. Під час цього черв’яки використовують ресурси мережі та можуть спричинити збої в мережі, перевантаження поштових серверів або сповільнення доступу до веб-ресурсів.

Черв’яки мають подібні функції до вірусів, але вони не є програмами, які відкриваються користувачем для інфікування програм. Після того, як черв’яки потрапляють у систему, вони створюють копії себе в мережі та розповсюджуються на всі недостатньо захищені сервери та комп’ютери. Для захисту від червів рекомендується встановити оновлені версії операційних систем, виконувати регулярні оновлення та застосовувати особистий брандмауер для захисту від зовнішніх атак [22].

2.3 Троянській кінь

Натомість, віруси-троянці виглядають для користувачів як корисні програми і призводять до їх завантаження. Це шкідливе програмне забезпечення, яке приховується під видом легітимних програм, але насправді ними не є. Вони стають активними, коли виконується програмний файл, до якого вони прикріплені, і поширюються користувачами. Троянці не так легко виявляються, як звичайні віруси, і проявляють свої наслідки після інфікування. Базово, троянці містять два файли: перший – це файл, який надісланий користувачу і відкриває порт на комп’ютері для зловмисника, а другий – це файл, який запускає зловмисник для доступу до системи користувача. Зловмисники можуть отримати особисту інформацію з комп’ютера жертви, таку як паролі, кредитні дані і інші важливі документи. Оскільки троянські програми залишають вразливість в системі, зловмисники можуть легко встановлювати додаткове шкідливе програмне забезпечення. Щоб уникнути троянського коня, потрібно застосовувати комплексну стратегію захисту, а також регулярно оновлювати всі використовувані програми для зменшення вразливостей системи [22].

2.4 RootKit

Rootkit – це вид шкідливого програмного забезпечення, створений для надання несанкціонованого доступу та контролю над пристроєм жертви

зловмисникам. Більшість rootkit-ів впливають на операційні системи та програмне забезпечення, але деякі можуть впливати й на апаратні засоби та програмне забезпечення. Rootkit-и вміло приховують своє існування й залишаються активними, поки залишаються невиявленими. Після отримання доступу до комп'ютерів rootkit-и дозволяють кіберзлочинцям красти фінансову та особисту інформацію, встановлювати шкідливе програмне забезпечення або використовувати пристрої як частину ботнета для поширення спаму та проведення DDoS-атак. Важко визначити, які файли фактично змінив rootkit, який модуль завантажується у ядро, та, які мережеві служби він слухає та діє на них за допомогою відповідної команди. Проте існують методи, такі як збереження контрольних сум найбільш базових команд та потенційних точок зараження rootkit-ом, для подальшої перевірки [22].

2.5 Атаки соціальної інженерії

У сфері кібербезпеки багато людей ставлять за мету захист від хакерів, які використовують технічні вразливості для атак на мережі даних. Проте, є ще один спосіб проникнення в організації та мережі, який використовує вразливість людей. Цей метод полягає в обмані людей з метою отримання доступу до мереж даних або розкриття інформації, і відомий як "соціальна інженерія". Узагальнюючи, соціальна інженерія – це вплив на людей, щоб вони надали доступ або розкрили інформацію. Такі атаки спрямовані на обхід заходів безпеки, які застосовуються особами або організаціями. Жертвами атак методом соціальної інженерії може стати будь-хто, але найчастіше це стосується старших людей з обмеженими технічними знаннями, тих, хто має обмежений контакт з людьми, а також осіб, які схильні до імпульсивної поведінки. Для запобігання можливим атакам слід утримувати особисті/приватні дані в таємниці, перевіряти тих, хто намагається зв'язатися, перевіряти URL-адреси та уникати ненадійних джерел [22].

2.6 Атаки на застосунки

Під час атаки на застосунки кіберзлочинці намагаються отримати доступ до незаконних доменів. Зловмисники зазвичай розпочинають з аналізу рівня застосунків і пошуку вразливостей у коді програми. Хоча деякі атаки націлені на певні мови програмування, багато застосунків різних мов можуть стати жертвами атак. Вразливості можуть існувати як у власному коді, так і у відкритих фреймворках та бібліотеках. Вони створюють можливості для зловмисників використовувати застосунки у виробництві. Кіберзлочинці користуються різними методами, такими як використання вразливостей у коді, проблеми через застарілі сертифікати або недостатню автентифікацію [22].

2.7 Криптографічні атаки

Атаки на криптографію відбуваються, коли зловмисник намагається порушити криптосистему, виявляючи слабкі місця у коді, шифрі, криптографічному протоколі або управлінні ключами. Ці атаки поділяються на пасивні та активні. Пасивні атаки відбуваються без втручання в канал зв’язку і полягають у несанкціонованому доступі до інформації, тоді як активні атаки включають зміну або ініціювання несанкціонованої передачі даних. Пасивні атаки часто спрямовані на крадіжку інформації, у той час як активні атаки включають зміну даних без дозволу. Обидва типи атак можуть порушити цілісність та конфіденційність чутливої інформації [22].

2.8 Атаки-захоплення

Це форма кібератак, під час яких атакуючий намагається отримати контроль над комп’ютерними системами, програмним забезпеченням та мережевими зв’язками [22]. Більшість кібератак в певному сенсі базуються на захопленні, і злом є звичайною, хоча й незаконною, дією із серйозними наслідками для обох сторін – як для атакуючого, так і для жертви. Такі атаки

можуть включати захоплення повітряних суден або управління броньованим транспортним засобом. Існують різноманітні типи атак захоплення, серед яких:

- захоплення браузера;
- захоплення сеансу;
- захоплення домену;
- захоплення буфера обміну;
- захоплення системи доменних імен DNS;
- захоплення Інтернет-протоколу IP;
- захоплення сторінки.

2.9 Фішингові атаки

Сьогодні фішинг є однією з найпоширеніших кіберзагроз. За прийнятим у світі визначенням, фішинг – це тип онлайн-шахрайства, що спрямований на споживачів, відправляючи електронні листи, які намагаються симулювати відомі джерела. Злочинці відтворюють провайдерів Інтернету, банки, важливі компанії або урядові органи. Основна мета таких атак – отримати чутливу інформацію, таку як логіни, паролі, дані кредитних карток та доступ до мережі. Соціальна інженерія використовується для отримання цих даних, зазвичай шляхом натискання на шкідливе посилання чи відкриття шкідливого вкладення через телефон або електронну пошту [22].

Про масштаби цієї загрози свідчить і статистика. За різними оцінками, зловмисники щодня надсилають 3,4 мільярда шкідливих електронних листів, а Google блокує близько 100 мільйонів фішингових листів. За даними Cisco Umbrella, 46% атак на організації – це фішингові атаки, і 96% з них спрямовані на корпоративні електронні адреси (рис 2.1) [20].

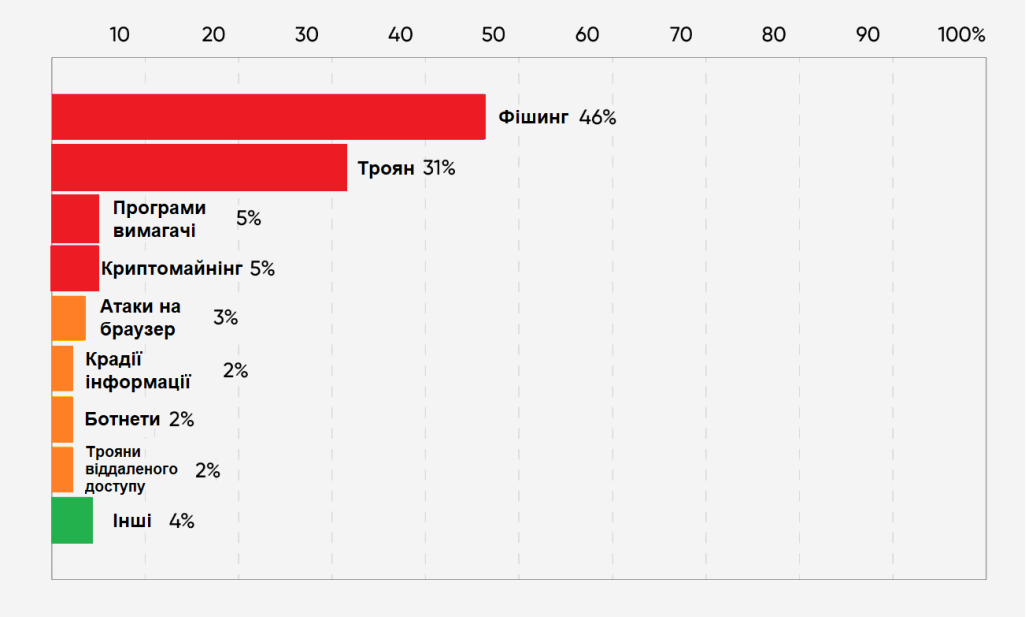

Рисунок 2.1 – Статистика кібератак

Види фішингу:

- Email фішинг – найпоширеніший і найефективніший метод. Зловмисники надсилають електронні листи, які виглядають легітимно (тобто насправді спрямовують користувачів на надійний веб-сайт або онлайн-ресурс), але насправді змушують одержувача поділитися конфіденційною інформацією. Повідомлення можуть містити посилання на підроблені веб-сайти або сервіси, які максимально точно копіюють оригінал. Фішинг зазвичай відбувається у великих масштабах.

Одним із видів шахрайства є цільовий фішинг. Він націлений на конкретну особу або організацію. У цьому випадку зловмисники можуть працювати більш ефективно, враховуючи спеціалізацію та інтереси своєї "мішені".

- Смішинг – це тип фішингової атаки, коли зловмисники отримують конфіденційну інформацію, змушуючи користувачів натиснути на шкідливе посилання в SMS-повідомленні. Нижче наведено приклад такого повідомлення, яке я отримав від невідомої мені людини.

На рис. 2.2 зображено повідомлення від невідомої особи, яка представляється відомим українським поштовим сервісом, інформує користувача про те, що виникла проблема з доставкою його посилки, і просить перейти за шкідливим посиланням.

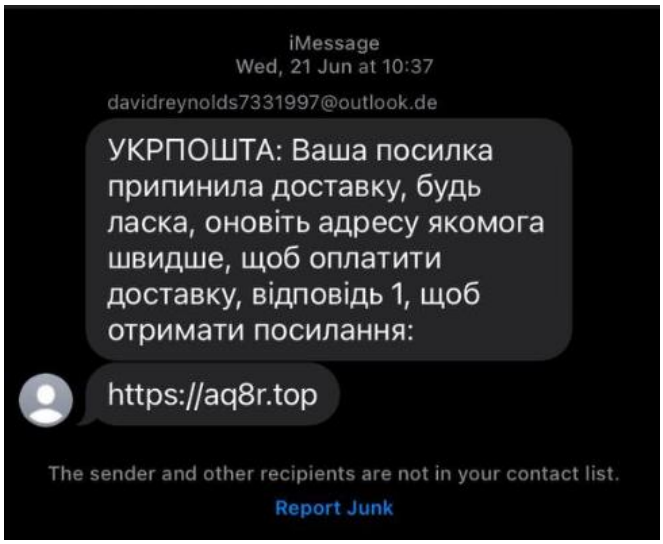

Рисунок 2.2 – Приклад смішингу

- Baiting – це техніка соціальної інженерії, в якій шахраї використовують маніпулятивні "повідомлення-приманки" (акції, лотерейні виграші, знижки на товари та послуги). Ці повідомлення спонукають людей до певних дій і допомагають зловмисникам отримати інформацію. Прикладами цієї техніки є такі повідомлення, як наведені нижче:

На рис. 2.3 зображено повідомлення від невідомої особи, яка інформує користувача про нібито створення нового облікового запису, надсилає логін і пароль до нього та повідомляє про суму на цьому обліковому записі, залишаючи шкідливе посилання. Повідомлення спрямоване на людську жадібність, тому що побачивши логін та пароль від облікового запису, на якому є велика сума грошей, значна більшість людей перейде за шкідливим посиланням в пошуку “легких грошей” [20].

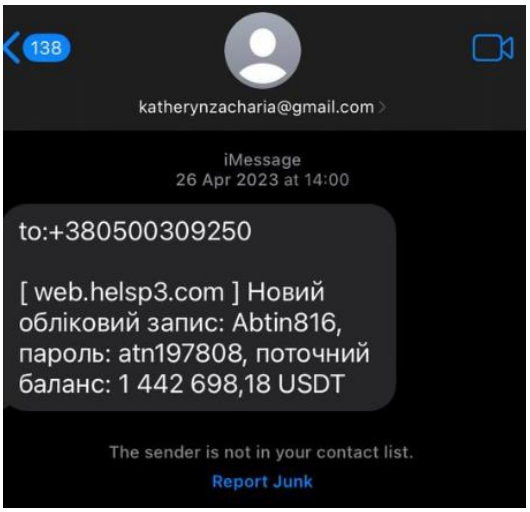

Рисунок 2.3 – Приклад фішингу

2.10 Боти та ботнети

Бот – це програмне забезпечення, яке виконує повторювані, автоматизовані та заздалегідь визначені завдання. Вони часто наслідують або замінюють поведінку людей та працюють набагато швидше, оскільки є автоматизованими. Боти можуть виконувати корисні функції, такі як обслуговування клієнтів чи індексація пошукових систем, або використовуватися для отримання повного контролю над комп’ютером як шкідливе програмне забезпечення. Такі програми можуть бути запрограмовані або взяті під контроль для зловживання обліковими записами користувачів, відправки спаму чи виконання інших шкідливих дій.

Слово "ботнет" походить від поєднання слів "робот" та "мережа". Ботнети складаються з великої кількості програмних агентів, кожен з яких керується віддалено. Ці агенти здатні діяти як єдине ціле та спілкуються з подібними машинами для виконання різноманітних завдань. Такі мережі часто використовуються для відправки спаму. Ботнет перебуває під контролем атакуючого та може представляти собою мережу тисяч зомбі-комп’ютерів або навіть сотень тисяч [22].

2.11 Dos та DDos атаки

Атаки типу "відмова у обслуговуванні" (DoS) – це кібератаки, під час

яких зловмисник виводить з ладу роботу комп'ютера, мережі або онлайн-сервісу за допомогою атаки з одного комп'ютера.

Існують два способи виконання атаки DoS: переповнення та відмова. Атаки переповнення відбуваються, коли сервер отримує занадто багато даних у буфері, що призводить до зупинки його роботи. Атаки з відмовою використовують вразливості системи жертви, щоб вимкнути її.

Розподілені атаки типу "відмова у обслуговуванні" (DDoS) виникають, коли декілька систем працюють разом, щоб надіслати координовану атаку DoS на одну ціль.

Головна відмінність полягає в тому, що замість того, щоб атакувати з одного місця, ціль атакується з багатьох місць одночасно (рис. 2.4) [23].

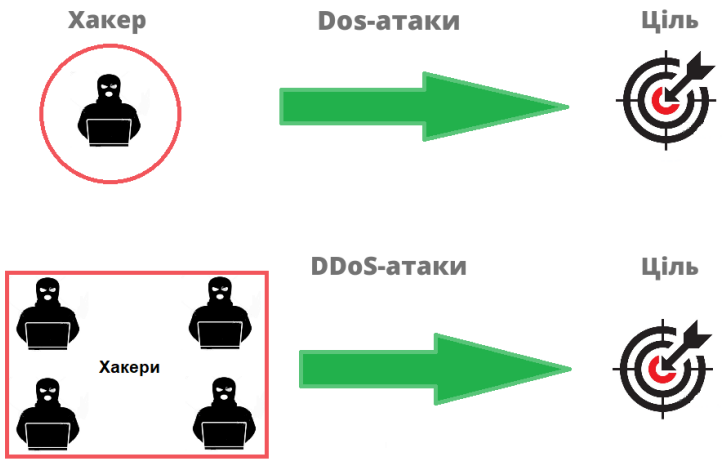

Рисунок 2.4 – Dos та DDos атаки

DDoS-атаки застосовуються частіше через такі переваги:

- Ці атаки можуть використовувати більше пристроїв для запуску потужної атаки.
- Оскільки атакуючі системи розподілені випадковим чином – іноді навіть по всьому світу – складно зрозуміти, звідки відбувається атака.
- Важко визначити справжніх зловмисників, оскільки вони приховуються за багатьма системами.

- Зі зростанням кількості пристроїв IoT у світі збільшується і кількість атак, оскільки зловмисники можуть використовувати їх як частину ботнетів.

Особливості DoS і DDoS-атак:

- Простота виявлення. Оскільки DoS надходить з одного місця, його походження легше виявити та відключити з'єднання. У випадку DDoS-атаки, що відбувається з декількох віддалених місць, важче визначити її походження.
- Швидкість атаки. З урахуванням того, що DDoS-атака відбувається з декількох місць, її можна запустити набагато швидше, ніж DoS-атаку, яку здійснюють з одного місця. Збільшена швидкість атаки ускладнює її виявлення, що означає збільшення завданого шкоди.
- Об'єм трафіку. DDoS-атака використовує декілька віддалених машин (зомбі або ботів) одночасно. Це означає, що вона здатна передавати великі обсяги трафіку з різних місць та швидко перевантажувати сервер.
- Спосіб виконання. DDoS-атака координує декілька хостів, заражених шкідливим програмним забезпеченням (ботами). У результаті вона створює ботнет, яким управляє командно-контрольний (C&C) сервер. У той же час DoS-атаку зловмисники зазвичай здійснюють з однієї машини [22].

2.12 Атаки на паролі

Це один із найпоширеніших видів атак у сфері кібербезпеки. Такі атаки можна спрямовувати як проти корпоративних, так і проти особистих цілей. Основна мета – здійснити заволодіння паролями до будь-яких областей, що потребують пароль, таких як соціальні мережі, технологічні сервіси або програмне забезпечення, використовуване користувачами чи організаціями. Зазвичай люди або організації обирають прості паролі, щоб не забути їх. Наприклад, користувачі соціальних мереж можуть розкривати частину інформації про свої паролі на своїх профілях. Ця інформація може включати улюблені команди, місце народження, дату народження, інформацію про

співмешканця або партнера та інші деталі, які стосуються особистого життя. Дані відомості є дуже цінними для кіберзлочинців, тому їх поширення може полегшити атаки на паролі [22].

3 ОГЛЯД ТА АНАЛІЗ ІСНУЮЧИХ МЕТОДІВ ЗАХИСТУ ВІД РІЗНИХ ТИПІВ КІБЕРАТАК

У сучасному цифровому світі, де інформація стала ключовим ресурсом, а комп’ютерні системи та мережі відіграють вирішальну роль у практично всіх сферах діяльності, питання кібербезпеки набуває надзвичайної важливості. Зростання залежності від технологій і використання цифрових платформ призводять до появи нових викликів і загроз для безпеки інформації.

Кібератаки набувають все більшої складності та вдосконаленості, використовуючи різні методи та техніки для злому захисту та отримання несанкціонованого доступу до даних та систем. У цьому контексті, існування ефективних методів захисту стає надзвичайно важливим завданням для забезпечення безпеки інформації, конфіденційності даних та недопущення можливих катастрофічних наслідків внаслідок кібератак.

У даному розділі буде детально розглянуто та проаналізовано різноманітні методи захисту від різних типів кібератак. Мета полягає у висвітленні ключових аспектів, стратегій та підходів до захисту інформації від широкого спектру загроз, що існують у сучасному цифровому середовищі. Буде висвітлено найбільш ефективні та передові підходи до кібербезпеки, спрямовані на забезпечення стійкості та надійності систем захисту в умовах постійно зростаючої загрози кібератак – від аналізу та оцінки існуючих методів захисту до розробки рекомендацій та рекомендованих практик.

3.1 Антивірусне програмне забезпечення

Це один із перших та основних методів захисту. Антивірусні програми допомагають виявляти та блокувати загрози, такі як віруси, черв’яки, троянські програми та інші шкідливі програми. Антивірусні програми використовуються для виявлення та видалення комп’ютерних вірусів. Віруси постійно

еволюціонують, що ускладнює їх виявлення антивірусними програмами, і навіть при регулярному використанні антивірусних програм неможливо гарантувати 100% безпеку.

Розробники антивірусів постійно вдосконалюють свої технології для боротьби з цим явищем, включаючи системи запобігання вторгненням на основі хостів: Hostbased Intrusion Prevention System (HIPS), пісочниці (Sandbox) та системи запобігання вторгненням на основі віртуальних середовищ: Virtual-based Intrusion Prevention System (VIPS). Ці технології дозволяють користувачам активно контролювати процеси в своїх системах і приймати рішення про доступ до різних функцій операційної системи.

Сьогодні проактивні методи захисту, такі як HIPS та Sandbox, стають все більш популярними. Ці дві технології активно інтегруються в найпопулярніше антивірусне програмне забезпечення: NOD32 та Антивірус Касперського, які використовують HIPS, та Avast Antivirus, який використовує Sandbox. Поєднання цих методів може значно підвищити ефективність антивірусної системи. Регулярне оновлення антивірусного ПЗ є ключовим аспектом забезпечення кібербезпеки. Це дозволяє уникнути нових загроз, захистити важливі дані та забезпечити надійність роботи комп’ютерної системи.

Ефективність оновлення антивірусного програмного забезпечення можна виразити у таких пунктах:

- Постійне оновлення для виявлення нових загроз:

Антивірусне програмне забезпечення постійно оновлюється, щоб виявляти та блокувати нові віруси, троянські програми, черв’яки та інші шкідливі програми. Кіберзлочинці постійно вдосконалюють свої методи, тому важливо, щоб ваш антивірус завжди був актуальним для ефективного захисту.

- Запобігання експлуатації вразливостей:

Оновлення антивірусного ПЗ допомагає запобігти експлуатації вразливостей в операційних системах та інших програмах. Багато вірусів та

шкідливого ПЗ використовують вразливості, щоб проникнути в систему, і актуальне антивірусне ПЗ допоможе їх блокувати.

- Оновлення сигнатур та аналізу поведінки:

Сигнатури в антивірусному програмному забезпеченні – це підписи, які використовуються для виявлення вірусів. Регулярні оновлення включають нові сигнатури для виявлення нових загроз. Також, антивіруси використовують аналіз поведінки, і оновлення допомагають покращити цей аспект виявлення загроз.

- Захист важливих даних і конфіденційності:

Оновлене антивірусне ПЗ допомагає захистити важливі дані, які можуть бути викрадені або пошкоджені шкідливими програмами. Це особливо важливо для корпоративних мереж та організацій, де зберігаються конфіденційні дані.

- Забезпечення надійності та продуктивності системи:

Оновлене антивірусне ПЗ допомагає підтримувати надійність і продуктивність комп’ютерної системи. Віруси та інші загрози можуть сповільнювати роботу системи, тому важливо, щоб антивірусний захист був завжди активним і оновленим [23].

3.2 Захист від атак соціальної інженерії та фішингових атак

Навіть за наявності найпотужніших систем кіберзахисту, ризик отримання зловмисниками доступу до конфіденційної інформації все одно існує. Все залежить від людського фактору. У більшості випадків шахраї не намагаються використовувати вразливості системи. Їхні дії спрямовані на людей, їхні слабкості, емоції, розгубленість та необережність. У цьому суть соціальної інженерії: маніпулюючи особливостями людської психології, хакери отримують потрібну їм інформацію.

Захист від атак соціальної інженерії вимагає комплексного підходу, який поєднує навчальні заходи для підвищення обізнаності співробітників з

технологічними рішеннями для посилення кібербезпеки. Великі підприємства повинні постійно адаптуватися до нових загроз і вдосконалювати свої стратегії захисту, щоб бути на крок попереду зловмисників.

- Навчальні програми

Тренінги з безпеки вчать співробітників розпізнавати спроби соціальної інженерії та реагувати на них. Симуляції атак соціальної інженерії (наприклад, фішингових кампаній) допомагають виявити вразливі місця та підготуватися до реальних загроз.

- Технічний контроль

- Застосування багатофакторної автентифікації (MFA) або впровадження підходів PAM, SSO або IAM значно ускладнює можливість несанкціонованого доступу до систем. Крім того, EDR може бути використаний для ефективного блокування шкідливого програмного забезпечення.

- Підвищення рівня фільтрації спаму через електронні поштові шлюзи дозволяє зменшити кількість успішних фішингових атак.

- Встановлення політик використання соціальних мереж обмежує можливості кіберзлочинців отримати доступ до інформації через ці платформи.

- Використання матриці рольового доступу до корпоративних цифрових ресурсів і сервісів компанії дозволяє ефективно керувати правами доступу користувачів.

- Використання парольних менеджерів і уникання зберігання конфіденційних авторизаційних даних на папері або незашифрованих носіях є важливими заходами для забезпечення безпеки.

- Політика і процедури

Це означає розробку та впровадження відповідних політик щодо основних процедур, які допомагають контролювати доступ до інформації та

ресурсів і таким чином зменшити ризик витоку даних. Необхідно створювати кодекси поведінки для обробки запитів на конфіденційну інформацію від третіх осіб та розповсюджувати їх серед усіх відповідних працівників.

- Залучення фахівців із кібербезпеки

Залучення зовнішніх фахівців з кібербезпеки для проведення незалежних аудитів та тестування безпеки, навчання персоналу та консультування щодо безпеки може допомогти отримати нові погляди на існуючі заходи безпеки та виявити можливі слабкі місця, які внутрішні команди організації могли упустити.

Захист від соціальної інженерії потребує не лише технічних заходів, але й культурних змін у сприйнятті кібербезпеки всередині компанії. Важливо створити середовище, де безпека є загальною відповідальністю всіх працівників. З огляду на ландшафт загроз, який постійно змінюється, компанії мають бути готові до швидкої адаптації своїх стратегій безпеки для ефективного протистояння атакам соціальних інженерів [20].

3.3 Криптографічні методи захисту від кібератак

Криптографічні методи захисту інформації – це спеціальні техніки шифрування, кодування або інших перетворень даних, що роблять їх незрозумілими без володіння відповідним ключем або методом дешифрування.

Криптографічний захист інформації є одним з найбільш надійних методів, оскільки він захищає самі дані, а не просто доступ до них (наприклад, зашифрований файл залишається незрозумілим, навіть, якщо носій буде вкрадено). Цей метод захисту реалізується за допомогою програм або наборів програм [11].

Криптографічний алгоритм, відомий як шифрувальний алгоритм, представляє собою математичну функцію, яка використовується для зашифрування та розшифрування даних. Цей алгоритм складається насправді

з двох різних функцій: одна призначена для зашифрування, а інша для розшифрування.

Існують два основних типи шифрування:

1) Симетричне шифрування, яке використовує загальний (секретний) ключ.

2) Асиметричне шифрування, відоме також як шифрування з відкритим ключем.

У симетричному шифруванні створюється ключ, який потім використовується для шифрування файлу. Після шифрування файлу його разом з ключем передають адресатові, а сам ключ передається окремо через безпечний канал зв’язку.

У випадку асиметричного шифрування, яке є більш складним, використовуються два ключі: відкритий і закритий. Одержувач повідомляє про свій відкритий ключ всім, хто бажає відправити йому зашифроване повідомлення. Закритий ключ залишається тільки у власника повідомлення. При використанні асиметричного шифрування, відправник використовує відкритий ключ одержувача для зашифрування повідомлення. При отриманні повідомлення, одержувач розшифровує його за допомогою свого закритого ключа. Хоча асиметричне шифрування є надійнішим, його використання може займати більше часу через складність обчислень, порівняно з симетричним шифруванням.

У сучасний період найбільш ефективним методом шифрування є AES (Advanced Encryption Standard). На даний момент, цей метод доступний у трьох варіантах – AES128, AES192 і AES256. Кожен з цих варіантів має свої особливості в застосуванні: AES128 використовується частіше для захисту інформації на мобільних пристроях, в той час як AES192 і AES256 використовуються на більш високих рівнях безпеки.

Цей стандарт був офіційно запроваджений у 2002 році і отримав

підтримку від компанії Intel, яка виробляє процесорні чіпи. Основна ідея AES полягає у використанні поліноміального подання кодів та операцій обчислення з двовимірними масивами, що відрізняє його від інших симетричних методів шифрування.

За даними уряду США, для того щоб зламати 128-бітний AES ключ, навіть найпотужнішому дешифратору знадобиться приблизно 149 трильйонів років. Однак, варто зауважити, що з розвитком комп'ютерної техніки за останні роки, час, потрібний для злому, може значно зменшитись.

Існує кілька способів здійснення криптографічного захисту: апаратний, програмний та програмно-апаратний. Апаратна реалізація криптографічного захисту вважається найбільш надійною, але водночас і найдорожчим методом. У цьому випадку інформація передається в електронній формі через порт обчислювальної машини всередину апаратної системи, де відбувається шифрування.

Проте, існує ризик перехоплення та підробки інформації під час передачі в апаратуру, який може бути здійснений за допомогою спеціально розроблених програм типу "вірусів". Програмна реалізація криптографічного захисту є дешевшою та більш гнучкою в реалізації, але вимагає додаткових заходів для захисту криптографічних ключів від перехоплення під час роботи програми та після її завершення.

Одним із способів захисту від "вірусних" атак є забезпечення повного звільнення пам'яті від криптографічних ключів, що використовувалися під час роботи програми, через механізми "збирання сміття". Також можна використовувати комбінацію апаратних і програмних механізмів криптографічного захисту, де програмна реалізація криптоалгоритмів поєднується з апаратним зберіганням ключів. Цей спосіб криптозахисту є досить надійним і не вимагає великих витрат. Однак, при виборі апаратних засобів для зберігання ключів, необхідно дбати про захист від перехоплення

під час їх зчитування з носія та використання в програмі.

Апаратне шифрування має кілька переваг порівняно з програмним, і це можна пояснити декількома причинами. По-перше, апаратна реалізація криптографічного захисту забезпечує більшу швидкість. Криптографічні алгоритми складаються з великої кількості складних операцій, які виконуються над бітами відкритого тексту. Універсальні комп'ютери мають обмежені можливості для ефективного виконання цих операцій, тоді як спеціалізоване обладнання здатне робити це набагато швидше.

По-друге, апаратуру шифрування легше фізично захистити від проникнення ззовні. Програми, які виконуються на персональних комп'ютерах, мають вразливості щодо змін, які можуть бути внесені зловмисниками за допомогою відладчиків, і ці зміни можуть залишитися непоміченими.

По-третє, встановлення апаратного шифрування є більш простим. У багатьох випадках, де потрібне шифрування, додаткове обчислювальне обладнання може бути зайвим. Апаратне шифрування можна легше впровадити в пристрої, такі як телефони, факси і модеми, порівняно з вбудовуванням в них програмного забезпечення. Навіть у випадку комп'ютерів, встановлення спеціалізованого шифрувального обладнання створює менше проблем, ніж модернізація програмного забезпечення для додавання функцій шифрування даних.

Шифрування даних розвивається дуже швидко, і технології постійно модифікуються для забезпечення надійності та ефективності. Наприклад, розглядаючи різні методи шифрування, можна зазначити гомоморфне шифрування, яке дозволяє виконувати операції додавання та множення над зашифрованими даними без їх попереднього розшифрування. Цей метод, хоча є новим, вже показав свої переваги, але його необхідно подальше вдосконалювати, щоб забезпечити високу стійкість та ефективність захисту

інформації. Також, пристрої апаратного шифрування з USB-інтерфейсом, які використовують малопотужні мікроконтролери, є цікавим напрямком для дослідження та вдосконалення, особливо у галузях з обмеженими ресурсами [12].

3.4 Захист від Dos та DDoS атак

Більшість DDoS-атак становлять небезпеку через свою абсолютну прозорість і “нормальність”. Це явище майже рутинне, оскільки, якщо помилку в програмному забезпеченні завжди можна виправити, то повне виснаження ресурсів є майже нормою. Багато адміністраторів стикаються з цим, коли ресурси машини (швидкість каналу) стають недостатніми або веб-сайт стає жертвою “slashdot effect” (“ефект /” – потужний сплеск відвідуваності веб-сайту, зазвичай невеликого, після того, як посилання на цей ресурс з’являлося на стрічці новин популярного мережевого видання або блогу). Термін, та й саме явище, з’явилися завдяки популярному інформаційному технологічному блогу Slashdot. Однак, якщо обмежити трафік і ресурси для всіх підряд, то можна захиститися від DDoS, але це призведе до втрати значної частини клієнтів [14].

Виходу з цієї ситуації практично немає, проте наслідки DDoS-атак і їхню ефективність можна значно знизити за допомогою правильного налаштування маршрутизатора, брандмауера і постійного моніторингу аномалій в мережевому трафіку.

Існують два типи атак DoS/DDoS, і найпоширеніший з них ґрунтується на концепції “Flood”, що означає завалення жертви великою кількістю пакетів. Flood може приймати різні форми, такі як ICMP, SYN, UDP і HTTP. Сучасні боти DoS можуть використовувати усі ці види атак одночасно, тому важливо передбачити належний захист від кожного з них заздалегідь.

- ICMP-flood

Цей метод полягає у навантаженні каналу і створенні навантаження на

мережевий стек шляхом постійних запитів ICMP ECHO (пінг). Його легко виявити, аналізуючи потоки трафіку в обидва боки: під час атаки типу ICMP-flood вони майже ідентичні. Є досить простий спосіб повного захисту, що ґрунтується на блокуванні відповідей на запити ICMP ECHO:

- #sysctl net.ipv4.icmp_echo_ignore_all=1;
- або використовуючи брандмауер: #iptables -A INPUT -p icmp -j DROP --icmp-type 8".

- SYN-flood. Цей метод атаки не лише переповнює канал зв’язку, але й вводить мережевий стек операційної системи в стан, коли він більше не може приймати нові запити на підключення. Ця атака ґрунтується на намаганні ініціювати велику кількість одночасних TCP-з’єднань через надсилання SYN-пакетів з неіснуючою зворотньою адресою. Після кількох спроб надіслати ACK-пакет на недоступну адресу, багато операційних систем ставлять невстановлені з’єднання у чергу. Тільки після n-тої спроби вони закривають з’єднання. Оскільки потік ACK-пакетів дуже великий, черга швидко заповнюється, і ядро відмовляє у спробах відкрити нове з’єднання. Розумні DoS-боти також аналізують систему перед атакою, щоб надсилати запити тільки на відкриті життєво важливі порти. Цю атаку легко виявити, спробувавши підключитися до одного з сервісів. Оборонні заходи зазвичай включають:

- збільшення черги "напіввідкритих" TCP-з’єднань:

sysctl -w net.ipv4.tcp_max_syn_backlog=1024;

- зменшення часу очікування відповіді "напіввідкритих" з’єднань:

sysctl -w net.ipv4.tcp_synack_retries=1;

- включення механізму TCP syncookies:

sysctl -w net.ipv4.tcp_syncookies=1;

- обмеження максимальної кількості "напіввідкритих" з’єднань з одного IP до конкретного порту:

iptables -i INPUT -p tcp --syn --dport 80 -m iplimit --iplimit-above 10 -j DROP.

- UDP-flood

Цей тип атаки характеризується безкінечним надсиланням UDP-пакетів на порти різних UDP-сервісів з метою перевантаження смуги пропускання. Його легко зупинити, обмеживши кількість з'єднань до DNS-сервера зовнішнього світу та встановивши ліміт на кількість з'єднань за одиницю часу:

- iptables -i INPUT -p udp --dport 53 -j DROP -m iplimit --iplimit-above 1.

- HTTP-flood

Це один із найпоширеніших способів Flood на сьогоднішній день. Він полягає у безкінечному надсиланні HTTP-запитів GET на порт 80 з метою завантажити веб-сервер так, щоб він був не в змозі обробляти всі запити. Переважно ціллю атаки не є кореневий каталог веб-сервера, а скрипти, які виконують ресурсозатратні завдання або працюють з базою даних. Для боротьби з HTTP-flood важливо налаштувати веб-сервер та базу даних для зменшення впливу атаки і відсіювати DoS-ботів за допомогою різних заходів.

Переважно, необхідно збільшити максимальну кількість одночасних з'єднань до бази даних і використати перед веб-сервером Apache легкий і продуктивний nginx, який буде кешувати запити і видачу статичних файлів [15].

3.5 Штучний інтелект як метод захисту від кібератак

Щоб протистояти кіберзагрозам, організації звертаються до кваліфікованих груп кібербезпеки, які використовують передові технології, насамперед штучний інтелект (ШІ), який швидко виявляє та протидіє шкідливій діяльності та зміцнює мережу від загроз.

Визнання потенціалу штучного інтелекту призвело до того, що 76% компаній надають пріоритет штучному інтелекту та машинному навчанню у

своїх IT-бюджетах через величезну кількість даних, які необхідно проаналізувати для ефективного виявлення та протидії кіберзагрозам.

Оскільки прогнозується, що до 2025 року підключені пристрої генеруватимуть надзвичайно великі обсяги даних обсягом понад 79 дзета-байт, ручний людський аналіз стає неефективним, а штучний інтелект став важливим інструментом у боротьбі з кіберзлочинністю.

Згідно зі звітами, ринок кібербезпеки штучного інтелекту досяг 170 мільярдів фунтів стерлінгів у 2022 році та досягне вражаючої цифри 1020 мільярдів фунтів стерлінгів до 2032 року. Ці дані не здаються дивними, оскільки хакери також використовують нові технології для злочинної діяльності.

Зростаюча частота кібератак привернула увагу до потенційного використання штучного інтелекту в кібербезпеці. Згідно з опитуванням Economist Intelligence Unit, 48,9% керівників та експертів з безпеки у всьому світі вважають, що штучний інтелект та машинне навчання є потужними інструментами протидії сучасним кіберзагрозам. Крім того, у звіті Pillsbury підкреслюється, що 44% організацій по всьому світу вже використовують штучний інтелект для виявлення порушень безпеки.

У сфері кібербезпеки штучний інтелект створює безпечні програми за замовчуванням та усуває вразливості користувачів. Очищаючи негативні параметри за замовчуванням, штучний інтелект забезпечує конкретну точність питання, прискорює пошук і автоматизує механізм відповіді. Рішення на основі штучного інтелекту, такі як автентифікація користувачів за допомогою поведінкової біометрії, сприяють безпечній розробці застосунків та створюють безпечну екосистему даних, яка сприяє надійній інфраструктурі.

Штучний інтелект виявляє потенційно шкідливі дії та загрози, дозволяючи організаціям прогнозувати та запобігати кібератакам до того, як вони відбудуться. Завдяки автоматичному моніторингу на основі штучного інтелекту система захищена 24 години на добу, і організації можуть вживати активних

заходів для захисту своїх цифрових активів від шкідливих наслідків.

Складність кіберзагроз, таких як соціальна інженерія та програми-вимагачі, робить покращення кібербезпеки надзвичайно важливими, оскільки організації мають справу з великими обсягами даних, які потребують аналізу для виявлення потенційних ризиків через традиційні методи захисту для виявлення та запобігання таким атакам. Впровадження інноваційних рішень є невід'ємною частиною ефективної боротьби з цими загрозами.

- Зниження витрат. Автоматизація, що забезпечується штучним інтелектом, дозволяє знизити витрати в різних областях кібербезпеки. Штучний інтелект автоматизує рутинні завдання, такі як аналіз журналів, оцінка вразливостей та управління виправленнями, зменшуючи потребу в ручній роботі та заощаджуючи дорогоцінний час та людські ресурси.

Точність виявлення загроз, що забезпечується штучним інтелектом, також може допомогти зменшити витрати. Традиційні підходи до кібербезпеки можуть подавати помилкові сигнали або пропускати певні загрози, що може призвести до того, що час і ресурси будуть витрачені на вирішення неіснуючих проблем, а реальні випадки кіберзлочинності будуть пропущені.

- Підвищена масштабованість. Традиційні технології кібербезпеки часто відчувають труднощі з обробкою великих обсягів даних, що генеруються в складних підключених середовищах. Штучний інтелект характеризується масштабованістю, яка дозволяє йому одночасно обробляти та аналізувати великі обсяги даних з різних джерел. Алгоритми штучного інтелекту можуть ефективно аналізувати журнали мережевого трафіку, системні журнали, поведінку користувачів та інформацію про загрози. Завдяки такій масштабованості штучний інтелект виявляє тонкі ознаки кіберзагроз, які можуть уникнути уваги людських аналітиків, і забезпечує розширений рівень захисту.

До найбільш небезпечних загроз належать вимагання, соціальна інженерія, відмова в обслуговуванні або розподілена відмова в обслуговуванні (DoS, DDoS),

особливо ті, що впливають на ланцюжок поставок.

Загроза кіберзлочинності змусила злочинців використовувати нові тактики і технології, знизивши поріг для кібератак. Зараз кіберзлочинці пропонують послуги підписки та комплекти для початківців, тому проблеми кібербезпеки зростають. Використання великої мовної моделі, такої як ChatGPT, для написання шкідливого коду підкреслює потенційні ризики в цифровому середовищі.

Однією з відмінностей штучного інтелекту є здатність постійно вчитися та адаптуватися. Системи штучного інтелекту постійно отримують новий досвід роботи з даними, щоб підтримувати гнучкість і покращувати можливості виявлення і реагування на загрози.

За даними Forbes, 76% компаній вже включили штучний інтелект і машинне навчання в свої IT-бюджети, що свідчить про широке визнання цінності цих технологій. Деякі важливі переваги використання штучного інтелекту в кібербезпеці включають:

- Використання: виявлення та запобігання загрозам однією з сильних сторін штучного інтелекту є його здатність виявляти загрози. Він аналізує великі обсяги даних з різних джерел і розпізнає ненормальні моделі поведінки користувачів, які можуть вказувати на кібератаку. Наприклад, якщо працівник натискає фішинговий електронний лист, штучний інтелект може виявити цю зміну та своєчасно повідомити про потенційні загрози безпеці. При виявленні потенційної загрози система на основі штучного інтелекту відправляє тривожне повідомлення в службу безпеки, забезпечуючи швидкий і ефективний відповідь. Штучний інтелект знижує ризик атак і обмежує можливі наслідки кібер-залякування шляхом автоматизації дій з реагування на інциденти, таких як ізоляція вразливих систем або блокування шкідливих дій [17].

ВИСНОВКИ

Ця робота узагальнює проблеми та рішення в галузі кібербезпеки на основі останніх технологічних досягнень. Для надання детальної інформації про кібербезпеку, роботу поділено на три розділи: основи та історія кібербезпеки та кібератак; огляд та аналіз впливу різних типів кібератак на рівень інформаційної безпеки користувачів, огляд та аналіз існуючих методів захисту від різних типів кібератак. Цей поділ важливий для розуміння основних компонентів кібератак та для надання комплексних рішень для проблем безпеки.

У розділі основ та історії кібербезпеки та кібератак перераховані технічні та нетехнічні причини, які спричиняють зростання кібератак. Кібератаки є динамічними і впливають на всі комп'ютерні системи та середовище Інтернету, змінюючи формат атак та цільову аудиторію. Перенесення соціального життя до Інтернет-середовища збільшує кількість кібератак та їх руйнівний вплив. Помилки та вразливості в програмному забезпеченні, недоліки мережевих протоколів, збільшення кількості пристроїв, підключених до мережі, та складність критичних систем збільшують ризики кібербезпеки. Крім того, віртуалізація соціального життя, надмірне використання соціальних мереж, збільшення знань зловмисників та необережне використання Інтернету також підвищують ризики безпеки в цифровому світі.

У розділі про огляд та аналіз впливу різних типів кібератак на рівень інформаційної безпеки користувачів пояснюються основні компоненти стратегій атак, які використовують вразливості системи та сторонніх програм для експлуатації. Кібератаки використовують добре підготовлені зловмисні кодові блоки для експлуатації вразливостей комп'ютерних систем.

Розповсюджені зловмисне програмне забезпечення (віруси, черви, rootkit'и, вимагання викупу тощо), інструменти взлому, атаки на застосунки, атаки на доступ, криптографічні атаки, DoS та DDoS атаки, «людина посередині», фішинг – можна визначити як типові загрози та атаки в галузі кібербезпеки. Нещодавно з'явилися інструменти атак в Інтернеті, що обслуговують кібератаки. Це збільшує кількість атак і ускладнює процеси виявлення.

Показано загальні атаки на кожному рівні та потенційні рішення для повного розуміння мережевої безпеки. Атаки, як правило, спрямовані на протоколи певного рівня для успішності. Мережеві атаки можна класифікувати за рівнями: атаки на фізичний рівень (прослуховування), атаки на рівень даних (фальсифікація: MAC, ARP та ін.), атаки на мережевий рівень («людина посередині»), атаки на рівень транспорту (розвідка), атаки на сеансовий рівень (захоплення), атаки на рівень представлення (фішинг) та атаки на рівень додатків (експлойти). Основні причини успішності атак виникають через вразливості в мережевих протоколах та неправильну конфігурацію мережевих пристроїв. Ці протоколи можна перерахувати як ARP, DNS, DHCP, FTP, ICMP, IP, TCP, UDP і т.д. Наприклад, при передачі пакетів по мережі, за допомогою протоколу IP, відсутній механізм контролю точності та конфіденційності цих пакетів. Тому інформація в пакетах може бути розкрита та змінена під час їх передачі. Так само, оскільки відповіді DNS не перевіряються, користувачі підключаються до серверів, створених зловмисниками, замість фактичного сервера. Існуючі вразливості протоколів мають бути зменшені, повинні додаватися нові протоколи, а мережеві пристрої повинні бути налаштовані правильно та повністю для захисту даних під час їх переміщення через комп'ютерні мережі.

Для ефективного захисту комп'ютерної системи від зловмисників необхідно співпрацювати фахівцям з кібербезпеки, організаціям, розробникам програмного забезпечення та країнам для надання широкого захисту. У цьому

контексті рішення можна розділити на технічні та нетехнічні. При розгляді кібератак важливими є: адміністративно-базове управління, політики, стандарти, процедури, оцінка ризиків, управління постачальниками, призначені відповідальності та навчання, що є критичними нетехнічними концепціями. Навіть, якщо фахівці з кібербезпеки створюють найкращу систему захисту, належного захисту не буде, якщо користувачі цієї системи недостатньо підготовлені.

Технічні рішення використовують технологічні досягнення та науку для створення розумних застосунків для боротьби зі зловмисниками. Технічні рішення можна розділити на три групи: технології та платформи, використані інструменти та застосування штучного інтелекту та науки про дані. Криптографія захищає цілісність та конфіденційність даних. Контроль доступу обмежує доступ до даних, що підвищує рівень безпеки. Великі дані дозволяють аналізувати великі обсяги даних для виявлення невідомих патернів та зловмисних ознак атак. Техніки віртуалізації відокремлюють програмні застосунки від апаратних компонентів, що підвищує їх придатність та знижує вартість, а також скорочує час простою у разі кібератак. Обчислювальна хмара надає активне управління загрозами, високий рівень безпеки даних, масштабованість, високу доступність та ефективне відновлення даних. Технологія блокчейн допомагає перевіряти консистентність даних та виявляти деякі складні атаки. Статистичні методи допомагають інтерпретувати та виявляти патерни в даних. Видобуток даних виявляє та виділяє невідомі патерни в великих наборах даних. Техніки машинного навчання допомагають додавати нові функції до існуючих систем виявлення атак. Крім того, ці інноваційні технології машинного навчання покращують інтелект систем виявлення в обличчі останніх кібератак.

Незважаючи на те, що зазначені технічні досягнення значно покращують можливість виявлення порушень даних, виявлення вразливостей у

комп’ютерних системах та мережах зв’язку, а також підвищують точність систем виявлення атак, все ще є деякі виклики для ефективного виявлення нових та складних кібератак. Ці виклики полягають в тому, що складність атак зростає, атаки стають автоматизованими завдяки кібератакам як послугам, інтелектуальні атаки обходять системи виявлення, алгоритми на основі машинного навчання роблять припущення про дані, що містять упередження, класифікація мільйонів мережевих з’єднань є складною, робота з високовимірними даними є складною, захист кількох компонентів виявляється складним, і безпека часто перетворюється на людський фактор.

ПЕРЕЛІК ВИКОРИСТАННИХ ДЖЕРЕЛ

1. Ю. В. Завгородня. Історія становлення кібервійни як складової політичного процесу. – Crossref. – Листопад 2023. – 72. – 42-46 с. – Режим доступу: https://doi.org/10.32782/app.v72.2023.6.

2. Історія кібербезпеки: від зародження ідеї до наших днів. [Електронний ресурс]. – Режим доступу: https://www.education.ua/blog/48055/.

3. The History of Cyber Security: A Detailed Guide [Infographic] [Електронний ресурс]. – Режим доступу: https://www.knowledgehut.com/blog/security/history-of-cyber-security.

4. Кібератака. [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/Кібератака.

5. Р. В. Бараненко. Кібератаки як одна з форм кібертероризму. – Інформатика, обчислювальна техніка та автоматизація. 2021. – 32(71). – 45-50 с. – Режим доступу: https://doi.org/10.32838/2663-5941/2021.1-1/07.

6. Yuchong Li. A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. /Yuchong Li, Qinghui Liu. – Energy Reports, 2021. – November 2021. – 7. – 8176-8186 pp. – Режим доступу: https://doi.org/10.1016/j.egyr.2021.08.126.

7. Omer Aslan A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. / Omer Aslan, Semih Serkant Aktug, Merve Ozkan Okay, Abdullah Asim Yilmaz. – Electronics – March 2023. – 12(6). – 1-42 pp. – Режим доступу: https://doi.org/10.3390/electronics12061333.

8. Андрій Лисюк. Огляд сучасних кібератак та методів протидії. // Кибезагрози для України в глобалізованому світі. – Травень 2013. – [Електронний ресурс]. – Режим доступу: https://www.slideshare.net/slideshow/20130531-andriylysyuk-cyberthreats/22244263.

9. Кібербезпека: актуальні загрози та методи захисту. [Електронний ресурс]. – Режим доступу: https://lemon.school/blog/kiberbezpeka-aktualni-zagrozy-ta-metody-zahystu.

10. Актуальні проблеми сучасної науки і правоохоронної діяльності.– Режим доступу: https://univd.edu.ua/general/publishing/konf/26_11_2019/pdf/89.pdf.

11. Криптографічні методи захисту інформації. Контроль цілісності програмних та інформаційних ресурсів. [Електронний ресурс]. – Режим доступу: https://classmill.com/659/112/m/xnb7A.

12. Іванов Р.Є. Використання криптографічних методів для захисту даних у ПК. / Іванов Р.Є., Писаренко Л.Д // Перспективні напрямки сучасної електроніки (19-20 квітня 2018). – 2018. – 65-69 с. – Режим доступу: https://ed.kpi.ua/wp-content/uploads/conferences/2018/2018-065-069.pdf.

13. Найкращі методи запобігання та захисту від DDOS-атак. [Електронний ресурс]. – Режим доступу: https://iitd.com.ua/news/najkrashhi-metodi-zapobigannja-ta-zahistu-vid-ddos-atak/.

14. Методи боротьби з Dos або DDos атаками. [Електронний ресурс]. – Режим доступу: https://wiki.tntu.edu.ua/Методи_боротьби_з_Dos_або_DDos_атаками.

15. DoS-атака. [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/DoS-атака.

16. Роль штучного інтелекту в кібербезпеці: передбачення та запобігання атакам. [Електронний ресурс]. – Режим доступу: https://eba.com.ua/rol-shtuchnogo-intelektu-v-kiberbezpetsi-peredbachennya-ta-zapobigannya-atakam/.

17. Корпоративна кібербезпека: Роль ШІ у захисті даних. [Електронний ресурс]. – Режим доступу: https://www.bdo.ua/uk-ua/insights-2/information-materials/2024/corporate-cybersecurity-ai-role-in-data-protection.

18. AI in Cyber Security: Pros and Cons, and What it Means for Your Business.

[Електронний ресурс]. – Режим доступу: https://www.terranovasecurity.com/blog/ai-in-cyber-security.

19. AI in Cybersecurity: Exploring the Top 6 Use Cases. [Електронний ресурс]. – Режим доступу: https://www.techmagic.co/blog/ai-in-cybersecurity/.

20. Фішинг допомагає маніпулювати людьми заради даних. Як захиститися від кіберзагроз. [Електронний ресурс]. – Режим доступу: https://www.gen.tech/post/sho-take-socialna-ingeneria#:~:text=Email%20фішинг%20(англ.,змушують%20одержувача%20поділитися%20конфіденційною%20інформацією.

21. A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks and Solutions. [Електронний ресурс]. – Режим доступу: https://www.researchgate.net/publication/369186216_A_Comprehensive_Review_of_Cyber_Security_Vulnerabilities_Threats_Attacks_and_Solutions.

22. Антивірусний захист локальної мережі як засіб боротьби з правопорушеннями в кіберпросторі. [Електронний ресурс]. – Режим доступу: https://univd.edu.ua/general/publishing/konf/26_11_2019/pdf/89.pdf.

23. DoS проти DDoS-атак — що це таке та як від них захиститися. [Електронний ресурс]. – Режим доступу: https://gigatrans.ua/ua/news/dos-protiv-ddos-atak-v-chem-raznica-i-kak-ot-nih-zash-ititsya

ДОДАТОК А

ISSN 2519-2310 CS&CS, Issue 2(24) 2023

УДК 004.056.5

ВПЛИВ РІЗНИХ ФОРМ КІБЕРЗАГРОЗ НА СТІЙКІСТЬ ІНФОРМАЦІЙНИХ СИСТЕМ: АНАЛІЗ ТА СТРАТЕГІЇ ЗАХИСТУ

Євген Осадчий[1], Марина Єсіна[1,2], Віктор Онопрієнко[2]

[1] Харківський національний університет імені В.Н. Каразіна, майдан Свободи, 4, Харків, 61022, Україна
xa12850357@student.karazin.ua, m.v.yesina@karazin.ua
[2] АТ «Інститут Інформаційних технологій», вул. Коломенська 15, Харків, 61166, Україна
v25258@gmail.com

Надійшла: Грудень 2023. Прийнята: Грудень 2023.

Анотація: *Дана робота присвячена дослідженню проблематики кібербезпеки в контексті сталого розвитку сучасного інформаційного суспільства. Починаючи з огляду різноманітних форм кіберзагроз, у статті запропоновано аналіз їхнього впливу на конфіденційність, цілісність та доступність інформації. Критична залежність сучасного суспільства від інформаційних технологій, робить тематику захисту від кіберзагроз надзвичайно актуальною. В межах роботи запропоновано аналіз зростання кількості та складності кіберзагроз, що вимагає постійного удосконалення та оновлення стратегій захисту від них. Важливим етапом висвітлення теми є аналіз впливу різних форм кіберзагроз на сучасні інформаційні системи. Розглянуто основні різновиди фішингу та соціальної інженерії, а також наслідки впливу вірусів, троянських програм та інших шкідливих програм. Детальний огляд цих аспектів дозволяє визначити ключові питання та небезпеки, які виникають в контексті проблематики кіберзагроз. Також, стаття містить матеріали, присвячені різним стратегіям захисту. Вона розглядає існуючи стратегії для захисту інформаційних систем, включаючи виявлення вразливостей, використання багатофакторної автентифікації та заходи для забезпечення стійкості. Загальні висновки даної роботи підсумовують необхідність постійного оновлення та адаптації стратегій захисту, щодо зростаючої складності кіберзагроз у світі швидкого технологічного розвитку. В цілому, дана робота є ще одним кроком у розумінні сутності викликів, які пов'язані із проблематикою забезпечення кібербезпеки в сучасному інформаційному суспільстві.*

Ключові слова: *кіберзагроза, аналіз та захист, стійкість інформаційних систем, стратегії захисту.*

1. Вступ

У сучасному інформаційному суспільстві питання кібербезпеки стають надзвичайно актуальними, оскільки з кожним днем зростає обсяг цифрової активності та залежність від інформаційних технологій. Разом із швидким розвитком технологій зростає і рівень кіберзагроз, які стають важливим аспектом забезпечення безпеки в Інтернет просторі. Ці загрози викликають серйозні проблеми, а також стають причиною порушення конфіденційності, цілісності та доступності інформації. У межах цієї роботи в стислому вигляді розглянуті різноманітні форми кіберзагроз та їхній вплив на сучасні інформаційні системи (ІС), а також можливі заходи для захисту від них в умовах постійно зростаючого цифрового середовища.

Актуальність теми зумовлена впливом відразу кількох ключових аспектів. По-перше, інформаційні технології стали не тільки необхідною частиною повсякденного життя, але і критично важливим ресурсом для функціонування великої кількості суспільних, комерційних та господарських процесів. По-друге, зростання залежності від цих технологій відкриває нові можливості для кіберзлочинців, які використовують різноманітні та вдосконалені методи для атак на ІС. Забезпечення надійності і безпеки ІС стає надзвичайно важливим завданням, оскільки кіберзагрози, такі як атаки на мережеві структури, витоки конфіденційної інформації та шкідливі програми, можуть мати серйозні наслідки для економіки, політики та суспільної безпеки. У цьому контексті розуміння різних форм кіберзагроз та їхнього впливу стає стратегічно важливим для розробки ефективних заходів захисту, що відповідають викликам сучасного інформаційного простору.

Зростання кількості та складності кіберзагроз стає серйозним викликом для сфери кібербезпеки. Різноманітність атак, включаючи витончені техніки фішингу, атаки з використанням шкідливого програмного забезпечення (ПЗ) та атаки на інфраструктуру, свідчать, що кі-

ISSN 2519-2310 CS&CS, Issue 2(24) 2023

берзлочинці постійно вдосконалюють свої методи, адаптуючись до новітніх технологій та змін у сфері кібербезпеки [1]. Неперервний розвиток кіберзагроз вимагає не лише реактивних, але й проактивних стратегій захисту. Організації та індивіди, що прагнуть залишатися попереду, повинні не лише оновлювати свої системи та ПЗ, але й розвивати нові методи виявлення та запобігання кібератак. Важливість цього завдання зумовлена тим, що відповідальність за захист ІС стає не тільки завданням технічних спеціалістів, але й ключовою складовою стратегічного управління будь-якою організацією чи державною установою. У цьому контексті огляд різних форм кіберзагроз та їхнього впливу стає невід'ємною частиною ефективного й безпечного управління, спрямованого на забезпечення стабільності та надійності функціонування сучасних ІС.

Проведення аналізу впливу кіберзагроз на стійкість ІС є невід'ємною частиною вдосконалення стратегій кібербезпеки в умовах постійного еволюційного середовища [2]. З урахуванням стрімкого розвитку технологій та збільшення кількості цифрових аспектів нашого життя, зростає і сфера кіберзагроз, що накладає серйозний вплив на ІС.

Ця стаття має на меті розглянути проблематику кібербезпеки в контексті сучасних реалій й пропонує оглядовий аналіз різноманітних різновидів кіберзагроз, який охоплює їх вплив на конфіденційність, цілісність та доступність інформації. Зокрема, надаючи огляд найновіших тенденцій у сфері кібербезпеки, автори роботи мають на меті виокремити ключові аспекти безпеки, що піддаються ризику внаслідок сучасних кібератак.

Важливим етапом у запропонованому аналізі є визначення різних стратегій захисту, які спроможні ефективно відповідати викликам безпеки сучасного кіберпростору. Слід під креслити, що розглянуті стратегії враховують, як технічні, так і стратегічні аспекти, котрі спрямовані на удосконалення стійкості сучасних ІС та забезпечення їхньої функціональності в умовах постійного впливу широкого спектру загрози інформаційної безпеки (ІБ).

2. Різновиди кіберзагроз та їх вплив на ІС

2.1 Фішинг та соціальна інженерія

Фішинг та соціальна інженерія стали неодмінною частиною сучасного цифрового простору, ставши важливими елементами кібербезпеки. Ці методи атак, спрямовані на отримання конфіденційної інформації через маніпулювання психологією користувачів, стали більш витонченими та поширеними, викликаючи серйозні загрози для особистої та корпоративної безпеки. Цей розділ розглядає методи фішингу та соціальної інженерії, їх вплив на користувачів та пропонує практичні підходи до захисту від цих загроз [1].

2.1.1 Фішинг: відомі методи та їх варіації

Фішинг – це один із найбільш поширених методів атак в сфері кібербезпеки, який використовує соціальні інженерні техніки для отримання конфіденційної інформації, такої як паролі, номери банківських карт або особисті дані, від користувачів. Нижче наведено узагальнений перелік найбільш поширених методів і варіацій фішингу, наслідків їх впливу на користувачів та можливих стратегій захисту.

Основні методи фішингу:

- *Електронна пошта (E-mail): підступні листи, що виглядають як від відомих вам компаній чи сервісів, які закликають вас ввести конфіденційні дані на фіктивних веб-сайтах.*
- *Соціальні мережі та месенджери: фішингові атаки через популярні соціальні мережі та месенджери, де атакуючі видають себе за знайомих чи колег.*
- *Веб-сайти: створення фішингових веб-сайтів, які імітують офіційні ресурси для отримання особистої інформації.*

ISSN 2519-2310 CS&CS, Issue 2(24) 2023

Варіації фішингу:

- *Розмовний фішинг – вішинг (Vishing): фішинг через телефонні дзвінки, де атакуючий намагається отримати конфіденційну інформацію від потенційної жертви.*
- *Смішинг (Smishing): атаки через SMS-повідомлення, де у користувачів намагаються виманити особисті дані через текстові повідомлення.*
- *Spear Phishing або таргетований фішинг: атаки, де зловмисники висококваліфіковано атакують конкретні цілі - фізичні особи та/чи організації.*
- *Соціальна інженерія: використовує психологічні аспекти впливу на свідомість персоналу сучасних ІС. Як метод атаки, не лише спрямований на експлуатацію технічних й організаційних вразливостей діючої системи захисту, але й ефективно використовує психологічні прийоми для масштабування наслідків атаки. Розгляд впливу соціальної інженерії на психологічний стан користувачів ІС та їх вразливість, є ключовим аспектом безпеки в онлайн середовищі. Зловмисники використовують такі методи, як створення терміновості, виклик емоцій, та швидкі перевтілення в авторитетність, щоб викликати потрібну реакцію у потенційної жертви.*

2.1.2 Ефективні стратегії захисту від загроз фішингу.

- *Навчання та професійна відповідальність:* завчасне передбачення фішингових атак розуміє під собою безперервне навчання користувачів сучасних ІС, розпізнавати характерні ознаки шахрайства. Тому, регулярні тренінги та інструкції персоналу, можуть значно підвищити рівень їх профільних компетенцій.
- *Використання антивірусних програм:* встановлення та регулярне оновлення антивірусних програм є ефективним заходом захисту від фішингу. Вони виявляють та блокують шкідливі віруси та веб-сайти.
- *Багатофакторна автентифікація:* використання багатофакторної автентифікації додає додатковий шар захисту, оскільки для входу необхідні два чи більше види автентифікації. Багатофакторна автентифікація дедалі стає необхідністю в умовах постійного зростання фішингових атак. Аналіз відомих інцидентів безпеки показує, що використання не лише паролів, але й інших методів ідентифікації, таких як біометричні дані чи одноразові коди, робить процес автентифікації значно більш надійним. Це зменшує ймовірність «успіху» атак та робить доступ до особистих облікових записів складнішим для зловмисників.
- *Управління паролями:* широке застосування бездротових мереж підвищує ризик несанкціонованого доступу до особистої (приватної) та/чи корпоративної інформації. В цьому сенсі одним із найважливіших заходів безпеки є коректне адміністрування паролями. Користувачі мають створювати складні та унікальні паролі для кожного облікового запису і регулярно їх змінювати.
- *Впровадження механізмів багатофакторної автентифікації:* додатково зміцнює захист доступу до особистих/корпоративних даних [3].
- *Оновлення ПЗ та операційних систем:* є ключовим аспектом безпеки. Своєчасне встановлення оновлень та патчів безпеки дозволяє виправляти виявлені уразливості та запобігати можливим атакам зловмисників.
- *Використання шифрування* даних на пристроях та під час обміну інформацією через бездротові мережі є також невід'ємною частиною захисту чутливих даних від фішингу. Шифрування забезпечує конфіденційність та цілісність інформації під час передачі її через мережі, в т.ч. незахищені.
- *Обмеження доступу до інформації.* є додатковим кроком з протидії фішингу, тому користувачі ІС повинні ретельно контролювати, кому та за яких умов нада-

ISSN 2519-2310 CS&CS, Issue 2(24) 2023

ють (делегують) доступ до своїх особистих даних та/чи службових повноважень при роботі з ПЗ та/чи мережевим устаткуванням корпоративної ІС.

Інтеграція зазначених стратегій сприятиме підвищенню поточного рівню захисту інформаційних ресурсів від загроз фішингових атак та покращити безпеку особистих та/чи конфіденційних корпоративних даних при їх зберіганні й циркуляції між користувачів в онлайн середовищі.

2.2 Віруси та шкідливе ПЗ

Шкідливе ПЗ є важливою складовою у загальному спектрі загроз ІБ. В загальному випадку її основною метою є завдання шкоди інформаційним і апаратним ресурсам сучасних ІС. Нижче наведено перелік найбільш характерних (часто використовуваних) різновидів шкідливих програм та їх способи їх поширення:

- *Комп'ютерні черв'яки (або трояни): самостійні програми, які розповсюджуються через носії даних та/чи мережеву взаємодію без необхідності подальшого мануального втручання (супроводження) з боку їх розробника.*
- *Рекламні віруси: програми, що намагаються розповсюджувати рекламу або навіть змінюють (підмінюють) сторінки веб-сайтів.*
- *Шпигунське ПЗ: програми, які збирають конфіденційну, в тому числі, технологічну інформацію, без відома її користувачів.*

Вплив на інформаційні системи: наслідки використання шкідливого ПЗ для інформаційних систем можуть передбачати втрату конфіденційності, порушення цілісності даних та обмеження доступу до важливих ресурсів.

Протидія шкідливим програмам: використання антивірусного ПЗ, засобів міжмережевого екранування, систем виявлення вторгнень тощо. Також треба акцентувати увагу на важливості своєчасного оновлення ПЗ та вдосконалення кіберграмотності користувачів ІС.

2.3 Відмова в обслуговуванні та DDoS атаки

2.3.1 DDoS атаки

DDoS (*Distributed Denial of Service - розподілені атаки з відмовою в обслуговуванні*) є серйозною загрозою для сучасних ІС, що здатна призводити до великих збоїв у роботі вебсерверів та мережевої інфраструктури. Цей розділ присвячений аналізу різних типів DDoS атак, їх впливу та ефективним заходам для запобігання відмові в обслуговуванні. На сьогоднішній день ці атаки досі залишаються однією з найбільш поширених та руйнівних форм реалізації деструктивного впливу на функціонування сучасних ІС. Вони спрямовані на перевантаження ресурсів цільового сервера, мережі чи програми (програмного додатку), шляхом навмисного відправлення надмірного злочинного трафіку. Розгляд цієї теми є надзвичайно важливий, оскільки *DDoS* атаки можуть призвести до відмови в обслуговуванні та серйозно зашкодити бізнес та чи промисловим/технологічним процесам. За останні роки збільшилась частота та підвищилась складність реалізації *DDoS*.

Так, наприклад, зловмисники додатково використовують атаки підсилення (як своєрідний різновид забезпечення, або каталізатор цих атак) та синтез ботнетів, для максимізації впливу й наслідків основної атаки. Зокрема, атаки підсилення, такі як *DNS Amplification* та *NTP Amplification*, дозволяють помітно збільшити обсяг надлишкового (постановочного) трафіку і тим самим відчутно перевантажити мережеві з'єднання цільового об'єкту-жертви.

- *Відмова в обслуговуванні та її вплив на систему*

DDoS атаки можуть призвести до відмови в обслуговуванні, зробивши ресурси недоступними для легітимних користувачів. Це може викликати серйозні фінансові втрати, погіршення репутації компанії та втрату клієнтів.

ISSN 2519-2310 CS&CS, Issue 2(24) 2023

- *Захист від DDoS атак*

Захист від *DDoS* атак вимагає комплексного підходу. В цьому сенсі важливо мати системи моніторингу трафіку, які виявлятимуть аномальні патерни, що можуть бути характерними для *DDoS* атак. Використання *CDN* (*Content Delivery Network*) може розподіляти трафік та мінімізувати вплив атак. Також, вкрай важливо мати системи фільтрації та обробки трафіку, які можуть відокремити легітимний трафік від атак.

2.3.2 Особливості реалізації атак підсилення

DNS Amplification

- *Збільшення обсягу відповідей:* атакуючі використовують *DNS*-сервери як посередників для збільшення обсягу трафіку. Вони відправляють запити до DNS-серверів з підробленими адресами цільової жертви. *DNS Amplification* базується на тому, що DNS-запити можуть бути короткими, але відповіді можуть бути значно більшими. Атакуючі використовують це, щоб збільшити обсяг зловмисного/паразитного трафіку, використовуючи ресурси легальних *DNS*-серверів.
- *Відсилання запитів у великому масштабі:* атакуючі відправляють велику кількість підроблених DNS-запитів відразу до великої кількості DNS-серверів, збільшуючи тим самим відповіді, які спрямовані на жертву атаки.

NTP Amplification

- *Використання NTP-серверів:* ці атаки використовують *Network Time Protocol (NTP)* для збільшення обсягу паразитного трафіку. Атакуючі відправляють підроблені запити відразу до великої кількості діючих *NTP*-серверів.

Провокування значної сукупності *DNS* та *NTP* серверів до одночасного формування ними відповідей на масштабні короткі злочинні запити, котрі формуються в межах *атак підсилення,* ґрунтується на тому, що такі відповіді можуть бути значно більшими чим запити, що й дозволяє атакуючим збільшити паразитний трафік.

2.3.3 Синтез та використання ботнетів (Botnet-based DDoS)

Синтез та наступне використання ботнетів у *DDoS* атаках є ефективним та небезпечним методом перевантаження мережевих ресурсів цільового об'єкта. Розглянемо деякі основні особливості цього процесу.

Синтез ботнетів DDoS:

- *Створення ботнетів:* зловмисники використовують різноманітні методи для зараження тисяч або навіть мільйонів пристроїв, перетворюючи їх на боти.
- *Координовані атаки:* дозволяє атакуючим синхронізувати дії ботів, направляючи трафік на цільовий сервер одночасно, збільшуючи таким чином вплив атаки.
- *Розподілена відмова в обслуговуванні:* ботнет *DDoS* атаки призводять до розподіленої відмови в обслуговуванні, внаслідок чого цільовий об'єкт стає недоступним для легітимних користувачів.

Особливості DDoS ботнетів:

- *Інфікування:* зараження пристроїв шляхом використання шкідливого ПЗ, експлуатації вразливостей та/або методів соціальної інженерії.
- *Приховане управління:* зловмисники використовують різноманітні методи для прихованого управління ботами, уникнення їх виявлення та блокування.
- *Збільшення ресурсів атаки:* використання ботнетів для збільшення (посилення) обсягу нелегітимного злочинного трафіку та «силового» впливу на цільовий сервер.

Заходи захисту:

- *Мережевий моніторинг:* постійний моніторинг мережі для виявлення аномалій та надмірного трафіку, які можуть вказувати на DDoS атаку.

ISSN 2519-2310 CS&CS, Issue 2(24) 2023

- *Виявлення та блокування ботів:* використання систем виявлення ботів для ідентифікації та блокування зламаних пристроїв у ботнеті.
- *Системи фільтрації трафіку:* впровадження швидкодіючих (хмарних) систем фільтрації трафіку, які блокують надмірний трафік та «відсікають» шкідливий.
- *Захист Інтернету речей (IoT):* збільшення поточного рівня безпеки пристроїв IoT, щоб унеможливити їх використання в якості ботів.

2.4 Інші типи кіберзагроз та їхні методи впливу на системи

У світі кібербезпеки існує розмаїття кіберзагроз, які відображаються у різних формах та методах впливу на ІС. Тому приділимо увагу й іншим типам загроз ІБ, зокрема атакам на безпеку мережі та застосунків, уточнюючи їх методи впливу та заходи із захисту.

Атаки на безпеку мережі:

- *Перехоплення трафіку (Man-in-the-Middle):* тип атаки, при якому зловмисники здійснюють перехоплення трафіку між взаємодіючими сторонами, що може призвести до доступу до конфіденційної інформації.
- *Атаки на DNS (Domain Name System):* методи атак на інфраструктуру *DNS* з метою спрямовування трафіку на злочинний ресурс та/чи посилення атак (*див. вище*).

Атаки на застосунки:

- *Хакерські атаки на вразливості коду (SQL Injection, XSS):* техніки використання вразливостей коду для впровадження зловмисного коду або отримання несанкціонованого доступу.
- *Атаки на автентифікацію та онлайн сесії*: методи обходу механізмів автентифікації та зловживання сесій для несанкціонованого доступу.

Вплив на інформаційні системи:

- *Втрата конфіденційності та цілісності даних:* можливі наслідки атак на безпеку мережі і додатків, зокрема, втрати конфіденційності та порушення цілісності даних.
- *Втрата доступності сервісів:* ці атаки можуть впливати на доступність інформаційних систем та відповідних онлайн послуг/сервісів.

Заходи для захисту:

- *Шифрування та/чи приховування (стеганографія) трафіку.*
- *Постійний моніторинг мережі, виявлення вторгнень та/чи припинення недекларованої мережевої активності.*

3. Аналіз вразливостей і можливих стратегії захисту

3.1 Виявлення вразливостей ІС

Виявлення вразливостей ІС, це ключовий етап в забезпеченні їхньої стійкості та захисту від кібератак. У світі, де загрози зростають щодня, ефективні методи виявлення вразливостей стають їх обов'язковою необхідністю [3]. Виявлення цих вразливостей у власних інформаційних системах – перший крок до їхнього ефективного захисту. Тому коротко розглянемо деякі з нових підходів, щодо виявлення вразливостей і розробці стратегій для їхнього негайного парирування.

Методи виявлення вразливостей:

- *Сканування портів та аналіз вразливостей:* автоматизовані засоби можуть проаналізувати «відкриті порти» та визначити потенційні точки входу для атак.
- *Статичний та динамічний аналіз коду:* виявлення вразливостей використовуваного ПЗ, через аналіз вихідного коду, дозволяє виявити вразливості, які можуть бути використані для вторгнень/атаки/витоку даних.

ISSN 2519-2310 CS&CS, Issue 2(24) 2023

- *Системи виявлення Інтранет-загроз:* моніторинг внутрішнього сегменту мережі для виявлення аномальної мережевої активності та потенційних загроз безпеки.
- *Ethical hacking та Penetration testing:* етичний хакінг (пентестінг) для виявлення існуючих вразливостей з метою їх подальшого усунення (в межах аудиту ІБ).

3.2 Стратегії захисту від різних типів кіберзагроз

Багатошаровий підхід до захисту:

- *Системи виявлення та захисту:* встановлення інтегрованих систем безпеки для виявлення та блокування атак в реальному часі (*IDS/IPS/DLP/HoneyNet* тощо).
- *Фільтрація трафіку:* використання систем фільтрації для блокування небезпечних пакетів трафіку на різних рівнях/сегментах мережі (*proxy, firewall, IPS* тощо).

Сегментація та ізоляція ресурсів:

- *Делегування прав доступу:* обмеження доступу до важливих ресурсів за допомогою делегування прав (*firewalls, біометричні системи, системи захисту від несанкціонованих дій, впровадження алгоритмів виконання сумісних дій та ін.*).

3.3 Заходи із забезпечення стійкості ІС до кібератак

Забезпечення стійкості ІС до кібератак – це необхідна передумова для збереження конфіденційності, цілісності та доступності даних. Сучасний кіберпростір вимагає від організацій постійно вдосконалювати свої стратегії захисту та вживати комплексних заходів для завчасного парирування існуючих загроз ІБ.

- *Захист від внутрішніх загроз.* Розробка та впровадження ефективної корпоративної політики ІБ (ПІБ), включаючи обмеження доступу та моніторинг внутрішніх користувачів, стає важливим етапом у попередженні можливих загроз зсередини.
- *Використання сучасних систем виявлення загроз.* Системи виявлення вторгнень та аномалій дозволяють вчасно виявляти та реагувати на небезпечні активності. Використання штучного інтелекту та машинного навчання (AI/LM) дозволяє автоматизувати процес виявлення навіть найскладніших кіберзагроз.
- *Захист мережі та захист умовного «периметру» безпеки.* Міжмережеві бар'єри та захист «зовнішнього» периметру безпеки, визначають умовну першу лінію захисту. Вони включають в себе використання *firewalls*, систем виявлення вторгнень (*IDS*) та засоби фільтрації трафіку (корпоративні *proxy* та *DLP* тощо) для блокування можливих атак/витоку даних на рівні мережі.
- *Управління доступом та автентифікація.* Забезпечення стійкості включає в себе також впровадження ефективної системи управління доступом та багатофакторної автентифікації. Це дозволяє обмежити доступ до чутливої інформації та ускладнює можливі атаки на облікові записи користувачів.
- *Регулярні аудити стану безпеки та оновлення ПЗ та ПІБ.* Проведення систематичних аудитів поточного стану ІБ для виявлення існуючих вразливостей та невикористаних можливостей є ключовим аспектом безпеки. Регулярне оновлення програмного та апаратного забезпечення дозволяє усувати виявлені вразливості та підтримувати систему в актуальному стані.

3.4 Вплив рівню технологічного розвитку у забезпеченні ІБ

Технологічний розвиток є неодмінним фактором впливу на рівень безпеки сучасних ІС. Постійний прогрес у галузі інформаційних технологій (ІТ) створює нові можливості для забезпечення ІБ та вимагає від організацій постійного адаптування до змін у кіберпросторі. Тож коротко розглянемо основні з найбільш перспективних технологій:

- *Штучний інтелект та машинне навчання (AI та LM)*

ISSN 2519-2310 CS&CS, Issue 2(24) 2023

Застосування технологій *AI* та *LM* в галузі кібербезпеки дозволяє автоматизувати виявлення та аналіз аномалій в мережах. Алгоритми машинного навчання можуть швидко адаптуватися до нових типів загроз, забезпечуючи більш ефективний захист.

- *Блокчейн для забезпечення «імунітету» до змін*

Технологія блокчейн визначається своєю децентралізацією та непроникністю до змін. У сфері кібербезпеки, вона може служити основою для безпечного зберігання та обміну конфіденційної інформації, запобігаючи атакам на централізовані системи.

- *Квантова обчислення та технології віртуалізації процесів (VR)*

З розвитком квантових технологій виникає можливість у нових методах аналізу мережевого трафіку, віртуалізації процесів, каскадування обчислювальних можливостей та криптографічного захисту даних. Квантові комп'ютери можуть «зламувати» традиційні криптографічні алгоритми, тому створення нових квантово-стійких захисних методів, дедалі стає все більш актуальним завданням ІБ.

- *Інтернет речей (IoT) та кіберфізичні системи*

Розширення Інтернету речей передбачає додавання та й маніпулювання величезними обсягами додаткових даних, що потребують їх ефективного захисту. Розвиток кіберфізичних систем дозволяє об'єднати в собі фізичний та кібер- світи, вимагаючи при цьому впровадження інноваційних технологій й методів безпеки.

- *Спрощення управління безпекою через Cloud Security*

Використання сукупності хмарних та *VR* технологій дозволяє компаніям зосередитися на вдосконаленні стратегій безпеки, адже адміністрування та оновлення захисних систем може бути здійснене централізовано [4].

4. Висновки

1. На сьогоднішній день кіберзагрози створюють загрози для конфіденційності, цілісності та доступності інформації. Зростання залежності суспільства від поточного рівня розвитку й впровадження ІТ підкреслює актуальність питання захисту ІС від кіберзагроз.

2. Проведено аналіз впливу різних типів кіберзагроз на ІС та розглянуті основні стратегії щодо їх захисту. Запропоновано огляд нових тенденцій у кібербезпеці і деяких інноваційних підходів з питань захисту від нових загроз. Підкреслено наявність нерозривного взаємозв'язку питань технологічного розвитку й фактичного стану можливостей із ІБ.

3. Підкреслено необхідність постійного оновлення й адаптації діючих стратегій захисту до зростаючої складності кіберзагроз. Звернено увагу, що захист ІС вимагає одночасного поєднання впровадження інноваційних технологій, глибокого розуміння сучасних тенденцій кібербезпеки та глобальної співпраці для ефективної протидії актуальним кіберзагрозам.

Список літератури

[1] Jon Erickson (2010). "Hacking: The Art of Exploitation"

[2] Edward Amoroso. (2010). "Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare"

[3] P.W. Singer та Allan Friedman (2014). "Cybersecurity and Cyberwar: What Everyone Needs to Know"

[4] International Journal of Computer Science and Information Technologies "Cybersecurity: A Journal of Technology, Society and Policy".

Received: on December 2023. **Accepted:** on December 2023.

Authors:
Osadchyi Yevhenii, CSD Student, V. N. Karazin Kharkiv National University, Kharkiv, Ukraine.
E-mail: xa12850357@student.karazin.ua
Yesina Maryna, Ph.D., Associate Professor, department of security of information systems and technologies, V. N. Karazin Kharkiv National University, Kharkiv, Ukraine; research associate-consultant of JSC "IT", Kharkiv, Ukraine.
E-mail: m.v.yesina@karazin.ua
ORCID: https://orcid.org/0000-0002-1252-7606

ISSN 2519-2310 CS&CS, Issue 2(24) 2023

Victor Onoprienko, Ph.D., CEO of JSC "IIT", Kharkiv, Ukraine.
E-mail: v25258@gmail.com

The influence of different forms of cyber threats on the stability of information systems: analysis and protection strategies

Abstract. This work is dedicated to the further investigation of cybersecurity issues in the context of the ongoing development of the current information industry. Starting with an overview of various forms of cyber threats, the article examines the analysis of their impact on the privacy, integrity and availability of information. The critical dependence of modern society on information technology makes the topic of protection against cyber threats extremely relevant. This work offers an in-depth analysis of the growth in the number and complexity of cyber threats, which requires constant improvement and updating of protection strategies against them. An important stage of coverage of the topic is the analysis of the impact of various forms of cyber threats on information systems. The main types of phishing and social engineering are considered, as well as the consequences of exposure to viruses, Trojans and other malicious programs. A detailed review of these aspects allows us to highlight the key issues and dangers that arise in the context of cyber threats. Also, the article contains materials devoted to various protection strategies. It examines effective strategies for protecting information systems, including identifying vulnerabilities, using multi-factor authentication, and measures to ensure resilience. The general conclusions of this work summarize the need for constant updating and adaptation of protection strategies in relation to the growing complexity of cyber threats in the world of rapid technological development. In general, this work is another step in understanding the essence of the challenges associated with the issue of ensuring cyber security in the modern information society.

Keywords: Impact, Cyber Threat, Analysis And Protection, Resilience Of Information Systems, Protection Strategies.