Міністерство освіти і науки України
Криворізький національний університет
Факультет інформаційних технологій
Кафедра комп’ютерних систем та мереж

КВАЛІФІКАЦІЙНА РОБОТА МАГІСТРА
за спеціальністю 123 «Комп’ютерна інженерія»

Тема роботи: «МЕТОДИ ЗАХИСТУ ТА НАЛАШТУВАННЯ КІНЦЕВИХ ПРИСТРОЇВ ПРАЦЮЮЧИХ З ДАННИМИ В ХМАРНИХ СЕРЕДОВИЩАХ»

Виконав _____ Є. О. Коростиленко

Керівник роботи _____ Ю. О. Кумченко

Нормоконтроль _____

Завідувач кафедри _____ А. І. Купін

Кривий Ріг
2025

Криворізький національний університет
Факультет інформаційних технологій
Кафедра комп'ютерних систем та мереж

Ступінь вищої освіти магістр
Спеціальність 123 «Комп'ютерна інженерія»

ЗАТВЕРДЖУЮ
Завідувач кафедри, голова циклової комісії

_____ А. І. Купін

"____" _____ 20__ року

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ МАГІСТРА

_____
(прізвище, ім'я, по батькові)
1. Тема роботи _____
_____
_____
керівник роботи _____,
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом вищого навчального закладу від "___"_____ 20__року №__
2. Строк подання студентом роботи _____
3. Вихідні дані до роботи _____
_____
_____
_____
_____
_____
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)_____
_____
_____
_____
_____
_____
5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)_____
_____
_____

6. Консультанти розділів роботи

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

7. Дата видачі завдання_____

КАЛЕНДАРНИЙ ПЛАН

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

Студент _____ _____
(підпис) (прізвище та ініціали)

Керівник роботи _____ _____
(підпис) (прізвище та ініціали)

РЕФЕРАТ

Пояснювальна записка: 107 сторінок, 40 рисунків, 4 таблиць, використаних джерела.

Кваліфікаційна робота магістра складається з трьох розділів.

Перший розділ було присвячено визначенню поняттям кібербезпека, хмарним обчисленням, загрозам у кіберсвіті, а також боротьбі з ними. Проведено опис існуючих методів та рівнів кібербезпеки, видам та особливостям змарних обчислень. Затронуто тему ризиків у сфері ІТ.

У другому розділі було розглянуто сучасний стан загроз у світі ІТ, поняття інформаційної безпеки, кібертероризму, та кіберпростору. Подана статистика за найбільшими загрозами в ІТ за останній час, розглянуто питаннякіберзагроз на національно-державному рівні, окрім того було досліджено вплив та статистику кіберзлочинів та кібертероризму, види та кількість атак різних груп кіберзлочинців у світі та результати розвитку кібербезпеки внаслідку їхньої діяльності.

Третій розділ присвячений розгляду різних видів аутентифікації та авторизації. Їх практичне використання, складність та особливості реалізації., переваги та недоліки різним методів та сфери їх використання, з наданням повного їх порівняння.

КОМП’ЮТЕРНІ СИСТЕМИ, КІБЕПРОСТІР, КІБЕРБЕЗПЕКА, КІБЕРШАХРАЙСТВО, КІБЕРТЕРОРИЗМ, АУТЕНТИФІКАЦІЯ, АВТОРИЗАЦІЯ, ХМАРНІ БАЗИ ДАНИХ.

ABSTRACT

Explanatory note: 107 pages, 40 figures, 5 tables, used sources.

The master's qualification work consists of three sections.

The first section was devoted to defining the concepts of cybersecurity, cloud computing, threats in cyberspace, and how to combat them. It described existing methods and levels of cybersecurity, as well as the types and characteristics of cloud computing. The topic of risks in the IT sphere was also touched upon.

The second section examined the current state of threats in the IT world, the concepts of information security, cyberterrorism, and cyberspace. Statistics on the most significant recent IT threats are presented, and cyber threats at the national level are examined. In addition, the impact and statistics of cybercrime and cyberterrorism, the types and number of attacks by various cybercriminal groups around the world, and the results of cybersecurity development as a result of their activities are investigated.

The third section is devoted to the consideration of various types of authentication and authorization. Their practical use, complexity and features of implementation, advantages and disadvantages of different methods and areas of their use, with a full comparison of them.

COMPUTER SYSTEMS, CYBERSPACE, CYBERSECURITY, CYBERCRIME, CYBERTERRORISM, AUTHENTICATION, AUTHORISATION, CLOUD DATABASES.

ЗМІСТ

1. ОСНОВИ КІБЕРБЕЗПЕКИ 10
1.1. Захист інформації 10
1.2. Типи загроз кібербезпеки 12
1.4. Класи продуктів у сфері кібербезпеки 14
1.5. Сучасні технології кібербезпеки 15
1.6. Загрози хмарних обчислень Cloud Security Alliance (CSA) 17
1.7. Вразливі місця хмарних обчислень 19
1.8. Система класифікації рівнів безпеки інформаційних систем 22
1.9. Алгоритми шифрування 27
1.10. Структура системи захисту хмарної бази даних 32
2. ЗАГРОЗИ ІТ СВІТУ 37
2.1. Кіберпростір. 37
2.2. Інформаційна безпека 42
2.3. Кібертероризм 48
2.4. Національно-державні загрози 51
2.5. Стирання меж між державними кіберзагрозами та кіберзлочинцями. .. 60
2.6. Втручання у вибори ..... **Ошибка! Закладка не определена.**
2.7. Програми-вимагачі 69
2.8. Кібершахрайство 72
2.9. Фішинг 76
2.10. Видача себе за іншу особу 79
3. ВИДИ АВТОРИЗАЦІЇ ТА ЇХ ПРАКТИЧНА РЕАЛІЗАЦІЯ 85
3.1. Ідентифікація, аутентифікація, авторизація. 85
3.2. Basic auth 87
3.3. Session auth 89
3.4. Token based auth 93
3.5. OAuth 2.0 100
3.6. Keycloak (SSO / OpenID Connect) 102
ВИСНОВОК 107
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 109

ПЕРЕЛІК СКОРОЧЕНЬ

ІБ – інформаційна безпека.

КБ – кібербезпека.

ІТ – інформаційні технології.

ПК – персональний компёютер.

VPN (virtual private network) – віртуальна приватна мережа.

API (Application Programming Interface) – інтерфейс прикладного програмування.

UDP (User Datagram Protocol) – Протокол датаграм користувача.

TCP (Transmission Control Protocol) – протокол управління передачею.

DNS (domain name system) – Система доменних імен.

ISO (international organization for standardization) – міжнародна організація стандартизації.

CSA (Cloud Security Alliance) – Альянс з безпеки хмарних технологій.

PKCS (Public Key Cryptography Standards) – Стандарти криптографії з відкритим ключем.

ІКТ – інформаційно-комунікаційних технологій.

ІТС – інформаційно-технічних систем.

CISA – Агентство з кібербезпеки та безпеки інфраструктури США.

SSL (Secure socket layer) – Цифровий сертифікат.

TLS (Transport layer security) – захист на транспортному рівні.

ACL (access control lists) – лист доступу.

HTTP (HyperText Transfer Protocol) – протокол передачі даних.

SSO (Single-sign on) – Одноразовий вхід.

LAN (Local Area Network) – локальна мережа.

WAN (Wide Area Network) – мережа, що охоплює великі географічні області.

IP (Internet Protocol) – протокол Інтернету.

FDH (Full Domain Hash) – повний хеш домену.

ДФА – Двофакторна автентифікація.

БФА (MFA, multifactor authentication) – багатофакторна автентифікація.

ЗОЗ – захоплення облікових записів.

DDoS (Distributed Denial of Service) – розподілена відмова в обслуговуванні.

IBAC (Identification Based Access Control) – Контроль доступу на основі ідентифікації.

ABAC (Attribute-Based Access Control) – контроль доступу на основі атрибутів.

ВСТУП

Упродовж останніх десятиліть світ стрімко поринув у епоху цифрових технологій. Інформаційні технології дедалі більше впливають на всі аспекти нашого життя – від медицини та освіти до транспорту, бізнесу й розваг. Ми користуємося смартфонами, які потужніші за комп'ютери, що колись займали цілі зали, спілкуємося на відстані тисяч кілометрів, проводимо фінансові операції за лічені секунди, а штучний інтелект допомагає вирішувати задачі, що раніше вимагали годин чи навіть днів.

Такий стрімкий розвиток ІТ відкриває людству неймовірні можливості. Автоматизація процесів підвищує ефективність виробництва, хмарні технології дозволяють працювати й навчатися з будь-якої точки світу, а великі дані допомагають робити точніші прогнози й ухвалювати обґрунтовані рішення. У медицині алгоритми машинного навчання можуть ефективно розпізнавати та виявляти захворювання на ранніх стадіях, у транспортній сфері автономні системи роблять дороги безпечнішими, а в освіті цифрові платформи персоналізують навчання.

Однак зі зростанням цифрових можливостей зростають і ризики. Кіберпростір, поруч із безліччю переваг, приховує значну кількість небезпек, про які ще десять років тому мало хто замислювався. Кіберзлочинці стають дедалі винахідливішими: вони знаходять слабкі місця навіть у найскладніших системах, використовують соціальну інженерію, зламують акаунти, крадуть персональні дані, паралізують роботу організацій за допомогою вірусів-вимагачів.

Саме тому питання надійного захисту в кіберсвіті сьогодні стоїть як ніколи гостро. Безпека перестала бути справою лише фахівців – вона стала спільною відповідальністю. Кожен користувач має усвідомлювати, що навіть одна вразливість – проста, на перший погляд, помилка чи необачний крок – може становити загрозу не лише для нього самого, а й для всієї організації, до якої він належить. У той час як компанії мають Сучасні системи кіберзахисту потребують регулярного оновлення програмного забезпечення, а також проведення систематичного аудиту безпеки, користувачам необхідно дотримуватися базових правил: створювати складні паролі, вмикати двофакторну автентифікацію, бути уважними до підозрілих листів і посилань.

Особливо важливо, що кіберзахист розвивається так само швидко, як і технології. Системи виявлення вторгнень, штучний інтелект, який аналізує поведінку користувачів, квантове шифрування – усе це стає новою зброєю у боротьбі з кіберзлочинністю. Проте жодна технологія не буде ефективною без розуміння та відповідальності людей, які її використовують.

Стрімкий розвиток ІТ-світу створює унікальні умови для прогресу, але водночас вимагає усвідомленості та обережності. У цифрову еру безпека – це не просто опція, а необхідність, яка дозволяє користуватися перевагами технологій без

страху перед їхньою зворотною стороною. І майбутнє належить тим, хто вміє поєднувати інновації з відповідальністю.

Актуальність дослідження. Зумовлена стрімким зростанням використання хмарних технологій у різних сферах діяльності. Кінцеві пристрої користувачів є основними точками доступу до хмарних сервісів, а отже – найбільш уразливими елементами інформаційних систем. Їх компрометація може призвести до витоку конфіденційних даних, порушення цілісності інформації та несанкціонованого доступу до хмарних ресурсів.

Мета і завдання дослідження. Мета дослідження зосередженні на сучасних методах кібератак на кінцеві пристрої, їх аналіз та розвиток методів кібербезпеки, які мають на меті протидії даним атак. Побачити розвиток систем кібербезпеки, як в локальному так і глобальному рівні.

Об'єкт дослідження. Кінцеві пристрої на які були здійснені атаки за декілька останніх років з відображенням їхньої статистики та атак, від яких вони постраждали. Статистика була зібрана з декількох різних джерел основним із яких були звіти з кіберпезпеки від компанії Microsoft.

Предмет дослідження – існуючі види аутентифікації та авторизації, складність їх реалізації, рівень безпеки та у яких випадках вигідно використовувати їх різні варіації.

Методи досліджень – аналіз, відображення статистики та рівень ураження кінцевих пристроїв від кібератак у всьому світі за декілька останніх років, з відображенням основних атак та груп, які їх використовували, а також наслідків та приблизної кількості інфікованих пристроїв.

Наукова новизна одержаних результатів. Зібрано дані з нововведень в питаннях кібербезпеки, а також розвитку різних видів кіберзагроз у світі. Проаналізовано статистику за кількістю і типами атак на кінцеві пристрої, та їх вплив на сучасний світ, та розглянуто ефективність протидії систем захисту.

Практичне значення отриманих результатів. Результати дослідження можна використати для порівняння існуючих методів аутентифікації та авторизації. Було проведено та надано повне порівняння всіх основних методів, їх недоліки, переваги, та складність реалізації у комп’ютерних мережах. У яких випадках той чи інше метод використовувати, та яку надійність вони мають.

Апробація роботи.

ОСНОВИ КІБЕРБЕЗПЕКИ

1.1. Захист інформації

Захист інформації забезпечується за допомогою використання деякого набору засобів. Таким чином, для запобігання втратам і витоку конфіденційних даних та інформації застосовуються такі види засобів, як:

- Фізичні;
- Апаратні та програмні;
- Організаційні;
- Нормативно-правові;
- Психологічні.

Фізичні засоби захисту інформації запобігають доступу сторонніх осіб до охоронюваної території. Серед найдавніших і найпоширеніших способів фізичного захисту використовували міцні двері, ґрати на вікнах та надійні замки. Для підвищення рівня захисту інформації використовуються пропускні пункти, де доступ контролюється як за допомогою персоналу, так і через спеціалізовані технічні системи. Для мінімізації ризиків втрати інформації доцільним є впровадження сучасних протипожежних систем. З метою забезпечення безпеки даних застосовуються фізичні засоби охорони, які спрямовані на захист інформації незалежно від типу носія – електронного чи паперового.

Програмне та апаратне забезпечення є ключовими елементами, які відіграють важливу роль у гарантуванні безпеки сучасних інформаційних систем.

Апаратні засоби – це пристрої, інтегровані в апаратну частину, які забезпечують обробку інформації. Програмні засоби належать до програм, які здатні відображати хакерські атаки. Окрім цього, до програмних засобів відносяться програмні комплекси, які здатні відновити втрачені відомості. За допомогою апаратної та програмної частин виконується резервне копіювання інформації, що дозволяє запобігати втратам важливої інформації.

Організаційні засоби захисту інформації сполучні з певними методами захисту: регламентацією, керування, примусом. Головними організаційними засобами є створення посадових інструкцій, проведення бесід із працівниками, а також впровадження систем покарань і заохочень. Завдяки ефективному використанню таких методів співробітники підприємства отримують детальну інформацію щодо роботи з конфіденційними даними, впевнено виконують свої зобов'язання та несуть відповідальність у разі надання неправдивої інформації, витоку або втрати важливих відомостей. [1]

Законодавчі засоби являють собою сукупність нормативно-правових актів, спрямованих на регулювання діяльності осіб, які мають доступ до чутливої

інформації. Вони встановлюють правила поводження з такими даними та визначають рівень відповідальності за їх втрату чи незаконне заволодіння.

Психологічні засоби являють собою комплекс дій, спрямованих на формування особистої зацікавленості громадян у збереженні достовірності та автентичності інформації. З метою стимулювання безпосереднього інтересу персоналу керівники використовують різноманітні форми заохочення. До психологічних засобів можуть відносити такі, як побудова корпоративної культури, де кожен робітник здатен почуватися, як вагома частина системи та стане зацікавленим в роботі та розвитку власного підприємства.

Кібербезпека перетинається з багатьма різними аспектами, але при цьому її головні напрямки можна розподілити на декілька ключових категорій:

Конфіденційність – це захист приватних чи корпоративних даних та інформації від доступу посторонніх осіб. Що може призвести до втрати або передачі чутливих даних.

Цілісність передбачає забезпечення незмінності та достовірності даних, що гарантує їх захист від будь-яких несанкціонованих змін або викривлень. У цьому контексті особлива увага приділяється моніторингу систем для виявлення та запобігання будь-яким неавторизованим втручанням, спрямованим на модифікацію інформації.

Доступність передбачає забезпечення доступу ресурсу для використання всіма людьми, для кого було надано дане право. За цих обставин запобігає перевантаженню чи атакам відмови в обслуговуванні, Атаки на відмову в обслуговуванні, які можуть спричинити недоступність використання ресурсів.

Безвідмовність забезпечує впевненість у тому, що певна дія чи подія справді мала місце, та надає можливість відстежити джерело такої дії.

Автентифікація та авторизація – посвідчує ідентичність користувачів та пристроїв, окрім цього визначає їхні права для доступ до даних та ресурсів.

Виявлення та реагування – це оперативне ідентифікування кіберзагроз із негайним реагуванням на них, що дозволяє мінімізувати збитки та забезпечує швидке відновлення стабільної роботи системи.

Освіта та підвищення рівня обізнаності – це ключові аспекти, які включають навчання користувачів і професіоналів базовим принципам кібербезпеки з метою забезпечення ефективного захисту від можливих загроз.

Дотримання законодавства і стандартів – забезпечення відповідності інформаційних систем та процесів згідно сучасних законодавчих і галузевих вимог з безпеки.

Стратегія кібербезпеки включає в себе такі головні складові:

Оцінка ризиків – вираження потенційних загроз, а також слабких місць в інформаційній системі.

Політика безпеки – формулювання стандартів, а також правил націлених на захист інформаційних ресурсів.

Навчання персоналу – отримання навичок фахівцям та працівникам для

Фізичний захист – забезпечення захисту й системи контролю доступу для головних ресурсів.

Технічний захист – налаштування засобів захисту, таких як фаерволи й системи упередження вторгненням.

Управління інцидентами передбачає швидке реагування на різноманітні події з подальшим їх детальним аналізом.

Аудит і моніторинг: перевіряти наявні системи на тотожність стандартам, а також відстеження їх активності.

Резервне копіювання – забезпечує збереження даних в сервері з можливістю їх відновлення.

Керування доступом – забезпечення доступу к ресурсам в залежності від рівнів повноважень користувачів. [2]

1.2. Типи загроз кібербезпеки

Кібербезпека займає важливе місце у сучасному цифровому світі. Зі збільшенням залежності людства від інтернету та різноманітних цифрових технологій її значення лише зростає разом з потенційними кількістю пов’язаних з цим загроз. Таким чином, зловмисники постійно створюють все нові методи атак та вдосконалюють вже існуючі, які здатні поставити під загрозу репутацію, дані, фінанси, як окремих осіб, так і бізнесу та компаній. З чого випливає, що від різноманітних фішингових атак, і до складних цілеспрямованих зломів, спектр загроз в сфері кібербезпеки величезний та різноманітний. Таким чином, для ефективної протидії подібним загрозам необхідно глибоко усвідомлювати їхню природу та розуміти механізми їхнього функціонування.

Фішинг

Належить до типу соціальної інженерії, в якій зловмисники видають себе за довірену сторону, з ціллю переконати потенційну жертву в передачі конфіденційної інформації, такої як наприклад, паролі чи номера банківських карт. Зустрічаються різні типи фішингу, серед яких цільовий фішинг, відомий як спірфішинг, або ж вейлінг, який спрямований на високопосадовців.

Криптоджекінг

Кіберзлочинці завантажують скрипт майнінгу на комп'ютер чи веб-сайт іншої людини з ціллю майнінгу криптовалюти за допомогою використання обчислювальних ресурсів. Дане нелегальне застосування ресурсів інших людей не тільки уповільнює роботу інфікованої системи, а також призводить до збільшення рахунків за енергоспоживання для жертв криптоджекінгу. Окрім фінансових втрат, тривале використання інформаційних систем може привести до зношення та раптових відмов, які можуть значно впливати на надійність та експлуатаційну довговічність пристроїв, створюючи загрозу їхньому стабільному функціонуванню.

Атаки які застосовують штучне та машинне навчання

Атаки які застосовують штучне та машинне навчання стає новим етапом кіберзагроз, в якому хакери починають застосовувати передові технології з метою збільшення та вдосконалення кібератак, що здійснюється завдяки використанню технологій машинного навчання. З їхньою допомогою зловмисники оперативно опрацьовують величезні обсяг даних, при цьому виявляючи слабкі місця у системах

захисту пристроїв, та автоматично налаштовуються для обходу різноманітних захисних механізмів.

Також за допомогою штучного інтелекту кіюерзлочинці розробляють більш переконливі та достовірні фішингові кампанії, окрім того вони хитро маскують шкідливе програмне забезпечення, роблячи його важчим для виявлення, з ціллю невидимих кібератак для більшості традиційних засобів захисту та виявлення. Дана тенденція робить призводить до необхідності постійного оновлення, розвитку та модернізації систем безпеки для протидії сучасним загрозам.

Сталкерське програмне забезпечення

Сталкерське програмне забезпечення, відомі також під назвами шпигунське чи службове програмне забезпечення, що здатні непомітно проводити моніторинги активності користувачів на пристрої без відома останнього. Вони здатні здійснювати такі дії, як відстеження дзвінків, текстових повідомлень, історії браузера, місцезнаходження, а також захоплення екрана у реальному часі.

Дані програми за частую застосовуються в комерційних чи батьківських цілях з метою моніторингу дій дітей чи працівників. Однак, потрапивши в руки зловмисників, відстеження програмного забезпечення стає засобом порушення конфіденційності, вимагання або будь-яких других кіберзлочинних дій. Варто систематично перевіряти свій пристрій на присутність підозрілих програм й дотримуватись заходів для забезпечення належного рівня безпеки. [3]

DoS-атака

DoS-атака, також відома як відмова в обслуговуванні – даний вид кібератаки, спрямований на пряме втручання у стабільну роботу цільової системи, служби, сервісу чи мережі, що унеможливлює її використання кінцевими користувачами. Такий вплив здійснюється шляхом створення надмірного навантаження на систему величезною кількістю вхідних запитів, що призводить до тимчасового або навіть постійного виходу ресурсів з ладу.

Якщо зловмисник застосовує декілька заражених комп’ютерів, зазвичай об’єднаних у ботнет, для одночасного надсилання численних запитів до цільового ресурсу, створюється можливість реалізації розподіленої атаки типу DDoS. Такий підхід посилює ефективність атаки та значно ускладнює процес протидії, адже вона ініціюється одночасно з кількох незалежних джерел.

Атаки на ланцюжок поставок

Атаки ланцюгів поставок спрямовані здебільш на вразливі місця в логістиці поставок продуктів та послуг. Замість того щоб спрямовувати атаки безпосередньо на кінцеві організації чи споживачів, зловмисники зосереджуються на більш вразливих ланках ланцюга постачання, таких як постачальники програмного забезпечення, підрядники чи виробники обладнання. Мета цих атак полягає в тому, щоб проникнути у продукти та послуги на ранньому етапі, забезпечуючи поширення шкідливого програмного забезпечення або інших загроз ще до їх потрапляння до кінцевого користувача чи організації.

Цей тип нападу несе значну загрозу, через те що він обходить стандартні способи виявлення та захисту, що застосовуються в організаціях. Одним із прикладів є модифікація програмного забезпечення протягом етапу розробки або

розповсюдження, внаслідок чого навіть надійні джерела несвідомо розповсюджують шкідливе програмне забезпечення.

Внутрішні загрози

Внутрішня загроза відноситься до загрози, безпосередньо зв’язана з діяльністю чи бездіяльністю фахівців, підрядників, працівників чи інших людей, які мають доступ до приватних ресурсів. Хоча більшість працівників працюють в інтересах виробництва чи фірми, помилки, недбалість або зрада – можуть призвести до критичних порушень в системі безпеки.

Певні внутрішні загрози можуть з’являтися спонтанно, у випадку, якщо працівник ненароком надсилає приватну або вразливу інформацію неправильному одержувачу. Також загрози бувають навмисними, наприклад, спричинені розлюченими або жадними працівників, які навмисно пробують викрасти або зіпсувати чутливі дані. Без різниці, чи була шкідлива дія похибкою або навмисною дією, слід звертати достатню увагу системі безпеки, зосереджену на запобігання, виявлення та протидію внутрішнім ризикам.

Цільова атака

Цільова атака відноситься до кібератак, які спрямовані на певну, конкретну організацію, фізичну особу чи інфраструктуру. На противагу масовим атакам, коли зловмисник зосереджується на величезній кількісті потенційних постраждалих, цілеспрямовані атаки зосереджуються на високому ступені індивідуалізації та зазвичай вимагають тривалої й ретельної підготовки.

Кіберзлочинці, які здійснюють цільові атаки, зазвичай спрямовані на отримання конкретних даних або ресурсів, а їхня мотивація може варіюватися від отримання фінансової вигоди до здійснення промислового шпигунства чи реалізації політично мотивованих задумів. Враховуючи високий рівень специфічності та складності подібних атак, вони представляють значну загрозу для організацій і потребують застосування ретельно розроблених заходів безпеки, а також ефективних процедур для їх виявлення та запобігання.

1.3. Класи продуктів кібербезпеки

Засоби захисту інфраструктури

Такі продукти гарантують безпеку, як фізичних так і віртуальних даних. Окрім створення систем управління та моніторингу, вони розробляють рішення для контролю доступу, а також механізми для моніторингу та попередження зовнішнім загрозам. Дані засоби застосовуються для протидії DDoS-атакам та захисту власної хмарної інфраструктури.

Засоби захисту мереж

Програмні рішення в такій ніші націлені на гарантування безпеки для мережевих ресурсів й трафіку, що використовуються в межах відповідної мережі. До них належать системи моніторингу мережі, рішення для знаходження та попередження вторгненням типу IDS/IPS, VPN, відомі як віртуальні приватні мережі, а також інші інструменти для керування, контролю й сегментації мережевого середовища.

Засоби захисту додатків

Головна увага приділяється забезпеченню безпеки для програмної частини системи. До неї входять такі засоби, як статичний та динамічний аналіз коду, веб-шлюзи, а також вимог для забезпечення захисту від кіберзагроз, зв'язаних з застосування веб-додатків.

Засоби захисту даних

Дані інструменти забезпечують захист інформації на протязі будь-яких етапах її життєвого циклу: від моменту створення до повного видалення. Вони охоплюють шифрування, маскування даних, управління ключами, системи попередження витоку чуткої інформації, а також інші технології для забезпечення безпеки.

Засоби захисту користувачів

Головна увага спрямована на забезпечення захисту для пристроїв кінцевих клієнтів від фішингових атак, кібершахрайства та інших можливих загроз. У фокусі – рішення для підвищення обізнаності й компетентності користувачів, а також впровадження багаторівневих методів аутентифікації.

Захист робочих станцій, кінцевих точок

Переглянуті заходи спрямовані на підвищення захисту персональних пристроїв, таких як комп'ютери, мобільні телефони та інші засоби цифрового доступу. У цьому контексті застосовуються антивірусні програми, системи керування мобільними пристроями, механізми контролю застосунків на рівні пристрїв, а також спеціалізовані рішення для протидії шкідливому програмному забезпеченню.[4]

1.4. Сучасні технології кібербезпеки

Сучасні технології кібербезпеки безперервно еволюціонують та вдосконалюються, прагнучи ефективно протистояти всезростаючому числу та підвищеному рівня загрози й складності, як старих, так і нових кіберзагроз.

Машинне навчання та штучний інтелект

Зазначені технології дозволяють системам кібербезпеки здійснювати навчання на основі накопичених даних, що формує здатність ідентифікувати загрози або аномалії в поведінці системи, які можуть залишитися непоміченими для людини. У такий спосіб штучний інтелект працює та аналізує величезні обсяги даних з високою швидкістю, забезпечуючи виявлення складних закономірностей і прогнозування можливих кібернетичних атак.

Блокчейн

Історично створений як основа для криптовалют, блокчейн сьогодні знаходить широке застосування в галузі кібербезпеки, гарантуючи збереження даних у їхній оригінальній формі та захист від зовнішнього втручання. Завдяки технології розподіленого реєстру забезпечується надійне, захищене та прозоре зберігання інформації, унеможливлюючи будь-які маніпуляції з даними.

Безпека на основі поведінки

Сучасні системи безпеки ретельно досліджують і аналізують різноманітні поведінкові характеристики користувачів. Серед таких параметрів можна виділити,

наприклад, швидкість, з якою користувач набирає текст, або особливості руху курсора миші. Ці показники використовуються для оцінки та підтвердження легітимності користувача, визначаючи, чи справді система взаємодіє з реальною людиною, чи це може бути автоматизований процес або стороннє проникнення. Завдяки такому підходу забезпечується підвищений рівень безпеки, оскільки аналіз поведінки робить складнішим обман цих механізмів.

Автоматизоване та інтегроване тестування безпеки

У сучасних умовах, коли складність програмних систем і додатків постійно зростає, інтеграція процесів тестування безпеки на початкових етапах розробки стає життєво необхідною дією. Акцент на раннє виявлення можливих недоліків забезпечує значну економію часу та ресурсів у майбутньому. Використання сучасних автоматизованих інструментів дозволяє здійснювати моніторинг і виявлення потенційних вразливостей у режимі реального часу, при цьому дозволяє досить сильно підвищити рівень безпеки кінцевого продукту. Таким чином, забезпечення безпеки стає природною і невіддільною частиною життєвого циклу розробки.

Хмарна безпека

В процесі збільшення популярності хмарних технологій супроводжується підвищенням потреби у забезпеченні їхнього захисту. Сучасні рішення у сфері хмарної безпеки надають інструменти для шифрування даних, управління доступом та ідентифікації користувачів, щоб гарантувати надійний контроль і захищеність інформації в хмарному середовищі.

Zero Trust Architecture

Ця безпекова концепція базується на принципі, що жоден запит до ресурсів організації не може вважатися надійним за замовчуванням. Кожен запит, незалежно від його походження, має бути підданий ретельній перевірці.

Сучасні технології забезпечують всебічний багатоетапний захист, спрямований на зменшення ризиків кібернападів і мінімізацію можливих наслідків. Водночас вони постійно розвиваються, адаптуючись до динамічного і непередбачуваного середовища кіберзагроз.

Як захистити себе від кіберзагроз.

Регулярне оновлення програмного забезпечення є ключовим компонентом забезпечення безпеки. Переконайтеся, що ваша операційна система, інтернет-браузери та інші програми завжди працюють на основі актуальних версій.

Застосовуйте складні паролі, які є унікальними для кожного облікового запису. Регулярно оновлюйте їх, щоб знизити ймовірність несанкціонованого доступу.

Активуйте двофакторну аутентифікацію для додаткового рівня захисту. Це створює додатковий бар'єр для потенційних зловмисників, значно підвищуючи безпеку ваших акаунтів.

Будьте уважними під час взаємодії з електронними листами та вкладеннями. Уникайте відкривання підозрілих файлів або переходу за невідомими посиланнями, якщо не маєте впевненості у їхній безпечності.

Інсталюйте надійне антивірусне програмне забезпечення, при цьому перевіряйте та здійснюйте оновлення для своїх пристроїв. Це значно підвищить рівень безпеки ваших пристроїв від шкідливих програм й потенційних кібератак.

Мінімізуйте використання відкритих Wi-Fi мереж без крайньої потреби. Якщо з'єднання з публічними мережами є необхідним, застосовуйте VPN для шифрування вашого інтернет-трафіку та забезпечення конфіденційності переданої інформації.

Дбайте про захист своїх особистих даних. Уникайте публікації конфіденційної інформації у відкритому доступі та не використовуйте її у складі паролів.

Періодично перевіряйте активність своїх акаунтів, звертаючи увагу на нові повідомлення, незвичайні дії чи транзакції. Це допоможе своєчасно виявити потенційно небезпечну активність і прийняти відповідні заходи.[5]

1.5. Загрози хмарних обчислень Cloud Security Alliance.

Загрози в галузі хмарних обчислень, які виділяє Cloud Security Alliance (CSA), мають ключове значення для забезпечення безпеки цифрових даних та адаптації механізмів управління ризиками. CSA, як провідний постачальник послуг безпеки, публікує детальні рекомендації для підвищення захищеності найбільш критичних аспектів хмарних технологій. Їхній аналіз дозволяє краще розуміти природу загроз і впроваджувати відповідні заходи для запобігання шкідливим інцидентам.

Серед основних порад із забезпечення кібербезпеки слід звернути увагу на кілька базових протоколів. Насамперед, користувачам рекомендується уникати під’єднання до відкритих Wi-Fi мереж без вагомої потреби. У випадку необхідності таке підключення має супроводжуватись використанням технології VPN для шифрування трафіку, що мінімізує ризик перехоплення даних. Також радиться дбайливо ставитися до захисту персональної інформації – не використовувати конфіденційні дані у відкритих джерелах або паролях. Регулярний моніторинг стану акаунтів, включно з перевіркою на наявність підозрілих дій, транзакцій чи активності, є ще однією важливою практикою.

Класифікація загроз у хмарних обчисленнях охоплює низку значущих ризиків, які заслуговують на особливу увагу:

1. Втрати чи витік даних. Це одна із найсерйозніших загроз для компаній та кінцевих споживачів. Видалення даних через помилкові дії постачальника послуг або форс-мажорні обставини, як-от пожежа чи технічна аварія, спричиняє непоправні наслідки для організацій.
2. Компрометація облікових записів або доступу до послуг. Цей ризик пов’язаний із можливістю викрадення облікових даних зловмисниками, що дозволяє отримати привілейований доступ до хмарних ресурсів. З метою запобігання цьому корпораціям слід ретельно обмежувати обмін обліковими даними між зацікавленими сторонами та застосовувати багатофакторну аутентифікацію.
3. Критичні уразливості інтерфейсів прикладного програмування (API). Хмарні користувачі взаємодіють зі службами через API, що може стати вектором атак при недостатньо налаштованому контролі доступу чи моніторингу. Надійна аутентифікація та захищені методи спілкування з API є необхідними умовами захисту ресурсів.

4. Атаки типу DDoS. Вони здатні паралізувати доступ користувачів до даних чи сервісів та створюють серйозну загрозу для доступності ресурсів у публічних хмарах. Постачальники хмарних послуг зобов'язані надати надійний рівень безпеки інфраструктури, що знизить ризик недоступності у випадку атак.
5. Ризик «шкідливого інсайдера». Уразливості можуть виникати через недобросовісні дії авторизованих користувачів, таких як співробітники чи партнери організації. Це ставить під загрозу конфіденційність, цілісність і доступність критичної інформації компанії.
6. Несанкційонований доступ до даних. Незаконне вилучення або перегляд даних конкурентами є однією з найнеприємніших ситуацій для будь-якої компанії. Хоча шифрування інформації допомагає знизити цей ризик, важливо пам'ятати про необхідність належного контролю за ключами шифрування.
7. Зловживання хмарними сервісами – залишається актуальною проблемою через відсутність суворих реєстраційних процедур у провайдерів хмарних обчислень. Механізми авторизації, що часто зводяться до наявності діючої кредитної картки, роблять доступ до хмарних послуг відносно відкритим. Це, у поєднанні з недостатньо ефективними методами виявлення шахрайства на етапі реєстрації, створює сприятливі умови для зловмисників. Вони можуть використовувати сучасні хмарні моделі, такі як платформа як сервіс (PaaS) та інфраструктура як сервіс (IaaS), для реалізації злочинних намірів.
8. Недостатня належна обачність у виборі хмарного провайдера – також є поширеною проблемою. Хоча основними перевагами хмарних обчислень вважаються скорочення витрат, можливість доступу до масштабованих ресурсів та зростання рівня безпеки, організації часто нехтують проведенням ретельного аналізу середовища хмарного провайдера (Cloud Service Provider, CSP). Це може призвести до виникнення розриву між очікуваннями та реальними механізмами безпеки, що пропонуються провайдерами. Для забезпечення належного рівня захисту, організаціям слід детально вивчати пропозиції CSP, а також оцінювати потенційні ризики, які супроводжують їх впровадження.
9. Процес міграції віртуальних машин серед гібридних або об'єднаних хмарах є ще одним викликом, який може бути вразливим до атак. Ненадійні механізми передачі даних можуть створити можливість для кіберзлочинців одержати несанкційонований доступ до інформації та перенаправити її на ненадійні сервери. Оскільки віртуалізація є основою архітектури IaaS, вона стає головною мішенню для кібератак. Впровадження ефективних методів шифрування та посилених заходів захисту в хмарних інфраструктурах здатне мінімізувати ризики, пов'язані з небезпечною міграцією віртуальних машин.

Загальна проблема вразливостей притаманна всім моделям хмарних обчислень через недосконаліть механізмів ізоляції між базовими складовими інфраструктури, платформ та програмного забезпечення.

При передаванні критично важливих даних і застосунків на хмарні платформи необхідно враховувати характерні особливості цих сервісів, потенційні загрози,

прозорість і ефективність засобів безпеки, а також актуальні технологічні пропозиції. Лише всебічний аналіз зазначених аспектів дозволить забезпечити належний рівень захисту та ефективне використання хмарних технологій.[6]

1.6. Вразливі місця хмарних обчислень

Перехоплення сесії означає випадки, коли хакери надсилають команди веб-додатку з метою отримання незаконного доступу до даних або використовують слабкі місця сервісу для виконання таких дій, як видалення користувацької інформації чи розсилка спаму через Інтернет.

Вихід за межі віртуальної машини – це вразливість, яка дає змогу зловмиснику виконати код на віртуальній машині, що надає можливість порушити її безпеку. Таким чином, стає реальним взаємодіяти безпосередньо з гіпервізором, отримуючи доступ до операційної системи хоста й інших віртуальних машин. Для захисту необхідне впровадження системи виявлення шкідливих дій на рівні віртуальних машин.

Застаріла криптографія створює загрозу через використання ненадійного або відсутність достатнього шифрування, що може призвести до розшифрування конфіденційних даних. Щоб уникнути подібних ризиків, слід забезпечити збереження справжніх даних у зашифрованому вигляді, належне управління ключами та використання продуманих алгоритмів.

Несанкціонований доступ до інтерфейсу управління загрожує безпеці хмарних послуг. Інтерфейс управління надає користувачам повноваження контролювати послуги. Однак у разі порушення безпеки зловмисники можуть отримати повний контроль над додатками та даними користувачів.

Інтернет-протокол може бути джерелом уразливості через брак способів аутентифікації, які не передбачені базовим протоколом. Це дозволяє атакуючим впроваджувати шкідливий трафік у мережу. Крім того, протоколи IP, UDP і TCP піддаються різноманітним атакам, наприклад DoS, а також ризику перехоплення сесій.

Відновлення даних у хмарній інфраструктурі сприяє динамічному перерозподілу ресурсів між користувачами. Проте ця функція може стати причиною витоку інформації, крадіжки та інших загроз. Зважаючи на те, що багато організацій співпрацюють із третіх сторін у процесах відновлення даних, важливо враховувати всі ризики та ретельно перевіряти безпеку постачальника послуг.

Система виставлення рахунків у хмарних обчисленнях розрахована на оптимізацію роботи з ресурсами, такими як зберігання даних, облікові записи користувачів і процесинг. Вразливості можуть виникнути в процесі обробки даних для виставлення рахунків, що загрожує фінансовими втратами через витік або маніпуляцію цією інформацією.

Замок постачальника означає залежність користувача хмарної платформи від конкретного провайдера. Це може створити суттєві проблеми при переході до іншого постачальника. Основною причиною такої ситуації є брак єдиних стандартів, що ускладнює зміну провайдера без значних труднощів. Перехоплення сесії означає

випадки, коли хакери надсилають команди веб-додатку з метою отримання незаконного доступу до даних або використовують слабкі місця сервісу для виконання таких дій, як видалення користувацької інформації чи розсилка спаму через Інтернет.

Вихід за межі віртуальної машини – це вразливість, яка дає змогу зловмиснику виконати код на віртуальній машині, що надає можливість порушити її безпеку. Таким чином, стає реальним взаємодіяти безпосередньо з гіпервізором, отримуючи доступ до операційної системи хоста й інших віртуальних машин. Для захисту необхідне впровадження системи виявлення шкідливих дій на рівні віртуальних машин.

Застаріла криптографія створює загрозу через використання ненадійного або відсутність достатнього шифрування, що може призвести до розшифрування конфіденційних даних. Щоб уникнути подібних ризиків, слід забезпечити збереження справжніх даних у зашифрованому вигляді, належне управління ключами та використання продуманих алгоритмів.

Несанкціонований доступ до інтерфейсу управління загрожує безпеці хмарних послуг. Інтерфейс управління надає користувачам повноваження контролювати послуги. Однак у разі порушення безпеки зловмисники можуть отримати повний контроль над додатками та даними користувачів.

Інтернет-протокол може бути джерелом уразливості через брак способів аутентифікації, які не передбачені базовим протоколом. Це дозволяє атакуючим впроваджувати шкідливий трафік у мережу. Крім того, протоколи IP, UDP і TCP піддаються різноманітним атакам, наприклад DoS, а також ризику перехоплення сесій.

Відновлення даних у хмарній інфраструктурі сприяє динамічному перерозподілу ресурсів між користувачами. Проте ця функція може стати причиною витоку інформації, крадіжки та інших загроз. Зважаючи на те, що багато організацій співпрацюють із третіх сторін у процесах відновлення даних, важливо враховувати всі ризики та ретельно перевіряти безпеку постачальника послуг.

Система виставлення рахунків у хмарних обчисленнях розрахована на оптимізацію роботи з ресурсами, такими як зберігання даних, облікові записи користувачів і процесинг. Вразливості можуть виникнути в процесі обробки даних для виставлення рахунків, що загрожує фінансовими втратами через витік або маніпуляцію цією інформацією.

Замок постачальника означає залежність користувача хмарної платформи від конкретного провайдера. Це може створити суттєві проблеми при переході до іншого постачальника. Основною причиною такої ситуації є брак єдиних стандартів, що ускладнює зміну провайдера без значних труднощів..

Перехоплення сесії означає випадки, коли хакери надсилають команди веб-додатку з метою отримання незаконного доступу до даних або використовують слабкі місця сервісу для виконання таких дій, як видалення користувацької інформації чи розсилка спаму через Інтернет.

Вихід за межі віртуальної машини – це вразливість, яка дає змогу зловмиснику виконати код на віртуальній машині, що надає можливість порушити її безпеку.

Таким чином, стає реальним взаємодіяти безпосередньо з гіпервізором, отримуючи доступ до операційної системи хоста й інших віртуальних машин. Для захисту необхідне впровадження системи виявлення шкідливих дій на рівні віртуальних машин.

Застаріла криптографія створює загрозу через використання ненадійного або відсутність достатнього шифрування, що може призвести до розшифрування конфіденційних даних. Щоб уникнути подібних ризиків, слід забезпечити збереження справжніх даних у зашифрованому вигляді, належне управління ключами та використання продуманих алгоритмів.

Несанкціонований доступ до інтерфейсу управління загрожує безпеці хмарних послуг. Інтерфейс управління надає користувачам повноваження контролювати послуги. Однак у разі порушення безпеки зловмисники можуть отримати повний контроль над додатками та даними користувачів.

Інтернет-протокол може бути джерелом уразливості через брак способів аутентифікації, які не передбачені базовим протоколом. Це дозволяє атакуючим впроваджувати шкідливий трафік у мережу. Крім того, протоколи IP, UDP і TCP піддаються різноманітним атакам, наприклад DoS, а також ризику перехоплення сесій.

Відновлення даних у хмарній інфраструктурі сприяє динамічному перерозподілу ресурсів між користувачами. Проте ця функція може стати причиною витоку інформації, крадіжки та інших загроз. Зважаючи на те, що багато організацій співпрацюють із третіх сторін у процесах відновлення даних, важливо враховувати всі ризики та ретельно перевіряти безпеку постачальника послуг. [7]

Система виставлення рахунків у хмарних обчисленнях розрахована на оптимізацію роботи з ресурсами, такими як зберігання даних, облікові записи користувачів і процесинг. Вразливості можуть виникнути в процесі обробки даних для виставлення рахунків, що загрожує фінансовими втратами через витік або маніпуляцію цією інформацією.

Замок постачальника означає залежність користувача хмарної платформи від конкретного провайдера. Це може створити суттєві проблеми при переході до іншого постачальника. Основною причиною такої ситуації є брак єдиних стандартів, що ускладнює зміну провайдера без значних труднощів.

Таблиця 1.1. Співставлення моделей загроз та їх аналіз

Характеристика моделі загроз	Моделювання загроз від Microsoft	TAM	PTA	Модель загроз для персональних мереж	Моделювання загроз у всебічній обчислювальній парадигмі	Модель Аміні-Джаміла
Виявлення та класифікація активів	✓		✓	✓	✓	✓
Встановлення ролей користувачів						✓
Ідентифікація сфер безпеки					✓	✓
Оцінка надійності					✓	✓
Сканування сфер безпеки						✓
Виявлення загрози	✓	✓		✓	✓	✓
Виявлення вразливості				✓	✓	✓
Здійснення контрзаходу					✓	✓
Оцінка та вимірювання загроз	✓	✓		✓	✓	✓
Оцінка та вимірювання вразливостей				✓		✓
Визначення нових активів, загроз, вразливих місць					✓	✓

1.7. Система класифікації рівнів безпеки інформаційних систем

Рівень безпеки інформаційної системи визначається застосовуваною технологією захисту та її ефективністю. У міжнародній практиці безпека систем класифікується на сім класів, які об'єднані в чотири рівні:

1. Рівень D: позначає відсутність належного захисту. Системи цього рівня мають слабкі механізми забезпечення безпеки, що дозволяє стороннім особам одержати доступ до внутрішньої інформації.
2. Рівень C: характеризується застосуванням довільного доступу. Він поділяється на два класи – C1 та C2. У класі C1 реалізовано поділ даних між користувачами, при цьому доступ до певних даних мають лише конкретні групи користувачів. Для аутентифікації застосовується запит пароля, а система оснащена апаратними та програмними засобами захисту. Клас C2 додає механізми забезпечення підзвітності користувачів через ведення журналу реєстрації доступів.
3. Рівень B: містить усі характеристики рівня C із додатковими елементами безпеки. Клас B1 передбачає розробку політик безпеки, застосування довіреної обчислювальної бази для управління мітками безпеки та реалізацію примусового управління доступом. Системи цього класу проходять ретельний аналіз і тестування вихідного коду та архітектури. Більш розвинений клас безпеки B2 охоплює такі механізми, як позначення всіх системних ресурсів

секретними мітками, реєстрація подій щодо створення прихованих каналів пам'яті, модульне структурування довіреної обчислювальної бази, формальна політика безпеки та висока стійкість до зовнішніх загроз. Клас B3 додає функції оповіщення адміністратора про порушення політики безпеки, аналіз прихованих каналів та механізми відновлення даних після збоїв програмного чи апаратного забезпечення.

4. Рівень A – найвищий рівень безпеки, це системи з доведеною математично коректною реалізацією політики безпеки, які забезпечують максимальний рівень захисту інформації. Основними особливостями рівня A будуть:
   Усі вимоги, які є до рівня B3 виконані, а саме мандатне керування доступом, чітка ізоляція процесів, повний аудит подій безпеки, захист від обходу механізмів контролю доступу. Визначена формальною моделлю безпеки – політика безпеки описується математично (формальна специфікація), а також визначено, як система повинна поводитися в будь-якому стані, а також формальною верифікацією – доведено (математично), що реалізація системи відповідає формальній моделі безпеки, а також аналізується коректність не лише концепції, а й реалізації самої системи. Окрім цього, безпека рівня A контролює весь життєвий цикл системи, має захищене проєктування, і контролює всі етапи циклу – контроль розробки, тестування, постачання та модифікацій, має захист від закладок і несанкціонованих змін. Також слід зазначити, що має комплекс засобів захисту, який дозволяє ізолювати всі критичні механізми системи, й унеможливлює модифікацію та обхід системи без порушення її цілісності. Зазвичай системи з рівнем захисту A застосовуються для обробка надзвичайно секретної інформації, використовуються у військових, розвідувальних та державних системах, а також у середовищах з максимальними вимогами до довіри. [8]

Контроль доступу є основним методом забезпечення інформаційної безпеки, передбачаючи управління доступом користувачів до ресурсів або системи. Ця концепція включає ідентифікацію, аутентифікацію та авторизацію. Історично першим підходом був контроль на основі ідентифікації користувача (Identification-Based Access Control, IBAC), який базувався на простому зв’язку між користувачем і доступом до системних ресурсів. Однак зі зростанням кількості мереж і користувачів цей підхід демонстрував обмеженості в аспектах масштабованості та контролю.

Для вирішення проблем IBAC було розроблено нові моделі, зокрема контроль доступу на основі ролей (RBAC). Цей підхід забезпечує доступ згідно до ролі клієнта, яка визначається принципом найменших привілеїв – тобто кожна роль отримує мінімально достатні дозволи для виконання певного обсягу завдань. Проте використання RBAC у великих організаціях зі складними адміністративними структурами виявило труднощі у визначенні привілеїв для різних ролей.

У відповідь на ці виклики була представлена модель керування доступом на основі атрибутів (ABAC). У цій моделі доступ визначається за специфічними характеристиками користувача, наприклад, датою народження або службовою

інформацією. Проте узгодження необхідного набору атрибутів між різними організаціями виявилося складним завданням.

Усі моделі контролю доступу базуються на процесі аутентифікації користувачів під час звернення до ресурсів чи систем. Ці методи вимагають чіткої координації між доменами та часто ускладнюють делегування адміністративних прав, що іноді обмежує функціонал систем або може порушити принцип найменших привілеїв.

Керування доступу, який побудований атрибутів ABAC є розширенням традиційної моделі контролю доступу зосереджений на ролях RBAC, пропонуючи значне розширення функціональності. Основні переваги ABAC зосереджені на:

- Можливість делегування повноважень для визначення атрибутів.
- Децентралізоване управління атрибутами та їх функціями.
- Перехрестя атрибутів дозволяє реалізувати комплексні політики конфіденційності і доступу.

Це дає організації змогу зберігати свою незалежність, забезпечуючи водночас продуктивну співпрацю. Окрім цього, система здійснює автоматизовані перевірки довіри, які можна переглядати за потреби.

Ця модель управління доступом сприяє збереженню автономності організацій, водночас забезпечуючи ефективну та гнучку співпрацю. Крім того, вона дозволяє автоматично налагоджувати довірчі відносини, які можна перевірити за потреби.

Однією з ключових проблем безпеки у хмарному середовищі залишається захист даних. До основних викликів належать забезпечення конфіденційності, доступності, коректного розміщення даних та їх безпечної передачі. Ризики включають втрату інформації, перебої в сервісі, зовнішні атаки чи багатокористувацьке недобросовісне використання. Цілісність даних визначається їхнім захистом від змін чи втрати несанкціонованими особами. Постачальники послуг хмарних обчислень несуть відповідальність за підтримку точності і цілісності даних власних клієнтів.

Користувачі також очікують високого рівня конфіденційності своїх персональних чи ділових даних. Для досягнення цього застосовуються різноманітні стратегії контролю доступу. Забезпечення конфіденційності безпосередньо залежить від надійності хмарної інфраструктури. Таким чином, гарантування цілісності, безпеки та конфіденційності інформації є фундаментальними аспектами роботи хмарних систем. Щоб досягти цього, необхідна постійна розробка й впровадження інноваційних методів захисту.

Архітектура хмарної системи зазвичай містить три взаємодіючі компоненти: клієнт або ж просто корисчтувач, хмарний сервер та третій довірений агент (TPA). Клієнт відправляє та зберігає власні дані на сервера, які надаються хмарним провайдером (CSP). TPA відповідає за періодичну перевірку цілісності даних клієнта та повідомлення про можливі зміни або похибки у них. При використанні послуг стороннього постачальника збільшується ризик витоку конфіденційної інформації у разі зламу системи або ненадійності самого постачальника. Одним із рішень цієї проблеми є шифрування даних безпосередньо на боці клієнта перед передачею їх до

хмари. Запити виконуються шляхом отримання зашифрованих даних з подальшою дешифрацією на стороні клієнта. Однак при роботі з базами даних це рішення може ускладнити процеси аналітики, оскільки для обробки запитів часто необхідно отримувати більшу кількість даних, ніж потрібно для кінцевого результату. На рисунку 1.1 відображається стандартна архітектура хмарного сховища даних.

Рисунок 1.1 – Архітектура хмарного сховища даних

Контроль доступу є одним із найважливіших механізмів безпеки у хмарних системах. Однак класичні моделі, такі як RBAC або ACL, стають недостатньо ефективними через специфіку хмарного середовища. Аналіз сучасних тенденцій показує, що найкращим рішенням буде застосування моделі ABAC для управління доступом у хмарних обчисленнях (Рисунок 1.2). Її адаптивність до динамічних умов експлуатації дозволяє враховувати різноманітні потреби багатьох користувачів і організацій із власними політиками безпеки. Наприклад, різні домени можуть використовувати різні стандарти авторизації: списки контролю доступу (ACL), декларації SAML чи політики XACML.

ABAC моделюється на основі чотирьох ключових компонентів:

1. Запитуюча сторона – надсилає запити до хмарного сервісу, ініціюючи тим самим виконання певних дій, передбачених функціоналом даного сервісу.
2. Хмарний сервіс – представлений сукупністю програмних та апаратних компонентів, оснащених мережевим інтерфейсом і запрограмованими операціями для обробки запитів.
3. Ресурс – є об'єктом взаємодії, на який спрямовані дії одного або декількох хмарних сервісів і який представляє сутність, залучену в процесі виконання операцій.
4. Навколишнє середовище – виступає як контейнер інформації, що може застосовуватися у випадках прийняття рішень, як надання доступу. Ця інформація включає дату й час або інші характеристики, які не обов’язково повинні бути прив’язані до конкретної сутності.

Модель управління доступом, заснована на атрибутах застосовує наступні ключові особливості:

1. Ієрархічна організація політик, яка базується на принципах абстракції і інкапсулювання для спрощення управління та структурного упорядкування.
2. Система складається з множини політик, кожна з яких може мати власний підхід до реалізації.
3. Для створення логіки прийняття рішень кожна політика містить окремі алгоритми оцінювання і виконання.
4. Не використовується єдиний універсальний підхід до опису механізмів роботи кожної політики, що дозволяє забезпечити варіативність та гнучкість в побудові моделей доступу.
5. Підтримка різноманітних стратегій реалізується ефективно завдяки адаптивності моделі до різних вимог і умов.
6. ABAC демонструє високу ступінь розширюваності та гнучкості, що дозволяє її налаштовувати відповідно до специфічних контекстів управління доступом.

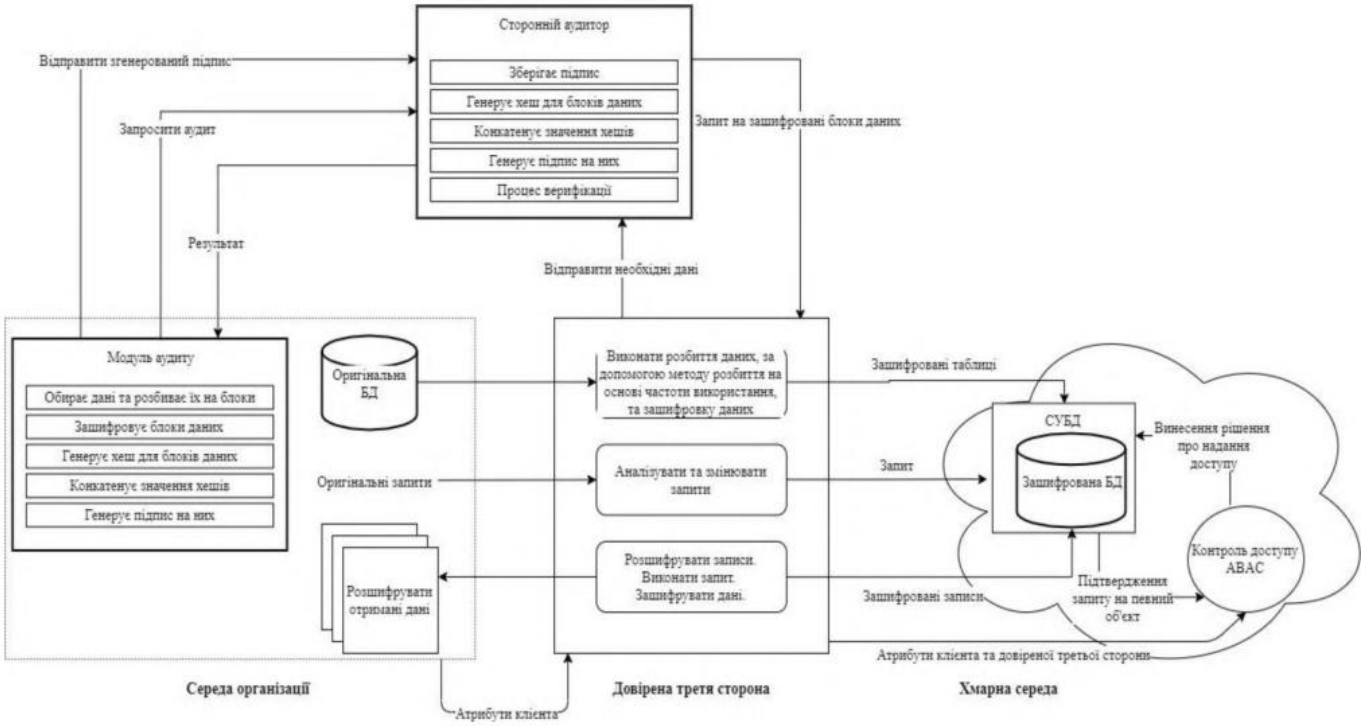


Рис. 1.2 – Схема архітектури системи аудиту зашифрованих даних та контролю доступу на основі атрибутів.

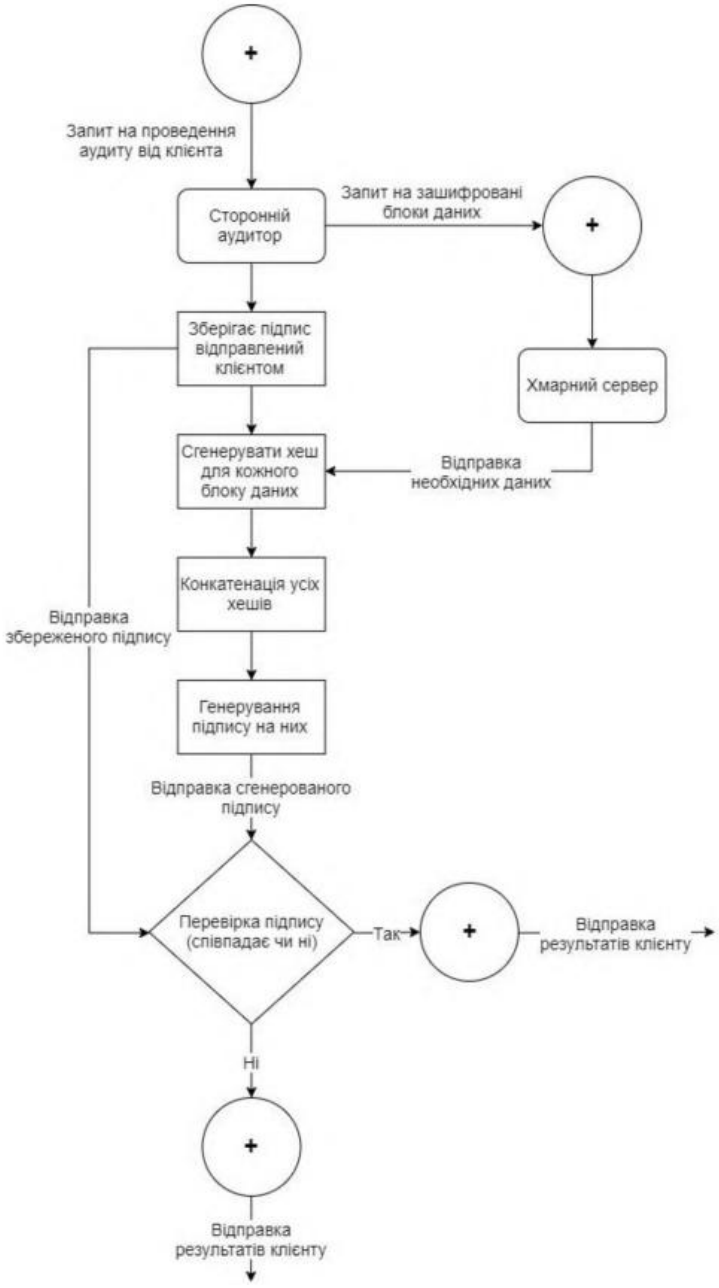


Рисунок 1.3 – Контроль доступу безпеки в хмарних сервісах

1.8. Алгоритми шифрування

Сучасна криптографія відзначається широким використанням відкритих алгоритмів шифрування, які дозволяють застосовувати обчислювальні засоби для забезпечення інформаційної безпеки. Сьогодні існує десятки перевірених методів шифрування, які, за умови використання ключа належної довжини та правильної реалізації алгоритму, забезпечують такий рівень захисту, що шифрований текст стає надзвичайно складним для розшифрування за допомогою криптоаналізу.

Основними вимогами до криптографічних методів захисту інформації є:

– Можливість розшифрування повідомлення виключно при наявності відповідного ключа.

- Кількість операцій, які необхідно виконати для визначення ключа на основі частини повідомлення та його відкритого тексту, має бути не меншою за загальну кількість можливих ключів.
- Обчислювальна складність розшифрування методом перебору ключів повинна мати нижню межу, яка перевищує потужності сучасних комп'ютерів, з урахуванням розвитку мережевих обчислень у майбутньому.
- Знання самого алгоритму шифрування не повинно погіршувати надійність системи безпеки.
- Мінімальні зміни в ключі повинні суттєво змінювати вигляд зашифрованого тексту навіть при використанні одного й того самого алгоритму.

Алгоритм повинен мати можливість реалізації в програмному або апаратному забезпеченні, при цьому зміна довжини ключа не повинна значно впливати на якість функціонування алгоритму.[9]

Серед основних напрямів застосування криптографії виділяють:

- Забезпечення аутентичності даних та їх юридичної значимості під час передачі або зберігання за допомогою алгоритмів електронного підпису та їх перевірки згідно зі стандартом RFC 4357 і сертифікатів формату X.509.
- Захист конфіденційності даних і контроль їхньої цілісності, зокрема через використання асиметричного шифрування та механізмів імітозахисту від підміни інформації. Ці заходи регламентуються ДСТУ Р 34.12-2015.
- Забезпечення безпеки системного та прикладного програмного забезпечення, включно з моніторингом несанкціонованих змін або порушень у роботі систем.
- Управління критично важливими компонентами системи відповідно до затверджених процедур і правил.
- Аутентифікація учасників обміну даними для встановлення довіри між сторонами.
- Захист з'єднань із використанням протоколу TLS.
- Захист IP-з'єднань через застосування протоколів IKE, ESP і AH.

Механізми захисту інформації в системах захисту критичної інформаційної інфраструктури (ЗКЗІ) підпорядковані реалізації багаторівневого підходу до безпеки, що включає різноманітні криптографічні методи та архітектурні рішення.

Захист конфіденційності збереженої чи переданої інформації реалізується через алгоритми шифрування, які забезпечують недоступність даних для несанкціонованого доступу й унеможливлюють їх компрометацію. При встановленні комунікаційного зв'язку ідентифікація надійності сторін застосовується за допомогою електронно цифрового підпису, який відіграє критичну роль в процесах аутентифікації.

У контексті цифрового документообігу застосування електронного підпису має подвійну функцію: гарантувати автентичність документа та забезпечувати захист від

повторного використання або нав'язування. Крім цього, обов'язковим є перевірка достовірності використаних ключів під час валідації електронних підписів.

Цілісність даних забезпечується застосуванням цифрового підпису як засобу захисту від їх модифікації, а також інтеграцією функцій асиметричного шифрування, що створює додатковий рівень безпеки. Для контролю цілісності використовуються криптографічні хеш-функції або алгоритми імітозахисту, хоча вони не дозволяють встановлювати авторство документа.

Захист від повторного використання інформації гарантується впровадженням криптографічних функцій електронного підпису у процеси шифрування чи імітозахисту. Кожна мережева сесія супроводжується генерацією унікального ідентифікатора значної довжини, що виключає можливість випадкового збігу, а його перевірка проводиться приймаючою стороною – сервером або комп'ютером.

Для уникнення ризику нав'язування чи втручання сторонніх осіб у комунікаційні процеси запроваджуються засоби цифрового підпису, що виступають гарантами захищеності каналу передачі даних і надійності встановленого зв'язку. Окреслені механізми забезпечують високий рівень інформаційної безпеки в сучасних системах ЗКЗІ.

Основні методи криптографічного захисту інформації можна класифікувати різними способами, але найчастіше їх поділяють за способом використання та типом ключа:

- Безключеві методи – це методи, в яких не використовуються ключі або інші засоби, такі як хеш-функції, генерація псевдовипадкових чисел чи односторонні перестановки.
- Перетворення з таємним ключем зосерджено на методах, що передбачають використання ключа, зокрема секретного ключа. До них відносяться симетричне шифрування, ідентифікація, хеш-функції й цифровий підпис.
- Перетворення з відкритим ключем зосереджено на методах, які використовують два ключі одночасно: відкритий, також відомий, як публічний та закритий, або ж приватний. Прикладами є асиметричне шифрування та цифровий підпис.

Таким чином, сучасна криптографія представляє собою багаторівневий підхід до забезпечення інформаційної безпеки, що інтегрує найсучасніші технології для ефективного захисту даних.

Методи симетричного шифрування та розшифрування – це засоби, за допомогою якого ключі шифрування та розшифрування являються або однаковими, або можуть бути просто обчисленими один з одним, надаючи спільний ключ, який при цьому є й таємним. Визначений метод шифрування володіє великою кількістю різних представників. [10]

Сучасні алгоритми симетричного шифрування представлені наступними найбільш розпоширеними системами й алгоритмами:

1. Система Lucifer – блочний симетричний алгоритм шифрування даних, розроблений компанією IBM у рамках дослідницької програми з комп'ютерної криптографії на початку 1970-х років.
2. Стандарт шифрування даних (Data Encryption Standard, DES) – симетричний алгоритм шифрування даних, затверджений урядом США та застосовуваний із 1976 року до кінця 1990-х. Згодом алгоритм став використовуватися в міжнародній практиці.
3. Міжнародний алгоритм шифрування даних (International Data Encryption Algorithm, IDEA) – блочний симетричний криптографічний алгоритм, запатентований швейцарською компанією Ascom.
4. Розширений стандарт шифрування (Advanced Encryption Standard, AES, Rijndael) – сучасний симетричний блочний алгоритм шифрування, прийнятий урядом США як стандарт у сфері захисту даних і станом на 2006 рік є одним із найпоширеніших у світі.
5. Blowfish – алгоритм блочного симетричного шифрування, створений Брюсом Шнайєром у 1993 році на основі криптографічної мережі Фейстеля.
6. ДСТУ 28147-89 – блокова криптографічна схема, що може реалізовувати функції потокового шифрування при використанні методу гамування.

Методи асиметричного шифрування базуються на використанні двох ключів для кожного учасника протоколу: відкритого для шифрування та закритого для розшифрування. Закритий ключ неможливо обчислити з відкритого за прийнятний проміжок часу. До сучасних асиметричних криптосистем належать: [11]

1. Схема McEliece – криптографічна система з відкритими ключами, що базується на теорії алгебраїчних кодів і використовує рандомізацію в процесі шифрування. Алгоритм зумовлює свою стійкість складністю декодування повних лінійних кодів.
2. Алгоритм Діффі-Хеллмана – криптографічна техніка, що використовує дискретне піднесення до степеня для обміну ключами.
3. Схема ElGamal – удосконалена криптографічна система з відкритими ключами, основана на складності обчислення дискретного логарифма у скінченному полі, яка подібна до алгоритму Діффі-Хеллмана.
4. RSA – популярна криптографічна система з відкритими ключами, безпека якої забезпечується через складність факторизації великих чисел.

Вимоги до використання засобів криптографічного захисту інформації (ЗКЗІ) спрямовані на забезпечення безпеки та конфіденційності інформації. ЗКЗІ використовуються для захисту даних через перевірку електронного підпису, шифрування та контроль хешів, особливо у корпоративних мережах і загальнодоступних інформаційних системах. Персональні засоби криптографічного захисту інформації призначені для охорони персональних даних користувача. При цьому особливу увагу варто приділяти захисту даних, які можуть містити відомості, пов'язані з державною таємницею, адже відповідно до законодавства, ЗКЗІ не дозволено використовувати для обробки таких даних. Перед початком роботи ЗКЗІ

головним етапом є перевірка програмного забезпечення, яке постачається. Істотну роль грає перевірка цілісності пакета установки шляхом порівняння контрольних сум, наданих постачальником. Після встановлення слід визначити рівень потенційних загроз і, відповідно до цього, обрати тип ЗКЗІ: програмні, апаратні або комбіновані апаратно-програмні рішення. Водночас значення має й правильне розташування системи захисту в інфраструктурі організації.

Електронний підпис є унікальним цифровим елементом документа, створеним за допомогою криптографічних алгоритмів. Його основне призначення полягає у забезпеченні цілісності документа, запобіганні несанкціонованим змінам та підтвердженні його авторства.

Сертифікат електронного підпису представляє собою окремий документ, що гарантує автентичність і належність електронного підпису його власнику через відкритий ключ. Цей сертифікат створюється і видається спеціалізованими організаціями – засвідчувальними центрами.

Власником сертифіката електронного підпису є особа, на ім’я якої зареєстровано цей сертифікат. Він функціонує завдяки двом ключам: закритому та відкритому. Закритий ключ використовується для створення електронного підпису, у той час як відкритий ключ служить для перевірки його справжності завдяки криптографічному зв’язку між цими двома ключами.

Типи електронного підпису включають такі категорії:

- Простий електронний підпис;
- Некваліфікований електронний підпис;
- Кваліфікований електронний підпис.

Простий електронний підпис забезпечується, наприклад, паролями, які захищають доступ до даних чи документів, або іншими схожими засобами ідентифікації власника.

Некваліфікований підпис створюється шляхом криптографічного перетворення даних із використанням закритого ключа. Завдяки йому можна встановити особу підписанта та перевірити, чи не було внесено несанкціонованих змін до документа.

Кваліфікований підпис відрізняється від некваліфікованого лише тим, що його сертифікат має бути виданий засвідченим центром, який має офіційний статус.

Застосування технологій електронного підпису є найбільш поширеним в обміні документацією. У межах внутрішнього документообігу він використовується для підтвердження чи затвердження документів, тобто виконує функцію особистого підпису або печатки. У зовнішньому документообігу наявність електронного підпису є критичним аспектом, оскільки він виступає як юридичний доказ.

Особливістю документів із електронним підписом виступає їх довготривала юридична значимість. На відміну від традиційних паперових документів з рукописними підписами або печатками, ці документи не піддаються фізичному зношенню чи пошкодженню і можуть зберігатися безстроково, не втрачаючи своєї правової сили. [12]

Алгоритми створення електронного підпису:

- Full Domain Hash (FDH) та Public Key Cryptography Standards (PKCS). Останній охоплює цілу групу стандартних алгоритмів, що застосовуються в різних ситуаціях.
- DSA і ECDSA – стандарти, прийняті у США для створення електронного підпису.
- ДСТУ Р 34.10-2012 – актуальний стандарт для створення електронного підпису в Росії, який замінив попередній ДСТУ Р 34.10-2001. Чинність останнього офіційно завершилася 31 грудня 2017 року.
- Країни Євразійського союзу користуються стандартами, повністю ідентичними російським.
- СТБ 34.101.45-2013 – білоруський національний стандарт для цифрового електронного підпису.
- ДСТУ 4145-2002 – стандарт, який регламентує створення електронного підпису в Україні, а також низка інших подібних стандартів.

Варто зазначити, що алгоритми створення електронного підпису можуть виконувати різні завдання та відповідати конкретним цілям, серед яких:

- Груповий електронний підпис.
- Одноразовий цифровий підпис.
- Довірений електронний підпис.
- Кваліфікований та некваліфікований підпис, а також інші види.

1.9. Структура системи захисту хмарної бази даних

Головною проблемою симетричного шифрування є необхідність передання секретного ключа, який використовується для розшифрування даних. Це створює ризик його перехоплення сторонніми особами, оскільки кожен, хто отримає доступ до цього ключа, зможе розшифрувати інформацію. Натомість в асиметричному шифруванні використовуються дві взаємопов'язані частини ключів – пара ключів. Відкритий ключ є публічним і доступний для кожного, хто хоче зашифрувати інформацію. Закритий ключ (приватний) зберігається конфіденційно та належить лише тій особі, яка має право розшифрувати дані. Важливо зазначити, що розміри закритого ключа значно перевищують параметри секретного ключа у симетричному шифруванні.

Інформацію, зашифровану відкритим ключем, можна розшифрувати лише за допомогою відповідного закритого ключа, використовуючи той самий алгоритм. Так само, якщо дані були зашифровані приватним ключем, їх можна розкодувати виключно за допомогою пов’язаного відкритого ключа. Завдяки цьому уникають потреби передачі приватного ключа, адже публічний ключ доступний відкрито. Однак головним недоліком асиметричного шифрування є його низька швидкість порівняно з симетричним методом, а також висока потреба в обчислювальних ресурсах для процесів шифрування та розшифрування.

Щодо токенів автентифікації – це спеціальні пристрої або електронні інструменти (зокрема апаратні токени, USB-ключі чи криптографічні модулі), які застосовуються для ідентифікації особи у цифровому середовищі. Наприклад, клієнт банку може використовувати токен для отримання доступу до свого рахунку. Токени можуть функціонувати як заміна пароля або працювати разом із ним. Таким чином, токен виконує роль своєрідного електронного ключа для забезпечення доступу. Це компактний фізичний пристрій, призначений для захисту особистої інформації користувача, ідентифікації його під час входу в систему або організації безпечного віддаленого доступу до різних ресурсів. Також він суттєво полегшує процес автентифікації.

Основним слабким місцем будь-якого токена залишається ризик його втрати чи крадіжки. Проте ймовірність злому або компрометації можна суттєво знизити завдяки дотриманню заходів персональної безпеки, таких як використання замків, сигналізацій або інших захисних заходів. Крім того, украдений токен стає непридатним для зловмисників, якщо технологія двофакторної автентифікації впроваджена належним чином.[13]

Зазвичай для автентифікації користувач вводить персональний ідентифікаційний номер (PIN) у поєднанні з інформацією, яка міститься на самому токені. Це забезпечує додатковий рівень безпеки під час доступу до систем чи ресурсів.Головною проблемою симетричного шифрування є необхідність передання секретного ключа, який використовується для розшифрування даних. Це створює ризик його перехоплення сторонніми особами, оскільки кожен, хто отримає доступ до цього ключа, зможе розшифрувати інформацію. Натомість в асиметричному шифруванні використовуються дві взаємопов'язані частини ключів – пара ключів. Відкритий ключ є публічним і доступний для кожного, хто хоче зашифрувати інформацію. Закритий ключ (приватний) зберігається конфіденційно та належить лише тій особі, яка має право розшифрувати дані. Важливо зазначити, що розміри закритого ключа значно перевищують параметри секретного ключа у симетричному шифруванні.

Інформацію, зашифровану відкритим ключем, можна розшифрувати лише за допомогою відповідного закритого ключа, використовуючи той самий алгоритм. Так само, якщо дані були зашифровані приватним ключем, їх можна розкодувати виключно за допомогою пов’язаного відкритого ключа. Завдяки цьому уникають потреби передачі приватного ключа, адже публічний ключ доступний відкрито. Однак головним недоліком асиметричного шифрування є його низька швидкість порівняно з симетричним методом, а також висока потреба в обчислювальних ресурсах для процесів шифрування та розшифрування.

Щодо токенів автентифікації – це спеціальні пристрої або електронні інструменти (зокрема апаратні токени, USB-ключі чи криптографічні модулі), які застосовуються для ідентифікації особи у цифровому середовищі. Наприклад, клієнт банку може використовувати токен для отримання доступу до свого рахунку. Токени можуть функціонувати як заміна пароля або працювати разом із ним. Таким чином,

токен виконує роль своєрідного електронного ключа для забезпечення доступу. Це компактний фізичний пристрій, призначений для захисту особистої інформації користувача, ідентифікації його під час входу в систему або організації безпечного віддаленого доступу до різних ресурсів. Також він суттєво полегшує процес автентифікації.

Основним слабким місцем будь-якого токена залишається ризик його втрати чи крадіжки. Проте ймовірність злому або компрометації можна суттєво знизити завдяки дотриманню заходів персональної безпеки, таких як використання замків, сигналізацій або інших захисних заходів. Крім того, украдений токен стає непридатним для зловмисників, якщо технологія двофакторної автентифікації впроваджена належним чином.

Зазвичай для автентифікації користувач вводить персональний ідентифікаційний номер (PIN) у поєднанні з інформацією, яка міститься на самому токені. Це забезпечує додатковий рівень безпеки під час доступу до систем чи ресурсів.

Багатофакторна автентифікація, знана також як multifactor authentication (MFA), – це покращений метод перевірки доступу до комп'ютерних систем, який вимагає від користувача надання більш ніж одного способу підтвердження своєї особи. Однією з підкатегорій БФА є двофакторна автентифікація (ДФА), яка забезпечує ідентифікацію за допомогою двох різних елементів аутентифікації.

Двофакторна автентифікація використовується у багатьох популярних сервісах, таких як Google та Microsoft. Наприклад, коли ви входите у свій обліковий запис із нового пристрою, окрім введення логіна і пароля, система запитує додатковий код підтвердження. Такий код може бути шестизначним (випадок з Google) або восьмизначним (випадок з Microsoft). Його можна отримати за допомогою SMS, голосового дзвінка, попередньо сформованого списку одноразових кодів або через спеціальний додаток-аутентифікатор, який генерує нові паролі кожні кілька секунд.

Налаштування цих методів здійснюються безпосередньо в обліковому записі відповідного сервісу. Сьогодні велика кількість провідних онлайн-платформ, як-от Google, Microsoft, Yandex, Dropbox чи Facebook, підтримують двофакторну автентифікацію. Користувачі можуть налаштовувати ці сервіси так, щоб використовувати єдиний додаток-аутентифікатор для генерації кодів. Серед популярних програм такого типу є Google Authenticator, Microsoft Authenticator, Authy та FreeOTP.

Для прикладу можна розглянути хмарне сховище iCloud від Apple. Доступ до нього також захищений двофакторною автентифікацією. Під час входу система надсилає запит на авторизацію через мобільний пристрій. Користувач підтверджує цей запит і отримує шестизначний код, який необхідно ввести для завершення процесу аутентифікації. Такий підхід значно підвищує рівень захисту даних в хмарі. Навіть якщо зловмисник отримає доступ до вашої електронної пошти та пароля, без підтвердження другорядним захисним фактором йому не вдасться зламати ваш обліковий запис.

Переваги використання двофакторної автентифікації через мобільний пристрій очевидні. Мобільний телефон завжди під рукою, тому не потрібно носити з собою

додаткові апаратні ключі. Крім того, коди підтвердження генеруються щоразу нові, що робить процес входу значно безпечнішим порівняно з використанням лише пароля.

Проте існують також певні недоліки такого підходу:

- Мобільний пристрій потребує стабільного сигналу мережі у момент авторизації. Якщо з'єднання відсутнє, є ризик не отримати повідомлення з кодом підтвердження.
- У разі передачі телефона іншій особі є ризик доступу до облікових записів або можливості отримання спаму в майбутньому.
- SMS із кодами можуть бути перехоплені зловмисниками за допомогою спеціальних методів атаки.
- Надсилання текстових повідомлень вимагає певного часу для обробки, що може призводити до невеликих затримок у разі автентифікації.

Загалом, двофакторна автентифікація є ефективним інструментом для захисту облікових записів і даних, хоча для її максимальної ефективності важливо враховувати можливі ризики й обирати оптимальні методи застосування.

Сучасні смартфони є інструментами, які широко використовуються для отримання електронних листів і SMS. Зазвичай електронна пошта на мобільному пристрої постійно залишається активною. Це створює певні ризики, адже всі акаунти, де використовується електронна пошта як основний елемент входу, можуть бути скомпрометовані в разі доступу до вашого телефону (перший фактор – пошта, другий фактор – сам пристрій). Таким чином, смартфон поєднує обидва фактори в одному пристрої. Проте зазначені ризики не завжди стосуються всіх сервісів, наприклад, сервісу хмарного зберігання iCloud. У цьому разі шестизначний код надсилається не через електронну пошту чи SMS, а безпосередньо у вигляді сповіщення. Це мінімізує ризик перехоплення повідомлення.

Резервне копіювання є одним із ключових методів забезпечення безпеки даних. Воно передбачає створення копії інформації з метою можливого відновлення у випадку її пошкодження чи втрати. Цей процес дозволяє зберегти дані навіть у разі виникнення критичних ситуацій, таких як умисне знищення важливої інформації або несанкціоноване видалення.

Об'єктами резервного копіювання можуть бути файли, папки, системні дані, образи віртуальних машин чи файлові системи. Для визначення параметрів резервного копіювання використовуються такі ключові поняття:

- Recovery Point Objective (RPO) – цільова точка відновлення, яка визначає часовий інтервал для створення резервних копій. У випадку втрати даних відновлення можливе на момент останньої RPO.
- Recovery Time Objective (RTO) – цільовий час відновлення, що визначає максимальний час, необхідний для повного відновлення доступу до даних користувачами.

Для підготовки підприємств до можливих катастроф слід також враховувати:

- Disaster Recovery Point Objective (DRPO) – цільову точку відновлення при катастрофах.
- Disaster Recovery Time Objective (DRTO) – час, який потрібен для повного функціонування після відновлення системи.

Існують різні рівні та типи резервного копіювання:

- Повне резервне копіювання (Full Backup або L0) створює повну копію даних. Воно є найбільш надійним методом, оскільки забезпечує точну відповідність між оригіналом і копією.
- Диференційне резервне копіювання (Differential Backup або L1) включає зміни, що сталися після останнього повного копіювання. Цей метод займає більше часу і простору порівняно з додатковим копіюванням, але значно швидше здійснює відновлення.
- Додаткове резервне копіювання (Incremental Backup або L2) зберігає лише ті зміни, що відбулися після будь-якого попереднього резервного копіювання. Для здійснення такого процесу потрібно менше ресурсів, однак повне відновлення займає більше часу через необхідність перегляду всіх попередніх копій.

Використовується також позначення Lx – система стандартів для опису методу резервного копіювання. Наприклад, якщо послідовність операцій виглядає як L0, L5, L3, L2, L4, відновлення здійснюється в наступному порядку: L0, L2, L4.[14]

Своєчасне й регулярне резервне копіювання особливо у хмарних середовищах суттєво знижує ризик втрати критично важливої інформації.

Висновок за розділом: Окрім практичної користі, знання з кібербезпеки формують відповідальну цифрову культуру. Вони сприяють розумінню того, як поводитися в онлайн-середовищі, як захищати власну приватність і чому варто критично оцінювати інформацію. У світі, де кібератаки стають інструментом економічного та політичного впливу, базова кіберграмотність є не лише технічною навичкою, а й елементом особистої та національної безпеки.

2. ЗАГРОЗИ ІТ СВІТУ

2.1. Кіберпростір.

Сучасне інформаційне суспільство, становлення і розвиток якого були офіційно визнані представниками країн Великої вісімки під час Окінавської зустрічі в липні 2000 року, засноване на інтеграції комп'ютерних та телекомунікаційних технологій. Розвиток цього суспільства визначається двома фундаментальними законами, що формують його напрям і динаміку.

Перший із них належить Гордону Муру, співзасновнику компанії Intel. Його закон передбачає, що кількість транзисторів у процесорах подвоюється кожні півтора року. Це спостереження стало основою для появи нових елементів інформаційної інфраструктури, наділених унікальними характеристиками. Закон Мура забезпечив прискорення обчислювальних процесів і збільшення обсягів оброблюваної інформації, що, у свою чергу, сприяло створенню в кінці XX століття інформаційного простору. Цей глобальний простір спроможний реалізувати оперативну і багатофакторну обробку даних, дозволяючи приймати стратегічно обґрунтовані рішення та ефективно використовувати наявні ресурси в найрізноманітніших умовах.

Другий визначний закон пов'язаний із Робертом Меткалфом, який розробив ключові мережеві технології. Згідно з його законом, цінність мережі зростає пропорційно квадрату кількості її вузлів. Це правило підкреслює важливість розгалужених мережевих структур у побудові інформаційного суспільства, де тісна взаємодія мереж формує єдиний інформаційний простір. Особливу роль цей закон відіграє у розвитку сучасних інформаційно-телекомунікаційних технологій, які сьогодні є базисом соціально-економічного й управлінського прогресу. Ці технології докорінно змінили способи функціонування різноманітних суспільних та державних інституцій, справляючи істотний вплив на формування високотехнологічного середовища та покращення якості інформаційних послуг як у фізичній, так і у віртуальній сферах.

Окремо варто виділити кілька ключових аспектів їхнього впливу:

1. Інформаційно-телекомунікаційні технології стали потужним двигуном розвитку сучасного суспільства та світової економіки, корінним чином трансформуючи механізми діяльності соціальних структур і державних органів.

2. Вони ввійшли до числа визначальних чинників створення організованого й інтегрованого інформаційного середовища, яке змінює якість обслуговування користувачів як у реальному світі, так і онлайн. Новітні технології сприяють вдосконаленню роботи інформаційно-аналітичних структур, підвищують ефективність управління та сприяють прийняттю раціональних, науково обґрунтованих рішень.

Завдяки поступовій інтеграції віртуального та реального середовищ за допомогою інформаційно-технологічних систем і мережевих технологій, здатних функціонувати як єдиний координаційний механізм, а також через упровадження інноваційного програмного забезпечення, було створено феномен кіберпростору. Кіберпростір є високотехнологічною моделлю об’єктивної реальності, де інформація про об’єкти, події чи процеси:

- представлена у вигляді сигналів, символів, звуків, статичних або динамічних зображень, а також інших форм;
- зберігається на спеціалізованих фізичних носіях даних;
- постійно передається та обробляється через інформаційні технології та мережеву інфраструктуру.

Сучасні інформаційно-комунікаційні технології не лише трансформують структуру соціальної взаємодії, але й створюють нові перспективи для оптимізації суспільного розвитку та управлінських процесів.

Вперше термін "кіберпростір" зафіксований в Окінавській хартії глобального інформаційного суспільства та Конвенції про кіберзлочинність, прийнятій 23 листопада 2001 року. У період виникнення цього поняття його регулювання базувалося на загальних правових механізмах, які охоплювали суспільні відносини. Ці механізми були зорієнтовані на певні об’єкти, інтереси сторін правовідносин, а також на комп’ютерні мережі, які забезпечували їхню взаємодію. З часом концепція кіберпростору зазнала трансформації, здобувши широкий спектр тлумачень, що відображають його багатогранність і розвиток.[15]

Зокрема, розуміння кіберпростору може бути визначене через такі підходи:

1. Відповідно до міжнародного стандарту, це середовище, яке виникає завдяки інтеракції між людьми, програмним забезпеченням та інтернет-послугами через використання технологічних пристроїв і мереж. Воно існує виключно у віртуальному вигляді, без фізичної форми.
2. За нормативною базою США – це сфера, в якій застосовуються електронні й електромагнітні засоби для збереження, модифікації та передачі даних через мережеві системи та пов’язану з ними фізичну інфраструктуру.
3. Офіційні документи Європейського Союзу визначають кіберпростір як віртуальний простір, у якому циркулюють електронні дані глобальних персональних комп’ютерів.
4. У межах офіційної нормативної бази Великобританії кіберпростір трактується як сукупність усіх видів мережевої і цифрової діяльності – контенту та дій, що здійснюються через цифрові мережі.
5. Відповідно до офіційних документів Німеччини, кіберпростір охоплює всю інформаційну інфраструктуру, доступну через інтернет і яка не обмежується жодними територіальними кордонами.

Кіберпростір можна охарактеризувати через декілька ключових аспектів:

- Це багатогранний віртуальний простір, створений за допомогою інформаційних систем. Він може охоплювати як складні цифрові світи, так і простіші варіанти, такі як електронна пошта чи глобальні навігаційні системи.
- Виступає як комунікаційне середовище, утворене комплексом взаємозв'язків між складовими кіберінфраструктури, включаючи електронні пристрої, комп'ютерні мережі, програмне забезпечення та інформаційні ресурси, що слугує задоволенню певних потреб у сфері інформації.
- Представляє собою штучне електронне середовище, де діють цифрові інформаційні об'єкти. Воно формується завдяки роботі кібернетичних систем управління та обробки даних і забезпечує доступ до ресурсів, створення електронних продуктів, обмін інформацією та співпрацю в реальному часі, наприклад у контексті надання послуг чи електронної торгівлі.
- Простір, який виникає завдяки функціонуванню інформаційно-комунікаційних систем, де відбуваються процеси трансформації даних: їх генерування, збереження, передача, обробка і видалення в цифровому форматі.
- Сукупність об'єктів інформаційної інфраструктури, що перебувають під управлінням автоматизованих інформаційних систем з одночасною циркуляцією відповідних даних.
- Інтегроване середовище, сформоване гармонійним поєднанням інформаційних процесів, побудованих на основі взаємопов'язаних і узгоджених принципів роботи інформаційних і телекомунікаційних систем.

Як випливає з наведених міркувань, найхарактернішими рисами кіберпростору як штучно створеної субстанції, формування якої зумовлене такими факторами, як зміна характеру людської діяльності, пов'язаної зі прийняттям рішень, впровадження електронних і цифрових методів створення, обробки, зберігання та передачі інформації, а також перехід від традиційного паперового документообігу до електронного, є його унікальні можливості. Ці можливості включають створення безлічі зв'язків між окремими індивідами та соціальними групами, а також надання різних інформаційних послуг, що підкреслює більшість експертів.

З огляду на специфічні характеристики кіберпростору як середовища, де можуть реалізовуватися сплановані деструктивні дії (наприклад, несанкціоноване втручання в інформаційно-телекомунікаційні системи, блокування або виведення з ладу їхніх критично важливих елементів, підрив оборонних автоматизованих систем управління, транспортних і енергетичних інфраструктур, економічної та фінансової системи), поряд із наземною, морською і повітряно-космічною сферами цей простір стає ключовим у сучасному розумінні безпеки. Крім того, кіберпростір постає своєрідним мостом між поняттями інтернету та кібернетики (Рисунок 2.1).

Це дозволяє:

– виокремити в цьому середовищі структуру взаємозв'язків між суб'єктами й об'єктами інформаційної та кібернетичної інфраструктури;

– окреслити злочини, втручання та загрози, які виникають через характерні особливості існування й передачі інформації;

– визначити потенційних «ключових акторів»;

– розглядати кіберпростір із позицій як віртуальної, так і реальної (електронної, комунікаційної, кібернетичної, інформаційної та навіть психологічної) складової.

У цьому контексті кіберпростір постає додатковим виміром бойового середовища, в якому вирізняють фізичний рівень (інфраструктура, кабелі, маршрутизатори), семантичний рівень (дані) і синтаксичний рівень (протоколи передачі даних).

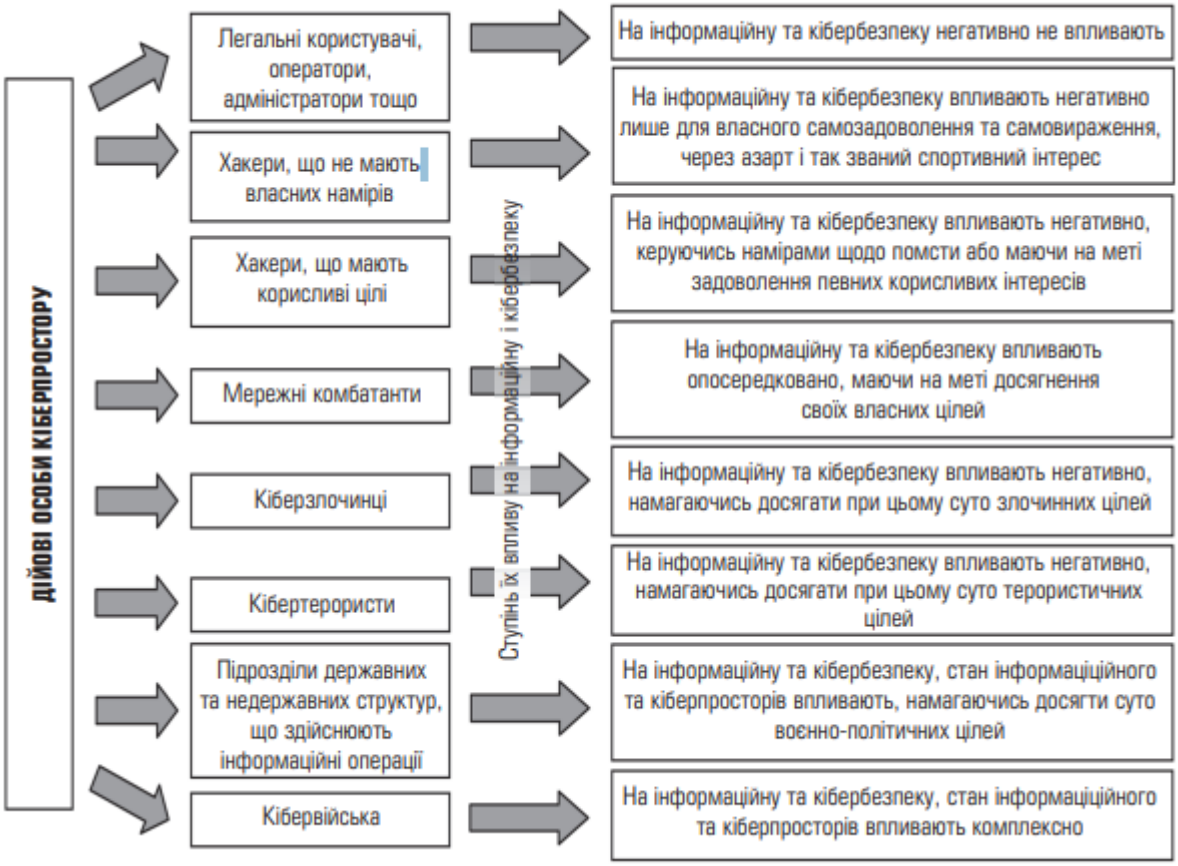


Рисунок 2.1 – Дійові особи кіберпростору та їхній вплив на кібербезпеку

Аналіз переваг та викликів сучасної системи глобальної маршрутизації У комп'ютерних мережах термін "маршрутизація" означає процес передачі пакета даних, адресованого логічним чином, від джерела до місця призначення через низку проміжних вузлів. Система маршрутизації охоплює механізми, правила та протоколи, які забезпечують функціонування цього процесу. Інтернет, як глобальна система з'єднаних комп'ютерних мереж, використовує подвійну структуру маршрутизації: внутрішньомережеву (intra-domain) і зовнішньомережеву, також відому як глобальна або міжмережева маршрутизація (inter-domain). Для глобальної маршрутизації встановлено єдиний набір правил і протоколів, що регламентують обмін інформацією у межах всієї мережі. Основні елементи системи глобальної маршрутизації включають мережеві префікси (ідентифікатори окремих комп'ютерних мереж), автономні системи (AS), які є об'єднанням одного чи кількох мережевих префіксів під

спільним управлінням, та протокол маршрутизації BGP-4. Цей протокол забезпечує обмін даними між автономними системами щодо досяжності мережевих префіксів відповідно до запрограмованого алгоритму та додаткових адміністративних правил, які ще називають політиками маршрутизації. Маршрутизація на рівні Інтернету характеризується двома ключовими підходами для оптимізації пошуку оптимального маршруту. По-перше, кожен вузол приймає рішення про напрямок передачі даних покроково, орієнтуючись виключно на власну інформацію, таку як локальні метрики, активні мережеві інтерфейси та таблиці маршрутизації. По-друге, використовується агрегування адресного простору в підмережі з використанням мережевих префіксів формату "адреса мережі/довжина маски". Таким чином, таблиці маршрутизації містять маршрути лише до мережевих префіксів, а не до всіх можливих адрес. Глобальна маршрутизація визначається як процес передачі інформації про маршрути між автономними системами через протокол BGP-4 (Рисунок 2.2). Вона успадковує основні властивості внутрішньомережевої маршрутизації – покрокове прийняття рішень та агрегування адрес – завдяки чому забезпечується її масштабованість навіть за умов швидкого зростання Інтернету. Проте безпечність цієї системи викликає дискусії. Головною проблемою є довірчий характер функціонування BGP-4, який не забезпечує механізмів перевірки достовірності отриманих даних. Як наслідок, вузли (тобто автономні системи) мають можливість оголошувати недостовірну інформацію про доступність маршрутів або маніпулювати атрибутами маршрутів для створення ілюзії їхньої привабливості. Відсутність механізмів валідації вхідної інформації в протоколі BGP-4 створює потенційні вразливості для маніпуляцій. Наприклад, автономна система може неправомірно заявити про наявність маршрутів до префіксів, які їй не належать, або оголосити про нібито коротші маршрути, що створює загрози для цілісності та безпеки даних. Отже, хоча сучасна система глобальної маршрутизації забезпечує високу масштабованість і ефективність функціонування Інтернету, значущі виклики у сфері інформаційної безпеки залишаються нерозв'язаними. Удосконалення протоколу BGP-4 шляхом впровадження механізмів перевірки достовірності та авторства повідомлень могло б значно підвищити стійкість системи до потенційних кібератак.

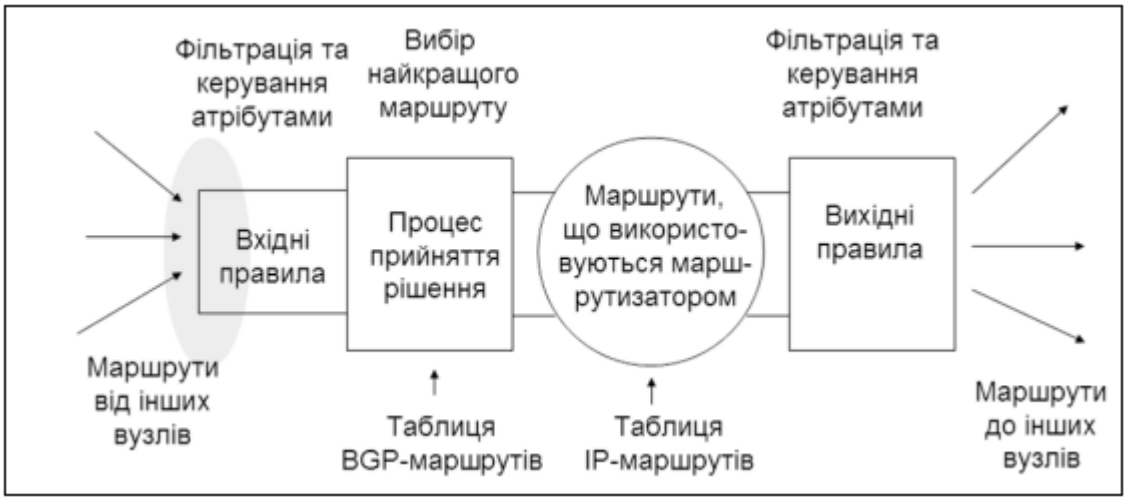


Рисунок 2.2 – Функціональна схема протоколу маршрутизації BGP-4

2.2. Інформаційна безпека

Інформаційна безпека (ІБ) за своєю сутністю становить стан захищеності інформаційного середовища держави, що передбачає усунення загроз або потенційної шкоди властивостям об’єктів безпеки, які взаємопов’язані з інформацією та її інфраструктурою. У цьому контексті забезпечується безперешкодний розвиток, ефективне використання та вдосконалення національної інформаційної сфери в інтересах захисту держави. (Рисунок 2.3).

Рисунок 2.3 – Схема характеристики Інформаційної безпеки

Складові інтересів ІБ щодо інформації, інформаційних систем і технологій як об'єктів безпеки можна згрупувати в такі категорії: доступність – можливість своєчасно отримати необхідну інформаційну послугу; цілісність – актуальність, несуперечливість та захищеність інформації від руйнування й несанкціонованих змін; конфіденційність – захист інформації від несанкціонованого доступу(Рисунок 2.4).

Ключовими загрозами, що можуть порушувати ці категорії, а також негативно впливати на компоненти інформаційної системи, спричиняючи їхній збій, втрату або знищення, є розголошення інформації, її виток чи несанкціонований доступ(Рисунок 2.5). [16]

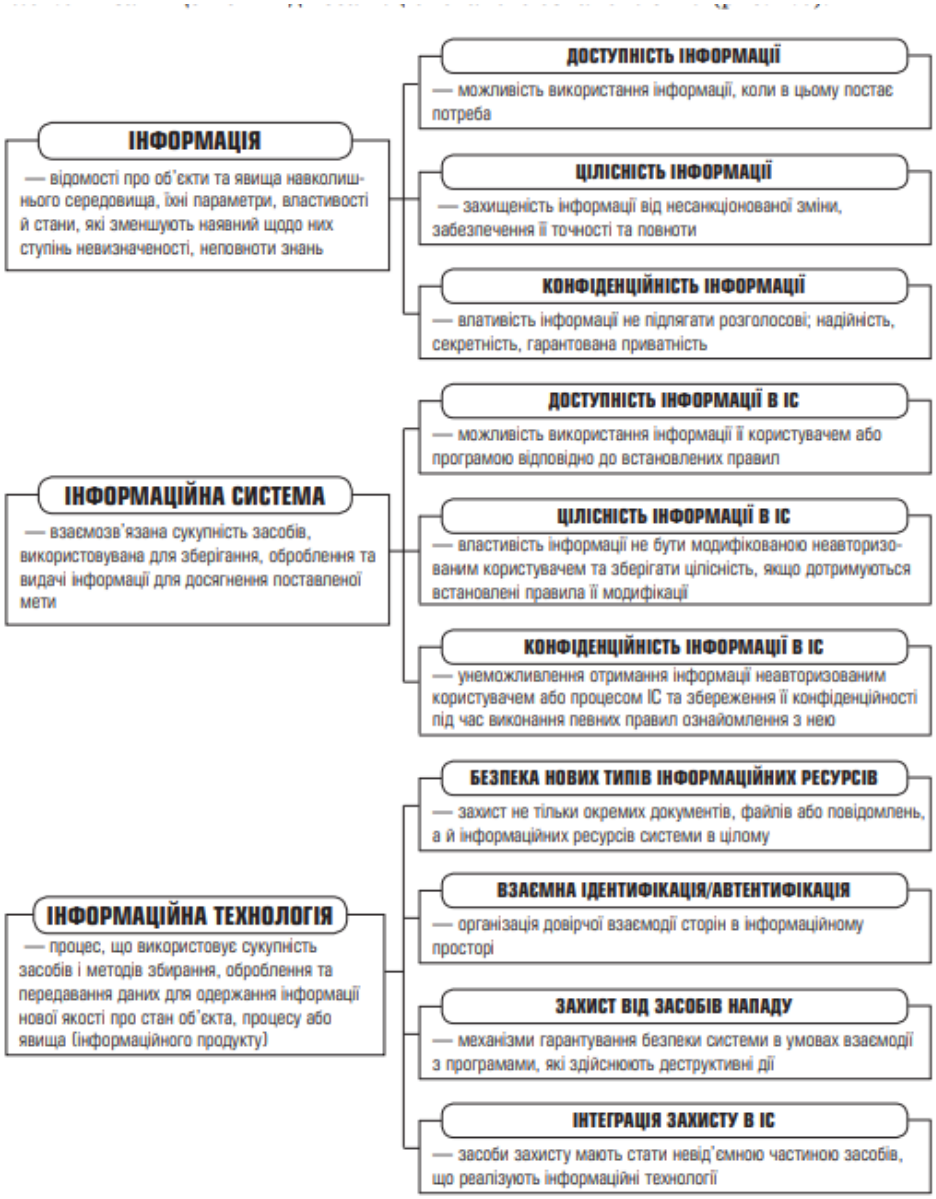


Рисунок 2.4 – Інформаційні системи та технології інформаційної безпеки

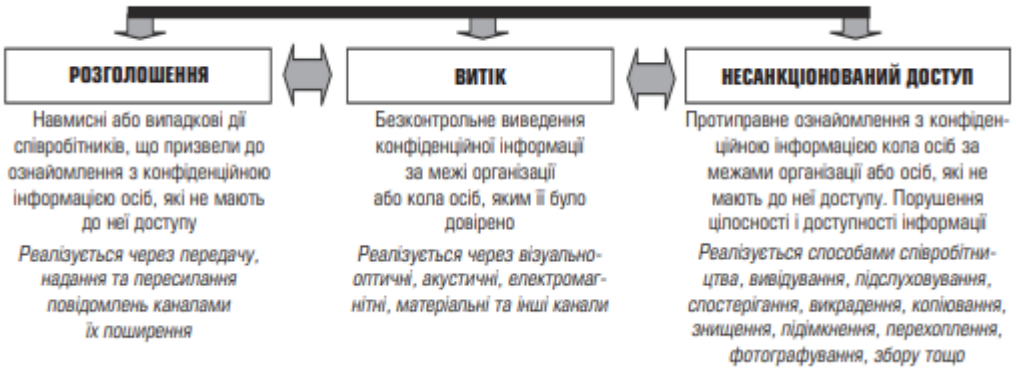


Рисунок 2.5 – Способи нанесення збитку інформаційній безпеці

Методи, спрямовані на запобігання загрозам і забезпечення належного рівня інформаційної безпеки, доцільно класифікувати наступним чином(Рисунок 2.6 та 2.7):

• Сервіси мережної безпеки, які включають механізми захисту інформації, що обробляється в межах розподілених обчислювальних систем і мереж;

• Інженерно-технічні методи, головною метою впровадження яких є запобігання витоку інформації через технічні канали;

• Правові та організаційні методи, що формують нормативно-правову основу для регламентації і управління діяльністю у сфері забезпечення інформаційної безпеки;

• Теоретичні методи забезпечення, які вирішують завдання формалізації різних процесів, пов’язаних із забезпеченням інформаційної безпеки.

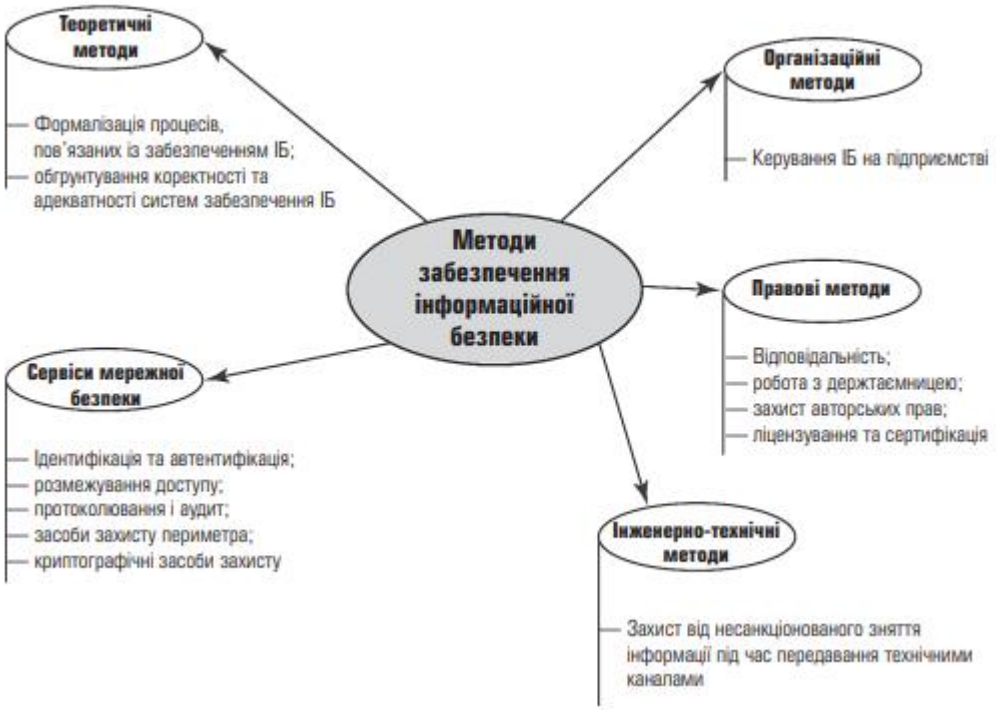


Рисунок 2.6 – Основні методи забезпечення інформаційної безпеки

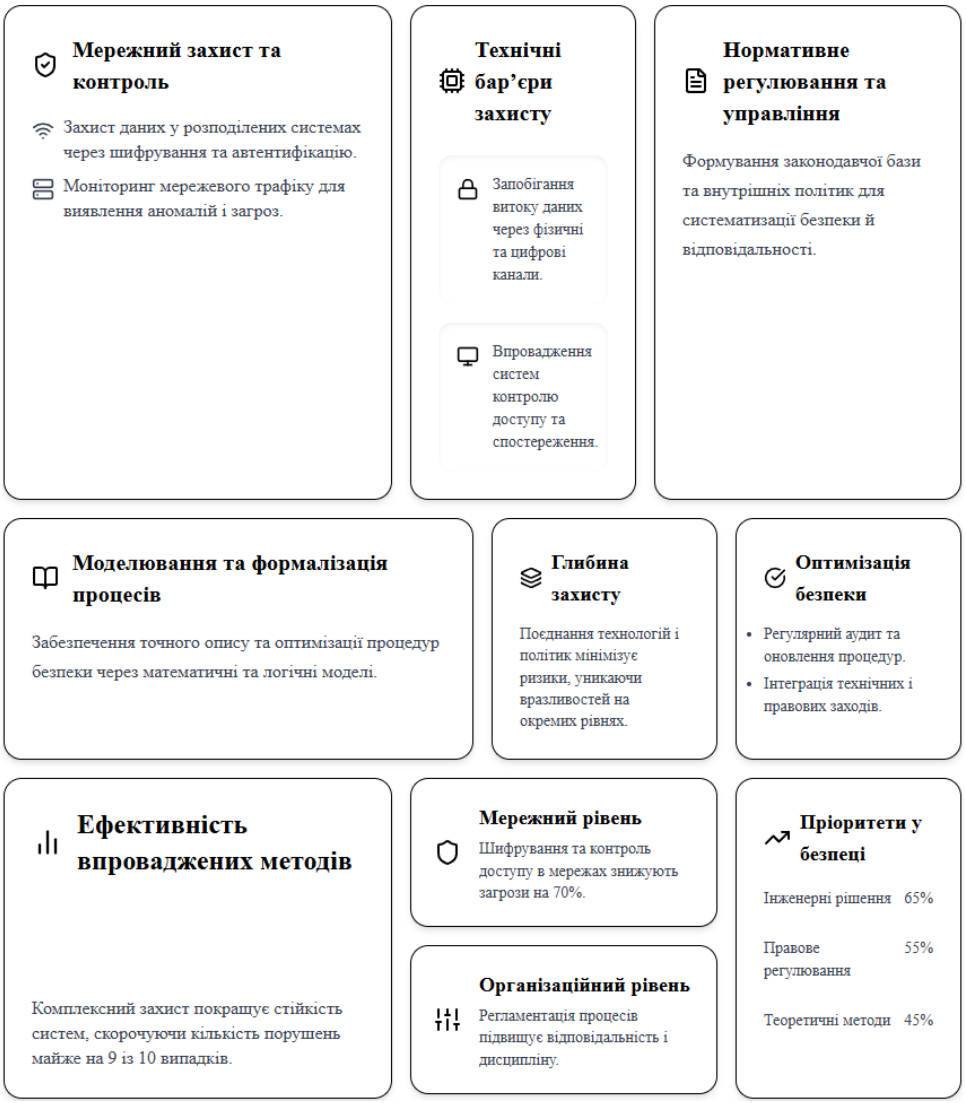


Рисунок 2.7 – коротка характеристика методів забезпечення інформаційної безпеки

З розвитком інформаційно-комунікаційних технологій (ІКТ), інформаційно-технічних систем (ІТС) та глобальної мережі Інтернет світове суспільство отримало безпрецедентні можливості в обміні даними, але одночасно стало надзвичайно вразливим до зовнішніх кібернетичних загроз. Це включає відкриті спроби впливу протиборчих сторін на інформаційний та кіберпростори одна одної шляхом використання сучасної обчислювальної техніки, спеціалізованого устаткування та програмного забезпечення. Такі дії зазвичай пов'язані з кібервтручаннями і створенням дестабілізуючого впливу на різні об'єкти, використовуючи технологічний потенціал інформаційного та кіберпростору. У результаті виникають так звані кіберзагрози, які несуть небезпеку не лише для цього простору, але й для людської свідомості. [17]

Для уникнення неоднозначного трактування термінів, Інтерпол надає класифікацію інцидентів у цій сфері та розділяє їх на такі групи:

– інциденти, безпосередньо пов’язані із комп’ютерами, як-от втручання в роботу обчислювальних систем, порушення авторських прав на програмне забезпечення, викрадення даних чи комп’ютерних ресурсів;

– інциденти за участі комп’ютерів, що супроводжують протиправні дії, наприклад, фінансове шахрайство;

– мережеві інциденти, що ведуть до укладання незаконних угод.

Інциденти у сфері високих технологій розглядаються як події, що реалізують певні загрози і порушують встановлений рівень безпеки інформаційно-комунікаційних систем. Управління такими інцидентами передбачає реєстрацію даних про стан безпеки й стабільності систем, передавання цієї інформації до відповідних пунктів для обробки й аналізу, ухвалення рішень та формування керуючого впливу на проблемні об’єкти.

Варто зазначити, що значний інтерес у контексті класифікації кібернетичних загроз і втручань викликає підхід, запропонований Конвенцією Ради Європи від 2001 року, яка має на меті протидію кіберзлочинності. У межах цієї Конвенції ідентифіковано чотири основні категорії подібних правопорушень.

Перша група охоплює інциденти, спрямовані на порушення конфіденційності, цілісності та доступності комп’ютерних даних і систем. Згідно із зазначеним документом, такі дії можуть включати:

– Несанкціонований доступ до інформаційного середовища, що передбачає протиправне умисне проникнення до комп’ютерної системи чи її сегментів, а також до інформаційних ресурсів (ІР) супротивних сторін, із обходом існуючих заходів безпеки.

– Втручання в дані, що виражається у протиправному зміненні, пошкодженні, видаленні, фальсифікації або блокуванні комп’ютерних даних і керуючих команд шляхом кібератак на інформаційні системи, мережі та ресурси, зокрема державного чи військового управління.

– Втручання в роботу системи шляхом порушення її функціонування або створення перешкод через розробку і поширення зловмисного програмного забезпечення (ПЗ), використання апаратних закладок чи здійснення радіоелектронного впливу на технічні пристрої й системи телекомунікацій.

– Незаконне перехоплення, яке охоплює несанкціоноване аудіовізуальне або електромагнітне отримання даних, які не призначені для публічного доступу та передаються в телекомунікаційній мережі з обходом захисних заходів.

– Незаконне використання чи вилучення комп’ютерного та телекомунікаційного обладнання.

Друга група порушень стосується шахрайства й підробки, пов’язаних із застосуванням комп’ютерних технологій:

– Підробка документів за допомогою електронних засобів, яка передбачає навмисне протиправне внесення змін, видалення або блокування даних з метою зниження достовірності документів.

– Шахрайство із застосуванням комп’ютерних технологій через втручання у функціонування інформаційних систем задля отримання протиправної економічної вигоди.

Третя група включає дії, пов’язані з поширенням протиправної інформації в мережах, зокрема контенту, пов’язаного з дитячою порнографією.

Четверта група охоплює правопорушення в сфері авторського права та суміжних прав (Рисунок 2.8).

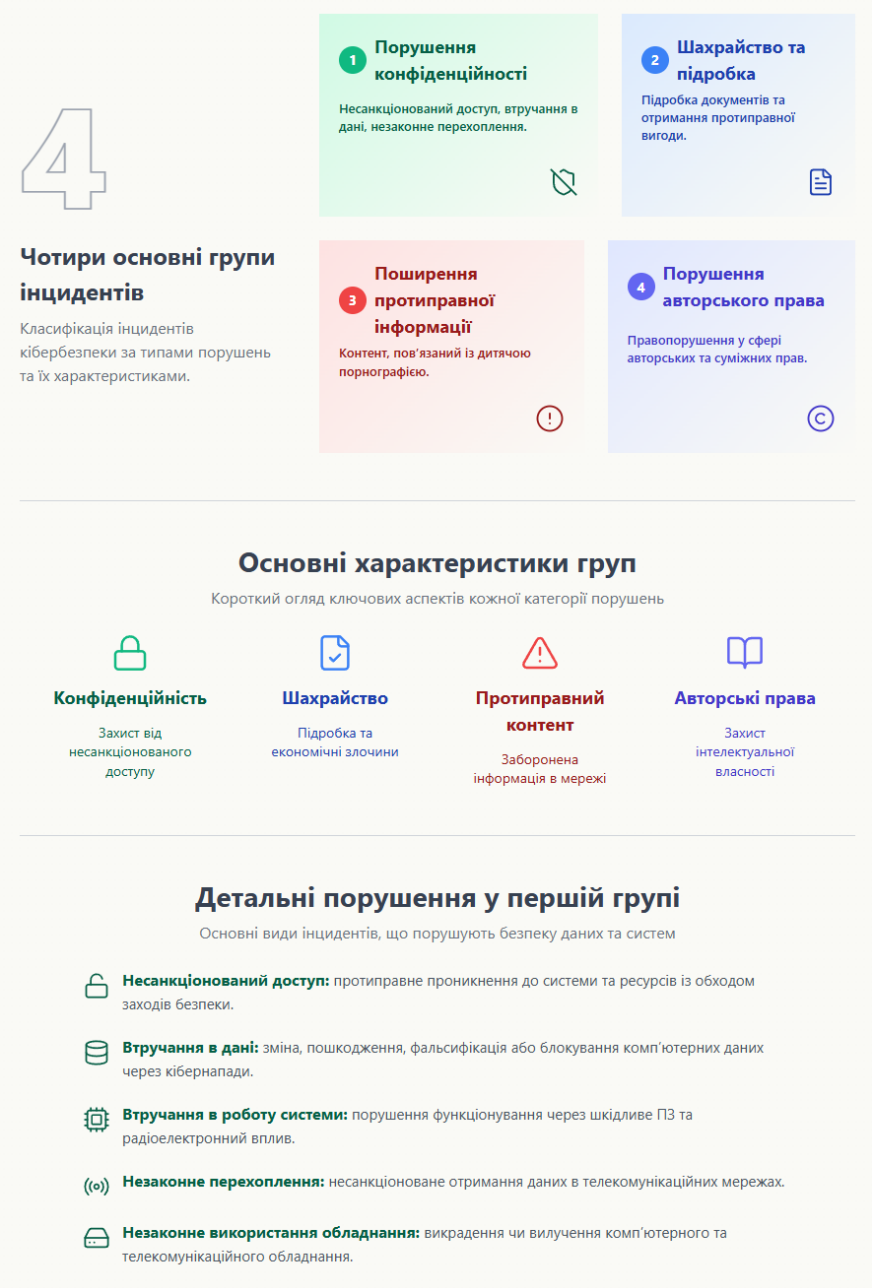


Рисунок 2.8 – Характеристика основних груп порушення кібербезпеки

У Сполучених Штатах відповідно до чинного законодавства протиправними вважаються дії, такі як несанкціонований доступ до інформації на комп’ютерах урядових органів, навмисне пошкодження або порушення їхньої роботи. Серед таких злочинів також зазначаються шпигунство, шахрайство, погрози, вимагання та

шантаж, а також використання комп’ютера для інших незаконних дій. До перелічених правопорушень входить торгівля викраденими чи підробленими пристроями доступу, що дозволяють отримувати фінансові кошти, товари або послуги. Це стосується й передачі комп’ютерних паролів чи подібної інформації, навмисного пошкодження майна, обладнання, систем зв’язку. Крім того, незаконне перехоплення і розголошення повідомлень (незалежно від способу передачі), порушення конфіденційності електронної пошти або голосових повідомлень, модифікація чи отримання збережених у пам’яті комп’ютера даних без дозволу та створення перешкод для санкціонованого доступу до інформації також вважаються злочином.

У Великобританії серед протиправних дій пов’язаних із інформаційними технологіями виділяють умисний незаконний доступ до комп’ютерів або внутрішніх даних, розголошення персональної інформації та створення або розповсюдження порнографічних матеріалів.

У Німеччині аналогічні правопорушення охоплюють несанкціонований доступ до комп’ютерних даних, модифікацію або приховання інформації без належного дозволу, підробку чи незаконне використання даних. Сюди ж належать руйнування технічного обладнання або вивід його з ладу, порушення таємниці телекомунікацій, комп’ютерне шахрайство і втручання в функціонування телекомунікаційних систем.

У Франції незаконні дії в сфері інформаційних технологій зазвичай включають перехоплення, крадіжку, використання або розголошення переданих повідомлень, нелегальний доступ до автоматизованих інформаційних систем, створення перешкод їхній роботі, знищення чи зміна даних в електронних системах. До порушень належать введення забороненої інформації в пам'ять комп’ютера, недотримання правил роботи з персональними даними, незаконний збір та обробка інформації, перевищення строків зберігання даних і несанкціоноване їх використання. Також злочинами вважається пошкодження й викрадення документів, обладнання та інформаційних систем або втручання в їхню роботу. Додатково у Франції під правопорушеннями згадують передачу даних з картотек чи ЕОМ іншій державі, копіювання секретної для національної безпеки інформації або ознайомлення сторонніх осіб із нею. Кримінальна відповідальність також передбачена за терористичні акти за допомогою цифрових технологій. [18]

2.3. Кібертероризм

Кібертероризм є суспільно небезпечною діяльністю, що навмисно проводиться в кіберпросторі або з використанням його технічних можливостей. Її здійснюють як окремі особи, так і організовані групи з терористичними цілями. Така діяльність включає заздалегідь сплановані та політично вмотивовані кібератаки на інформаційно-телекомунікаційні системи із застосуванням сучасних технологій (Рисунок 2.9).

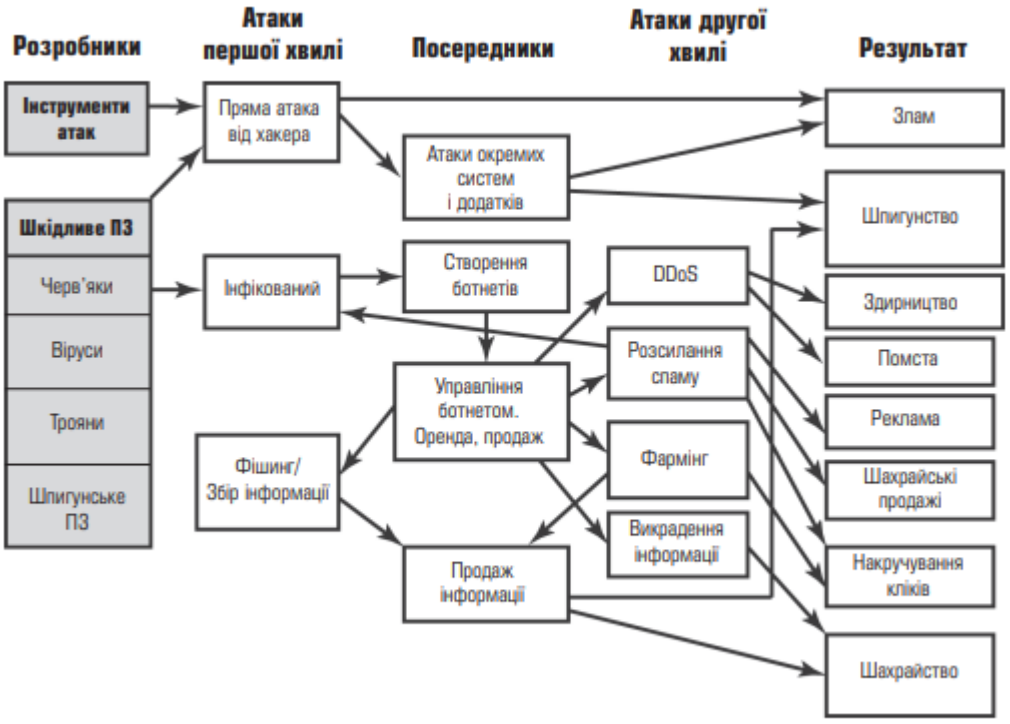


Рис. 1.30. Індустрія сучасного кібертероризму

Рисунок 2.9 – Індустрія сучасного кібертероризму

Сфера впливу кібернетичних технологій є доволі широкою – від формування помилкових рішень або провокування панічних настроїв до втручання в канали зв'язку та навігаційні системи. Наслідками подібних дій можуть стати, наприклад, внесення некоректного IP-адресу, порушення цілісності існуючої інформації, дестабілізація роботи критично важливих компонентів інформаційної чи кібернетичної інфраструктури держави. Це може призвести до серйозних змін у суспільно-політичній ситуації в державі та регіоні, ускладнення міжнародних відносин чи інших негативних наслідків, які становлять загрозу для життя і здоров'я громадян. Основні особливості кібернетичних технологій включають: [19]

– високу ефективність кібератак;

– невизначеність джерела атаки у просторі й часі та його віддаленість від цілі;

– несумісність часових рамок між самою атакою та її підготовчим процесом;

– потенціал організації багаторівневих атак на різні інформаційно-телекомунікаційні системи з багатьох напрямків одночасно.

У своїй діяльності методи кібертероризму можуть включати:

– нанесення збитків окремим елементам інформаційного та кібернетичного простору;

– руйнування апаратного обладнання, мереж електроживлення та компонентів інформаційно-телекомунікаційних систем (ІТС), а також створення перешкод за допомогою спеціальних програм, біологічних або хімічних засобів;

– викрадення чи знищення суспільно важливих інформаційних, програмних і технічних ресурсів кібернетичного простору шляхом подолання захисних систем, впровадження вірусів та різних прихованих інструментів;

– вплив на програмне забезпечення та інформацію з метою її викривлення або модифікації;

– розкриття або опублікування закритої інформації про державну інформаційну інфраструктуру, суспільно значущі військові інформаційні системи, шифрувальні коди та принципи їхньої роботи, що супроводжується загрозами;

– захоплення медійних каналів для поширення дезінформації, чуток, демонстрації сили терористичної організації та оголошення її вимог;

– знищення або цілеспрямоване блокування ліній зв'язку, штучне перевантаження комутаційних вузлів;

– проведення інформаційних і психологічних операцій.

Кібертероризм, як одна зі складових кіберзлочинності, займає вагоме місце серед загроз національній безпеці та інтересам України. Відповідно до соціологічних досліджень, на його поширення наразі впливають такі фактори:

1. Високий професійний рівень українських програмістів, яких активно залучають навіть провідні компанії світового масштабу, такі як Microsoft.

2. Швидка здатність молоді освоювати технічні новинки, про які раніше вони не мали жодних знань.

3. Швидкі темпи комп’ютеризації – кількість комп’ютерів в Україні щороку подвоюється – та значне збільшення числа інтернет-користувачів (з 500 тисяч у 2000 році до 5,8 мільйона у 2005-му).

До основних причин виникнення цих загроз експерти зараховують такі моменти:

– Недостатня увага органів державної влади до проблем інформатизації, попри очевидну економічну перспективу національного інтернет-сегмента.

– Відсутність необхідної державної фінансової підтримки як фундаментальних, так і прикладних досліджень у сфері боротьби з кіберзлочинністю.

– Відставання українського законодавства в галузі інформаційних технологій від нормативно-правових стандартів розвинених країн у межах глобального інформаційного простору.

– Низька пропускна здатність та ненадійність комунікаційного обладнання і каналів зв’язку.

– Недостатньо ефективна політика захисту комп’ютерних мереж і відсутність необхідних технічних засобів для забезпечення безпеки конфіденційної інформації у базах даних.

– Зростання можливостей для негативного інформаційного впливу на особу, суспільство та державу через нові телекомунікаційні технології, що стрімко розвиваються.

– Перехоплення електронної пошти, паролів і файлів завдяки доступним програмним засобам, які використовують зацікавлені особи чи організації.

У таких умовах основним напрямком для керівництва України є налагодження взаємодії та координації зусиль правоохоронних органів, спецслужб і судових

структур. Особливо важливо залучати Службу безпеки України (СБУ), Службу зовнішньої розвідки (СЗР), Державну службу спеціального зв'язку та захисту інформації (ДССЗЗІ), а також Міністерство внутрішніх справ (МВС). Їхня діяльність має бути спрямована на забезпечення безпеки національного інформаційного простору, посилення кіберзахисту вітчизняної ІТ-інфраструктури та активну протидію кіберзагрозам із внутрішніх і зовнішніх джерел.

Однак стримувати фізичне знищення технічних засобів, дезорганізацію роботи інформаційних систем й мереж, а також порушення функціонування об'єктів впливу (інформації, що циркулює в інформаційно-телекомунікаційних системах, баз даних і програмного забезпечення), стає дедалі складніше через зростання активності кіберзлочинців.

Вирішенню даних проблем заважає низка чинників:

– складність забезпечення захисту міжмережевої взаємодії;

– наявність вразливостей і помилок у програмному забезпеченні, операційних системах і утилітах, які публічно розповсюджуються мережею;

– некоректне або неефективне адміністрування систем;

– слабкий захист даних у багатьох сучасних мережних протоколах;

– недоліки в конфігурації систем безпеки чи навіть повне нехтування їх впровадженням.

Ці обставини пояснюють високу ефективність кібератак, майже кожна з яких досягає запланованого результату, що підкреслює нагальну потребу у виявленні подібних загроз і запобіганні їх наслідкам.

Серед головних заходів, які сприятимуть розв'язанню цих завдань, варто виділити дослідження вразливостей програмного забезпечення за даними таких організацій, як Bugtraq (http://www.securityfocus.com) і CERT (http://www.cert.com). Додатково необхідно впроваджувати інструменти для розпізнавання атак, використовувати програмні рішення, які дозволяють аналізувати всі мережеві пакети, спеціалізоване аналітичне програмне забезпечення разом із логами операційних систем і мережевими журналами. Важливим також є застосування евристичних механізмів захисту й сучасних антивірусних рішень для зменшення ризиків.

2.4. Національно-державні загрози

Минулого року кіберзагрози, пов'язані з національними державами, ще раз продемонстрували, що кібероперації – чи то з метою шпигунства, знищення чи впливу – відіграють постійну допоміжну роль у ширших геополітичних конфліктах. У війнах у Європі та на Близькому Сході Росія та Іран зосередили свою загрозливу діяльність на своїх головних противниках у цих боях, Україні та Ізраїлі відповідно. Тим часом довДСТУрокова зосередженість Пекіна на контролі над Тайванем призвела до того, що китайські загрозливі актори активно атакували тайванські підприємства, які також проникали в країни навколо Південно-Китайського моря, щоб отримати інформацію про військові навчання та національну політику. Далі наведено знімок активності за номерами.

Сполучені Штати стабільно входять до числа країн, які найбільше постраждали від кіберзагроз національних держав, які спостерігає Microsoft, що є відображенням великого представництва США в нашій клієнтській базі та ролі, яку Сполучені Штати відіграють у дослідженнях і розробках і геополітичних подіях. Крім Сполучених Штатів і Великої Британії, яка була п'ятою країною за кількістю нападів цього року, більшість спостережуваної нами кіберзагрози, пов'язаної з державою, була зосереджена в місцях активного військового конфлікту або підвищеної регіональної напруги: Ізраїль, Україна, Об'єднані Арабські Емірати та Тайвань. Сектор освіти та досліджень став другим найбільш об'єктом загрози для національних держав (Рисунок 2.11).

У 2024 році освіта та дослідження стали другим сектором, який найбільше націлений на національну державу. Окрім надання розвідувальних даних, таких як дослідження та обговорення політики, освітні та дослідницькі установи часто використовуються як полігони для загроз, перш ніж вони переслідують свої фактичні цілі (Рисунок 2.10, Рисунок 2.12 та Рисунок 2.13).

Наприклад, фішинг QR-коду, техніка, яка зараз широко використовується для компрометації облікових записів користувачів у великих масштабах і створення точки входу для атак компрометації бізнес-електронної пошти (ККЕП), про які йдеться далі в цьому розділі, став широко використовуватися в цілеспрямованих атаках на цей сектор ще в серпні 2023 року.

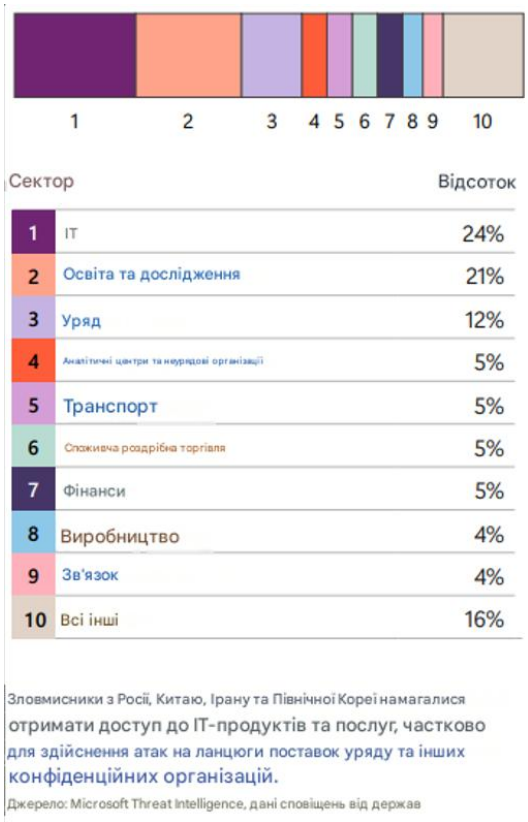


Рисунок 2.10 – 10 найбільших цільових секторів для кібератак

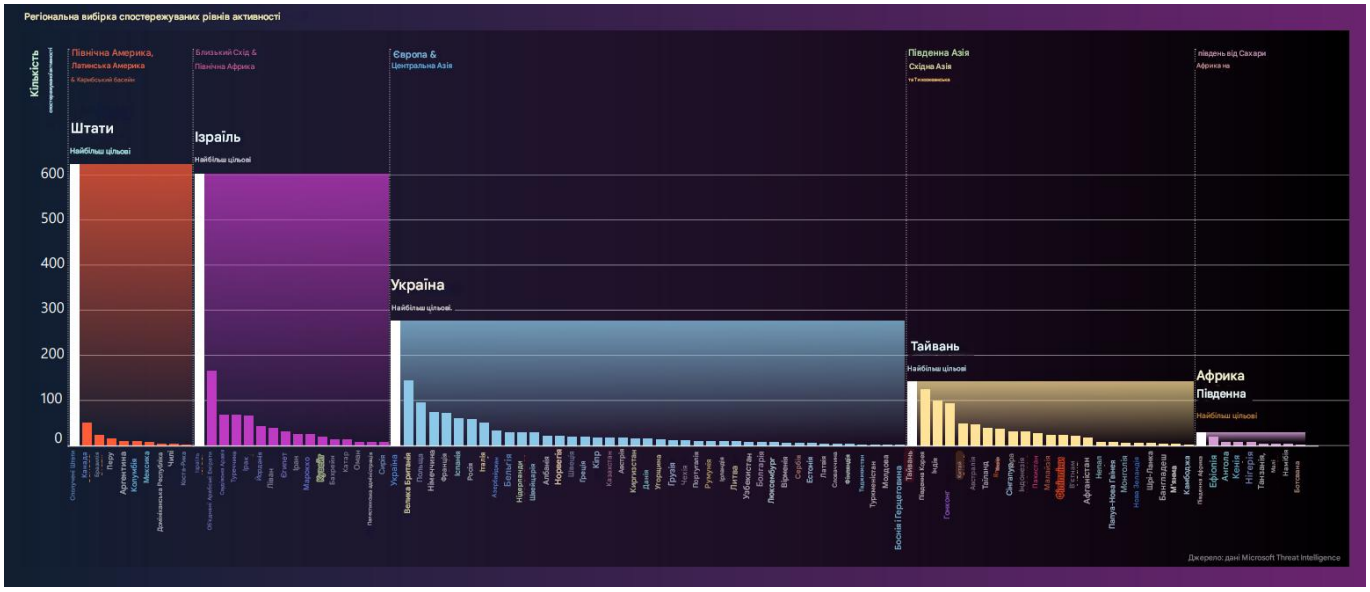


Рисунок 2.11 – Цільові загрози кіберзлочинів на державному рівні

Рисунок 2.12 – Лідери рейтингу країн за рівнем загрози кіберзлочинності

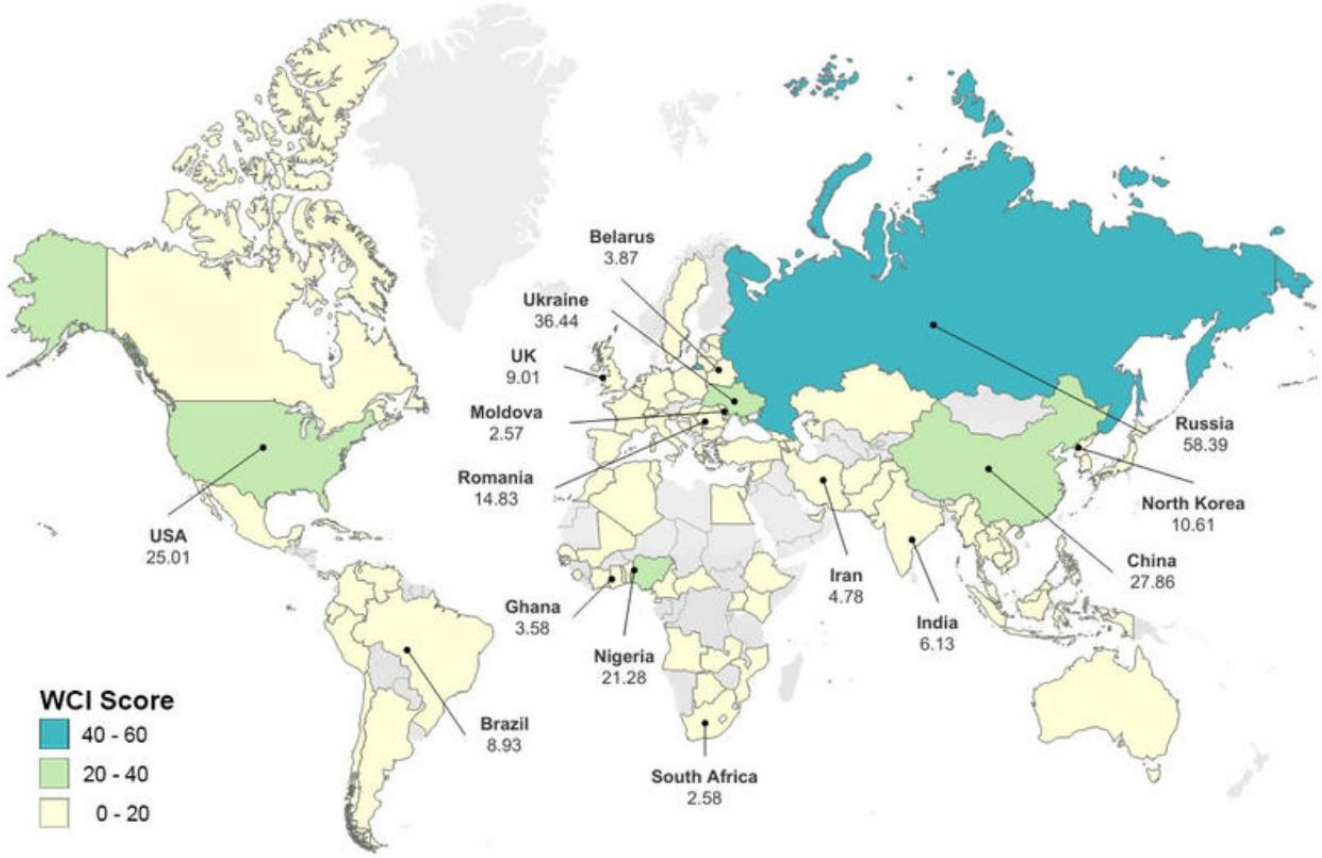


Рисунок 2.13 – Рейтинг країн за рівнем кіберзлочинності

Російські хакери, як державні, так і незалежні, активно беруть участь у різноманітних кібератаках, які можуть мати руйнівні наслідки для інфраструктури, економіки та політичної стабільності багатьох країн.

Одним із ключових аспектів російської кіберзагрози є використання інформаційних технологій для досягнення політичних і стратегічних цілей. Російські хакери, часто пов'язані з державними установами або підтримувані державою, втручаються у вибори, дезінформують громадську думку, а також здійснюють кібершпигунство. Наприклад, у 2016 році група Fancy Bear, пов'язана з російськими спецслужбами, втрутилася у вибори президента США, поширюючи фейкові новини та дані, отримані в результаті злому серверів Демократичної партії.

Окрім політичних цілей, Росія активно використовує кібератаки для підриву критичної інфраструктури інших країн. Відомі випадки атак на енергетичні системи, водопостачання, фінансові мережі та інші важливі елементи інфраструктури. Ці атаки можуть призвести до значних економічних втрат і порушення роботи життєво важливих систем.

Ще однією серйозною загрозою є створення та розповсюдження кібервійськ і кіберзлочинних угруповань, які діють не лише в інтересах держави, а й з комерційних мотивів. Ці групи займаються кібершантажем, крадіжкою даних, розповсюдженням шкідливого програмного забезпечення та створенням фальшивих фінансових схем.

Крім того, Росія активно розвиває свій кіберпотенціал, нарощуючи потенціал гібридної війни, де кібератаки відіграють ключову роль поряд з традиційними

військовими методами. Це посилює глобальну напругу та загрожує безпеці як окремих країн, так і всього світового співтовариства. [20]

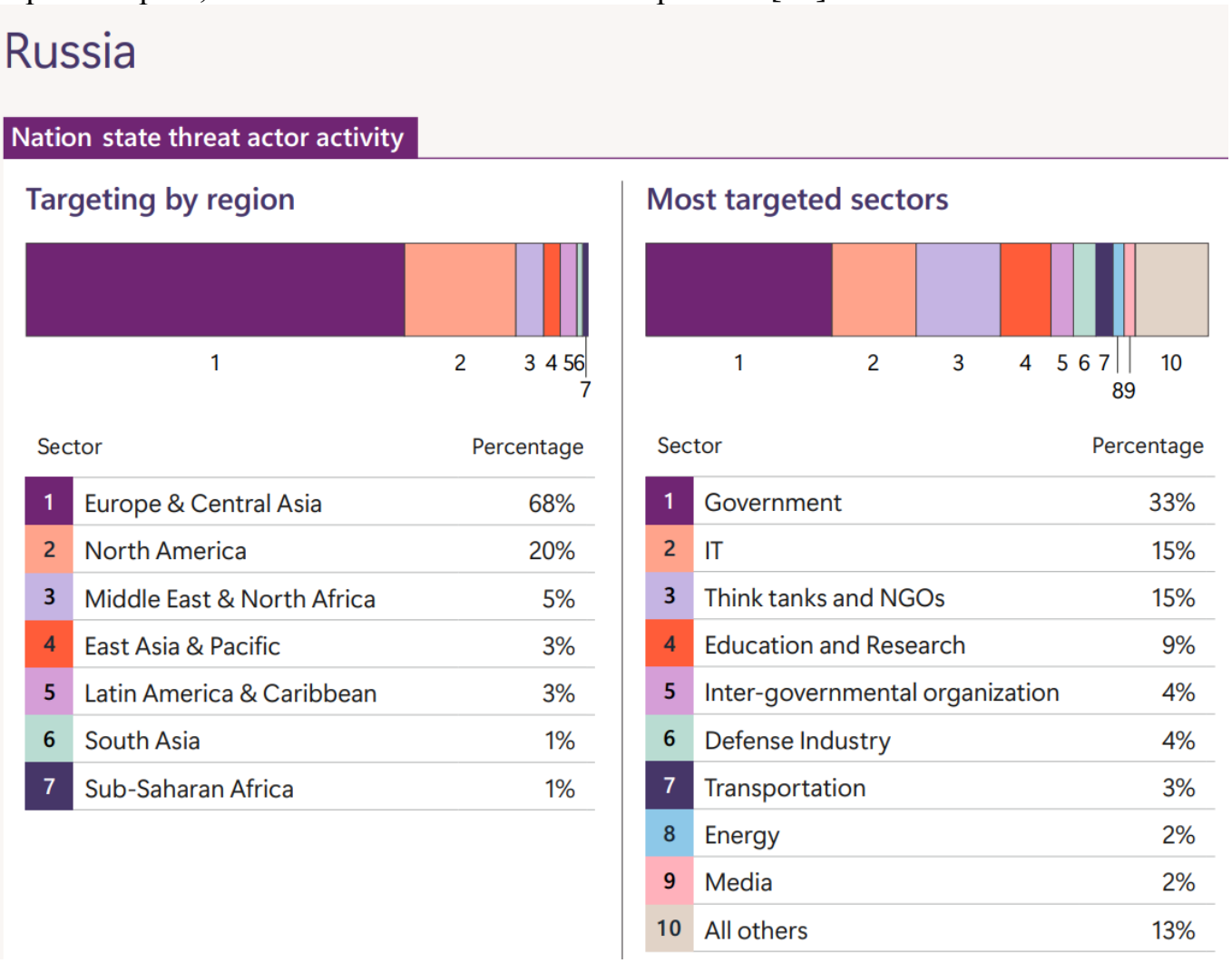


Рисунок 2.14 – статистика активності хакерів Росії по регіонам та сферам життя

Приблизно 75% цілей були в Україні або держави-члени НАТО, оскільки Москва прагне зібрати розвіддані про політику Заходу щодо війни. Україна залишається країною, на яку найбільше нападають російські актори.

Російські хакери зосередили свої дії проти європейських і північноамериканських урядових установ і аналітичних центрів, ймовірно, для збору розвідданих, пов’язаних з війною в Україні. Актори, такі як Midnight Blizzard, також націлилися на IT-сектор, припускаючи, що він частково планував атаки на ланцюги поставок, щоб отримати доступ до мереж клієнтів цих компаній для подальших операцій (Рисунок 2.14).

Кіберзагроза з боку Китаю вважається більш масштабною у порівнянні з російською у сучасному світі. Вона формується у поєднанням державних стратегій, технологічного потенціалу, економічних інтересів і діяльності як офіційних структур, так і пов’язаних з ними груп. На відміну від хаотичних або злочинних кібератак, багато китайських операцій є системними, довгостроковими та стратегічними.

Кібершпигунство вважається одним з ключових напрямків китайської кіберактивності. Його цілями часто є уряди, міжнародні організації, оборонні

структури та високотехнологічні корпорації. Китайські хакерські групи прагнуть отримати інтелектуальну власність, інновації, дані про постачання та виробництво, а також політично конфіденційну інформацію. Такий підхід дозволяє прискорити власний технологічний розвиток, зменшивши потребу в тривалих і дорогих дослідженнях, а також зміцнити свої економічні позиції в глобальній конкуренції.

Ще одним важливим аспектом є намір Китаю розширити свій вплив у цифровому просторі. Це очевидно у створенні інфраструктурних проектів, таких як ініціативи Цифрового шовкового шляху, а також у поширенні китайських телекомунікаційних технологій і технологій спостереження по всьому світу. Хоча ці технології можуть принести користь, вони також викликають занепокоєння, оскільки країни побоюються можливого прихованого доступу до критично важливих даних або можливості дистанційного керування.

Окрім того, деякі операції, приписувані китайським групам, спрямовані на підрив стійкості іноземних систем. Це включає спроби проникнення в енергетичні, транспортні, комунікаційні та інші критичні мережі. Навіть якщо атаки не завдають прямої шкоди, сама наявність шкідливого коду або потенційних бекдорів створює значні ризики для національної безпеки держав.

Окремим напрямком є інформаційні операції. Китайські організації можуть використовувати кіберпростір для поширення сприятливих наративів, контролю над інформаційними потоками, впливу на громадську думку та формування міжнародного іміджу. Хоча ці дії не завжди є прямими нападами, вони можуть впливати на політичну динаміку та дестабілізувати інформаційне середовище.

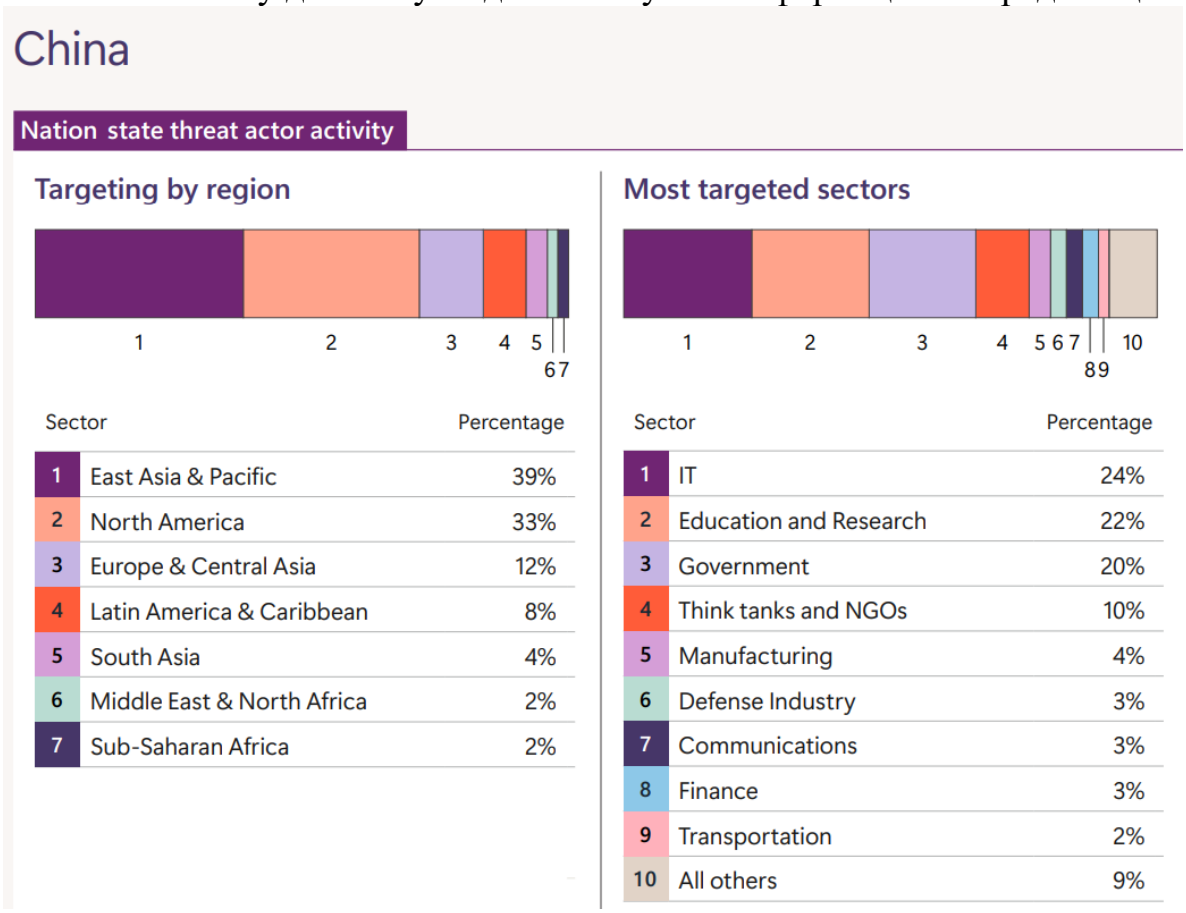


Рисунок 2.15 – статистика активності хакерів Китаю по регіонам та сферам життя

Зусилля китайських загрозливих хакерів залишаються такими ж, як і за останні кілька років, з точки зору цільових географічних регіонів та інтенсивності націлювання на місце. У той час як численні загрозливі суб'єкти націлені на Сполучені Штати в різних секторах, цільові дії на Тайвані здебільшого обмежені одним загрозливим суб'єктом – Flax Typhoon.

Більшість загрозливої діяльності Китаю спрямована на збір розвідданих і особливо поширена в країнах АСЕАН навколо Південно-Китайського моря. Granite Typhoon і Raspberry Typhoon були найактивнішими в регіоні, тоді як Nylon Typhoon продовжував націлюватися на урядові та зовнішньополітичні організації по всьому світу (Рисунок 2.15).

Іран активно використовує кібероперації як інструмент зовнішньої політики та засіб асиметричної відповіді на військовий і економічний тиск. Через це багато операцій мають ознаки державної координації та стратегічної спрямованості.

Однією з ключових рис є орієнтація на кібершпигунство. Іранські групи часто націлюються на урядові установи, оборонні структури, енергетичний сектор та дослідницькі центри. Використовуються фішингові кампанії, шкідливе програмне забезпечення й соціальна інженерія для отримання доступу до конфіденційних даних. Такий підхід дозволяє збирати розвіддані та впливати на політичні рішення інших держав.

Другою особливістю є активне застосування деструктивних атак. Серед найвідоміших технік – використання wiper-вірусів, спрямованих на знищення даних та порушення роботи інфраструктури. Такі атаки часто мають символічний або помстивий характер і можуть бути відповіддю на економічні санкції чи військові дії.

Третьою характерною рисою є діяльність проксі-груп. Іран нерідко використовує напівофіційні або пов'язані з державою хакерські угруповання для здійснення операцій із заперечуваною причетністю. Це ускладнює атрибуцію атак і дає можливість вести більш агресивну діяльність без прямого політичного ризику.

Також важливо, що іранські кібероператори активно працюють у сфері інформаційних маніпуляцій. Створення фейкових акаунтів, поширення дезінформації та вплив на громадську думку за кордоном – частина ширшої стратегії інформаційного впливу.

У сукупності ці особливості роблять іранську кіберзлочинність багатогранним і складним явищем, яке поєднує шпигунство, деструктивні атаки та інформаційні операції в рамках державної стратегії.

ран активно використовує кібероперації як інструмент зовнішньої політики та засіб асиметричної відповіді на військовий і економічний тиск. Через це багато операцій мають ознаки державної координації та стратегічної спрямованості.

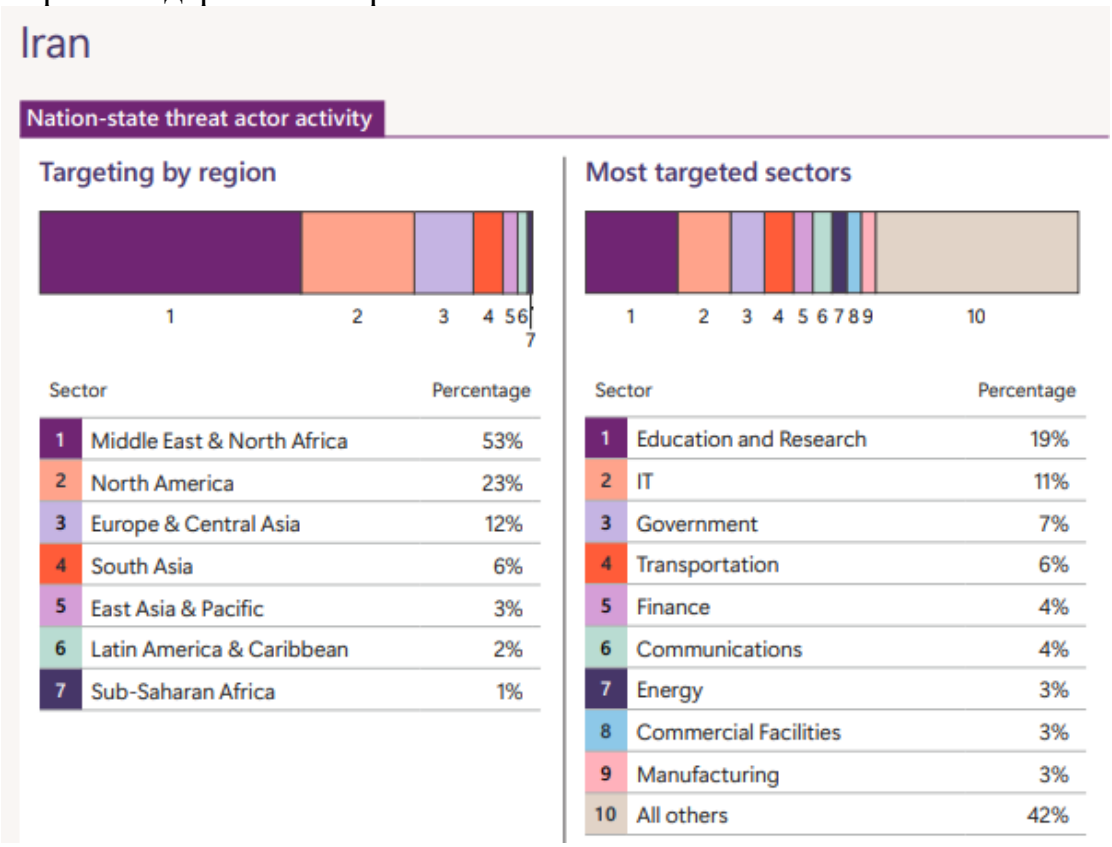
Однією з ключових рис є орієнтація на кібершпигунство. Іранські групи часто націлюються на урядові установи, оборонні структури, енергетичний сектор та дослідницькі центри. Використовуються фішингові кампанії, шкідливе програмне забезпечення й соціальна інженерія для отримання доступу до конфіденційних даних. Такий підхід дозволяє збирати розвіддані та впливати на політичні рішення інших держав.

Другою особливістю є активне застосування деструктивних атак. Серед найвідоміших технік – використання wiper-вірусів, спрямованих на знищення даних та порушення роботи інфраструктури. Такі атаки часто мають символічний або помстивий характер і можуть бути відповіддю на економічні санкції чи військові дії.

Третьою характерною рисою є діяльність проксі-груп. Іран нерідко використовує напівофіційні або пов'язані з державою хакерські угруповання для здійснення операцій із заперечуваною причетністю. Це ускладнює атрибуцію атак і дає можливість вести більш агресивну діяльність без прямого політичного ризику.

Також важливо, що іранські кібероператори активно працюють у сфері інформаційних маніпуляцій. Створення фейкових акаунтів, поширення дезінформації та вплив на громадську думку за кордоном – частина ширшої стратегії інформаційного впливу.

У сукупності ці особливості роблять іранську кіберзлочинність багатогранним і складним явищем, яке поєднує шпигунство, деструктивні атаки та інформаційні операції в рамках державної стратегії.



	Sector	Percentage
1	Middle East & North Africa	53%
2	North America	23%
3	Europe & Central Asia	12%
4	South Asia	6%
5	East Asia & Pacific	3%
6	Latin America & Caribbean	2%
7	Sub-Saharan Africa	1%

	Sector	Percentage
1	Education and Research	19%
2	IT	11%
3	Government	7%
4	Transportation	6%
5	Finance	4%
6	Communications	4%
7	Energy	3%
8	Commercial Facilities	3%
9	Manufacturing	3%
10	All others	42%

Рисунок 2.16 – статистика активності хакерів Ірану по регіонам та сферам життя

Іран приділяв значну увагу Ізраїлю, особливо після початку війни Ізраїлю та ХАМАС. Іранські актори продовжували націлюватися на США та країни Перської затоки, включаючи ОАЕ та Бахрейн, частково через нормалізацію їхніх зв'язків з Ізраїлем і сприйняття Тегераном того, що вони обидва сприяють військовим зусиллям Ізраїлю (Рисунок 2.16).

Цілі Ірану були зосереджені на освіті, IT та уряді в рамках збору стратегічної розвідувальної інформації. Іранські rs,thpkjxbyws часто націлюються на IT-сектор, щоб отримати доступ до кінцевих клієнтів, у тому числі в уряді та оборонно-

промисловій базі (DIB). «Інші» включають засоби масової інформації та аналітичні центри чи НУО, на які Іран часто орієнтується, щоб отримати інформацію про дисидентів, активістів та осіб, які можуть впливати на формування політики.

Кіберзлочинність, пов'язана з Північною Кореєю, є однією з найбільш організованих і агресивних у світі, і її особливості чітко відображають специфіку державної стратегії та політичної ізоляції цієї країни. Північна Корея використовує кібероперації як важливий інструмент ведення асиметричної війни, економічної агресії та отримання фінансування для державних потреб, зокрема через кіберзлочинність.

Однією з основних характеристик північнокорейських кіберзлочинних груп є високий рівень організованості та фінансування, що дозволяє їм здійснювати складні та масштабні кібератаки. Північнокорейські хакерські угруповання, такі як Lazarus Group, мають добре розвинену інфраструктуру для здійснення глобальних атак. Ці групи активно працюють в різних сферах – від кібершпигунства до фінансових крадіжок.

Особливої уваги заслуговує використання кіберзлочинцями Північної Кореї методів для отримання фінансування. Наприклад, вони здійснюють кібернапади на банки та криптовалютні платформи, що дозволяє їм отримувати величезні суми грошей для фінансування державної машини, яка страждає від міжнародних санкцій. Один з найбільш відомих випадків – це хакерська атака на банк в Бангладеш у 2016 році, коли було викрадено понад 80 мільйонів доларів.

Також Північна Корея активно займається кібершпигунством, націлюючись на урядові установи, організації, що займаються науковими дослідженнями, а також військові об'єкти. Це дозволяє країні збирати важливу інформацію для зміцнення своєї обороноздатності та політичних амбіцій.

Не менш важливим аспектом є розповсюдження шкідливого програмного забезпечення, яке використовується для деструктивних атак на інфраструктуру інших країн, а також для маніпулювання економічними системами та критичними інфраструктурами. Наприклад, атака WannaCry у 2017 році, яка спричинила глобальні проблеми з безпекою, була приписана саме північнокорейським хакерам.

Оскільки Північна Корея не має доступу до багатьох традиційних джерел фінансування через міжнародні санкції, кіберзлочинність є важливим каналом для підтримки її економіки. У поєднанні з високим рівнем кіберспеціалізації та фінансування це робить північнокорейську кіберзлочинність однією з найбільш небезпечних у світі.

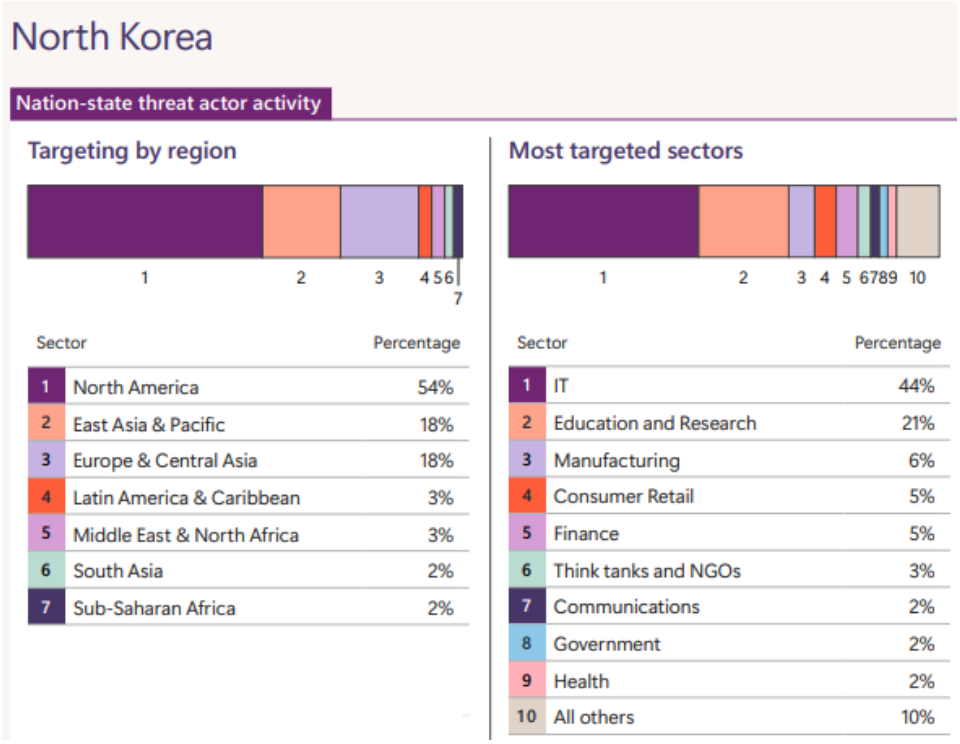


Рисунок 2.17 – статистика активності хакерів Північної Кореї по регіонам та сферам життя

Сполучені Штати залишаються країною, на яку найбільше націлені північнокорейські загрози, але Велика Британія піднялася цього року на друге місце. Категорія «Інші» включала 44 інші країни, на які націлені північнокорейські загрозливі кіберзлочинні дії (Рисунок 2.17).

Північнокорейські загрози найбільше націлювалися на IT-сектор, зокрема для проведення дедалі складніших атак на ланцюги поставок програмного забезпечення. Вони також продовжували активно націлюватися на експертів у секторі освіти для збору розвідданих. Категорія «Інше» включала ще сім секторів.

2.5. Стирання меж між державними кіберзагрозами та кіберзлочинцями.

В останні року пов’язані з державою кіберзагрози все частіше використовували злочинні інструменти та тактики – навіть самі злочинці – для просування своїх інтересів, стираючи межі між зловмисною діяльністю, що підтримується національною державою, та діяльністю кіберзлочинців.

Корпорація Майкрософт спостерігала, як суб’єкти загроз національної держави проводять операції з метою отримання фінансової вигоди, залучають кіберзлочинців для збору розвідданих про українську армію та використовують ті самі інформаційні викрадачі, системи командування та контролю та інші інструменти, які віддають перевагу спільноті кіберзлочинців.[2]

З 2017 року північнокорейські хакери вкрали 3 мільярди доларів у криптовалюті

Північнокорейські загрозливі суб’єкти вже давно стоять на цій розмитій лінії, проводячи фінансово мотивовані операції, щоб забезпечити фінансування державної скарбниці та пріоритетних ініціатив. За оцінками ООН, з 2017 року північнокорейські

хакери викрали криптовалюту на суму понад 3 мільярди доларів США, лише у 2023 році сума пограбувань склала від 600 до 1 мільярда доларів США. Повідомляється, що ці вкрадені кошти фінансують більше половини ядерної та ракетної програм Північної Кореї.

З 2023 року Microsoft виявила три основні північнокорейські групи загроз – Jade Sleet, Sapphire Sleet і Citrine Sleet, – які були особливо активними у нападах на криптовалютні організації. Крім того, Північна Корея також може втягнутися в гру з програмами-вимагачами. Moonstone Sleet, новий північнокорейський актор, ідентифікований у травні 2024 року, розробив спеціальну версію програми-вимагача під назвою FakePenny, яку він розгорнув в організаціях аерокосмічної та оборонної сфери після викрадання даних із уражених мереж. Така поведінка свідчить про те, що актор мав на меті як збір розвідувальних даних, так і монетизацію доступу до них.

За межами Північної Кореї Microsoft спостерігала загрозливих іранських національних держав, які шукали фінансової вигоди від деяких своїх наступальних кібероперацій. Це знаменує собою зміну в порівнянні з попередньою поведінкою, згідно з якою атаки програм-вимагачів, розроблені так, щоб виглядати фінансово мотивованими, насправді були руйнівними.

напади. Наприклад, кібероперація впливу, яку проводила група Корпусу вартових ісламської революції (IRGC), яку ми відстежуємо як Cotton Sandstorm (також відома як Emennet Pasargad), продавала викрадені дані ізраїльського веб-сайту знайомств через двох своїх кіберджерела у період з вересня 2023 року по лютий 2024 року. Персони також пропонували видалити певні окремі профілі зі свого сховища даних за певну плату.

Тим часом російські зловмисні кіберзлочинці дедалі ширше впроваджують шкідливе програмне забезпечення у свої операції, окрім цього, ймовірно, передають частину кібершпигунських завдань іншим злочинним угрупованням. У червні 2024 року група Шторм-2049 (UAC-0184) застосувала Xworm та Remcos RAT – комерційне шкідливе ПЗ, що часто використовується у злочинній діяльності, – для компрометації принаймні 50 українських військових пристроїв. При цьому не було зафіксовано очевидного використання отриманого доступу кіберзлочинцями, що вказує на те, що ця група діяла на підтримку інтересів російського уряду.

У червні-липні 2023 року Microsoft спостерігала, як Aqua Blizzard, яку пов'язують з Федеральною службою безпеки, передала доступ до 34 інфікованих українських пристроїв кіберзлочинному угрупованню Storm-0593 (відомому також як Invisimole). Під час передачі Aqua Blizzard використала сценарій Powershell, який завантажував шкідливе ПЗ із сервера, що контролювався Storm-0593. Подальші дії включали створення командно-контрольної інфраструктури Storm-0593 та розгортання маяків Cobalt Strike на більшості пристроїв. Один із маяків був налаштований з доменом dashcloudew.uk, що, згідно із висновками Microsoft, був зареєстрований цією групою та використовувався раніше для фішингових кампаній проти українських військових систем. Це підтверджує той факт, що Storm-0593 продовжує операції зі збору розвідданих у рамках підтримки цілей російських урядових структур. [22]

Багатогранність гібридної війни

Конфлікти, що тривають в Україні та на Близькому Сході, ілюструють, як деякі країни використовують як кіберпідходи, так і кампанії впливу для досягнення своїх цілей. Ця діяльність поширюється за межі географічних кордонів зон конфлікту, демонструючи глобалізований характер гібридної війни.

Як Іран використовує кібероперації впливу, щоб принизити Ізраїль

Після початку війни Ізраїлю та ХАМАС Іран посилив свої кібер-операції, вплив і кібер-вплив проти Ізраїлю. З 7 жовтня 2023 року по липень 2024 року майже половина операцій в Ірані, за якими спостерігала Microsoft, були націлені на ізраїльські компанії (Рисунок 2.18).

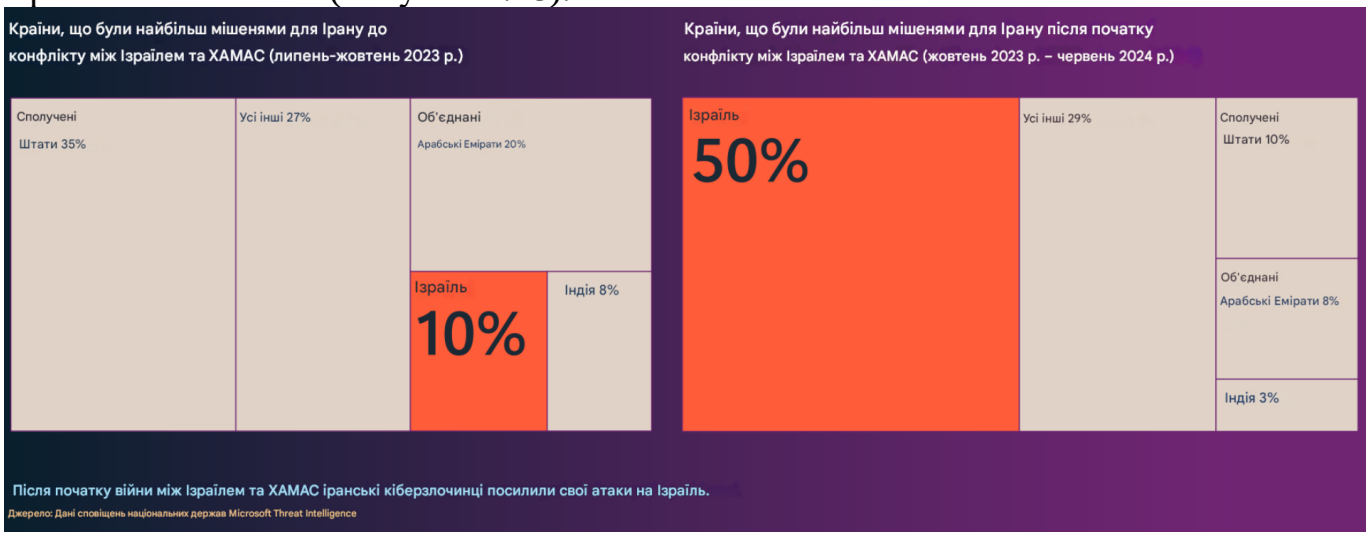


Рисунок 2.18 – Статистика кібератак на країни для Ірану з липня - жовтень 2023 р. та з жовтня – червень 2024 р.

Іранські групи також розширили свої операції впливу за допомогою кібернетичних засобів за межі Ізраїлю, зосередившись на підриві міжнародної політичної, військової та економічної підтримки військових операцій Ізраїлю.

У листопаді 2023 року групи IRGC провели кібероперації впливу, націлені на американських контролерів води, виготовлених в Ізраїлі та Бахрейні, у відповідь на нормалізацію зв'язків Бахрейну з Ізраїлем.

Microsoft Threat Intelligence оцінює, що підрозділ IRGC, відомий як Shahid Kaveh Group, який ми відстежуємо як Storm-0784, був відповідальним за псування контролера водопостачання в Пенсільванії відомою під назвою «CyberAv3ngers», залишивши повідомлення про те, що ізраїльські системи є законними цілями.

Протягом усього конфлікту іранські хакери використовували кіберперсон для трансляції та посилення своїх деструктивних атак проти ізраїльських підприємств, намагаючись спроектувати силу та посилити вплив своїх кібероперацій. Протягом двох днів після нападу ХАМАС на Ізраїль Іран провів кілька нових операцій впливу. Впливовий актор Сефід Флуд запустив в Інтернеті персон «Сльози війни» та «Хамса1948».

Перший видавав ізраїльських активістів, які критикували те, як ізраїльський прем'єр-міністр Біньямін Нетаньяху впорався із заручниками, тоді як другий намагався переконати арабо-ізраїльтян насильницько протистояти ізраїльській владі

та протестувати на підтримку жителів Гази. Microsoft Threat Intelligence оцінює, що Storm-0842, підрозділ Міністерства розвідки та безпеки Ірану (MOIS), запустив іншу кіберперсону, «KarMa», наступного дня після початку війни, видаючи себе за ізраїльтян, які прагнуть усунути Нетаньяху з посади.

Іранські хакери також почали видавати себе за партнерів після початку війни. Microsoft вважає, що компанія Cotton Sandstorm використовувала назву та логотип військового крила ХАМАС, бригад Аль-Касам, для поширення неправдивих повідомлень про заручників у Газі та надсилання ізраїльтянам погрозливих повідомлень. Інший канал у Telegram, який ми оцінюємо, керував Міністерство розвідки та безпеки Ірану (MOIS), яке також використовувало логотип бригад Аль-Касама, погрожувало ізраїльським військовим і витоку їхніх особистих даних. Залишається незрозумілим, чи діяв Іран за згодою ХАМАС.

Широкомасштабна тактика Росії для шпигунства за українськими військовими та її союзниками. Російські хакери зосереджені на отриманні та крадіжці розвідданих українських бойовиків та міжнародних партнерів, які постачають їм зброю.

Використовувані методи можуть завдати ненавмисної шкоди, створюючи ризик для комп'ютерних мереж у всьому світі.

З червня 2023 року зловмисники, пов'язані з російською військовою розвідкою (ГРУ) і ФСБ, використовували принаймні два недисципліновані підходи, щоб отримати доступ до українських військових і суміжних військових пристроїв:

1. Черв'яки, що передаються через USB: Aqua Blizzard – афілійована з Федеральною службою безпеки Росії (ФСБ) дійова особа, яка з 2013 року атакувала українські організації – щодня отримувала доступ до 500-750 українських пристроїв через USB-доставку файлу Windows ShortCut і сильно захищеного Powershell або VBScript (Рисунок 2.19). Сценарії встановлюють команду та контроль, що полегшує крадіжку файлів певних типів. Оскільки зловмисне програмне забезпечення та зловмисне програмне забезпечення USB важко локалізувати, і вони можуть потрапляти на пристрої поза межами діяльності Aqua Blizzard, існує підвищений ризик того, що USB та зловмисне програмне забезпечення потраплять до мереж за межами України та до військових систем партнерів.

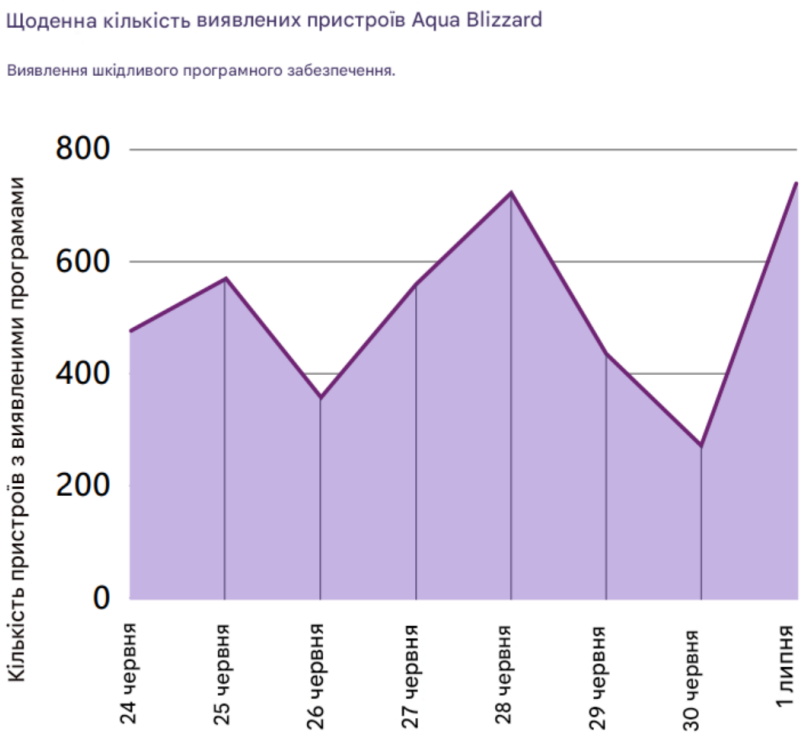


Рисунок 2.19 – Статистика виявлення шкідливого програмного забезпечення за добу, які атакувала українські організації

2. Бот Amadey і торренти: Secret Blizzard, афілійована з ФСБ, і Seashell Blizzard, пов'язана з ГРУ, отримують доступ до якомога більшої кількості пристроїв, перш ніж шукати цікаві пристрої. Secret Blizzard зробила це, керуючи сторонніми інфікуваннями, такими як багатоцільові боти Amadey, щоб завантажити спеціальний інструмент розвідки, який допомагає операторам вирішити, чи варто розгортати бекдор першого етапу. Seashell Blizzard пропонує шкідливі, піратські версії програмного забезпечення Microsoft через торренти, часто просуваючи їх на українських файлообмінних сайтах, щоб закріпитися в мережах (Рисунок 2.11).

Midnight Blizzard загрожує ланцюгу постачання IT

Російські хакери розкидають широкі мережі, щоб отримати інформацію про західні організації, які беруть участь у політичній, військовій та гуманітарній підтримці України. Midnight Blizzard намагалася отримати доступ до IT-компаній частково для широкого невибіркового доступу до систем. Історично склалося так, що цей суб'єкт використовує ланцюги постачання IT-програмного забезпечення та послуг, щоб націлитися на подальших клієнтів в урядових та інших політичних організаціях у Північній Америці та Європі. Корпорація Майкрософт прозоро повідомляла про зусилля Midnight Blizzard проти наших мереж, і ми були не єдиними цілями IT-сектору (Рисунок 2.20). Історія Midnight Blizzard компрометації ланцюжків постачання та постійне переслідування IT-організацій свідчить про те, що широко поширена компрометація залишається головним ризиком для постачальників у всьому світі.

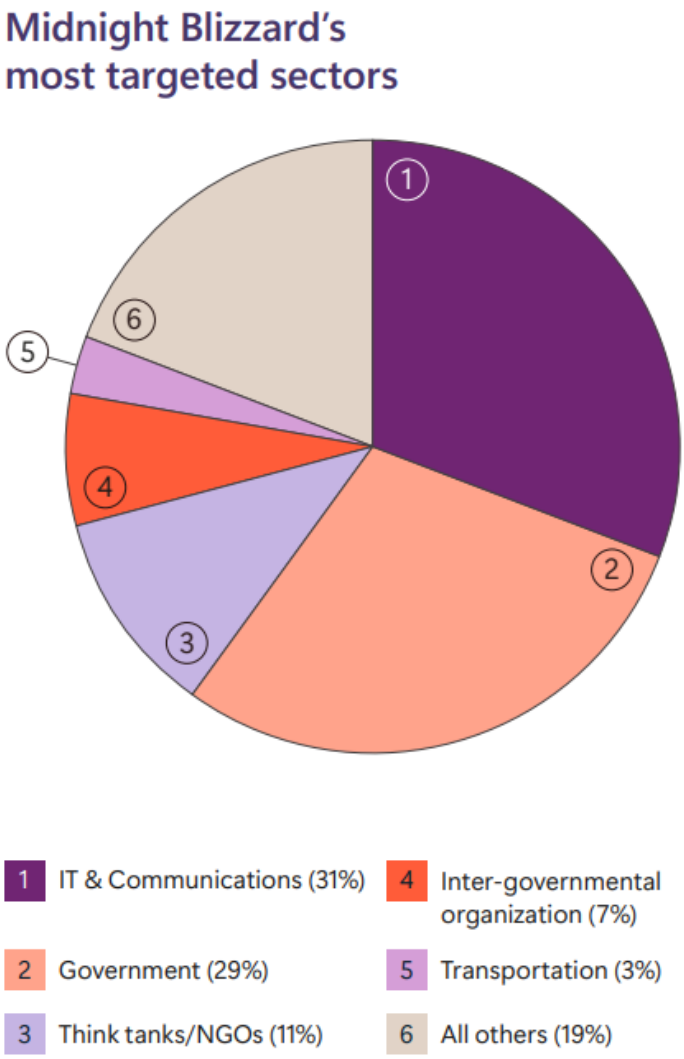


Рисунок 2.20 – Найбільші цільові сектори на яких зосереджена Midnight Blizzard

Midnight Blizzard загрожує ланцюгу постачання IT

Системи оперативних технологій (OT) знаходяться під загрозою гібридної війни

Критична інфраструктура є ключовим об'єктом фізичних ударів і кібератак у сучасних гібридних конфліктах. З кінця 2023 року корпорація Майкрософт помітила збільшення кількості повідомлень про атаки на незахищені OT-пристрої, що піддаються доступу до Інтернету, які контролюють критичні процеси в реальному світі. Як більш детально обговорювалося в попередніх випусках цього звіту, це особливо занепокоєння, враховуючи, що ці системи часто мають неадекватні методи безпеки, зокрема залишаються без виправлень, використовують паролі за замовчуванням або навіть взагалі не використовують паролі.

Обладнання OT у системах водопостачання та водовідведення (WWS) у Сполучених Штатах піддалося численним атакам із жовтня 2023 року по червень 2024 року різними державними суб'єктами, зокрема пов'язаними з IRGC CyberAv3ngers (відстежуваними в Microsoft як Storm-0784) та проросійськими хакерами. CyberAv3ngers та проросійська група Cyber Army of Russia, здійснювати, заявляти або посилювати атаки, які, ймовірно, мають на меті залякати цільові країни, щоб вони

капітулювали або припинили підтримку Ізраїлю та України відповідно (Рисунок 2.21).

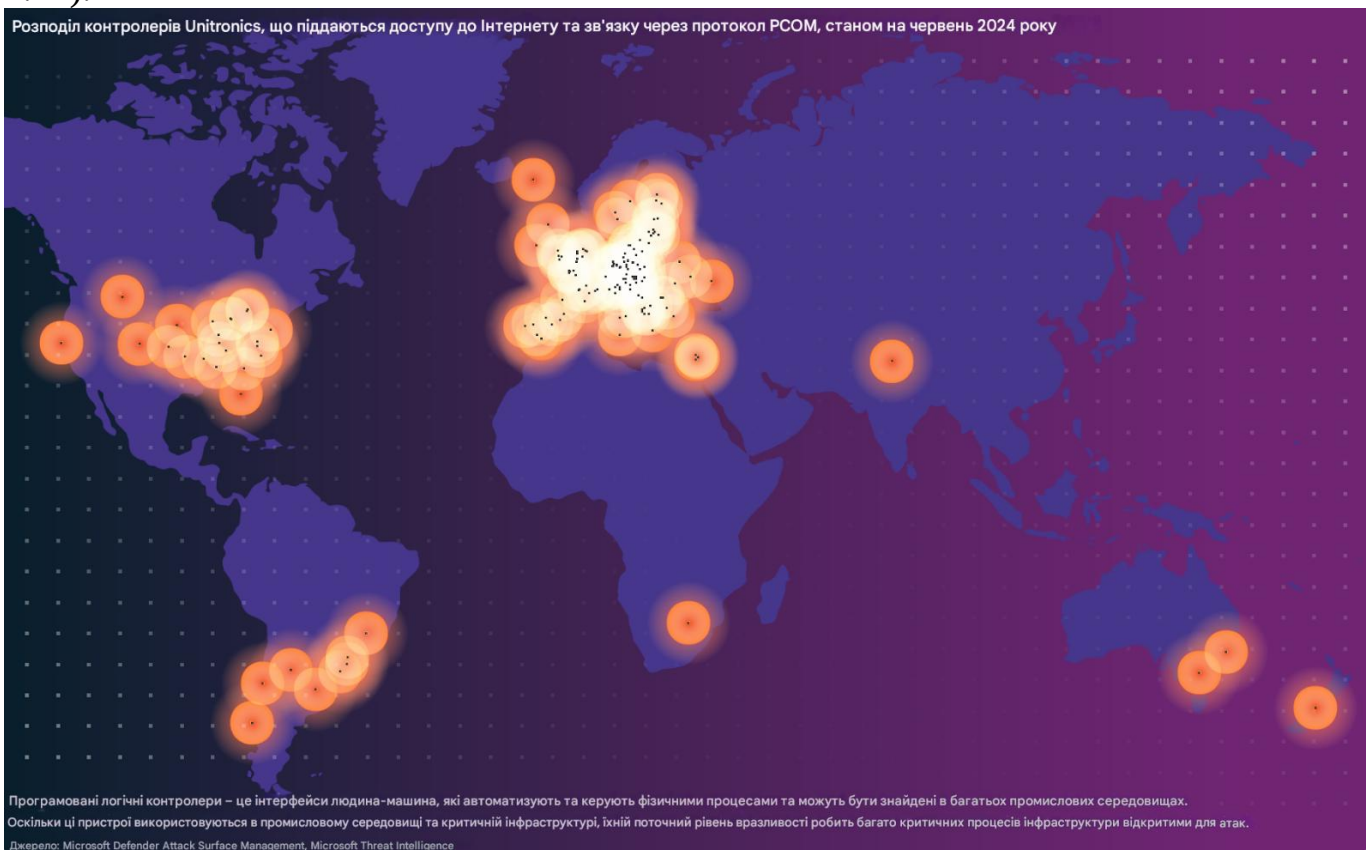


Рисунок 2.21 – Розподіл контролерів Unitronics, що піддаються доступу до Інтернету та зв'язку через протокол PCOM, станом на червень 2024 року

Китайські хакери атакують військові та IT-структури в Південно-Китайському морі

Китайські кібератори Raspberry Typhoon, Flax Typhoon і Granite Typhoon інтенсивно атакували організації, пов’язані з IT, військовими та державними інтересами навколо Південно-Китайського моря (Рисунок 2.222).

Діяльність спрямована особливо на країни Асоціації держав Південно-Східної Азії (АСЕАН). Raspberry Typhoon був надзвичайно активним, успішно проникаючи у військові та виконавчі структури Індонезії та морських систем Малайзії напередодні рідкісних військово-морських навчань за участю Індонезії, Китаю та Сполучених Штатів у червні 2023 року. Так само Flax Typhoon зосереджувався на організаціях, пов’язаних зі спільними військовими навчаннями США на Філіппінах. З серпня 2023 року Flax Typhoon розширив свої цілі, включивши IT та державні організації на Філіппінах, Гонконгу, Індії та Сполучених Штатах.

З липня 2023 року Granite Typhoon зламав телекомунікаційні мережі в Індонезії, Малайзії, Філіппінах, Камбоджі та Тайвані. Діяльність цієї групи вказує на постійну схему стратегічних кіберзалучень китайських державних суб’єктів, спрямованих на збір розвідданих і потенційне переривання військової діяльності в стратегічно важливих районах, таких як Південно-Китайське море.

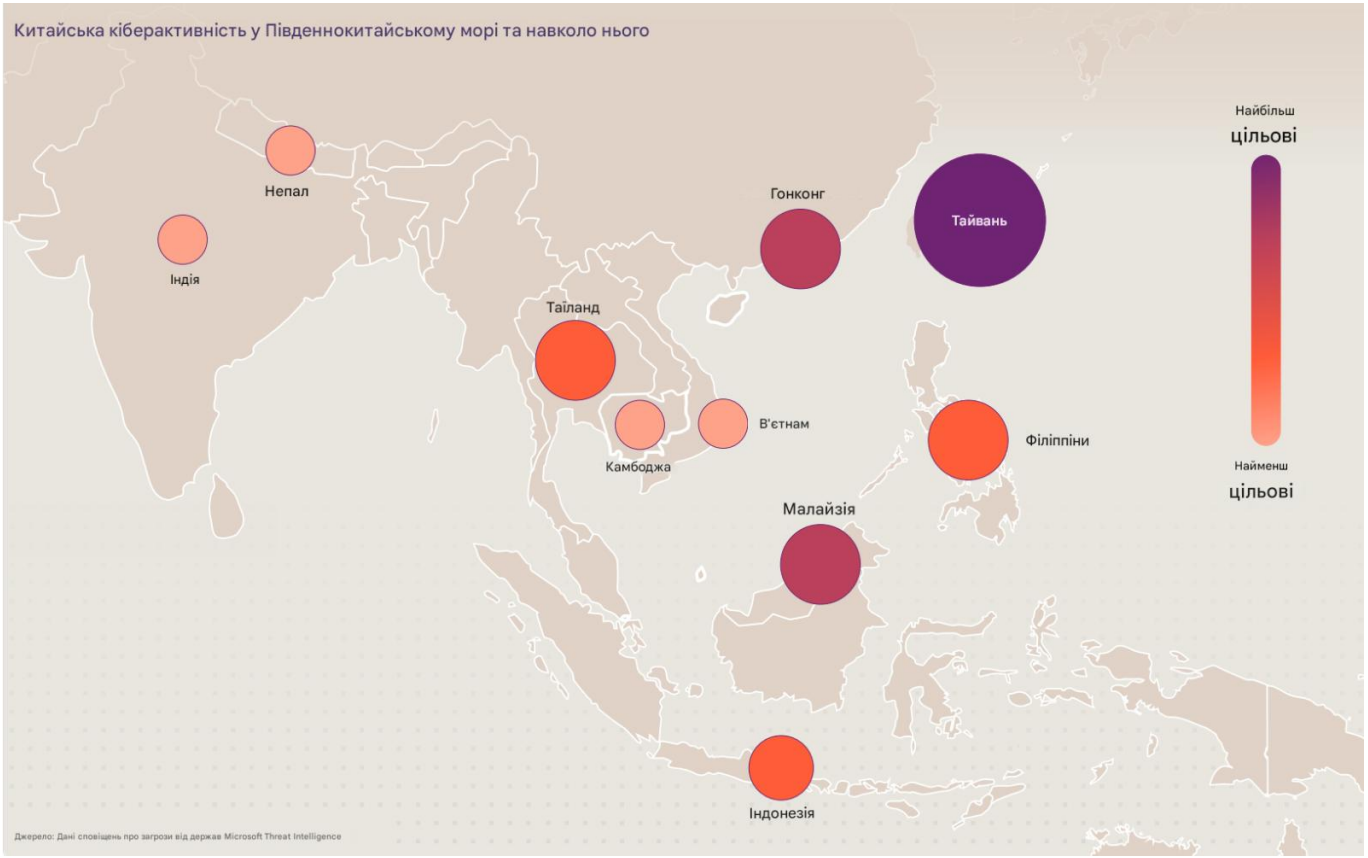


Рисунок 2.22 – Китайська кіберактивність у Південнокитайському морі та навколо нього

Стримування найсучасніших загроз

Як підкреслюється в цьому звіті, кібератаки зростають, а темпи атак, спонсорованих національною державою, зросли до такої міри, що зараз у кіберпросторі фактично точаться постійні бойові дії.

Зважаючи на понад 600 мільйонів атак на день, націлених лише на клієнтів Microsoft, має існувати компенсаційний тиск, щоб зменшити загальну кількість атак онлайн. Для стримування цієї зловмисної діяльності знадобиться надійне поєднання технологічних і геополітичних рішень. Це стримування може бути досягнуто двома способами – відмовою від вторгнень або накладенням наслідків. Хоча компаніям подобається

Корпорація Майкрософт може допомогти «заперечити» успішні кібератаки за допомогою інновацій і подальшого вдосконалення кібербезпеки, дотримання міжнародних правил зі стримуючими наслідками має лягати на уряди. Тому корпорація Майкрософт закликає уряди розглянути наступні дії для покращення дотримання міжнародного права та онлайн-норм шляхом зміцнення цифрової дипломатії, заДСТУрення суспільних повноважень і накладення значущих наслідків за кіберагресію.

І. Зміцнення міжнародних норм і дипломатії. Стримування вимагає ясності

очікування щодо прийнятної та неприйнятної поведінки. З цією метою Microsoft закликає уряди прийняти:

– Нові норми: Організація Об’єднаних Націй (ООН) та інші форуми мають визнати хмарні послуги та ланцюжок постачання інформаційно-комунікаційних

технологій (ІКТ) критичною інфраструктурою, яка заборонена для націлювання. Крім того, від держав слід очікувати виконання своїх зобов'язань щодо належної обачності для боротьби зі зловмисною діяльністю, яка походить з їх територій.

– Залучення багатьох зацікавлених сторін: Держави повинні прийняти більш інклюзивні дипломатичні процеси, які забезпечують участь критично важливих неурядових зацікавлених сторін в дискусіях про мир і безпеку в Інтернеті, включаючи провідних представників індустрії технологій і громадянського суспільства.

– Двосторонні угоди: окрім роботи на багатосторонніх форумах, уряди повинні вивчати потенційні двосторонні угоди як засіб встановлення очікувань і стримування небезпечних кібероперацій.

ІІ. Загострити приписування урядом зловмисної діяльності. Публічне приписування сприяє стримуванню, закликаючи до міжнародно неприйнятної поведінки та слугуючи необхідним попередником для нав'язування подальших наслідків. Нижче наведено способи, якими уряди можуть посилити вплив публічних заяв про присвоєння авторства:

– Уніфікованість: єдине агентство має опрацьовувати публічні заяви про приписування у стандартному форматі з детальним описом інциденту, відповідальних сторін, впливу, доказів, порушень правил, наслідків та будь-яких запобіжних заходів.

– Контекстуалізація: публічне приписування має також включати будь-яке ширше уявлення про діяльність суб'єкта загрози для підтримки більш повної відповідальності.

– Співпраця: повноваження кількох урядів у коаліції допомагають обґрунтувати висновки та зміцнити довіру до них. Уряди також повинні співпрацювати з технологічною індустрією для подальшої перевірки та з групами громадянського суспільства, щоб надати додатковий контекст щодо впливу та шкоди від кібератак.

ІІІ. Ввести стримуючі наслідки. Зростаюча кількість кібератак, спонсорованих національною державою, потребує більш рішучих дій уряду, які стримують зростання. Можливі стратегії реагування включають:

– Розширені контрзаходи: окрім публічного приписування, держави, які здійснюють незаконну кібердіяльність, повинні очікувати жорстких контрзаходів у відповідь, серед інших варіантів це включає цільові санкції.

– Колективні контрзаходи: Уряди повинні прийняти як законні колективні контрзаходи, запровадження кількома державами контрзаходів у відповідь на незаконні кібероперації, націлені на одну з них.

– Уточніть червоні лінії: відповідно до заборони Статуту ООН на «загрозу силою або її застосування», слід чітко вказати, що фінансовані державою кібервторгнення, які можуть бути використані для пошкодження або переривання критично важливих цивільних служб, становлять незаконну загрозу силою та призводять до більш значних наслідків у відповідь.

Більш надійна система стримування допоможе сприяти стабільності, захистити критичну інфраструктуру та уникнути деяких із найшкідливіших кібератак. Щоб підтримати це, уряди повинні поглибити партнерство між групами зацікавлених сторін для визначення необхідної критичної інфраструктури. Враховуючи зростаюче значення цієї технології, це також має включати важливу інфраструктуру ШІ та інтелектуальну власність, що стоїть за розробкою нових властивостей ШІ.

2.6. Програми-вимагачі

Тенденції

Програми-вимагачі залишаються однією з найсерйозніших проблем кібербезпеки. Серед наших клієнтів корпорація Майкрософт спостерігала зростання в 2,75 рази з року в рік кількості випадків, пов'язаних із програмами-вимагачами, керованими людьми (визначається як наявність принаймні одного пристрою, націленого на атаку програм-вимагачів у мережі).

Водночас відсоток атак, які досягли фактичної фази шифрування, зменшився за останні два роки втричі. Автоматичне припинення атак сприяло цій позитивній тенденції щодо зменшення успішних атак. У понад 90% випадків, коли атаки переходили до стадії викупу, зловмисник використовував некеровані пристрої в мережі або для отримання початкового доступу, або для віддаленого шифрування активів на етапі впливу (Рисунок 2.24).

Рисунок 2.24 – Статистика по групам та кількості атак за допомогою програм-вимагачів

Найпоширенішими методами початкового доступу залишаються соціальна інженерія, зокрема фішинг електронної пошти, фішинг SMS і голосовий фішинг, компрометація ідентифікаційної інформації та використання вразливостей у загальнодоступних програмах або операційних системах без виправлень. Зловмисники продовжують використовувати нещодавно виявлені загальні вразливості та ризики (CVE) із загальною системою оцінки вразливостей (CVSS)

вище 8. Коли зловмисник потрапляє в мережу, він змінює продукти безпеки або встановлює інструменти віддаленого моніторингу та керування (RMM), щоб вимкнути або уникнути виявлення та залишатися в мережі.

Ми спостерігали віддалене шифрування в 70% успішних атак, причому 92% походили з некерованих пристроїв у мережі, що підкреслювало необхідність для організацій реєструвати пристрої для керування або виключати некеровані пристрої з мережі.

Як кіберзлочинці втручаються в продукти безпеки

Зламавши організацію, зловмисники зазвичай починають із втручання в її рішення безпеки. Вимикаючи або змінюючи захист, зловмисники виграють час для встановлення шкідливих інструментів, викрадання даних для шпигунства чи здирництва та потенційних атак, таких як програми-вимагачі.

Корпорація Майкрософт постійно спостерігає за великою кількістю атак, пов'язаних із підробкою антивірусної програми. У травні 2024 року Microsoft Defender XDR виявив понад 176 000 інцидентів, пов'язаних зі зміною налаштувань безпеки, що вплинуло на понад 5600 організацій. У середньому за цей проміжок часу організації, які зіткнулися з діяльністю втручання, бачили понад 31 спробу.

Закріпившись у мережі, зловмисники проводять розвідку, щоб визначити наявні інструменти безпеки, або вони можуть перевірити заходи безпеки, скинувши інструменти чи корисне навантаження, наприклад зловмисне програмне забезпечення. У разі виявлення та блокування учасники можуть натомість втручатися в продукти безпеки, з якими вони стикаються. Зловмисники зазвичай прагнуть отримати доступ до привілейованих облікових записів у скомпрометованому середовищі, щоб вони могли використовувати підвищені привілеї для налаштування будь-яких параметрів політики, включаючи зміну параметрів безпеки. Корпорація Майкрософт спостерігала різні методи вимкнення або іншого втручання в політику безпеки, включаючи зміни реєстру Windows; шкідливі засоби, такі як NSudo (Defeat Defender), Defender Control, Configure Defender і ToggleDefender; спеціальні зловмисні PowerShell або пакетні сценарії та команди; та втручання водія.

Практичні рекомендації

1. Деякі рішення для виявлення та реагування кінцевих точок (EDR) забезпечують функції захисту від несанкціонованого доступу, які можуть допомогти запобігти зловмисникам вимикати налаштування безпеки.

2. Організації можуть налаштувати параметр Вимкнути злиття локального адміністратора, щоб обмежити можливість змінювати налаштування антивірусної політики локальною адміністрацією.

3. Сповіщення, які виявляють інструменти та активність підробки, можуть передувати доставці додаткового зловмисного програмного забезпечення або запуску зловмисних команд і повинні реагувати відповідним чином. Тому слід негайно вжити заходів щодо цих сповіщень.

Octo Tempest: практичний приклад і попередження

Помітною подією в еволюції атак програм-вимагачів після минулорічного звіту є збільшення кількості гібридних атак, націлених як на локальні, так і на хмарні

ресурси. У той час, коли досвідчені актори загрози продовжують додавати нові тактики, прийоми та процедури (TTP) до своїх і без того широких ігор, актор Octo Tempest (він же Scattered Spider) пропонує хороший приклад цієї еволюції та зростання.

Octo Tempest – фінансово вмотивована кіберзлочинна група, відома широкомасштабними кампаніями, які включають методи противника посередині (AiTM), соціальну інженерію та можливості заміни SIM-карт. Вперше помічений у 2022 році, він був націлений

організації мобільного зв'язку та аутсорсингу бізнес-процесів для ініціювання перенесення телефонних номерів (SIM-свопи). До середини 2023 року Octo Tempest стала афілійованою компанією ALPHV/BlackCat, керованої людиною програми-вимагача як послуга, і почала розгортати програмне забезпечення-вимагач ALPHV/BlackCat для жертв. У другому кварталі 2024 року Octo Tempest додала Qilin і RansomHub до своїх програм-вимагачів.

Octo Tempest використовує широкі методи соціальної інженерії, включаючи дослідження організації для виявлення цілей, а потім імітацію співробітників або учасників під час телефонних дзвінків, щоб обманом змусити технічних адміністраторів виконати скидання паролів або скинути методи багатофакторної автентифікації (MFA). Група також використовує заміну SIM-карти, щоб отримати доступ до номера телефону співробітника, а потім ініціювати самостійне скидання пароля облікового запису користувача.Octo Tempest використовує свій початковий доступ для здійснення широкого пошуку в мережі, щоб ідентифікувати документи, пов'язані з архітектурою мережі та іншою конфіденційною інформацією, а потім досліджує середовище, щоб перерахувати активи та ресурси в хмарних середовищах.

Група використовує технології керування пристроями, щоб просувати додаткові шкідливі інструменти, відключати/уникати продуктів безпеки або створювати нові віртуальні машини в хмарі організації. Окрім шифрування активів, група націлена на вилучення даних за допомогою фабрики даних Azure та автоматизованих конвеєрів для вилучення даних на сервери протоколу безпечної передачі файлів (SFTP).

Порушення дії програм-вимагачів

Минулий рік ще раз довів, що для боротьби з програмами-вимагачами потрібен багаторівневий підхід. Один із цих рівнів має зосередитися на перешкоджанні діям, відповідальним за цю діяльність у реальному світі. Команди Microsoft виступили лідерами в об'єднанні експертів із промисловості та правоохоронних органів для обміну інформацією про загрози та доказами щодо учасників програм-вимагачів, їхньої інфраструктури, ідентичності та навіть фінансів.

У травні 2024 року кібервідділ Федерального бюро розслідувань США (ФБР) визначив Octo Tempest своїм третім пріоритетом після Китаю та Росії, які створюють загрози для національних держав. Протягом періоду, охопленого цим звітом, корпорація Майкрософт надавала розвідувальні дані та докази, необхідні для арешту кількох учасників Octo Tempest та інших збоїв у правоохоронних органах, які зловживають програмами-вимагачами. Ми вважаємо, що наш внесок у ці державно-

приватні партнерства допомагає колективно підірвати технічні можливості та інфраструктуру групи, що зрештою призведе до її ліквідації.

Корпорація Майкрософт наполегливо підтримує нашу здатність ділитися інформацією відповідно до законодавства та політики, щоб боротися з найбільшими загрозами нашим клієнтам і нашому бізнесу. Незважаючи на те, що наша конкретна роль може відрізнятися в кожній операції, можливості корпорації Майкрософт для аналізу загроз і зв'язку з правоохоронними органами застосовуються й надалі будуть спрямовані на боротьбу з найбільшими загрозами, з якими ми стикаємося з боку злочинців і державних загроз.

2.7. Кібершахрайство

Тенденції

Випадки шахрайства та зловживання зростають у всьому світі як за обсягом, так і за складністю. Шахрайство є формою кіберзлочинності, і воно підриває безпеку, довіру та репутацію окремих осіб, підприємств і організацій будь-якого розміру та типу в кожному регіоні та галузі.

Зловмисники використовують уразливості в службах, програмах, онлайн-ресурсах, рекламних акціях і системах, щоб отримати шахрайський доступ. Вони використовують отримані ресурси для кібератак, фінансових злочинів або перепродажу активів. Всесвітній економічний форум22 повідомляє, що у 2023 році шахраї вкрали понад 1 трильйон доларів США у жертв у всьому світі. Це означає, що компанії втратили в середньому 1,5% прибутку через шахрайство23, тоді як споживачі зіткнулися з приголомшливими збитками у розмірі 8,8 мільярдів доларів США, що на 30% більше, ніж у 2022 році.

В епоху, коли цифрова трансформація прискорює майже всі типи бізнес-операцій, винахідливість і масштабованість тактики шахрайства продовжує кидати виклик стійкості в усьому світі. Організації стикаються з цілим шквалом шахрайства, як-от шахрайство з платежами та кодом швидкого реагування (QR), компрометація ділової електронної пошти (ККЕП), AiTM, відеофішинг і методи шахрайства з інвестиціями, такі як «різання свиней». [23]

Водночас боротьба з видаванням себе за іншу особу значно ускладнюється через дедалі простіший доступ до технології deep-fake, що дозволяє кіберзлочинцям створювати дуже переконливі підробки не лише голосів бізнес-лідерів, але навіть відео. Перехід до хмарних обчислень є палкою з двома кінцями. У той час як хмарні обчислення забезпечують масштабованість, еластичність, економію коштів і розширені обчислювальні можливості, які стимулюють інновації, вони надають ті самі переваги зловмисникам, посилюючи їхній потенціал неправомірної поведінки. Корпорація Майкрософт спостерігала за тим, як шахраї використовують хмарні служби для здійснення атак, крадіжки даних, видавання себе за користувачів, відмивання грошей і уникнення виявлення. Ці дії використовуються для різних типів шахрайства, таких як захоплення облікового запису, сквотінг домену, шахрайство з платежами та інші типи видавання себе за хмару.

Як зазначено на наступних сторінках, корпорація Майкрософт співпрацює з правоохоронними органами, галузевими партнерами та клієнтами, щоб активно боротися з цією незаконною діяльністю, захищати та відстоювати права наших клієнтів.

Постійно зростаюча загроза фінансового шахрайства з використанням кібермереж.

Кібернетичне фінансове шахрайство охоплює низку шахрайських дій, які здійснюються через Інтернет, зокрема інвестиційне шахрайство, ККЕП і шахрайство з технічною підтримкою. За даними ФБР, збитки через інвестиційне шахрайство перевищили всі інші типи онлайн-шахрайства, склавши понад 4,5 мільярда доларів США збитків лише у 2023 році.

Команди Microsoft, LinkedIn і Skype докладають зусиль із завчасного виявлення такої злочинної діяльності, і в 2023 році Microsoft призупинила понад 64 мільйони облікових записів із зловмисними службами. Ми також співпрацюємо з галузевими та правоохоронними органами, щоб перешкоджати цим акторам у реальному світі. Крім того, зараз ми працюємо з партнерами з правоохоронних органів над покращенням обміну розвідувальною інформацією про кіберзагрози для ліквідації злочинних операцій.

Наприклад, у травні 2024 року Microsoft співпрацювала з Індійським центром контролю за кіберзлочинністю, щоб закрити понад 1000 облікових записів Skype, залучених до переслідувань, шантажу, вимагання та фальшивих «цифрових арештів» шахраями, які видавали себе за поліцейських та інших посадових осіб. Відділ цифрових злочинів Microsoft бореться з фінансово мотивованими кіберзлочинами, використовуючи новаторські правові стратегії, найсучасніші технології та співпрацю для протидії загрозам для споживачів. Корпорація Майкрософт також працює над підривом кіберзлочинців, активно демонтуючи їхню операційну інфраструктуру, підриваючи їхню фінансову мотивацію та співпрацюючи з такими організаціями, як Національний альянс кіберкриміналістики та навчання США та Японський центр контролю за кіберзлочинністю, щоб покращити обмін оперативною інформацією. Оскільки світ усвідомлює постійну загрозу кіберзлочинності, ми бачимо, що все більше державних і приватних партнерів об’єднують зусилля, щоб зруйнувати злочинну інфраструктуру, притягнути їх до відповідальності та підтримати жертв кіберзлочинців.

Влада провела обшуки в семи місцях по всій Індії, перехоплюючи операції кіберзлочинців у реальному часі та збираючи суттєві докази, включаючи жорсткі диски комп’ютерів, мобільні телефони та ноутбуки, а також деталі фінансових операцій, записи розмов і стенограми. Загалом під час цієї операції було заарештовано 43 особи, багато інших досі перебувають під слідством. CBI, у координації з ФБР та міжнародними правоохоронними органами, продовжує відстежувати операції та фінансову діяльність мережі, щоб ідентифікувати та затримати додаткових підозрюваних у цьому поточному розслідуванні.

Наша співпраця з правоохоронними органами в боротьбі з кібершахрайством призвела до 30+ рейдів кол-центрів, 100+ арештів і дедалі суворіших тюремних сроків по всьому світу.

У жовтні 2023 року Microsoft і Amazon об’єднали зусилля для боротьби з мережею кіберзлочинців, яка шахрайствовала з технічною підтримкою понад 2000 організацій клієнтів у всьому світі. Після спільного розслідування ми надали Центральному бюро розслідувань Індії (CBI) кримінальне направлення, у якому виявлено кілька компаній, кол-центрів і осіб, які безпосередньо брали участь в «Операції Чакра II», операції правоохоронних органів, яка включала понад 75 злочинних рейдів по всій Індії для ліквідації організованих кіберфінансових злочинів. Незважаючи на зусилля правоохоронних органів і партнерів у державному та приватному секторах, складність, швидкість, вплив і серйозність кіберзлочинності зростає.

Кіберзлочинці використовують зростаючу екосистему кіберзлочинності як послуги (CaaS), а також технології штучного інтелекту для масштабних атак фішингу та соціальної інженерії. Водночас вони все частіше уникають заходів безпеки, таких як багатофакторна автентифікація (MFA), щоб проводити цілеспрямовані атаки. Як наслідок, боротьба з фінансовим шахрайством, пов’язаним з кібермережами, вимагає багатосторонньої відповіді. Розширення співпраці та зміцнення заходів з виявлення та запобігання є ключовими напрямками. Обізнаність громадськості, пильність і сприяння повідомленню про шахрайство також є життєво важливими компонентами запобігання цим злочинам і пом’якшення їхнього впливу.

Нові тенденції та кошмарні сценарії у світі електронної комерції

Незважаючи на те, що безпека платежів за наявності картки покращується завдяки мобільному гаманцю, чіпу Europay, Mastercard і Visa (EMV), а також технологіям зв’язку ближнього поля (NFC), шахраїв все ще приваблює електронна комерція або простір без картки (CNP), де платіжні картки фізично не присутні для транзакцій.

Очікується, що до 2028 року щорічні збитки, пов’язані з шахрайством з платежами в електронній комерції, у всьому світі перевищать 90 мільярдів доларів США28, причому значну частину економічного впливу нестимуть продавці та фінансові установи.

Безпека карток досягла численних досягнень, включаючи MFA, токенізацію та розширення послуг перевірки адреси. Однак проблеми з функціональною сумісністю та неповне впровадження запланованих удосконалень перешкоджають повсюдному застосуванню цих технологій.

Минулого року корпорація Майкрософт провела понад 1,6 мільярда оцінок ризиків для потенційного шахрайства з платежами та відхилила 1,58 мільярда доларів США у запитах на шахрайські транзакції. Ми помітили зростання кількості складних тактик шахрайства, націлених на вразливі місця в онлайн-транзакціях, зокрема злам веб-інтерфейсу, фішинг, спуфінг і створення синтетичної ідентифікації для викрадення облікових даних і інформації про платіжні інструменти. Традиційні методи, такі як використання великомасштабних витоків даних, залишаються поширеними, що дозволяє шахраям обходити перевірку ідентифікації та отримувати доступ до великих особистих даних. Зростання економіки CaaS також спрощує реалізацію складних схем шахрайства, надаючи швидкий доступ до викрадених даних і шахрайських інструментів.Водночас ми спостерігаємо відхід від застарілих методів

злому на користь таких методів, як фішинг і спуфінг для компрометації облікових даних і отримання доступу до платіжних інструментів.

Generative AI прискорює створення підроблених ідентифікаційних елементів, таких як високоякісні зображення, дипфейки та голосові імітації, що полегшує обман продавців і окремих осіб. Ця підроблена інформація про особу може або приховати справжню особу шахрая, або видати себе за жертву, щоб обдурити продавця, або видати себе за довіреного контакта, щоб обдурити жертву. Такий обман може ввести в оману систему ризиків продавця під час транзакцій або, якщо буде виявлено спочатку, може переконати службу підтримки клієнтів скасувати відхилення. Отже, це дозволяє шахраям незаконно отримувати товари чи послуги, використовуючи вкрадені методи оплати.

Окрім наведених вище загальних тенденцій, корпорація Майкрософт спостерігала такі конкретні методи, які використовуються для шахрайства з платежами електронної комерції:

- Методи перерахування становлять значні ризики в електронній комерції, оскільки відповідність нормативним вимогам не вимагає захисту всіх цифр у 16-значній схемі картки, що дозволяє вгадувати деякі цифри. Шахраї використовують загальнодоступні платіжні схеми та автоматизовані методи, щоб отримати деталі автентифікації, як-от коди верифікаційної вартості картки (CVV) або терміни дії. Щойно вони згенерують дійсні платіжні облікові дані, їх можна буде продати в темній мережі.

- Підробка біометричних даних і створення синтетичних ідентифікацій за допомогою генеративного штучного інтелекту є все більш загрозливими. Глибокі фейки, створені штучним інтелектом, можуть обійти біометричну безпеку в багатьох методах мобільних платежів, які покладаються на технології біометрії, властиві апаратному забезпеченню та операційним системам. Крім того, шахраї використовують штучний інтелект для створення реалістичних синтетичних ідентифікацій, щоб маніпулювати службами підтримки клієнтів продавців.

Практичні рекомендації

1. Включіть моделі ШІ та машинного навчання (ML) в існуючу політику і правила для виявлення незвичних моделей транзакцій і позначення потенційно шахрайських дій у режимі реального часу.

2. Використовуючи голос як фактор автентифікації, обов’язково враховуйте додаткові фактори через зростання аудіомоделей ШІ, здатних відтворювати окремі голоси.

3. Застосовуйте стратегії стримування на основі оцінки ризиків, використовуючи багаторівневий доступ до продукту та моніторинг поведінки клієнтів, щоб керувати зловмисним використанням штучного інтелекту та підробленими ідентифікаторами.

4. Застосуйте надійні заходи автентифікації для перевірки платіжних облікових даних і використовуйте токенізацію, щоб усунути необхідність зберігати повні номери карток.

5. Співпрацюйте з галузевими партнерами, використовуючи безпечні технології, такі як конфіденційне обчислення та середовище чистих кімнат, щоб покращити обмін даними та запобігти шахрайству, одночасно захищаючи конфіденційність.

6. Покращте аутентифікацію за допомогою FIDO, стійкого до фішингу.

2.8. Фішинг

Фішинг залишається постійною загрозою кібербезпеці.

За даними TrendMicro, кількість фішингових атак у 2023 році зросла на 58%, а фінансовий вплив у 2024 році оцінюється в 3,5 мільярда доларів США (Рисунок 2.25).

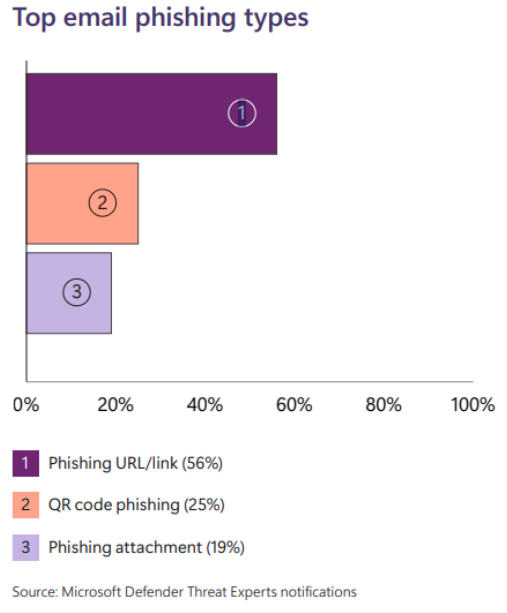


Рисунок 2.25 – Статистика використання фішингових атак по типам

Зловмисники продовжують використовувати давні та нові TTP для доступу до цілей, але цього року все більше занепокоєння викликає зловживання законними веб-сервісами та інструментами для розгортання фішингу.

Електронна пошта на основі програмного забезпечення як послуги (SaaS), інструменти розробника, служби captcha, хмарне сховище, відстеження кліків, маркетингові платформи, платформи для опитування клієнтів, менш відомі клієнти електронної пошти, а також інструменти резервного копіювання та масової розсилки електронною поштою – усе це було використано для цілого ряду шкідливих дій. Одна з ключових переваг використання цих служб полягає в тому, що вони можуть уникати систем виявлення, оскільки менш імовірно, що вони будуть завчасно заблоковані через встановлений рівень довіри та законне використання. Крім того, багато фішингових кампаній поєднують використання кількох законних служб одночасно, що ускладнює процес виявлення як для аналітиків, так і для автоматизованих систем. [24]

Фішинг QR-коду

QR-коди стали набагато поширенішими після пандемії, і тому користувачі їм більше довіряють. За своєю природою QR-коди приховують від користувача пункт

призначення. Приблизно в середині вересня 2023 року аналітики Microsoft спостерігали значне збільшення спроб фішингу з використанням цих кодів, що представляє унікальну проблему для постачальників засобів безпеки, оскільки вони відображаються як зображення під час потоку пошти та не читаються, поки не будуть відтворені.

Під час фішингу QR-коду зловмисники надсилають фішингові повідомлення, що містять код, закодований URL-адресою. У повідомленні одержувачу пропонується відсканувати QR-код своїм пристроєм, перенаправляючи його на підроблену сторінку входу, де йому буде запропоновано ввести свої облікові дані. Ця сторінка може містити можливості AiTM, які обходять деякі форми MFA.

Варто відзначити, що технологія виявлення зображень Microsoft Defender для Office 365 значно порушила фішингові атаки QR-коду, спричинивши зменшення кількості фішингових електронних листів із використанням цієї техніки атаки на 94% у період з жовтня 2023 року по березень 2024 року. Зловмисники постійно адаптують свої атаки у відповідь на ефективне виявлення та блокування, повертаючись до старіших, більш відомих тактик або витрачаючи час і зусилля на інновації.

Порушення ефективних методів, таких як фішинг QR-коду, є важливою частиною захисту мережі та даних. Хоча QR-коди, які є простими та квадратними з чорно-білим штрих-кодом, зберігаються під час фішингових атак, оскільки більше ефективне виявлення та блокування успішно знизило їхню ефективність, суб’єкти загрози вдалися до експериментів із різними візуалізаціями QR-кодів. Наприклад, QR-коди, що складаються з синього штрих-коду на червоному тлі, стали звичним явищем у фішингових атаках, доки цей варіант також не став неефективним.

Інші спроби ввести в оману обробку зображень включають розміщення чорної рамки навколо QR-коду або розміщення QR-коду у вкладенні. Хоча ефективні заходи виявлення та блокування значно зменшили кількість фішингових атак QR-кодів з мільйонів повідомлень, спостережених у 2023 році, протягом 2024 року учасники продовжували тестувати нові методи та інновувати старі, щоб знайти способи уникнути захисту та вплинути на організації.

Протягом квітня та травня 2024 року спостерігався сплеск спроб фішингу, націлених на користувачів Microsoft Teams. Зловмисники створили нового клієнта та зареєстрували домен спеціально для цієї атаки. Ці атаки часто включали в повідомлення QR-коди, які після сканування спрямовували користувачів на фішингові сайти AiTM. Типовими темами цих фішингових кампаній були видавання себе за Office, Microsoft або служби безпеки.

Компроміс корпоративної електронної пошти (ККЕП)

Атаки ККЕП залишаються поширеною загрозою, а маніпуляція правилами вхідних повідомлень є улюбленим методом (Рисунок 2.26).

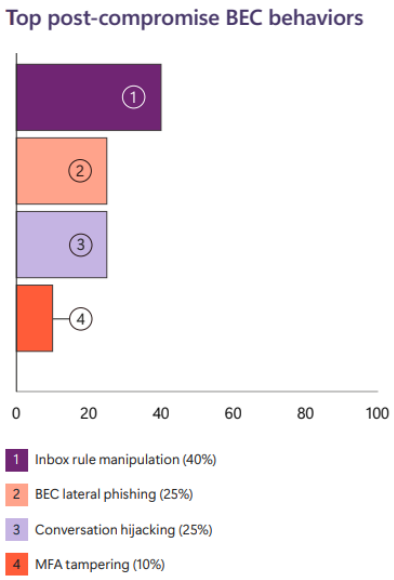


Рисунок 2.26 – Найпоширеніші види поведінки ККЕП після компрометації

Маніпулювання правилом папки "Вхідні": з'явився новий варіант, пов'язаний з маніпуляціями через використання API/додатків. Замість використання звичайних команд «New-InboxRule» або «Set-InboxRule», зловмисники тепер використовують «UpdateInboxRules». Це дозволяє їм перенаправляти електронні листи з ключовими словами, пов'язаними з обліковими даними чи фінансовими питаннями, у менш контрольовані папки, такі як «Спам», «Історія розмов» або «Видалені елементи», приховуючи свою шахрайську діяльність від безпосереднього зору користувача.

Бічний фішинг ККЕП: після компрометації облікового запису зловмисники прагнуть переміщатися всередині організації, націлюючись на кількох користувачів, щоб або отримати доступ до облікових записів із високим рівнем привілеїв, або обманом змусити користувачів оплачувати фальшиві рахунки. Це досягається шляхом надсилання фішингових електронних листів іншим користувачам в організації.

Викрадення розмови: зловмисник компрометує обліковий запис електронної пошти відправника та впроваджує себе в існуючий потік електронної пошти за допомогою схожого на вигляд облікового запису, зберігаючи відображуване ім'я відправника незмінним. Домен зламаного облікового запису, як правило, нещодавно створюється для шахрайства з фінансовими мотивами, щоб заманити користувачів.

Втручання MFA після атаки AiTM: після зламу облікового запису користувача зловмисник намагається додати додатковий пристрій для MFA, наприклад номер телефону для підтвердження двофакторної авторизації або реєстрації нового пристрою за допомогою автентифікатора, щоб підтримувати постійний доступ. Помічена інша поведінка, яка заслуговує на увагу після компромісу

Зловживання законними програмами: ми помітили, що зловмисники зловживають трьома новими законними інструментами для крадіжки поштових скриньок і ККЕП.

– Програмне забезпечення PerfectData: програма, інтегрована з Microsoft 365/Azure для надання послуг поштової скриньки та резервного копіювання.

Зловмисники використовували його для таємного доступу та крадіжки поштових скриньок скомпрометованих користувачів.

– Newsletter Software Supermailer: законне програмне забезпечення, яке використовується для створення та надсилання персоналізованих масових електронних листів та інформаційних бюлетенів. Зловмисники використовували його для проведення бокових фішингових атак із скомпрометованих облікових записів користувачів.

– eMClient: настільний поштовий клієнт для Windows і macOS. Зловмисники використовували це для викрадання поштових скриньок скомпрометованих користувачів. Низький і повільний ККЕП: зловмисники щодня непомітно читають невелику кількість електронних листів (від двох до п’яти) і рідко отримують доступ до файлів OneDrive/SharePoint, намагаючись уникнути виявлення. Ці малопрофільні атаки кинули виклик системам виявлення, які могли ідентифікувати їх лише шляхом кореляції з незвичними діями входу. Цільовий ККЕП: персоналізовані фішингові кампанії створюються з використанням місцевих мов, націлені на ІТ, фінансові та юридичні відділи з конкретними темами, такими як «оновлення програмного забезпечення» або «подання податку».

Наступні спеціальні стратегії значно підвищує рівень успішності компромісу.

1. Навіть якщо інструмент здається знайомим, не вважайте, що він безпечний. Наприклад, минулого року Microsoft виявила нову тенденцію, коли зловмисники зловживали трьома законними інструментами для зловмисних дій.

2. Більш витончені атаки. Іншою помітною тенденцією є персоналізація фішингових кампаній і вихідних повідомлень за допомогою місцевих мов.

3. Фішинг QR-кодів зростає, але ефективні заходи виявлення та блокування можуть значно зменшити кількість атак.

4. Тіньові ІТ або частини апаратного чи програмного забезпечення, які користувачі встановлюють без дозволу ІТ-відділу, становлять загрозу для організацій і роблять їх уразливими до фішингу та посткомпрометованих дій. ІТ-команди повинні періодично сканувати інфраструктуру, щоб виявити неавторизоване програмне або апаратне забезпечення та вжити заходів для виправлення.

2.9. Видача себе за іншу особу

Видача себе за іншу особу є ключовим методом, який використовують шахраї, щоб завоювати довіру своїх жертв. Хоча це має різні форми, видавання себе за законні компанії становить ризик як для клієнтів, так і для репутації компанії. Розглядаючи світ корпоративних імітацій, корпорація Майкрософт помітила, що шахраї підвищують витонченість і швидкість у всіх сферах.

Більшість фішингових кампаній цього року, націлених на споживачів, видавали себе за бренди онлайн-програмного забезпечення та послуг. Це не дивно, враховуючи цінність для зловмисників компрометації та використання облікових записів споживачів на платформах, які можуть охоплювати соціальні мережі, хмарне сховище, електронну пошту, електронну комерцію тощо. Фішинг стане менш

поширеним і менш прибутковим для зловмисників, оскільки все більше споживачів запровадять надійну MFA та безпарольну технологію (Рисунок 2.27). [25]

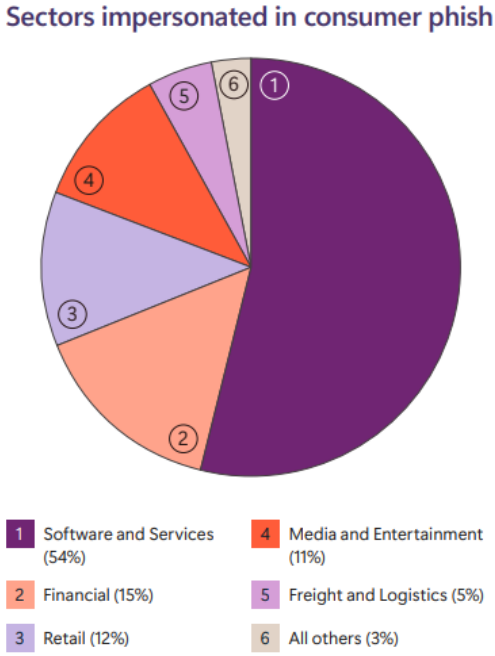


Рисунок 2.27 – Галузі, які підробляються в фішингових атаках на споживачів

Діпфейки

Більшість синтетичних медіа, створених штучним інтелектом, також відомих як «дипфейки», націлені або на спільноти (наприклад, неправдиві новини), або на окремих осіб (шахрайство). Як і інші загрози, засновані на видаванні себе за іншу особу, глибокі фейки існують у спектрі складності. Наприклад, загрозливий суб'єкт може використовувати фальшиві повідомлення електронної пошти та текстові повідомлення, щоб переконати працівників у тому, що начальник або колега потребують, щоб вони вжили заходів. Однак значне зростання рівня складності на горизонті призведе до серйозних змін, зокрема у верифікації особи.

За даними Gartner, до 2026 року 30% підприємств очікують, що перестануть вважати біометричну перевірку особи та рішення автентифікації надійними окремо.

Оскільки дипфейки стають все більш поширеними в бізнес-середовищі, організаціям доведеться застосовувати контрзаходи, наприклад вимагати додаткової перевірки транзакцій. У той же час Microsoft вивчає рішення щодо походження, щоб допомогти підвищити прозорість цифрового онлайн-контенту.31

Корпоративна імітація

Спуфінг домену включає різні класичні методи, які дозволяють видати себе за юридичних осіб. Одним із таких методів є схожі домени, які ми ідентифікували раніше: гомогліфні домени. Самозванці покладаються на те, що користувачі не помічають невеликі зміни символів, які використовуються в доменному імені, наприклад використання нуля замість літери «О» в доменному імені. Обманом змушуючи користувачів натискати посилання або відвідувати ці шахрайські веб-сайти, зловмисники можуть змусити їх поділитися конфіденційною інформацією, що потенційно може призвести до крадіжки фінансових даних або особистих даних.

Шахраї подвоїли різні форми імітації доменів, включаючи гомогліфи, сквотінг субдоменів і правдоподібну реєстрацію альтернативного домену. Сквотінг субдомену

передбачає створення субдомену в хмарній службі під надійним іменем для здійснення атак на електронну пошту, наприклад використання «contoso.onmicrosoft.com» як субдомену.

З іншого боку, ймовірна реєстрація альтернативного домену передбачає додавання слів або зміну домену верхнього рівня (TLD), щоб обдурити користувачів. Наприклад, реєстрація домену на кшталт «contoso.store».Корпорація Майкрософт почала пілотувати Entra Verified ID як елемент розширеної перевірки особи, вимагаючи від користувачів надавати офіційне посвідчення особи в ситуаціях, коли автентичність їх особи піддається сумніву. Початкові результати показують, що цей контроль дає багатообіцяючі результати, ефективно запобігаючи більшості спроб видавання себе за компанію. Продовжуючи тренувати моделі та створювати для масштабування, ми очікуємо подальшого покращення цих результатів.

Практичні висновки:

1. Навчіть співробітників стежити за доменами, які імітуються.

2. Під час увімкнення облікових записів і служб використання перевірених моделей ідентифікації та виявлення штучного інтелекту може значно зменшити ризик надання шахрайського доступу.

3. Навчіть співробітників, як перевіряти цілісність вмісту.

Стан технічного шахрайства (techscam)

Технічне шахрайство відноситься до шахрайства або шахрайства, які роблять ваш комп’ютер вразливим до додаткових шкідливих дій. Корпорація Майкрософт виявила, що більшість технічних шахраїв походять із шкідливих рекламних платформ. Існує кілька типів технічних шахрайств, кожна з яких має свій унікальний спосіб дії:

– Технічне шахрайство служби підтримки Microsoft/McAfee/Apple techscam: ці шахрайства видають себе за законні служби підтримки від провідних технологічних компаній, щоб обманом змусити користувачів надати конфіденційну інформацію або здійснити платежі за неіснуючі проблеми.

– Криптовалюта/фальшиві покупки: шахраї використовують зловмисну рекламу для просування шахрайських схем із криптовалютою або фальшивих торгових угод, заманюючи користувачів у фінансові пастки.

– Шахрайство зі зловмисними розширеннями веб-переглядача: ці шахрайські дії змушують користувачів установлювати розширення веб-переглядача, які можуть маніпулювати результатами пошуку, показувати нав’язливу рекламу або викрадати особисті дані.

– Шахрайство зі зловмисними сповіщеннями веб-переглядача: користувачів вводять в оману, дозволяючи веб-переглядач надсилати сповіщення від зловмисних сайтів, які потім бомбардують їх оманливими сповіщеннями або спробами фішингу.

Поточна ситуація з технічними шахрайствами є тривожною: статистика трафіку SmartScreen за період з 2022 по 2024 рік показує, що понад 90% шкідливого трафіку в браузері Edge пов'язано з технічними шахрайствами (Рисунок 2.28).

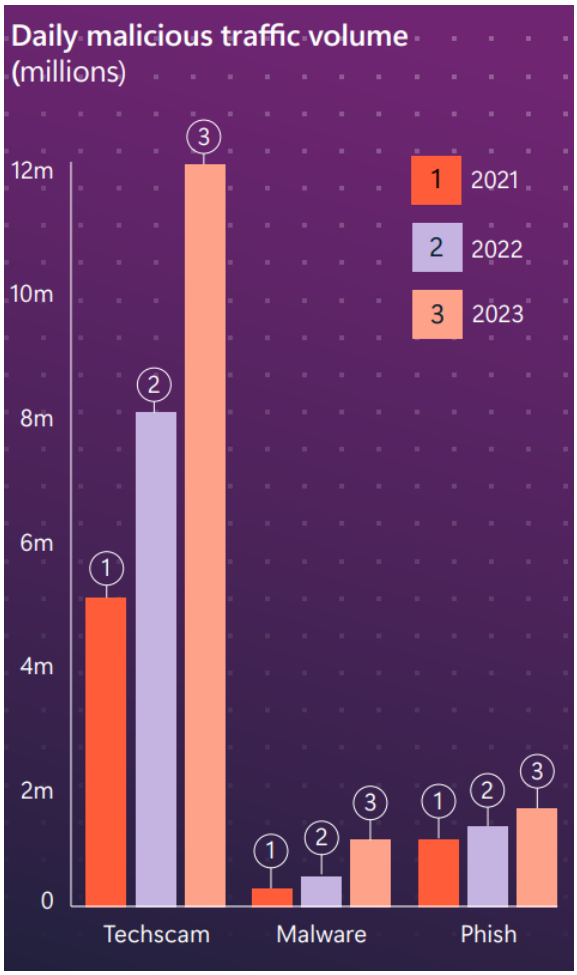


Рисунок 2.28 – Щоденний обсяг шкідливого трафіку (млн)

Щоденний обсяг трафіку технічного шаахрайства різко зріс, стрімко збільшившись з 2021 року, що різко контрастує з шкідливим програмним забезпеченням та фішингом за той самий період.

Серед технічних шахрайств найбільших фінансових збитків у всьому світі завдають шахрайства, пов'язані з інвестиціями та криптовалютою, а також шахрайства, пов'язані з технічною підтримкою. Загалом технічні шахрайства мають у 10 разів більший фінансовий вплив, ніж фішинг.

Тимчасовий характер зловмисних хостів на хмарних серверах, таких як Azure, DigitalOcean і CloudFront, створює значні труднощі для їх виявлення та нейтралізації. Хмарні сервери надають простий і економічно ефективний спосіб створення хост-сторінок. Більше того, понад 70% зловмисних об'єктів активні менше двох годин, що означає, що вони можуть зникнути ще до того, як їх виявлять. Така швидка зміна підкреслює необхідність більш гнучких і ефективних заходів кібербезпеки.

Дослідники Microsoft розробляють нову модель виявлення на основі штучного інтелекту для виявлення шахрайства за допомогою локальної невеликої мовної моделі, захищаючи першу жертву, яка побачила шахрайство, та повідомляючи про шахрайство SmartScreen для захисту інших користувачів.

Дослідники Microsoft також розробляють клієнтські сигнали для аналізу візуальних і структурних елементів сторінок технічних шахрайств. Ця нова функція має значний потенціал виявлення, особливо з огляду на те, що інциденти технічних шахрайств часто є короткочасними. Ця функція дозволяє нам швидше виявляти

загрози, що значно підвищує ефективність наших можливостей виявлення технічних шахрайств.

Практичні рекомендації:

1. Попередньо блокуйте відомі шкідливі домени, створюючи список блокування на основі архітектури доменів, таких як IP, Whois і PDNS (захисна система доменних імен), а також інформації про ланцюжки перенаправлення в журналах телеметрії, які зазвичай використовуються в операціях технічного шахрайства.

2. Постійно оновлюйте динамічне використання списків блокування, щоб випереджати розвиток тактики шахраїв.

Захоплення облікових записів (ЗОЗ, англійською ATOs)

У сфері бізнесу та споживання спостерігається постійне зростання кількості випадків злому облікових записів, крадіжок особистих даних та зловживання платіжними інструментами в контексті ЗОЗ (Рисунок2.29).

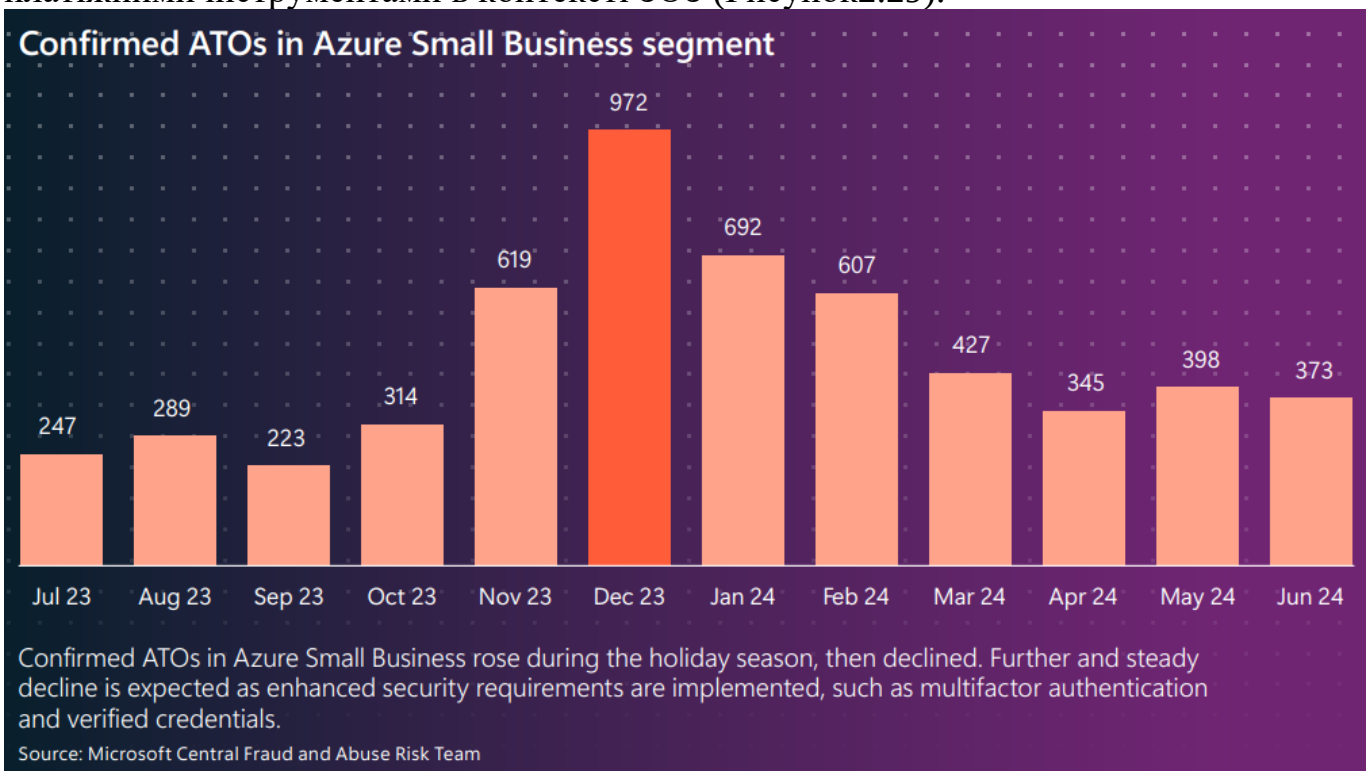


Рисунок 2.29 – Підтверджені захоплення облікових записів в сегменті Azure Small Business

Зловмисники вибирають найменш захищені облікові записи та найбільш вразливих осіб, тому важливо постійно підвищувати рівень захисту облікових записів. Хоча найкращою практикою для споживачів є наявність і підтримка актуальної MFA та пильний моніторинг облікових записів, для пом'якшення наслідків успішних зломів було створено цілу галузь.

В останні роки галузеві звіти вказують на зростання загрози у світі бізнес-бізнес та в сфері керованих онлайн-послуг. Оскільки злом останніх може вплинути на

кінцевих споживачів клієнтських підприємств, це додає ще один рівень складності та ризику.

Згідно з одним дослідженням, 29% інтернет-користувачів зараз стикалися з ЗОЗ, що на 22% більше, ніж у 2021 році. За той самий період кількість випадків захоплення бізнес-акаунтів зросла з 13% до 21%.

Згідно з моніторингом тенденцій Microsoft, багато облікових записів Microsoft, які були захоплені минулого року, не дотримувалися основних рекомендацій з безпеки облікових записів, таких як використання MFA. Незважаючи на появу більш досконалих методів хакерства, більшість випадків ЗОЗ все ще відбуваються за допомогою простих методів, таких як розпилення паролів, фішинг, кейлоггінг та використання паролів з попередніх атак, знайдених в Інтернеті.

Останнім часом Microsoft зазнала сплеску атак на «загальні», «групові» або «багатокористувацькі» облікові записи. Ці облікові записи зазвичай мають застарілі паролі, і оригінальний користувач може більше не контролювати їх. Загальні облікові записи зазвичай використовуються адміністраторами для зручності обслуговування, але їх важче захистити. Впровадження ефективної багатофакторної автентифікації є складним завданням, а виявлення порушень безпеки за допомогою розпізнавання шаблонів стає важким, коли доступ мають декілька користувачів. Крім того, відновлення облікових записів для постачальників послуг є проблематичним, що ускладнює повернення зламаних облікових записів їх законним власникам.

Практичні поради

1. Дотримання найновіших стандартів безпеки облікових записів є надзвичайно важливим для захисту від ризику ЗОЗ.

2. Хакери шукають слабкі місця в системі безпеки та сезонні можливості, коли власники облікових записів не зосереджені на моніторингу, щоб розширити масштаби своїх атак.

3. Розгляньте можливість переведення вашої бази користувачів на додаток для автентифікації, щоб забезпечити легке оновлення до нових стандартів MFA після їх випуску.

Висновок за розділом: у цьому розділі було розглянуто найбільші загрози в ІТ у сучасному світі. Окрім цього, було надано інформацію за найбільшими загрозами, а також надано статистики за різними типами атак, їх цілями та секторами взаємодії.

3. ВИДИ АВТОРИЗАЦІЇ ТА ЇХ ПРАКТИЧНА РЕАЛІЗАЦІЯ

3.1. Ідентифікація, аутентифікація, авторизація.

Ідентифікація

Ідентифікація - це процес, за допомогою якого користувач з'являється системі, тобто заявляє, хто він або вона.

Ключові особливості:

- Це заява про особу, а не перевірка;
- Сам по собі не гарантує, що ви є тим, за кого себе видаєте;
- Завжди передує автентифікації.

Використовується в:

- Форма входу (ім'я користувача або електронна пошта);
- JWT - під (суб'єктне) поле є ідентифікатором;
- Будь-який зовнішній ідентифікатор (наприклад, банківська картка, пропуск.

Аутентифікація — це процес підтвердження ідентичності користувача, програми або служби, що намагається отримати доступ до системи або ресурсу. Це важливий етап у забезпеченні інформаційної безпеки, оскільки він дозволяє системі перевірити, чи дійсно особа або пристрій є тими, за кого себе видають. (Рисунок 3.1).

Мета автентифікації:

1. Ідентичність: перевірка того, що користувач є тим, за кого себе видає.
2. Контроль доступу : обмежити доступ до певних ресурсів тільки авторизованим користувачам.
3. Підтримання безпеки : запобігання несанкціонованому доступу та зловживанням.

Важливість і мета аутентифікації.

Належна реалізація аутентифікації має вирішальне значення для забезпечення безпеки та конфіденційності даних у веб-додатках. Без надійної аутентифікації зловмисники можуть отримати доступ до конфіденційної інформації, порушити роботу програми або завдати шкоди користувачам. [26]

До основних завдань аутентифікації належать:

1. Перевірка облікових даних користувача (логін/пароль).
2. Використовуйте додаткові фактори автентифікації (наприклад, двофакторну автентифікацію).
3. Регулярна перевірка прав доступу та повноважень користувачів.

Рисунок 3.1 – Три компонента для отримання доступа до ресурсу

Рекомендації щодо реалізації аутентифікації

Для ефективного захисту даних рекомендуються наступні підходи:

- Зберігайте паролі в зашифрованому вигляді.
- Обмежити кількість невдалих входів.
- Використовуйте SSL/TLS для шифрування переданих даних.
- Періодично оновлюйте паролі та виконуйте перевірки безпеки.

Аутентифікація є ключовим елементом інформаційної безпеки, що забезпечує ідентифікацію та підтвердження автентичності суб'єктів інформаційних систем.

Сфери застосування аутентифікації

Аутентифікація застосовується практично в усіх сферах цифрової інфраструктури, де необхідний захист ресурсів та забезпечення конфіденційності даних. Основні сфери застосування включають:

Веб-додатки та сервіси;

- Мобільні додатки;
- Системи управління корпоративними даними (ERP, CRM);
- Електронна комерція та онлайн-банкінг;
- Державні інформаційні системи та електронне урядування.

Процес аутентифікації вирішує низку важливих завдань, спрямованих на захист і управління доступом до інформаційних ресурсів :

- Ідентифікація суб'єкта (визначення особи користувача);
- Авторизація (дозвіл або заборона доступу до конкретних ресурсів);
- Моніторинг активності користувачів (реєстрація дій і подій);
- Управління правами доступу (контроль привілеїв і ролей користувачів).

Рекомендації щодо застосування аутентифікації

Для ефективного впровадження аутентифікації необхідно враховувати наступні аспекти:

1. Використання безпечних механізмів зберігання паролів (хешування з сіллю);
2. Застосування багатофакторної аутентифікації (MFA) для підвищення рівня безпеки;
3. Регулярний моніторинг та аудит процесів аутентифікації;
4. Інтеграція аутентифікації із зовнішніми сервісами (OAuth, OpenID Connect).

Авторизація (Authorization)

Авторизація – це процес визначення, які дії дозволені користувачеві після успішної аутентифікації.

Ключові форми:

- Ролі (admin, user, moderator);

– Права (read, write, delete);
– Scopes (в OAuth2);
– ACL (access control lists).

Як легко запам'ятати:
Ідентифікація – це «покажи, хто ти»,
Аутентифікація – це «докажи, що ти – це ти»,
Авторизація – «що тобі дозволено». [27]

3.2. Basic auth

Basic Auth – це найпростіший спосіб аутентифікації, при якому логін і пароль передаються в кожному HTTP-запиті у вигляді base64-кодованого рядка.

Ідеально, коли потрібно просто і швидко, але ніколи не використовуйте його в публічних додатках без HTTPS.

Basic Auth – це мінімалізм у чистому вигляді.

Це не рішення «на роки» – це спосіб «вставити логін за 30 секунд» (Рисунок 3.2 та Рисунок 3.3).

Рисунок 3.2 – Схематична робота самої базової аутентифікації

Як працює:
Користувач вводить логін і пароль.
Ці дані кодуються в base64: username:password.
Base64 не шифрує, а просто кодує → потрібен HTTPS.
У кожному запиті відправляється заголовок:

```
Authorization: Basic YWRtaW46c2VjcmV0=
```

Сервер декодує заголовок і перевіряє логін/пароль вручну або через middleware
Middleware – це проміжний шар, який обробляє запит до (або після) основного обробника запиту.

Плюси:
– Налаштовується за 1 хвилину (наприклад, в Nginx або FastAPI);
– Не вимагає кукі, бази сесій, генерації токенів;
– Стандарт HTTP з 1990-х, реалізований у багатьох бібліотеках.

Мінуси:
– Навіть після логіну – логін і пароль надсилаються в кожному запиті
– «Вийти» неможливо – тільки очистивши кеш браузера або токен
– Перехоплення трафіку = крадіжка пароля
– Немає ролей, scopes, сесій
– Немає revoke, логів, контролю, аналітики

Де застосовується:

1. Підходить:
   - Адмін-панелі «для своїх»;
   - Внутрішні інструменти (за VPN);
   - Швидкі MVP, тестові API.
2. Не підходить:
   - Публічні веб-додатки;
   - SPA і мобільні клієнти;
   - Продакшн без HTTPS.

Приклад коду в FastAPI:

```
from fastapi import FastAPI, Depends
from fastapi.security import HTTPBasic, HTTPBasicCredentials

app = FastAPI()
security = HTTPBasic()

@app.get("/secret-resource")
def read_secret(credentials: HTTPBasicCredentials = Depends(security)):
    if credentials.username == "admin" and credentials.password == "secret":
        return {"message": "Welcome!"}
    return {"error": "Unauthorized"}
```

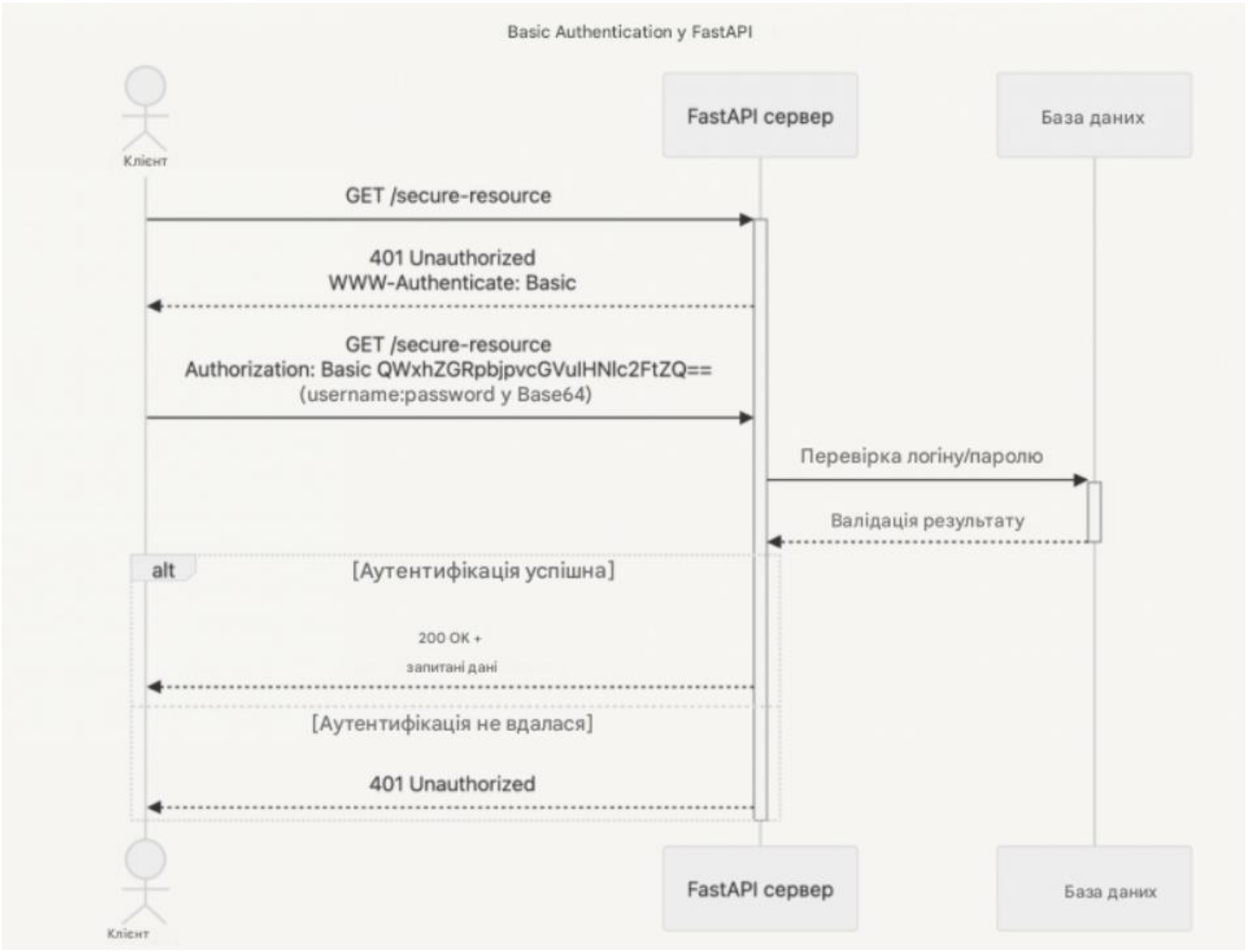


Рисунок 3.3 – Схема UML sequence діаграма послідовності дій

3.3. Session auth

Це старий, перевірений спосіб аутентифікації, який широко використовується в класичних веб-додатках (Django, Flask, Rails та ін.).

Схема роботи session based auth.

Користувач входить в систему – надсилає логін/пароль → POST /login з {«username»: «...», “password”: «...»}

Сервер перевіряє їх і створює сесію → Зберігаємо в пам'яті або базі зв'язок сесії з обліковим записом.

Сервер присвоює сесії унікальний ID (зазвичай – випадковий рядок) → Генеруємо session_id

Цей ID відправляється користувачеві в cookie → наприклад:

HTTP/1.1 200 OK

Set-Cookie: sessionid=abc123; HttpOnly; Path=/; Secure

При кожному наступному запиті браузер автоматично відправляє cookie → наприклад:

GET /profile HTTP/1.1

Host: example.com

Cookie: sessionid=abc123

Сервер за ID знаходить сесію і «впізнає» користувача → звіряємо сесію в базі і витягуємо обліковий запис, до якого прив'язана сесія.

Переваги:

- Простота впровадження: легко реалізується на багатьох фреймворках;
- Безпека: сесійний ID зберігається тільки на сервері, токен не містить чутливу інформацію;
- Просте управління: можна легко анулювати сесії, контролювати час життя;
- Менше навантаження на клієнта: вся логіка аутентифікації на сервері;
- Стійкість до XSS-атак: при правильній реалізації з HttpOnly cookies.

Недоліки:

- Зберігання стану: вимагає зберігання сесій на сервері (пам'ять/БД/Redis);
- Масштабованість: складніше розподіляти навантаження між серверами;
- Проблеми з CORS: ускладнюється робота при крос-доменних запитах;
- Вразливість до CSRF-атак: потрібні додаткові заходи захисту;
- Продуктивність: додаткові запити до сховища сесій.

Приклад у FastAPI:

Ось короткий приклад реалізації на FastAPI:

```
from fastapi import FastAPI, Depends, HTTPException, status, Response, Request
from fastapi.security import HTTPBasic, HTTPBasicCredentials
from pydantic import BaseModel
import uuid
import redis
from typing import Optional

app = FastAPI()
security = HTTPBasic()

# Підключення до Redis
r = redis.Redis(host="localhost", port=6379, db=0)
SESSION_EXPIRE = 3600  # 1 година

# Моделі даних
class User(BaseModel):
    username: str
    password: str

class UserInDB(User):
    hashed_password: str

# Заглушка для бази даних користувачів
fake_users_db = {
    «user1»: {
        «username»: «user1»,
        «hashed_password»: «password1»  # У реальному додатку використовуйте хешування паролів
```

```
        }
    }

    # Перевірка облікових даних
    def get_current_user(credentials: HTTPBasicCredentials =
Depends(security)):
        user = fake_users_db.get(credentials.username)
        if not user or user[«hashed_password»] !=
credentials.password:
            raise HTTPException(
                status_code=status.HTTP_401_UNAUTHORIZED,
                detail=«Неправильні облікові дані»,
                headers={«WWW-Authenticate»: «Basic»},
            )
        return user

    # Отримання користувача за сесією
    def get_user_by_session(request: Request):
        session_id = request.cookies.get(«session_id»)
        if not session_id:
            return None

        username = r.get(f«session:{session_id}»)
        if not username:
            return None

        return fake_users_db.get(username.decode())
    # Маршрути
    @app.post(«/login»)
    def login(response: Response, user: User =
Depends(get_current_user)):
        # Створення сесії
        session_id = str(uuid.uuid4())
        r.setex(f«session:{session_id}», SESSION_EXPIRE,
user[«username»])

        # Встановлення cookie
        response.set_cookie(
            key="session_id",
            value=session_id,
            httponly=True,
            max_age=SESSION_EXPIRE,
            samesite="lax",
            secure=True  # У production має бути True
        )

        return {«message»: «Успішний вхід»}

    @app.get(«/me»)
    def read_user(user: Optional[dict] =
Depends(get_user_by_session)):
        if not user:
```

```
            raise HTTPException(
                status_code=status.HTTP_401_UNAUTHORIZED,
                detail="Потрібна аутентифікація"
            )
        return {«username»: user[«username»]}

    @app.post(«/logout»)
    def logout(response: Response, request: Request):
        session_id = request.cookies.get(«session_id»)
        if session_id:
            r.delete(f«session:{session_id}»)
        response.delete_cookie(key=«session_id»)
        return {«message»: «Вихід виконано успішно»}
```

Цей приклад показує базову реалізацію сесійної аутентифікації з використанням FastAPI та Redis для зберігання сесій (Рисунок 3.4).

Ключові моменти:

- Сесійний ID генерується як UUID і зберігається в Redis з обмеженим часом життя.
- Кукі встановлюються з прапорцями HttpOnly і SameSite для захисту.
- Реалізовані основні ендпоінти: вхід, вихід і отримання інформації про поточного користувача.
- При виході сесія видаляється з Redis і кукі очищаються.

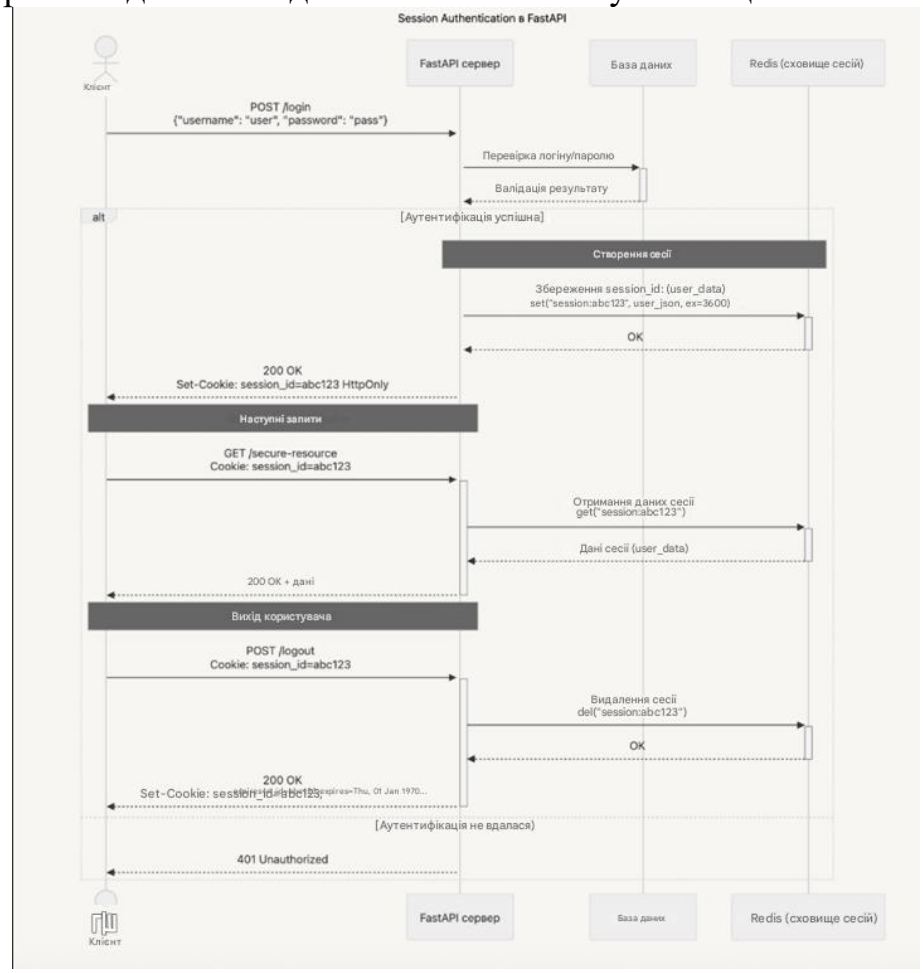


Рисунок 3.4 – UML sequence діаграма послідовності дій

3.4. Token based auth

Схема роботи token-based авторизації (Без refresh token) (Рисунок 3.5 та Рисунок 3.6).

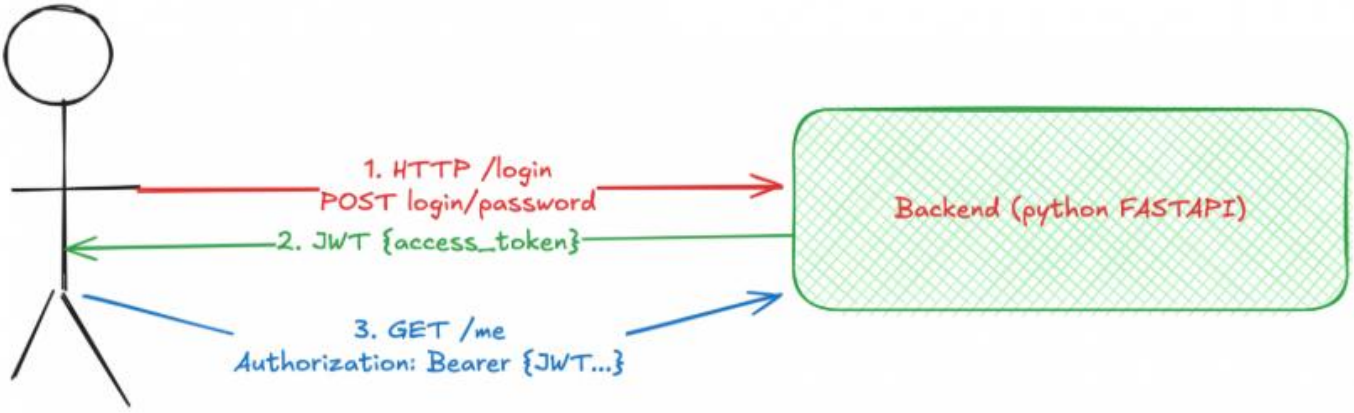


Рисунок 3.5 – Схема реалізації аутентифікації з токеном

Користувач відправляє логін і пароль → POST /login з {«username»: «...», “password”: «...»}.

Сервер перевіряє облікові дані → Порівнює логін і пароль з логін-паролем з бази/сховища.

Сервер створює JWT access token → За допомогою функції з пункту 2. По суті генерує спеціальний рядок і не зберігає його, просто повертає як результат методу.

Токен повертається користувачеві → У тілі відповіді або HttpOnly cookie.

Клієнт зберігає токен → У localStorage (небезпечно) або в cookie (безпечно).

LocalStorage – це сховище в браузері, де можна зберігати дані у форматі ключ:значення.

Подальші запити надходять з токеном → У заголовку: Authorization: Bearer <token>.

Сервер перевіряє підпис і exp токена → Якщо все первірка пройдена успішно – користувач авторизований.

Якщо exp пройшов, значить токен більше недійсний. → Повертаємося до пункту 1.

Токен може бути будь-яким, аби ти реалізував логіку процесингу. АЛЕ, зазвичай використовується JWT токен, оскільки це стало «зрозумілим стандартом» для реалізації авторизації.

JWT (JSON Web Token) – це токен, що складається з трьох частин, розділених крапками – header.payload.signature.

Кожна частина:

1. Header – метадані: тип токена та алгоритм підпису.
2. Payload – дані (claims): хто ви, термін дії, ролі тощо.
3. Signature – цифровий підпис (перевірка автентичності) </aside>

Передача токена здійснюється в заголовку HTTP Authentication: Bearer {your_token_here}

Base64 робить їх безпечними для передачі по HTTP:

- Без спецсимволів ({}, ", :);
- Без пробілів, переносів;
- Тільки ASCII: зручно в URL, заголовках.

Приклад токена:

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiYWRtaW4iOnRydWUsImlhdCI6MTUxNjIzOTAyMn0.KMUFsIDTnFmyG3nMiGM6H9FNFUROf3wh7SmqJp-QV30

Приклади інформації, яка може зберігатися в різних частинах токена:

Header:

```
{
"alg": "HS256",
"typ": "JWT"
}
```

Payload:

```
{
"sub": "1234567890", # user uid
"name": "John Doe", # user name (например, для фронта)
"admin": true, # роль пользователя
"iat": 1516239022, # время когда токен был выпущен секунды начиная с
01-01-1970
"exp": 1716666000 # время когда токен "протухнет"
}
```

Signature (Підпис. Це опціональна частина, без якої можно обійтися, але при цьому буде не можливо перевірити, хто випустив токен.):

a-string-secret-at-least-256-bits-long

Приклад генерації токена використовуючи пакет pyJWT:

```
import jwt
from datetime import datetime, timedelta

SECRET_KEY = "your-secret-key"
ALGORITHM = "HS256"

def generate_token(data: dict):
    payload = data.copy()
    payload["exp"] = datetime.utcnow() + timedelta(minutes=15)
    return jwt.encode(payload, SECRET_KEY, algorithm=ALGORITHM)

# Пример использования
token = generate_token({"sub": "user_id_123"})
print(token)
```

В payload можуть бути наступні функції, так звані claims (Табл. 3.1):

Таблиця 3.1 – Дані, які можуть зберігатися в токені.

Claim	Призначення	Чи є обов'язковим
Sub	ID користувача	так
Exp	Час закінчення терміну дії токена (timestamp)	так

Iat	Коли був створений	бажано
Nbf	«Не раньше ніж» (not before)	опціонально

Продовження таблиці 3.1

Iss	Хто створив токен (issuer)	опціонально
Aud	Для кого призначений (audience)	опціонально
Користувач	Наприклад, role, email, scopes	опціонально

Алгоритми підпису: HS256 vs RS256

HS256 – симетричний підпис. Один секретний ключ. Просто, але не масштабується.

RS256 – асиметричний. Приватний ключ для підпису, публічний – для перевірки. Краще для мікросервісів і OAuth2.

Найпоширеніші помилки:

- Не ставлять exp (і отримують «вічні» токени);
- Додають до токена пароль або чутливі дані;
- Використовують занадто короткий або слабкий SECRET_KEY;
- Відправляють токен без Bearer схеми в заголовку;
- Не верифікують підпис на сервері.

Refresh token flow

Refresh token використовується для отримання нового access token без повторної аутентифікації користувача. Його основна схема роботи:

При авторизації клієнт отримує два токени:

- Access token (короткочасний, наприклад 15-30 хвилин);
- Refresh token (довготривалий, наприклад 7-30 днів).

Коли access token закінчується:

- Клієнт відправляє refresh token на спеціальний endpoint (наприклад, POST /refresh);
- Сервер перевіряє валідність refresh токена;
- При успішній перевірці сервер генерує новий access token і повертає його клієнту;
- Опціонально: генерує новий refresh token (rotation strategy).

Схема запиту оновлення:

```
POST /refresh
Content-Type: application/json

{
  "refresh_token": "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ..."
}
```

Відповідь на запит:

```
{
  "access_token": "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVC...",
  "refresh_token": "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVC...", //
Опционально
```

```
  "token_type": "Bearer",
  "expires_in": 900
}
```

Особливості refresh токенів:

- Структура: Можуть бути JWT або просто випадкові рядки (UUID);
- Зберігання: Обов'язково в базі даних або Redis на стороні сервера;
- Безпека: Зберігаються на стороні клієнта в HttpOnly, Secure, SameSite=strict cookie або в захищеному сховищі.

Термін дії: Значно довше, ніж access токен, але має кінцевий термін

Рекомендації щодо реалізації:

1. Створюйте унікальний refresh token для кожного пристрою користувача;
2. Додайте fingerprint пристрою для додаткового захисту;
3. Використовуйте одноразові refresh токени (rotation strategy).

Вилучення JWT (revoke)

Одним із недоліків JWT є складність вилучення токенів, оскільки вони за замовчуванням є дійсними до закінчення терміну дії.

Існує кілька підходів до вирішення цієї проблеми:

1. Blacklist вилучених токенів (приклад в Redis):

```
def revoke_token(token):
    token_data = jwt.decode(token, SECRET_KEY,
algorithms=[ALGORITHM])
    jti = token_data.get("jti", token_data.get("sub"))  #
уникальный ID токена
    expiration = token_data["exp"] -
int(datetime.utcnow().timestamp())
    redis_client.setex(f"revoked:{jti}", expiration, "1")

def is_token_revoked(token):
    token_data = jwt.decode(token, SECRET_KEY,
algorithms=[ALGORITHM])
    jti = token_data.get("jti", token_data.get("sub"))
    return redis_client.exists(f"revoked:{jti}")
```

2. Контроль через Refresh токени:

- Зберігайте тільки refresh токени в базі даних;
- При логауті - видаляйте refresh токен з бази;
- Тримайте короткий термін дії access токенів.

3. Випуск з версією/ідентифікатором користувацької сесії:

```
def generate_token(user_id, session_id):
    return jwt.encode({
        "sub": user_id,
        "sid": session_id,  # Идентификатор сессии
        "exp": datetime.utcnow() + timedelta(minutes=15)
    }, SECRET_KEY, algorithm=ALGORITHM)

def verify_token(token, active_sessions):
    payload = jwt.decode(token, SECRET_KEY,
algorithms=[ALGORITHM])
```

```
        # Проверяем не только подпись, но и актуальность сессии
        if payload["sid"] not in active_sessions.get(payload["sub"],
[]):
            raise Exception("Token revoked")
        return payload
```

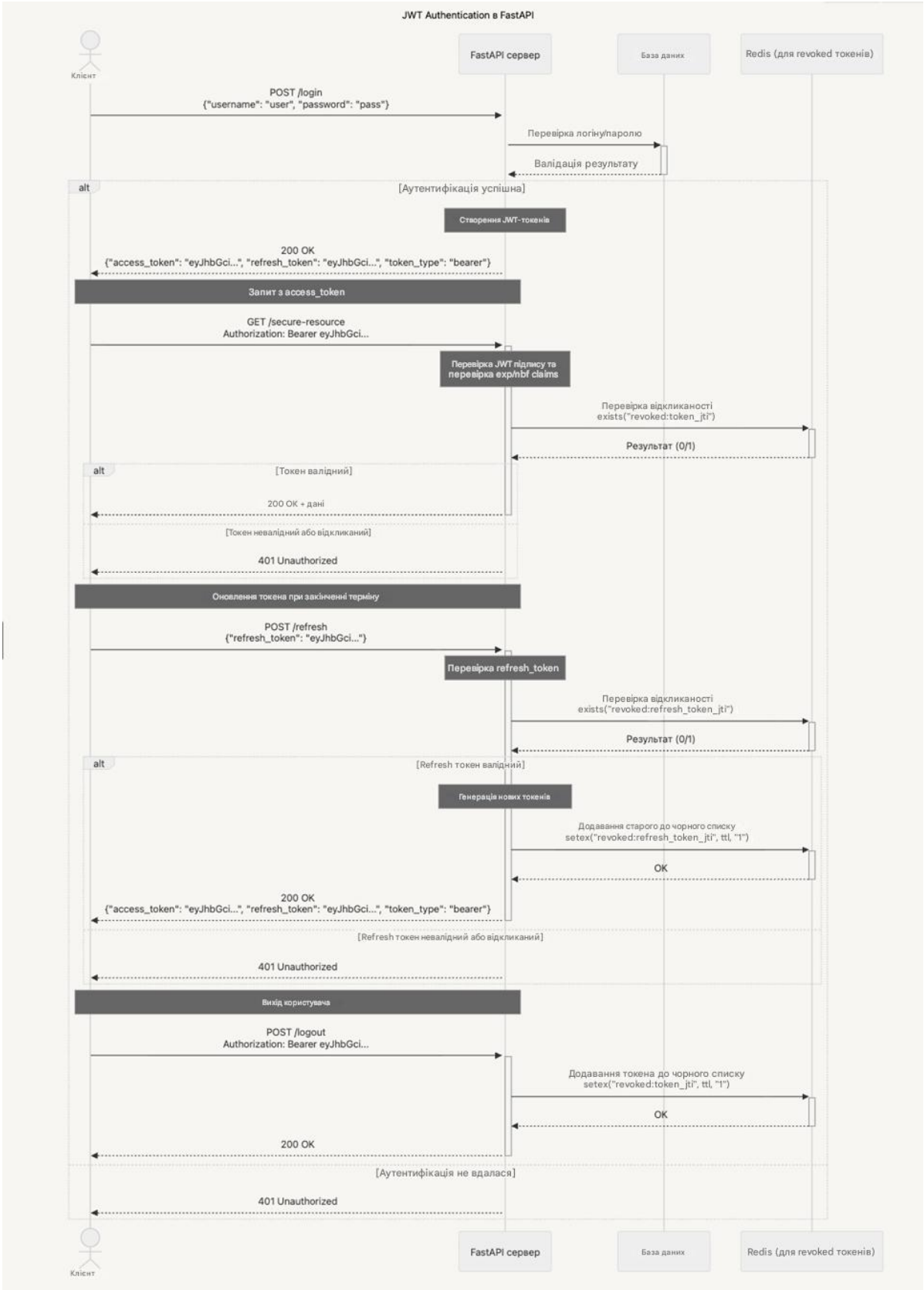


Рисунок 3.6 – UML sequence діаграма послідовності дій

Переваги:

- Stateless - сервер не зберігає сесії, що спрощує масштабування.
- Самодостатність - вся необхідна інформація міститься в токені.
- Крос-доменна робота - легко використовувати в мікросервісній архітектурі.
- Продуктивність - не потрібно звертатися до БД для перевірки авторизації.
- Гнучкість - можна включати різні claims (ролі, права тощо)
- Стандартизація - широко використовуваний формат з великою кількістю бібліотек

Розподіл відповідальності - можливість виділити авторизацію в окремий сервіс

Недоліки:

- Розмір - JWT зазвичай більший, ніж session ID (особливо з великою кількістю claims).
- Складність відкликання - немає вбудованого механізму відкликання (потрібна додаткова реалізація).
- Безпека зберігання - складно безпечно зберігати на клієнті.
- Витік інформації - payload не зашифрований, тільки закодований в Base64.
- Ускладнення при використанні refresh токенів - вимагає зберігання стану.
- Ризик XSS-атак - при неправильному зберіганні в localStorage.
- Незмінність - не можна змінити дані в токені без перевипуску.
- Токени, термін дії яких закінчився - до закінчення терміну клієнт продовжує використовувати неактуальний токен.

Таблиця 3.2 – Варіанти зберігання токенів на клієнтському пристрої

Сховище	Access Token	Refresh Token	Коментарі
HttpOnly Cookie	Добре	Найкращий варіант	Захист від XSS, вразливий до CSRF (потрібен додатковий захист)
localStorage	Небезпечно	Дуже небезпечно	Вразливий до XSS-атак
sessionStorage	Відносно безпечно	Небезпечно	Існує тільки під час сесії браузера
Memory (JS змінна)	Добре	Не рекомендується	Зникає при оновленні сторінки
IndexedDB	Залежить від реалізації	Небезпечно	Вимагає шифрування

Рекомендований підхід:

1) Access token: HttpOnly cookie або in-memory storage.
2) Refresh token: Тільки HttpOnly, Secure, SameSite=strict cookie.

Додаткові заходи безпеки:

- Anti-CSRF токени;
- Генеруйте унікальний токен для кожної сесії;

- Перевіряйте його при запитах, що впливають на стан;
- Fingerprinting пристрою;
- Прив'язуйте refresh токен до характеристик пристрою;
- Перевіряйте відповідність при оновленні токена.

SSO (Single-sign on)

SSO (Single Sign-On) – це механізм, за допомогою якого користувач входить в систему один раз, щоб отримати доступ до всіх пов'язаних систем без повторної аутентифікації.

Сам SSO – це поведінка, а не технологія, при цьому реалізується він через Keycloak, Okta, Azure AD і т. д.

Складові SSO:

- User (користувач) – хоче увійти, знає свій логін і пароль;
- Service Provider (SP) – сайт, на який він заходить (наприклад, GitLab);
- Identity Provider (IdP) – сервіс, який підтверджує особу (наприклад, Keycloak, Google, Okta).

Як це виглядає для користувача:

1. Заходиш на app1.company.com → логінишся;
2. Переходиш на app2.company.com → вже залогінений;
3. Переходиш в dashboard.partner.com → теж залогінений → без введення пароля.

Принцип роботи даного механізму:

1. Користувач заходить на Service A;
2. Його перенаправляють на IdP;
3. Він логіниться один раз;
4. IdP повертає токен або сесію;
5. Користувач отримує доступ до Service A;
6. При переході на Service B, той знову звертається до IdP → вже є сесія → вхід без пароля.

SSO працює через наступні протоколи:

1. SAML – старий, XML, часто в enterprise;
2. OpenID Connect (OIDC) – надбудова над OAuth2, сучасний стандарт;
3. Іноді – Kerberos (у Windows-доменних мережах).

Наприклад, припустимо, у тебе є три додатки:

- billing.domain.com;
- docs.domain.com;
- admin.domain.com.

З SSO:

Всі вони довіряють одному IdP (наприклад, Keycloak), при цьому користувач логіниться один раз – і отримує доступ до всіх трьох.

Переваги SSO:

- Зручно для користувачів (1 логін → багато доступів);
- Централізований контроль безпеки;
- Ідеально для корпоративного середовища, мікросервісів;
- Підтримує MFA, LDAP, OAuth2, Google Login та ін.

Недоліки SSO:

- Одна точка відмови (якщо IdP не працює – ніхто не увійде);
- Потрібно вміти правильно конфігурувати;
- Вимагає розуміння протоколів (OIDC/SAML).

3.5. OAuth 2.0

OAuth 2.0 – це протокол авторизації, який дозволяє додатку отримати доступ до даних користувача на іншому сервісі без передачі логіна та пароля.

OAuth 2.0 не являється аутентифікацією, а є доступ до ресурсів за довіреністю.

«OAuth2 – це протокол, який дозволяє додаткам діяти від імені користувача, не знаючи його пароля. Все через токени, все під контролем.»

Наприклад:

1. Ти логуєшся на сайті через Google:
2. Цей сайт не отримує твій пароль.
3. Google показує: «Цей додаток хоче отримати доступ до твоєї пошти».
4. Ти натискаєш «Дозволити».
5. Додаток отримує токен – і може читати твої листи (або те, що там запросили).

У даному процесі беруть участь:

- Resource Owner – користувач (ти);
- Client – додаток, який хоче отримати доступ (наприклад, Zoom, Notion);
- Authorization Server – хто видає токен (наприклад, Google);
- Resource Server – API, до якого клієнт хоче отримати доступ (наприклад, Gmail API).

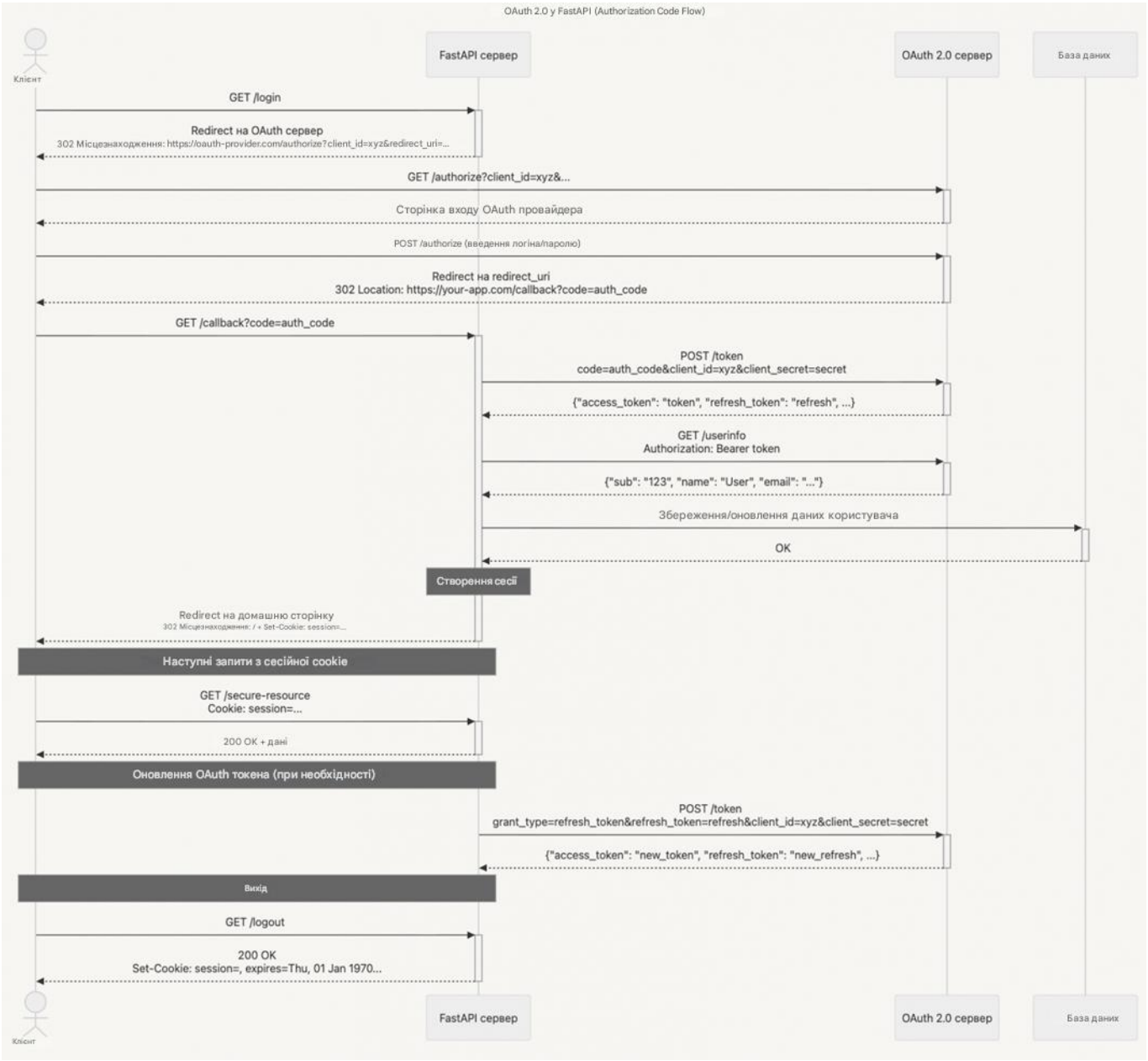


Рисунок 3.7 – UML sequence діаграма послідовності дія для OAuth 2.0

Основний потік: Authorization Code Flow

Етапи:

1. Клієнт (frontend) перенаправляє користувача на Google:
`<https://accounts.google.com/o/oauth2/auth?client\_id=...&redirect\_uri=>...`
2. Користувач входить у систему та дозволяє доступ
3. Google перенаправляє назад з code
`<https://your-app.com/callback?code=abc123>`
4. Сервер (backend) обмінює code на access token (і опціонально refresh token)
5. З цього моменту клієнт може використовувати JWT-токен:
`Authorization: Bearer <token>`

Access і Refresh Token

За аналогією з JWT-токеном, refresh-токен оновлює access-токен після закінчення терміну його дії

- Access Token – тимчасовий (часто 1 година), використовується для запитів до API
- Refresh Token – довготривалий, використовується для отримання нового access token без логіна.

OAuth ≠ Login

OAuth не займається питанням «хто ти», він вирішує питання «чи можна тобі це».

При цьому, якщо додати OIDC (OpenID Connect) – з'являється ID Token, який можна використовувати для OAuth2 як логін (SSO).

Плюси OAuth2

- Не вимагає передавати логіни/паролі іншим сервісам;
- Можна обмежити доступ за scope (read, write, profile);
- Працює з більшістю великих API;
- Основний протокол для «Увійти через Google/Facebook/GitHub».

Мінуси

- Складна конфігурація (client_id, redirect_uri, state);
- Є багато варіантів (flows): authorization code, client credentials, etc.
- Якщо зробити неправильно – легко відкрити вразливість.

3.6. Keycloak (SSO / OpenID Connect)

Keycloak – це готова система управління користувачами та авторизацією, яка реалізує протоколи OIDC (OpenID Connect) та OAuth2.0. Вона надає SSO, MFA, вхід через сторонні сервіси та централізований контроль доступу (Рисунок 3.8).

Keycloak – це все в одному: логін, токени, ролі, користувачі, OAuth2, OIDC, MFA і SSO.

Принцип роботи:

1. Користувач натискає «Увійти» в одному з додатків;
2. Браузер перенаправляє на Keycloak;
3. Keycloak логінить користувача (через форму, LDAP, Google тощо);
4. Повертає користувача з code назад у додаток;
5. Додаток обмінює code на access token, ID token, refresh token;
6. Користувач отримує доступ до сервісу;
7. В іншому додатку користувач вже авторизований (SSO).

Технічно:

- Keycloak – це Identity Provider (IdP);
- Працює через OIDC (додає аутентифікацію до OAuth2).

Видає токени:

- Access token (доступ до API);
- ID token (інформація про користувача);

– Refresh token (оновлення токенів).

Підтримує:

– JWT (RS256 за замовчуванням);
– Google/GitHub/LDAP як сторонні IdP;
– MFA (2FA), політики доступу, ролі, групи.

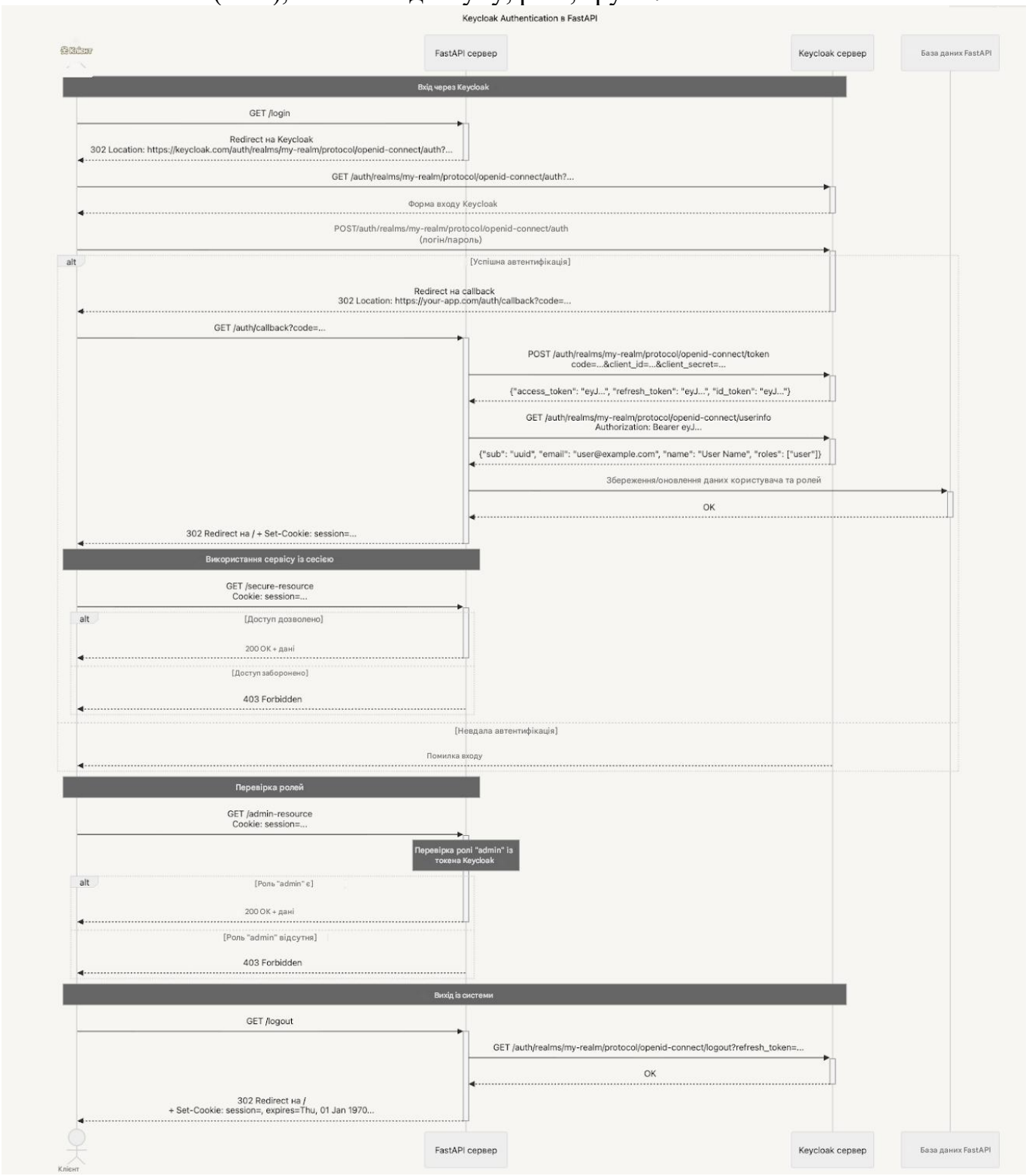


Рисунок 3.8 – UML sequence діаграма послідовності дія для keycloak

Переваги keycloak:

– Централізована аутентифікація

- Повноцінний SSO. Входить в одне – авторизований у всьому.
- Підтримка стандартів: OIDC, OAuth2, SAML.
- Гнучкість: UI логін, MFA, ролі, політики, custom flows.
- Масштабоване і стабільне: чудово підходить для production / enterprise.

Недоліки keycloak:

- Потрібно розібратися з реалами, клієнтами, маппінгами.
- Вимагає сервера з Keycloak або Docker.
- Єдина точка відмови (IdP): якщо Keycloak вийде з ладу – ніхто не зможе увійти.
- Складно для невеликих проєктів.

Область використання:

1. Мікросервісна архітектура;
2. Корпоративні платформи;
3. Додатки з безліччю клієнтів і ролей;
4. SSO через Google, GitHub, LDAP.

Не підходить для:

1. Найпростіші проекти без складних користувачів;
2. MVP з одним входом;
3. Там, де немає інфраструктури.

Приклад на FastAPI:

1. Додаток реєструється як «Client» в Keycloak.
2. Користувач входить в систему → повертається код.
3. FastAPI обмінює код на токени через HTTP-запит:

```
import requests

def exchange_code_for_token(code: str):
    res =
requests.post("<https://keycloak/auth/realms/myrealm/protocol/ope
nid-connect/token>", data={
        "client_id": "myapp",
        "client_secret": "secret",
        "grant_type": "authorization_code",
        "code": code,
        "redirect_uri": "<https://myapp/callback>"
    })
    return res.json()
```

Висновок за розділом:

Існують різні за способом та складністю способи авторизації у мережі. Для того, щоб було зручніше їх порівнювати, вони будуть подані у вигляді таблиці (Табл. 3.3).

Таблиця 3.3 – Порівняння різних видів авторизації

Критерії	Basic Auth	Session Auth	JWT Auth	OAuth 2.0	Keycloak (OIDC/SSO)
Тип	Проста передача паролів	За допомогою сесії (stateful)	Token-based (stateless)	Протокол авторизації	IdP-платформа (з реалізацією OAuth2/OIDC)
Стан зберігання даних	Stateless (кожен запит)	На серверы (пам'ять/БД)	Stateless (client)	Stateless (client)	Stateless (client +session IdP)
Місце зберігання даних	Authorization	В cookie (Sessionid)	В JWT-токене (payload)	В токенах (access/refresh)	В токенах, керуючих IdP
Механізм зберігання	Base64: `user:pass`	`Set-Cookie: sessionid`	`Aothorization: Bearer<JWT>`	`Aothorization: Bearer<token>`	`Aothorization: Bearer<token>`
Можливість виходу (logout)	Немає	Присутня	Частково (blacklist)	Присутня (revoke)	Присутня (endpoint/IdP logout)
Складність реалізації	Дуже легка	Легка	Середня	Складна (flows, scopes)	Складна (Keycloak, settings, UI)
Підходить для API	Ні	Ні	Так	Так	Так (enterprise)
Підтримка SSO	Немає	Немає	Часткова (при написанні IdP)	Присутня (OIDC)	Повноцінна SSO
Підтримка ролей/scopes	Відсутня	На сервері	В токені (claims)	В scopes	Через UI, токени, RBAC
Безпека	Слабка, при відсутності HTTPS	Добра, лише при HttpOnly	Залежить від зберігання токену	Висока при правильному налаштуванні	Висока, включає MFA та політики
Масштабованість	Погана	Треба шардувати сесії	Добра	Добра	Добра, присутній централізований контроль

Продовження таблиці 3.3

Підходить для мікросервісів	Ні	Ні	Підходить	Підходить	Ідеальний для систем enterprise
Де використовується	Тимчасові внутрішні API	Класичні форми/сайти	Сучасні SPA/API	Вхід через Google/доступ до API	Корпоративні, SSO, продакшн-платформи

ВИСНОВОК

У першому розділі було розглянуто основи кібербезпеки. Було описано про базові особливості з захисту інформмації, коротко розглянуто види захисту інформації у сучасному світі, розглянуто особливостіхмарних обчислень, їх види, переваги та недоліки, описані основні загрози та методи борьби з ними.

Даний розділ дозволяє поглибити свої знання про сучасні підходи до забезпечення кібербезпеки та особливості захисту інформаційних систем, включно з хмарними технологіями. Захист інформації є фундаментом безпечного функціонування будь-якої організації, адже дані – це цінний ресурс, який потребує конфіденційності, цілісності та доступності. Розуміння типів кіберзагроз, як наприклад шкідливе ПЗ, соціальна інженерія, фішинг, атаки на мережеву інфраструктуру та інші внутрішні загрози, дозволяє правильно оцінювати ризики та формувати ефективну політику безпеки.

Класи продуктів у сфері кібербезпеки, включно з антивірусами, міжмережевими екранами, системами виявлення та запобігання вторгнень, SIEM-платформами та засобами керування ідентичностями, створюють основу для технічного захисту. Сучасні технології, такі як Zero Trust, багатофакторна автентифікація, поведінкова аналітика та машинне навчання, значно підсилюють можливості автоматизації та раннього виявлення інцидентів.

Особливу увагу заслуговують загрози хмарних обчислень, визначені Cloud Security Alliance (CSA): неправильне налаштування сервісів, витоки даних, уразливості API, зловживання обліковими даними та недостатній контроль доступу. Разом із вразливими місцями хмарних систем вони формують специфічний набір ризиків, які потребують окремої стратегії захисту. У цьому контексті важливою є система класифікації рівнів безпеки інформаційних систем та використання ефективних алгоритмів шифрування, що забезпечують надійний захист даних у русі та під час зберігання.

Завершальною складовою є структура системи захисту хмарної бази даних, яка включає контроль доступу, шифрування, журналювання, моніторинг та регулярні оновлення. Усі ці елементи разом формують комплексний підхід до безпеки, що дозволяє ефективно протидіяти сучасним кіберзагрозам.

Другий розділ присвячений загрозам IT-світу, демонструє, наскільки стрімко розширюється сучасний кіберпростір та як зростає кількість ризиків, пов’язаних із цифровими технологіями. Кіберпростір став невід’ємною частиною глобальної інфраструктури, де взаємодіють мільярди пристроїв, користувачів і сервісів. Така масштабність створює не лише можливості, а й численні вразливості, які використовують кіберзлочинці, терористичні групи та навіть державні актори.

Інформаційна безпека виступає ключовим елементом захисту сучасного суспільства, забезпечуючи конфіденційність, цілісність і доступність даних. Розглянуті в розділі явища, такі як кібертероризм та національно-державні загрози,

підкреслюють, що кіберпростір став новим театром геополітичного протистояння. Держави активно використовують цифрові інструменти для шпигунства, саботажу та впливу на внутрішні процеси інших країн.

Особливо важливим є спостережуване стирання меж між діяльністю державних кіберугруповань та організованими кіберзлочинцями. Спільні інтереси, кооперація або взаємовигідне використання однакових методів роблять ці загрози складнішими для виявлення та протидії. Одним із найнебезпечніших проявів такого впливу є втручання у вибори, що підриває довіру до демократичних процесів та стабільність держав.

На практичному рівні сучасний користувач стикається з такими поширеними кіберзагрозами, як програми-вимагачі, кібершахрайство, фішинг та видавання себе за іншу особу. Програми-вимагачі здатні паралізувати цілі організації, шифруючи дані та вимагаючи викуп. Фішингові атаки та методи соціальної інженерії активно застосовуються для отримання доступу до конфіденційної інформації, фінансових даних і облікових записів користувачів. Особливо серйозну загрозу становить видавання себе за іншу особу, що набуває небезпечного масштабу в соціальних мережах та онлайн-платформах.

Узагальнюючи, розділ підкреслює, що кіберзагрози стають дедалі різноманітнішими й масштабнішими, а ефективна протидія їм вимагає поєднання державних заходів, технологічного розвитку та підвищення рівня цифрової грамотності користувачів.

У третьому розділі, було розглянуто практичні методи аутентифікації та авторизації у сучасному світі. Для кожного методу було розглянуто особливості практичної реалізації, складність їх побудови, а також переваги та недоліки, у кінці розділу було побудована таблиця з повним порівнянням розглянутих методів за різними критеріями.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Основи кібербезпеки. URL: https://moz.gov.ua/uk/osnovi-kiberbezpeki-2 (дата звернення: 30.11.2025).
2. Методи захисту інформації. URL: https://studfile.net/preview/11391767/ (дата звернення: 30.11.2025).
3. ПЕРШИЙ КРОК У НАУКУ. URL: https://essuir.sumdu.edu.ua/bitstream/123456789/72313/1/Pershyi_krok_2019.pdf (дата звернення: 30.11.2025).
4. Кібербезпека: актуальні загрози та методи захисту. URL: https://lemon.school/blog/kiberbezpeka-aktualni-zagrozy-ta-metody-zahystu (дата звернення: 30.11.2025).
5. Інформаційні технології прогнозування та моделювання кібербезпеки. URL:https://sites.google.com/view/blog-ua/інформаційні-технології-прогнозування-та-моделювання-кібербезпеки (дата звернення: 30.11.2025).
6. Зачист інформації в інформаційно-комунікаційних системах. URL: https://conf.ldubgd.edu.ua/documents/Zbirnyk_Zakhystinformatsii.pdf (дата звернення: 30.11.2025).
7. Підхід до побудови системи безпеки хмарних баз даних. URL: https://ela.kpi.ua/bitstream/123456789/31615/1/Tsap_magistr.pdf (дата звернення: 30.11.2025).
8. Цикл обробки персональних даних. URL: https://virtuapc.ru/network-security/cikl-obrabotki-personalnyh-dannyh-programmnaya-i-apparatnaya-zashchita-informacii/ (дата звернення: 10.11.2025).
9. Криптографічні засоби захисту інформації. URL: https://studfile.net/preview/5462915/page:18/ (дата звернення: 30.11.2025).
10. Dis stabetska PDF. URL: https://www.slideshare.net/slideshow/dis-stabetska/131241654 (дата звернення: 30.11.2025).
11. День науки – 2019. URL: https://kntu.kr.ua/file/content/8162/zbirnyk-tez-dopovidei-zdobuvachiv-vyshchoi-osvity-liv-naukovo-tekhnichnoi-online-konferentsii-nauka-v-tsntu-osnovni-dosiahnennia-ta-perspektyvy-rozvytku-za-pidsumkamy-provedennia-dnia-nauky-2020-.pdf (дата звернення: 30.11.2025).
12. Криптографічний захист інформації. URL: https://crashbox.ru/tools-to-help/kriptograficheskaya-zashchita-informacii-obzor-zakonodatelstva/ (дата звернення: 30.11.2025).
13. Наука виробництву. URL: https://journals.dut.edu.ua/index.php/dataprotect/article/download/2639/2538/ (дата звернення: 30.11.2025).
14. 2024-ITSec_збірник_v_1. URL: https://sci.ldubgd.edu.ua/bitstream/123456789/14350/1/2024-ITSec_%D0%B7%D0%B1%D1%96%D1%80%D0%BD%D0%B8%D0%BA_v_1.pdf (дата звернення: 30.11.2025).
15. Кафедра кібербезпеки та інформаційних технологій. URL: https://kn-it.info/wp-content/uploads/2020/10/Konspekt_MTKYS-41.pdf (дата звернення: 30.11.2025).

16. Інформаційне суспільств: технологічні, економічні та технічні аспекти становлення. URL: http://www.konferenciaonline.org.ua/data/downloads/file_1670705810.pdf (дата звернення: 30.11.2025).
17. Інформаційна безпека та інформаційні технології. URL: http://drforum.science/wp-content/uploads/2021/12/proceedings_ibit-2021.pdf (дата звернення: 30.11.2025).
18. Інформаційна та кібербезпека. URL: https://duikt.edu.ua/uploads/p_303_79299367.pdf?file=p_303_79299367.pdf (дата звернення: 30.11.2025).
19. Conference proceeding 09.08.2023. URL: http://www.wayscience.com/wp-content/uploads/2023/06/Conference-Proceedings-June-8-9-2023.pdf (дата звернення: 30.11.2025).
20. Вісник економіки 2010. URL : http://econom.lnu.edu.ua/files/downloads/Visnyk_Econom/043_2010/Visnyk_Econom_043_2010.pdf (дата звернення: 30.11.2025).
21. Звіт про цифровий захист Майкрасофт 2024. URL: https://www.microsoft.com/uk-ua/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024 (дата звернення: 30.11.2025).
22. Новини України. URL: https://biz.liga.net/ua/all/all/novosti/rosiiski-khakery-u-chervni-atakuvaly-50-ukrainskykh-viiskovykh-prystroiv-microsoft (дата звернення: 30.11.2025).
23. Детермінанти та імперативи розвитку міжнародних економічних відносин у контексті глобальної нестабільності. URL: http://confcontact.com/eim2021/EIM_2021_tom7.pdf (дата звернення: 30.11.2025).
24. Безпека інформаційно-комунікаційних систем. URL: https://elibrary.kubg.edu.ua/id/eprint/51358/1/Kostiuk_Y_Skladannyi_P_Bebeshko_B_Khorolska_K_Rzaieva_S_Vorokhob_M_BIKS_2025_FITM.pdf (дата звернення: 30.11.2025).
25. Прогноз кіберзагроз 2024. URL: https://www.h-x.technology/ua/blog-ua/cyber-threats-forecast-2024-ua (дата звернення: 30.11.2025).
26. Ідентифікація, аутентифікація, авторизація. URL: https://www.kaspersky.ru/blog/identification-authentication-authorization-difference/29123/ (дата звернення: 30.11.2025).
27. Блог по веб-розробці. URL: https://zabb.ru/blog-po-web-razrabotke-4/primeryi-koda-dlya-autentifikatsii-101623.html (дата звернення: 30.11.2025).