Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Факультет інформаційних технологій
(факультет)

Кафедра системного аналізу та управління
(повна назва)

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня бакалавра

Студента Степанова Івана Ігоровича

академічної групи 124-21ск-1

спеціальності 124 Системний аналіз

на тему: «Аналіз сучасних підходів до забезпечення безпеки веб-інфраструктури»

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**Інституційною**	
кваліфікаційної роботи	*к.ф.-м.н., проф. Ус С.А*			
розділів:	*2*			
Інформаційно-аналітичний	*к.ф.-м.н., проф. Ус С.А*			
Спеціальний розділ	*к.ф.-м.н., проф. Ус С.А*			
Рецензент				
Нормоконтролер	*к.ф.-м.н., доц. Хом'як Т.В.*			

Дніпро
2024

ЗАТВЕРДЖЕНО:
завідувач кафедри
Системного аналізу та управління
(повна назва)

_____ *к.т.н., доц. Желдак Т.А.*
(підпис) (прізвище,ініціали)

«____» _____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня *бакалавра*

студенту *Степанову І. І.* **академічної групи** *124- 21ск-1*
спеціальності: *124 Системний аналіз*
на тему «Аналіз сучасних підходів до забезпечення безпеки веб-інфраструктури»
затверджену наказом ректора НТУ «Дніпровська політехніка»
від *29.04.2024 р. №375-с*

Розділ	Зміст	Терміни виконання
1. Інформаційно-аналітичний розділ	*Проаналізуйте структуру об'єкта дослідження. Визначте предмет дослідження та проблему, що вирішується. Обґрунтувати методику виконання поставлених завдань*	06.01.2024 – 01.03.2024
2.Спеціальний розділ	*Розв'язати поставлені задачі: дослідити сучасні підходи до забезпечення безпеки веб-інфраструктур, включаючи криптографічні методи, блокчейн та штучний інтелект. Проаналізувати вплив інтеграції захисних механізмів на загальну безпеку веб-інфраструктур.*	01.03.2024 – 30.05.2024

Завдання видано _____ *проф. Ус С.А*
(підпис) (прізвище, ініціали)

Дата видачі: *06.01.2024 р.*

Дата подання до екзаменаційної комісії: _____

Прийнято до виконання _____ Степанов І. І.
(підпис студента) (прізвище, ініціали)

ЗМІСТ

ВСТУП

На сучасному етапі розвитку технологій, питання кібербезпеки стає все більш актуальним. В контексті стрімкого зростання числа веб-інфраструктур та їхнього значення у глобальній економіці, забезпечення їх безпеки виходить на передній план. Надійність та безпека веб-інфраструктур мають важливе значення для бізнесу, урядових структур, фінансових установ та звичайних користувачів.

Забезпечення безпеки веб-інфраструктур вимагає розуміння сучасних загроз, вміння передбачати потенційні кібератаки та ефективно реагувати на них.

Наукова актуальність обумовлена потребою систематизації існуючих знань та підходів у сфері кібербезпеки веб-інфраструктур. Особливу увагу приділено аналізу методів захисту, що дозволяють не тільки виявляти та нейтралізувати загрози, але й прогнозувати ризики, що можуть вплинути на стабільність та доступність веб-сервісів.

Основною метою дослідження є аналіз та оцінка ефективності сучасних підходів до забезпечення безпеки веб-інфраструктур, що включає в себе визначення найбільш дієвих стратегій захисту. Для досягнення цієї мети необхідно провести аналіз методів криптографічного захисту, технологій блокчейну, а також інших інноваційних підходів.

Об’єктом дослідження обрано процес забезпечення захисту інформації у веб-інфраструктурі, яка включає сервери, мережеве обладнання, програмне забезпечення та дані користувачів. Предметом є методи та технології захисту цих складових.

У рамках дослідження використовано ряд методів, включаючи теоретичний аналіз, моделювання, порівняльний аналіз та методи прийняття рішень в умовах невизначенності.

Таким чином, дана дипломна робота спрямована на аналіз актуальних проблем кібербезпеки, зокрема, захисту веб-інфраструктур.

РОЗДІЛ 1
Аналітичний

1.1 Актуальність, постановка проблеми

У світі, де веб-інфраструктура стає невід'ємною частиною бізнесу, освіти, медицини та інших сфер, зростає необхідність в забезпеченні безпеки цих систем. Сучасний світ переживає надзвичайно високі технологічні та цифрові зміни, що призводить до зростання ролі веб-інфраструктури. У зв'язку з цим, загрози кібербезпеці також значно зросли. Кібератаки стали не лише частими, але й досить різноманітними в своїх цілях та методах.

Через зростаючу взаємопов'язаність та залежність бізнесу від цифрових технологій, кіберзлочинність швидко набирає обертів. За інформацією поданою на сайті forbres [1] у 2023 році відбулося помітне зростання кількості кібератак, у результаті яких постраждало понад 343 мільйони людей. У період з 2021 по 2023 рік кількість витоків даних зросла на 72%, перевищивши попередній рекорд.

Люди в усьому світі використовують електронну пошту для особистого та професійного спілкування, що робить електронну пошту мішенню для кіберзлочинців і найпоширенішим переносником шкідливих програм. У 2023 році 35% шкідливих програм було доставлено електронною поштою, а понад 94% організацій повідомили про інциденти безпеки електронної пошти.

Оскільки ландшафт загроз постійно змінюється, важливо розуміти, як розвиваються кібератаки, які засоби контролю безпеки та види навчання працюють.

У 2023 році було виявлено 30 мільйонів нових зразків шкідливого програмного забезпечення. Це фактично на дві третини менше, ніж роком раніше.

У 2019 році 93,6% виявлених шкідливих програм були поліморфними, тобто здатними постійно змінювати свій код, щоб уникнути виявлення. Однак ми починаємо спостерігати впровадження інструментів на основі машинного навчання, які можуть виявляти спільні риси між будь-яким додатком і відомими сімействами шкідливих програм.

45% бізнес-комп'ютерів і 53% персональних комп'ютерів, які заразилися одного разу, були повторно інфіковані протягом того ж року.

Дослідження Університету Меріленду 2007 року показало, що раніше зловмисники атакували комп'ютери та мережі зі швидкістю одна атака кожні 39 секунд. У звіті Центру скарг на інтернет-злочинність за 2022 рік зазначено, що того року було 800 944 повідомлення. Це означає одну успішну атаку кожні 0,65 секунди. Примітно, що це не враховує спроби атак або ті, про які не було повідомлено.

84,7% опитаних організацій зазнали успішної кібератаки. Це менше, ніж 85,3% у 2022 році та 86,2% у 2021 році.

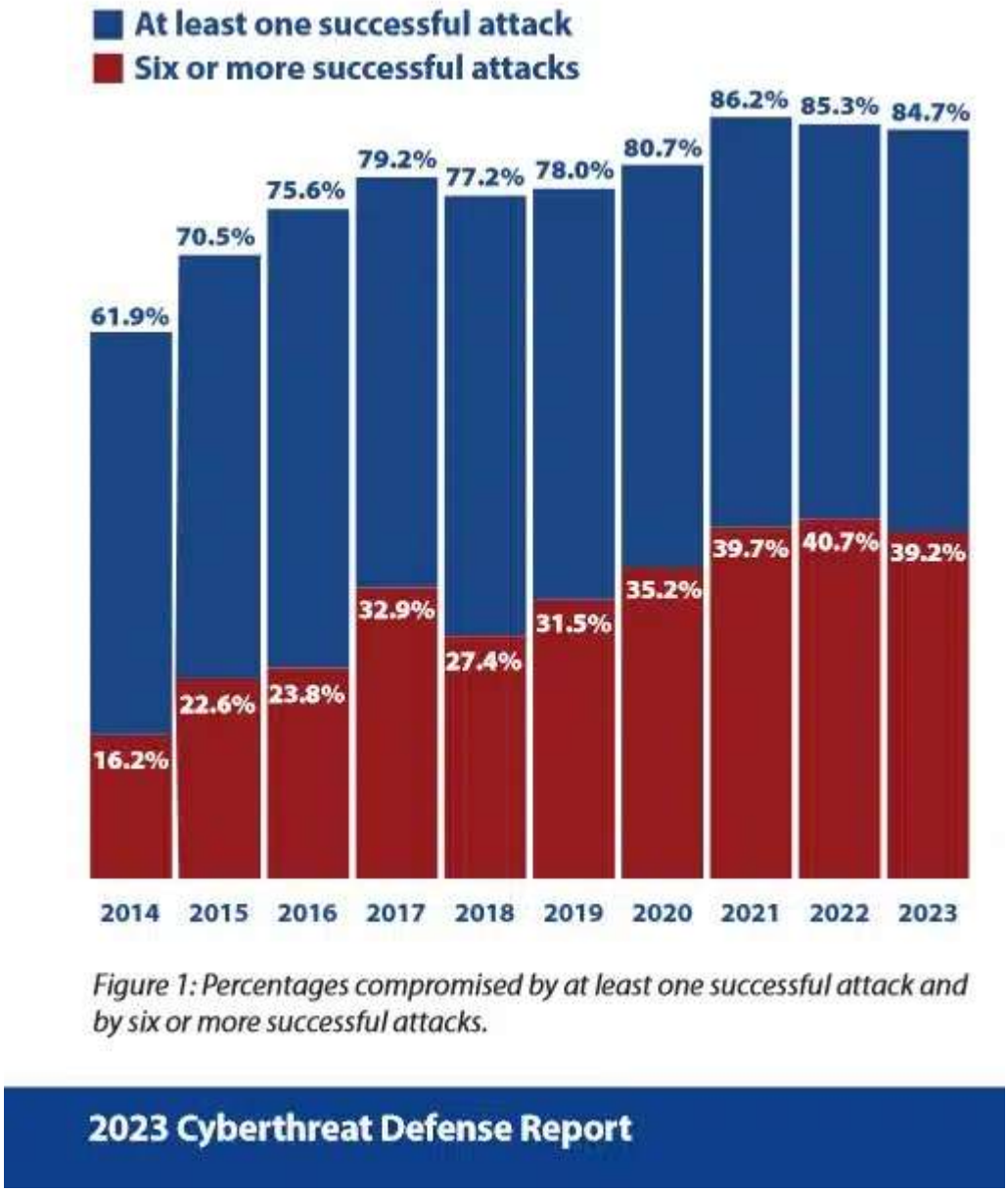

Рис. 1.1 Статистика кіберзлочинності за 2014-2023 роки (джерело [2])

Наслідки кібератак є далекосяжними та дорого коштують. Порушення даних коштує в середньому 4,45 мільйона доларів. У 2022 році скомпрометовані ділові електронні листи завдали збитків на 2,7 мільярда доларів. Ці тривожні цифри підкреслюють небезпеку кібервразливості та підкреслюють потребу в кваліфікованих спеціалістах із кібербезпеки.Зростання кількості кібератак та їх вплив на фінансові ресурси є серйозною проблемою, що вимагає негайних заходів для забезпечення безпеки веб-інфраструктури. Відмова від дії може призвести до подальшого

загострення ситуації та збільшення ризиків для користувачів та організацій. Тому актуальність дослідження питань кібербезпеки веб-інфраструктури стає все більш очевидною.

За останні роки рівень зараження програмами-вимагачами стрімко зріс, що значною мірою пов'язано зі зростанням важливості платформ для онлайн-навчання та дистанційної роботи.

За оцінками, тільки в першій половині 2023 року атаки програм-вимагачів у США коштували 449 мільйонів доларів США.

493,3 мільйона атак з використанням програм-вимагачів сталося у 2022 році, що дещо менше, ніж у попередньому році.

У лютому 2022 року Агентство кібербезпеки та безпеки інфраструктури повідомило, що інциденти з використанням програм-вимагачів сталися в 14 з 16 критично важливих секторів інфраструктури США.

Emsisoft повідомляє, що у 2023 році від програм-вимагачів постраждали 141 лікарня, 108 шкільних округів та 95 державних установ.

Згідно зі звітом за 2023 рік, 93% атак вірусів-здирників були спрямовані саме на сховища резервних копій, і 75% цих спроб були успішними.

Щогодини у світі відбувається понад 37 700 атак зловмисників. Це приблизно 578 атак з вимогами щохвилини.

У 2023 році штат Мен зазнав витоку даних, що призвело до втрати понад мільйона даних громадян.

У 2022 році американські навчальні заклади втратили приблизно $9,45 млрд через простої внаслідок атак зловмисників.

У 2023 році 66 окремих атак вимагачів коштували медичним установам США приблизно 14,7 мільярда доларів.

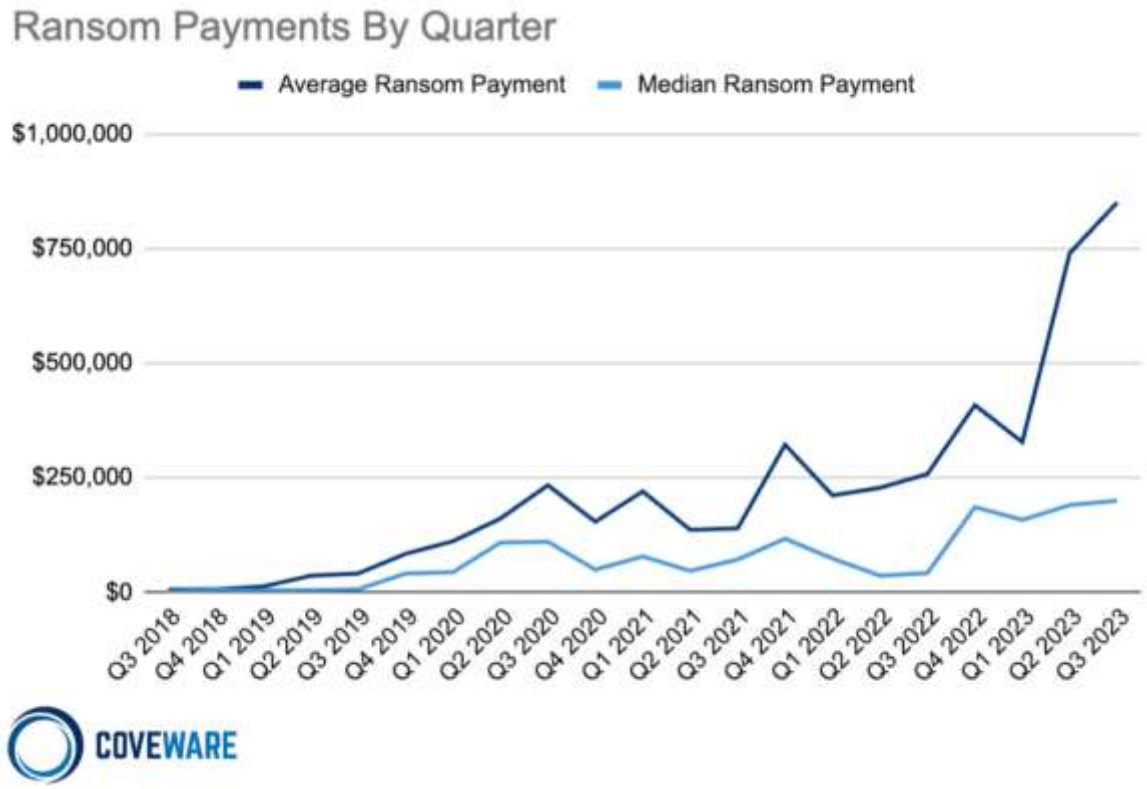

Рис. 1.2 Виплати викупів по кварталах за 2018-2023 роки (джерело [3])

Необхідно провести аналіз сучасних підходів до забезпечення безпеки веб-інфраструктури та розглянути стратегії для запобігання кібератак. Такий підхід є важливим для захисту інтересів користувачів та збереження фінансових ресурсів. Крім того, враховуючи стійкий розвиток кіберзлочинності та зростання впливу технологій, необхідно постійно оновлювати та покращувати заходи забезпечення безпеки. Тільки таким чином можна забезпечити ефективний захист веб-інфраструктури в умовах сучасного цифрового середовища.

1.2 **Опис об’єкта дослідження**

Веб-інфраструктура представляє собою комплексне середовище, що складається з множини технологічних елементів, таких як серверне обладнання, мережеві протоколи, системи управління базами даних, веб-

сервери, програмне забезпечення для розробки та взаємодії з користувачами через інтернет. Ці компоненти взаємодіють між собою для забезпечення доступності, надійності та безпеки веб-застосунків та сервісів.

Архітектура веб-інфраструктур постійно еволюціонує, відповідаючи на зростаючі вимоги до масштабування, продуктивності та безпеки. Інноваційні технології, такі як хмарні обчислення, контейнеризація та автоматизоване розгортання, дозволяють створювати все більш гнучкі та ефективні системи.

Особливу увагу у сфері веб-інфраструктур заслуговує питання безпеки. Сучасні загрози для веб-інфраструктур є дуже різноманітними та включають в себе атаки на вразливості програмного забезпечення, фішинг, DDoS-атаки, викрадення даних, шкідливе програмне забезпечення та багато іншого. Відповідно, об’єкт дослідження охоплює не тільки технічні аспекти архітектури веб-інфраструктур, але й стратегії та практики забезпечення їх безпеки.

Важливим елементом дослідження є аналіз сучасних інструментів та методологій для забезпечення безпеки веб-інфраструктур, включаючи шифрування даних, системи виявлення та запобігання вторгненням, регулярні оновлення та патчі безпеки, а також методи автентифікації та авторизації користувачів.

Для забезпечення всебічного підходу до безпеки, дослідження також повинне враховувати людський фактор, включаючи навчання користувачів основам кібергігієни та формування культури безпеки в організаціях. Це дозволяє не тільки захистити технічну частину інфраструктури, але й мінімізувати ризики, пов’язані з людськими помилками та ненавмисними діями, які можуть призвести до витоку чи компрометації даних.

1.3 Сучасні технології та стандарти безпеки веб-інфраструктур

Шифрування даних. Одним з основних способів захисту інформації є шифрування. Для захисту даних, що передаються через інтернет, широко

використовуються протоколи SSL (Secure Sockets Layer) і його наступник TLS (Transport Layer Security). Вони забезпечують шифрування даних між веб-браузером користувача і веб-сервером, запобігаючи їх перехопленню або модифікації третіми особами.

Системи виявлення та запобігання вторгненням (IDS/IPS). Системи виявлення вторгнення (IDS) і системи запобігання вторгненням (IPS) є критично важливими для виявлення спроб несанкціонованого доступу або атак на веб-інфраструктури. IDS аналізує трафік у мережі на предмет відхилень від норми, тоді як IPS активно блокує спроби атак.

Вогненні стіни (Firewalls). Вогненні стіни слугують першою лінією оборони веб-інфраструктур, контролюючи вхідний та вихідний мережевий трафік на основі встановлених правил безпеки. Вони допомагають запобігти несанкціонованому доступу до мережевих ресурсів.

Автентифікація та авторизація. Методи автентифікації, такі як багатофакторна автентифікація (MFA), вимагають підтвердження ідентичності користувача за допомогою кількох незалежних джерел, що значно знижує ризик несанкціонованого доступу. Авторизація визначає, які ресурси та дії доступні користувачу після його успішної автентифікації.

Web Application Firewall (WAF). Web Application Firewalls спеціалізуються на захисті веб-додатків шляхом фільтрації і моніторингу HTTP-трафіку між веб-додатком та Інтернетом. WAF ефективні проти XSS (cross-site scripting), SQL-ін'єкцій, фальсифікації міжсайтових запитів (CSRF) та інших веб-атак.

Стандарти безпеки в веб-інфраструктурі встановлюють вимоги та рекомендації для захисту інформації та IT-ресурсів від загроз і ризиків. Вони охоплюють аспекти безпеки даних, управління ризиками та фізичний захист, забезпечуючи надійність і конфіденційність інформаційних систем. Розглянемо наступні наступні стандарти безпеки:

ISO/IEC 27001 - це міжнародний стандарт, який визначає вимоги до системи управління інформаційною безпекою (ISMS). Він включає аспекти ризику, безпеки фізичних та IT-ресурсів.

PCI DSS (Payment Card Industry Data Security Standard) - стандарт безпеки даних для організацій, що обробляють платіжні картки. Він включає вимоги для захисту даних карткових власників.

NIST - національний інститут стандартів і технологій США розробляє рекомендації з кібербезпеки, які широко використовуються у світовій практиці для захисту інформації та інфраструктур.

SSL (Secure Sockets Layer) та TLS (Transport Layer Security) сертифікати є фундаментальними елементами забезпечення безпеки веб-інфраструктур. Вони використовуються для шифрування з'єднань між веб-сервером та браузером користувача, забезпечуючи конфіденційність та цілісність переданих даних.

Сертифікати SSL/TLS гарантують, що будь-які дані, передані між користувачем і сайтом, включаючи особисту інформацію, кредитні картки, логіни та паролі, залишаються приватними і захищеними від перехоплення третіми сторонами. Коли веб-сайт використовує SSL/TLS сертифікат, у браузері користувача відображається замок, що свідчить про захищене з'єднання, а URL починається з HTTPS замість HTTP.

Видання SSL/TLS сертифікатів здійснюється центрами сертифікації (CA), які діють як довірені треті сторони. Ці організації перевіряють ідентичність власника веб-сайту перед видачею сертифіката, що додає додатковий рівень довіри до сайту.

Існують різні типи SSL/TLS сертифікатів, включаючи:

Однодоменні сертифікати, які захищають один домен або субдомен.

Мультідоменні сертифікати, які дозволяють захистити кілька доменних імен за допомогою одного сертифіката.

Сертифікати з підтримкою необмеженої кількості субдоменів (Wildcard SSL), які захищають домен та всі його субдомени першого рівня.

Важливість SSL/TLS сертифікатів для сучасних веб-інфраструктур не може бути переоцінена. Вони не тільки підвищують рівень безпеки шляхом шифрування даних, але й впливають на довіру користувачів і можуть позитивно впливати на позиціонування сайту в пошукових системах, оскільки пошукові системи, такі як Google, вважають HTTPS одним із факторів довіри[4].

Таким чином, інтеграція SSL/TLS сертифікатів є ключовою стратегією для забезпечення безпеки веб-інфраструктур, захисту конфіденційності даних користувачів та підтримки високого рівня довіри та репутації веб-середовища.

1.4 Актуальні задачі

Сфера забезпечення безпеки веб-інфраструктур постійно розвивається, відповідаючи на нові виклики та загрози. Нижче наведено перелік актуальних задач, які стоять перед фахівцями у галузі кібербезпеки:

Захист від кібератак нового покоління. Сучасні кібератаки стають все більш складними та витонченими, що вимагає розробки нових методів захисту та вдосконалення існуючих інструментів безпеки. Зокрема, інтенсивно розвиваються методи захисту від фішингу, шкідливого програмного забезпечення, в тому числі з використанням штучного інтелекту для прогнозування та виявлення загроз[5].

Забезпечення безпеки даних. Захист конфіденційності та цілісності даних користувачів залишається критичною задачею. Це включає розробку ефективних методів шифрування, а також стратегій захисту даних на всіх етапах їх обробки та зберігання.

Управління ідентифікацією та доступом. Поліпшення систем управління ідентифікацією та доступом є важливим для забезпечення того, щоб тільки авторизовані користувачі мали доступ до ресурсів веб-інфраструктур. Розробка більш надійних систем автентифікації, включаючи

багатофакторну автентифікацію та біометричні методи, є ключовою в цьому процесі [6].

Забезпечення безперервності бізнесу та відновлення після атак. Розробка та впровадження планів відновлення після кібератак та забезпечення безперервності бізнес-процесів у випадку інцидентів безпеки є важливою задачею. Це включає резервне копіювання даних, відновлення систем після атак та запобігання втратам даних.

Комплаєнс та дотримання нормативних вимог. З підвищенням уваги до захисту даних, компанії повинні дотримуватись все більшої кількості законодавчих та регуляторних вимог, таких як GDPR в Європейському Союзі, CCPA в Каліфорнії, а також інших міжнародних та національних стандартів. Адаптація до цих вимог та забезпечення комплаєнсу є важливою задачею для бізнесів усіх розмірів [7].

Освіта та підвищення обізнаності з питань кібербезпеки. Зростаюча кількість кібератак, які використовують людський фактор, такі як соціальна інженерія та фішинг, вимагає посилення зусиль щодо освіти та підвищення обізнаності співробітників організацій. Розвиток культури кібербезпеки та навчання персоналу основам безпечної поведінки в інтернеті є ключовими для попередження багатьох загроз.

Розв'язання цих актуальних задач вимагає комплексного підходу, що включає як технологічні інновації, так і стратегічне планування на рівні організації. Важливим аспектом є також співпраця між компаніями, урядовими організаціями та освітніми інституціями для розробки та впровадження ефективних рішень у сфері кібербезпеки.

1.5 Огляд літератури

1.5.1 Актуальні задачі, моделі та методи для забезпечення безпеки веб-інфраструктур

Для огляду літератури зосередимося на актуальних задачах у галузі забезпечення безпеки веб-інфраструктур, аналізуючи моделі та методи, що використовуються для їх вирішення.

Моделі штучного інтелекту та машинного навчання для прогнозування та виявлення кібератак [8]. Сучасний розвиток технологій штучного інтелекту (ШІ) та машинного навчання (МН) відкриває нові перспективи для боротьби з кіберзагрозами. Інтеграція ШІ та МН в системи кібербезпеки дозволяє автоматизувати процеси ідентифікації та аналізу потенційних загроз, значно підвищуючи швидкість та ефективність виявлення атак. Особливу увагу заслуговують алгоритми глибокого навчання, які здатні аналізувати великі обсяги даних, виявляючи складні залежності та закономірності, які можуть вказувати на наявність кібератак.

Розвиток МН і ШІ не обмежується лише аналізом мережевого трафіку. Вони також застосовуються для аналізу поведінки користувачів, виявлення аномалій у роботі системи, що можуть свідчити про внутрішні загрози або атаки зсередини. Ці технології допомагають ідентифікувати слабкі місця в захисті інформації, аналізуючи поточні моделі поведінки та порівнюючи їх з відомими сценаріями атак.

Використання ШІ та МН в кібербезпекі також передбачає розробку алгоритмів прогнозування атак. Це означає, що системи не лише реагують на вже відбулі атаки, але й можуть прогнозувати потенційні загрози на основі аналізу поточних тенденцій та змін у мережевому середовищі. Такий підхід дозволяє заздалегідь вживати заходів для попередження можливих інцидентів, що забезпечує значно вищий рівень безпеки інформаційних систем.

Однак, інтеграція ШІ та МН у сферу кібербезпеки ставить перед дослідниками та розробниками низку викликів. По-перше, це питання етики та приватності: алгоритми аналізують великі обсяги даних, в тому числі персональні дані користувачів. По-друге, є ризик використання ШІ для розробки нових, більш складних кібератак. Тому важливо забезпечити, щоб розвиток технологій ШІ та МН в галузі кібербезпеки відбувався з урахуванням всіх потенційних ризиків та загроз.

Вивчення та розробка ШІ та МН в контексті кібербезпеки вимагає глибокого розуміння як самої технології, так і специфіки кіберзагроз. Це передбачає постійне оновлення знань та адаптацію до швидко змінювального середовища кіберзагроз, а також розробку нових методів захисту, які можуть ефективно протистояти найсучаснішим методам атак.

Блокчейн як інструмент захисту даних [9]. Блокчейн у сфері кібербезпеки відіграє ключову роль, пропонуючи новітні підходи до забезпечення надійності та цілісності даних. Ця технологія, базуючись на принципах децентралізації та криптографічного захисту, дозволяє створювати системи, де інформація зберігається у вигляді блоків, що неможливо змінити або видалити без відома всієї мережі. Така структура робить блокчейн ідеальним для захисту логів безпеки, цифрових сертифікатів та інших важливих записів.

Застосування блокчейна у кібербезпеці включає розробку надійних систем управління цифровими ідентифікаторами, захист транзакцій та забезпечення безпеки обміну даними. Завдяки криптографічному захисту та відсутності єдиної точки входу, блокчейн значно ускладнює проведення несанкціонованих дій, таких як подвійне витрачання коштів або зміна інформації.

Однак, інтеграція блокчейна у кібербезпеку пов'язана з певними викликами, включаючи питання масштабування та високі вимоги до обчислювальних ресурсів. Для вирішення цих проблем, дослідники та розробники працюють над створенням нових алгоритмів консенсусу та

оптимізацією архітектури блокчейн-мереж, щоб забезпечити швидку обробку транзакцій та високу пропускну спроможність системи.

Попри технічні та організаційні виклики, перспективи застосування блокчейна у кібербезпеці залишаються обнадійливими. Ця технологія пропонує нові можливості для створення безпечних, прозорих та відмінно захищених цифрових систем, які можуть ефективно протистояти сучасним кіберзагрозам. Розвиток блокчейн-рішень продовжуватиме відкривати нові горизонти у захисті інформації, підвищуючи надійність та безпеку цифрового світу.

Методи криптографічного захисту [10]. Криптографія залишається однією з найважливіших складових кібербезпеки, надаючи надійні засоби для захисту інформації від несанкціонованого доступу. Використання алгоритмів шифрування, таких як RSA, AES та ECC, дозволяє забезпечити конфіденційність та цілісність даних під час їх зберігання та передачі. Останнім часом особливу увагу приділяють розвитку квантової криптографії, яка обіцяє створити системи зв'язку, стійкі до будь-яких спроб дешифрування, навіть з використанням квантових комп'ютерів. Це відкриває нові перспективи для створення абсолютно безпечних комунікаційних каналів.

Однак, розвиток криптографічних методів також супроводжується появою нових викликів, зокрема, необхідністю постійного оновлення криптографічних ключів та алгоритмів для протидії розвитку засобів криптоаналізу. Це вимагає від організацій забезпечення високого рівня управління криптографічними ключами, що є важливою складовою загальної стратегії кібербезпеки.

Стандарти та регуляторні вимоги як інструмент комплаєнсу. Сучасний світ кібербезпеки не може існувати без чіткого дотримання міжнародних стандартів та регуляторних вимог. Норми, такі як ISO/IEC 27001, GDPR, PCI DSS, встановлюють вимоги до організацій щодо захисту персональних даних, управління інформаційними ризиками та забезпечення

конфіденційності інформації. Впровадження цих стандартів дозволяє компаніям не тільки підвищити рівень захисту даних, але й покращити довіру з боку клієнтів та партнерів.

Адаптація до регуляторних вимог вимагає від організацій гнучкості та готовності до постійного оновлення політик та процедур безпеки [11]. Це також передбачає регулярні аудити та оцінку вразливостей, щоб виявити та усунути потенційні слабкі місця в системах безпеки. Водночас, дотримання нормативних вимог стимулює розвиток індустрії кібербезпеки, сприяючи впровадженню інноваційних рішень та підвищенню загального рівня захищеності в інформаційному просторі.

Освіта та підвищення обізнаності у сфері кібербезпеки. Одним з ключових аспектів захисту від кіберзагроз є освіта та підвищення рівня обізнаності користувачів і фахівців у сфері кібербезпеки. Розвиток культури безпеки в організаціях починається з освітніх програм, які навчають працівників розпізнавати спроби фішингу, соціальної інженерії та інші види атак. Такі програми не лише сприяють зниженню ризику успішних кібератак, але й формують у співробітників відповідальне ставлення до обробки та зберігання конфіденційної інформації.

Значення освіти в сфері кібербезпеки виходить за межі корпоративного середовища, охоплюючи широкий спектр користувачів від дітей до літніх людей. Програми з освіти в галузі кібербезпеки, що впроваджуються у школах та університетах, допомагають підготувати молоде покоління до викликів сучасного цифрового світу.

Активна роль урядових та некомерційних організацій у розвитку освітніх програм з кібербезпеки також відіграє важливу роль у формуванні національної стратегії захисту кіберпростору. Ініціативи, спрямовані на підвищення обізнаності громадян про загрози в інтернеті та способи їх запобігання, сприяють створенню більш безпечного цифрового середовища.

Важливість інвестицій у освіту та навчання в області кібербезпеки не може бути переоцінена. Постійне оновлення знань та навичок дозволяє

фахівцям бути на крок попереду кіберзлочинців, ефективно протистоячи новим методам атак та забезпечуючи надійний захист інформаційних активів.

1.5.2 Характеристика підприємства Namecheap inc.

Namecheap Inc. є провідним реєстратором доменних імен і веб-хостинг компанією, заснованою у 2000 році Річардом Кіркендаллом. З головним офісом у Фініксі, штат Арізона, компанія за ці роки стала одним із найбільших незалежних реєстраторів у світі, обслуговуючи понад 10 мільйонів клієнтів та управляючи понад 17 мільйонами доменів. Namecheap пропонує широкий спектр послуг, включаючи реєстрацію доменів, веб-хостинг, VPN, а також послуги з охорони приватності доменів і інші додаткові сервіси.

З роками Namecheap продовжував розширювати свій спектр послуг, додаючи хостинг, захист і управління WordPress, що відображає зростаючі потреби його користувачів. Компанія відома своєю політикою прозорості, пропонуючи домени та хостинг за конкурентоспроможними цінами. Namecheap також активно підтримує інтернет-свободу та приватність в мережі, що виявляється у їх кампаніях проти законодавчих актів, що можуть обмежити ці аспекти.

Компанія має понад 1700 працівників у 18 країнах, що свідчить про її глобальний вплив та розширення. Namecheap також є прихильником інновацій у сфері технологій, що постійно підвищує задоволеність клієнтів, як показують численні позитивні відгуки користувачів, що оцінили їхні послуги в 4.7 з 5 на основі понад 2 мільйонів відгуків.

Namecheap відомий своєю соціальною відповідальністю, особливо під час кризи, такої як інвазія Росії в Україну, коли компанія активно підтримувала українські антивоєнні вебсайти та блокувала російські облікові записи у відповідь на військові дії та порушення прав людини.

На сьогоднішній день Namecheap продовжує бути лідером у галузі, надаючи своїм клієнтам інструменти для досягнення успіху в інтернеті і підтримуючи високий рівень обслуговування та інновацій. Це підкреслює їNamecheap Inc., заснована в 2000 році Річардом Кіркендаллом, є однією з провідних компаній у галузі реєстрації доменів та веб-хостингу. З головним офісом у Фініксі, штат Арізона, Namecheap зросла до значних масштабів, обслуговуючи понад 10 мільйонів клієнтів із понад 17 мільйонами доменів у своєму управлінні. Компанія пропонує широкий спектр послуг, включаючи реєстрацію доменів, веб-хостинг, VPN послуги та захист приватності доменів.

Відома своєю привітністю до інновацій, Namecheap вводила численні нововведення, що допомагають клієнтам розширювати свої онлайн-проекти. Завдяки наголосу на прозорість та доступність, Namecheap змогла забезпечити високий рівень задоволеності клієнтів, що відображається у їхніх численних позитивних відгуках.

Компанія також активно виступає за збереження інтернет-свобод та приватності, борючись проти законодавчих ініціатив, що можуть це обмежити. Це включає підтримку важливих ініціатив та кампаній, спрямованих на захист прав користувачів в інтернеті.

Namecheap має значну кількість співробітників у різних країнах, підтримуючи глобальний підхід до бізнесу із сильним акцентом на локальне обслуговування та підтримку клієнтів. Вони прагнуть надавати високоякісний сервіс, зосереджуючись на задоволенні потреб своїх користувачів по всьому світу.

1.5.3 Структура Namecheap Inc.

Структура Namecheap Inc. відображає її здатність ефективно реагувати на змінні вимоги ринку та потреби клієнтів.

Верховне керівництво взаємодіє з різними операційними та технічними відділами, що забезпечують щоденне виконання бізнес-процесів і реалізацію корпоративних цілей. Операційні підрозділи, такі як відділи реєстрації доменів, хостингу, SSL, консьєрж-сервісу та керований WordPress, зосереджені на наданні якісних послуг і підтримці клієнтів. Ці відділи грають ключову роль у підтримці репутації Namecheap як надійного постачальника інтернет-послуг.

Технічні підрозділи, включаючи управління ризиками, юридичний відділ, біллінг, TechOps та TechSup, забезпечують стабільність і безпеку операційних сервісів. Вони відіграють важливу роль у забезпеченні високих стандартів безпеки та ефективності, що є критично важливим для довіри та задоволення клієнтів.

Адміністративний відділ, що включає HR, People Partners, юридичний відділ та фінансовий відділ, підтримує внутрішню інфраструктуру та забезпечує необхідні ресурси для підтримки стабільного розвитку компанії. Ці відділи є основою для розвитку талантів та управління ресурсами, що дозволяє Namecheap постійно вдосконалювати свої послуги.

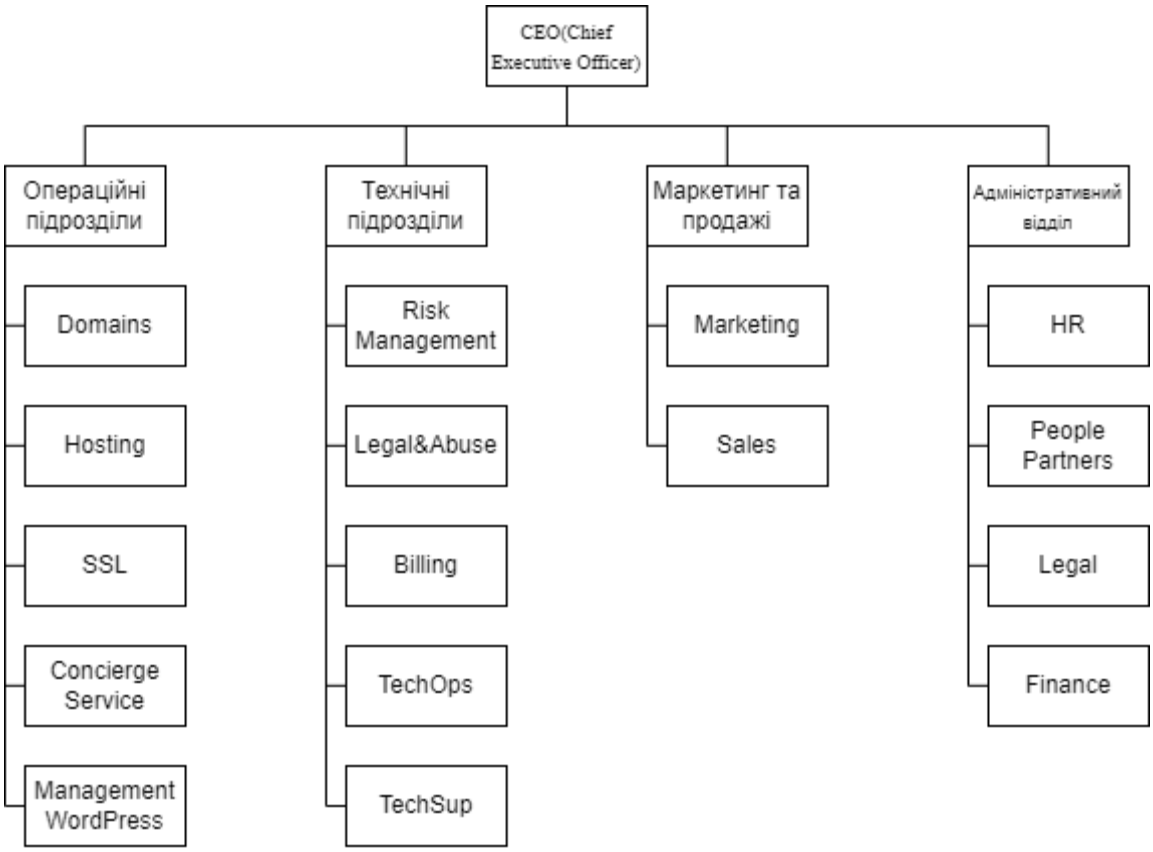

Рис. 1.3 Схема загальної структури підприємства

Розуміння цієї структури є ключовим для аналізу стратегічних рішень, прийнятих керівництвом Namecheap, і способів, яким Namecheap Inc. оперує як незалежний реєстратор доменів і веб-хостинг компанія, що надає широкий спектр інтернет-послуг. Компанія, заснована у 2000 році, швидко зростала завдяки своїм принципам доступності, прозорості та підтримки свободи інтернету. Namecheap обслуговує понад 10 мільйонів клієнтів і керує понад 17 мільйонами доменів, що свідчить про її значний вплив у галузі.

Структура компанії розроблена таким чином, щоб підтримувати гнучкість і швидкість реагування на змінні потреби ринку. Операційні підрозділи, такі як відділ реєстрації доменів, хостингу, SSL, та консьєрж-сервіс, прямо впливають на якість послуг і клієнтське задоволення. Технічні відділи займаються підтримкою інфраструктури і безпеки, а адміністративний блок забезпечує внутрішні операції та управління ресурсами.

Важливо відзначити, що Namecheap активно захищає приватність користувачів і виступає проти законодавчих змін, які можуть обмежити свободу інтернету. Це позиціонування не лише вигідно відрізняє компанію від конкурентів, але й зміцнює її репутацію як надійного партнера.

Розуміння структури Namecheap допомагає краще оцінити стратегічні ініціативи компанії та її здатність інновувати та адаптуватися до викликів ринку. Це також підкреслює, як важливо мати чітку організаційну структуру, що може ефективно підтримувати різноманітні бізнес-процеси в динамічному середовищі.

Бізнес-моделювання створено для того, щоб забезпечити інтегровану автоматизацію у керуванні підприємством. Такі системи передбачають проведення детального аналізу діяльності компанії до розробки проєкту. Результатом цього аналізу є висновок експертів, який містить рекомендації для вирішення проблем у керуванні. Виходячи з цього висновку, перед початком реалізації проєкту автоматизації здійснюється реорганізація бізнес-процесів, яка може бути істотною та складною для компанії. Часто буває важко переконати довготривалу команду адаптуватися до нових методів роботи. Такі всебічні перевірки підприємств завжди є складними і потребують застосування перевірених методологій та стандартів для моделювання складних систем.

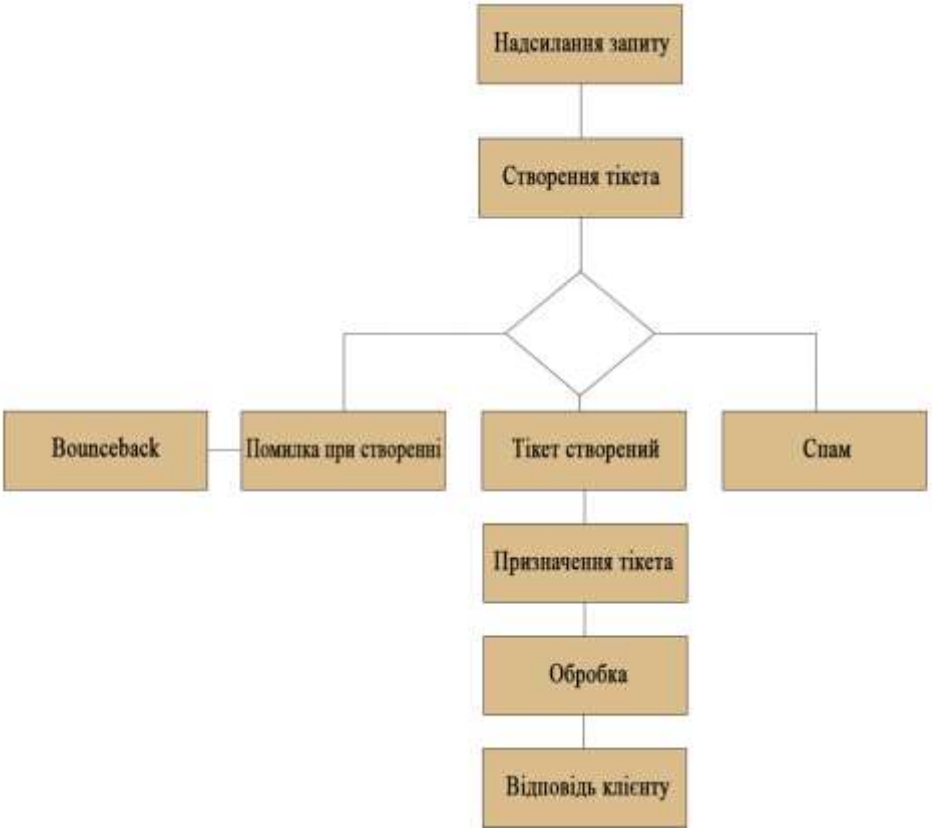

Рис. 1.4 Процес формування тікету

На зображенні схема процесу формування тікета заснована на електронному листі від клієнта. Процес включає такі етапи:

1. **Надсилання електронного листа від клієнта** — початковий етап, де клієнт сформував і надіслав запит.
2. **Автоматичне створення тікета** — система автоматично перетворює отриманий лист на тікет для подальшої обробки.
3. **Призначення тікета команді підтримки** — тікет надсилається відповідній групі підтримки для вирішення.
4. **Обробка тікета командою підтримки** — команда підтримки формує відповідь клієнту.
5. **Відповідь клієнту –** сформована відповідь надсилається клієнту

Ця схема надає чітке уявлення про процес взаємодії з клієнтом від моменту отримання запиту до інформування його про статус обробки.

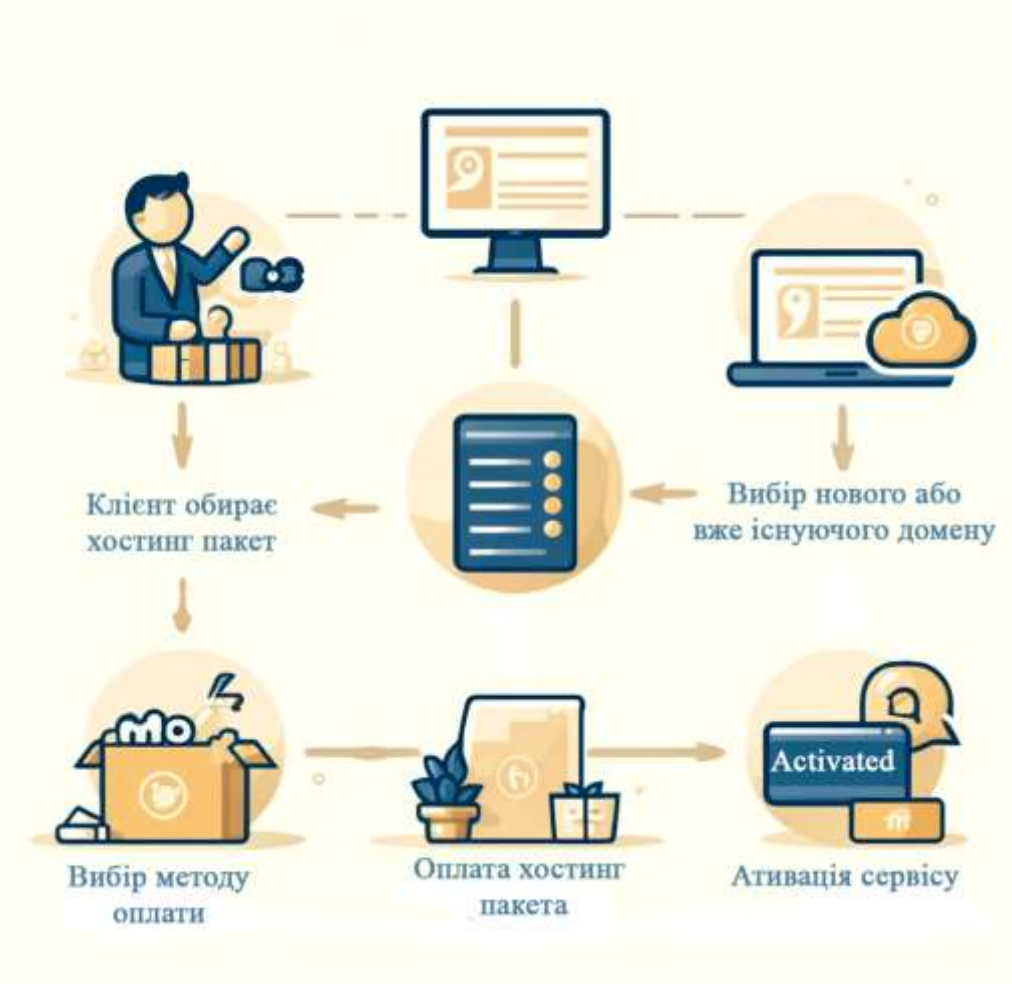

Рис. 1.5 Процес замовлення хостинг-пакету

Процес замовлення хостинг-пакету в моделі, представленій на рисунку, розгортається в кілька етапів, кожен з яких є важливим для забезпечення успішної взаємодії з клієнтом та впровадження хостинг-сервісів, а саме:

Вибір хостинг-пакета. Клієнт починає з вибору відповідного хостинг-пакету, що найкраще відповідає його потребам у веб-просторі, з огляду на такі параметри, як обсяг дискового простору, кількість доменів та пропускна спроможність.

Введення доменної інформації. Після вибору пакета клієнт вносить інформацію про свій існуючий домен або обирає новий домен. Це включає перевірку доступності доменного імені та його реєстрацію, якщо він новий.

Оплата. Завершальний крок перед активацією сервісу — це оплата обраного хостинг-пакету. Клієнт здійснює платіж за допомогою одного з

доступних методів оплати, які можуть включати кредитні карти, електронні гаманці або банківські перекази.

Активація сервісу. Після підтвердження оплати хостинг-сервіс активується. Клієнту надсилається вся необхідна інформація для доступу до управління хостингом, включаючи дані для входу в панель керування, налаштувань сервера, а також інструкції для розгортання веб-сайтів.

Цей процес демонструє, як замовлення хостингу може бути інтегрована та автоматизована для зручності клієнта та ефективності бізнесу.

Процес повернення коштів (рефанд) у компанії Namecheap включає декілька кроків та процедур, які забезпечують прозорість і справедливість обслуговування клієнтів. Коли клієнт вирішує відмовитися від послуги і зажадати повернення коштів, процес починається з подання заявки на рефанд через особистий кабінет на сайті Namecheap. Це перший крок, який дозволяє клієнту офіційно ініціювати процес і вказати причину повернення.

Заявка на рефанд розглядається службою підтримки, яка перевіряє відповідність запиту умовам повернення, які визначені в політиці компанії. Ці умови включають терміни, протягом яких можливе повернення, і категорії послуг, за які можуть бути повернуті кошти. Наприклад, веб-хостингові послуги можуть мати 30-денний термін для повернення, але це не застосовується до деяких інших послуг, як-от реєстрація доменів під час акцій.

Якщо запит відповідає умовам, процесується рефанд, який може зайняти кілька робочих днів. Виплати здійснюються на той же рахунок, з якого було проведено оплату. Якщо транзакція була здійснена через кредитну карту, кошти будуть повернуті на карту. Це вимагає взаємодії з платіжними системами і може потребувати додаткового часу.

У складних випадках, коли повернення коштів не може бути здійснено згідно стандартної процедури через специфіку транзакції чи порушення умов, справа може бути передана в юридичний відділ Namecheap для

подальшого аналізу та вирішення. Клієнту надається інформація про статус запиту та можливі альтернативи, якщо пряме повернення коштів неможливе.

Namecheap прагне забезпечити, що процес рефанду є якнайбільш простим і зрозумілим для клієнтів, з мінімумом незручностей. Підтримка клієнтів у таких ситуаціях відіграє важливу роль у підтримці високого рівня задоволеності клієнтів та їх довіри до компанії. Namecheap також використовує відгуки клієнтів під час процесу рефанду для аналізу і покращення своїх послуг та політики повернення.

1.5.4 Актуальні задачі для підприємства Namecheap

У контексті сучасного бізнес-середовища Namecheap стикається з низькою актуальних задач, які вимагають уваги та стратегічного підходу. Перш за все, збільшення конкуренції в галузі веб-хостингу та реєстрації доменів вимагає від Namecheap постійного інноваційного розвитку та удосконалення своїх послуг. Компанія повинна не тільки зберігати свою ринкову частку, а й активно залучати нових клієнтів, що можливо через розробку нових продуктів, поліпшення клієнтського досвіду та оптимізацію цінової політики.

Друге велике завдання — це забезпечення безпеки даних клієнтів. Зі зростанням загроз в інтернеті, Namecheap має зосередити увагу на посиленні заходів безпеки, що включає захист від DDoS-атак, шахрайства і витоку інформації. Це передбачає не тільки технічне удосконалення системи, а й просвітницьку роботу серед клієнтів щодо основ кібербезпеки.

Також компанія стикається з викликами управління міжнародним зростанням. З офісами і серверами у різних країнах, Namecheap повинен забезпечити стабільність та високу продуктивність своїх міжнародних операцій, що включає управління технічною інфраструктурою, локалізацію послуг і підтримку на місцевих ринках.

Крім того, Namecheap має активно реагувати на законодавчі зміни, які можуть вплинути на індустрію інтернет-послуг, особливо в контексті законів про приватність даних та управління інтернет-доменами. Це вимагає від компанії ведення активної правової політики та участі у відповідних галузевих та громадських дебатах.

На додаток, як компанія, що залучає значну кількість клієнтів через інтернет, Namecheap має відповідати на зміни у споживчих тенденціях та очікуваннях, що стосуються не тільки технологічних аспектів, а й екологічних, соціальних та управлінських практик. Вирішення цих задач дозволить компанії зберегти свою конкурентоспроможність і лідерські позиції на ринку.

Namecheap має перед собою ряд складних завдань, вирішення яких потребує стратегічного планування та адаптивності управління. Здатність компанії інновувати, адаптуватися до змін у ринковому середовищі та відповідати на очікування клієнтів визначатиме її довгостроковий успіх і стабільність.

Висновок за розділом 1

У першому розділі було проведено аналіз поточного стану безпеки веб-інфраструктур та визначено основні проблеми та виклики, з якими стикаються сучасні підприємства. Цей аналіз показав, що більшість компаній стикаються з постійними загрозами, які вимагають постійного моніторингу та оновлення захисних механізмів. Було досліджено різні види загроз, включаючи кібернапади, зломи, фішинг та інші види атак, що можуть завдати значної шкоди веб-інфраструктурам. Також було розглянуто актуальні тенденції в розвитку технологій для забезпечення безпеки веб-інфраструктур, включаючи новітні криптографічні методи, технології блокчейну та штучний інтелект. Крім того, було приділено увагу аналізу існуючих технологій виявлення та запобігання атакам, таких як системи виявлення вторгнень. Також було розглянуто регуляторні вимоги та

стандарти, що впливають на комплаєнс та захист даних у веб-інфраструктурах. Розглянуто приклади інтеграції захисних механізмів у веб-сайти та сервіси, а також вплив таких інтеграцій на загальну безпеку. Було відзначено, що інтеграція захисних технологій потребує планування та тестування для забезпечення їх ефективності та мінімізації впливу на продуктивність систем. На основі проведеного аналізу було виявлено, що багато підприємств не мають достатньої кількості ресурсів та знань для ефективного забезпечення безпеки своїх веб-інфраструктур. Також було розглянуто питання недостатньої обізнаності співробітників про основи кібербезпеки, що часто призводить до людських помилок та порушень безпеки. Це підкреслює необхідність у подальшому вивченні та впровадженні новітніх технологій та методів захисту. Таким чином, аналітичний розділ дозволив отримати чітке уявлення про поточний стан безпеки веб-інфраструктур та визначити напрямки для подальших досліджень.

РОЗДІЛ 2
СПЕЦІАЛЬНИЙ

2.1 Аналіз сучасних підходів до забезпечення безпеки веб-інфраструктур

Вдосконалення стратегій захисту доменів та серверів відбулось з останнього десятиліття індустрії кібербезпеки. Всі вони можуть бути умовно розділені на декілька ключових етапів:

Еволюція шифрування. Шифрування завжди було одним із основних засобів забезпечення безпеки інформації. Від самого початку епохи цифрових технологій розробка та удосконалення криптографічних систем відігравали важливу роль у захисті конфіденційності, цілісності та доступності даних. У ранні роки цифрової ери, коли інформаційні технології лише починали розвиватися, були популярними прості, але ефективні методи шифрування, такі як DES (Data Encryption Standard) і RSA (Rivest–Shamir–Adleman), які згодом виявилися недостатньо сильними для захисту від зростаючих обчислювальних можливостей і засобів декодування.

Розробка алгоритму DES була здійснена в 1970-х роках і це було значним кроком вперед у криптографії, але з часом, з розвитком комп’ютерних технологій, алгоритм став легким завданням для злому. Виникнення потреби у більш складних системах привело до створення RSA у 1977 році, який використовує двоключову криптографію та складається з відкритого і закритого ключів для шифрування та дешифрування даних відповідно. RSA був великим кроком уперед, оскільки він дозволив безпечний обмін ключами через незахищені канали.

З розвитком інтернету з'явилася потреба в глобальних стандартах для забезпечення безпеки онлайн комунікацій, що призвело до створення протоколів TLS (Transport Layer Security) та SSL (Secure Sockets Layer). Ці

протоколи використовують сучасні алгоритми шифрування та автентифікації для створення зашифрованого каналу між клієнтом і сервером, що значно знижує ризик перехоплення даних третіми особами.

Сучасні вимоги до безпеки вимагають більш складних та надійних методів шифрування. Однією з найсучасніших тенденцій у шифруванні є розробка алгоритмів, стійких до атак з використанням квантових комп'ютерів, які теоретично можуть легко розшифровувати алгоритми RSA та ECC (Elliptic Curve Cryptography). З'явилися нові напрямки, такі як пост-квантова криптографія, яка зосереджена на розробці шифрувальних систем, що можуть протистояти потенційним загрозам від квантових технологій.

Вдосконалення криптографічних технологій не зупиняється, і кожне нове покоління принесло суттєві покращення у захисті конфіденційної інформації. Введення нових стандартів, таких як AES (Advanced Encryption Standard), забезпечило більш високий рівень безпеки, здатність шифрувати великі обсяги даних та швидше обробляти їх при збереженні надійності. Ці алгоритми стали основою для захисту державних секретів, фінансових операцій та особистих даних користувачів по всьому світу.

Одним із головних напрямків розвитку криптографії є забезпечення стійкості до квантових атак, що ставить перед науковцями і розробниками складні завдання. Квантова криптографія, яка використовує квантові властивості частинок для генерації і розподілу ключів, є одним із найбільш перспективних напрямків. Цей метод заснований на принципах квантової механіки, таких як принцип невизначеності та заплутаність станів, що дозволяє забезпечити теоретично абсолютну безпеку комунікацій. Однак, квантова криптографія наразі залишається досить складною та дорогою для широкого застосування.

Крім того, з'являється все більше алгоритмів шифрування, що використовують математичні проблеми, стійкі до квантових обчислень. Такі методи, як решіткове шифрування та шифрування на основі хеш-функцій,

обіцяють стати надійними засобами захисту даних у майбутньому, коли з'являться повноцінні квантові комп'ютери.

Паралельно з цим, розвиток криптографії впливає на стандарти і політики безпеки в компаніях та організаціях. Важливим аспектом є розробка і впровадження політик шифрування, які регулюють вибір алгоритмів, управління ключами та процедури аудиту. Постійне оновлення цих політик дозволяє адаптуватися до нових загроз і викликів у галузі кібербезпеки.

Шифрування не обмежується тільки технічними аспектами. Воно також впливає на правові та етичні питання. З розвитком криптографії постає питання балансу між правом на приватність і потребами державного регулювання та нагляду. Це створює потребу у постійному діалозі між технологами, юристами та політиками для розробки відповідних законів, що враховують технічні інновації та суспільні цінності.

Останнім часом особливу увагу приділяється також і розвитку децентралізованих криптографічних технологій, таких як блокчейн, що можуть кардинально змінити підходи до забезпечення цілісності та невід'ємності даних. Застосування блокчейна у фінансових послугах, управлінні ланцюгами поставок та інших областях показує потенціал цієї технології для створення нових моделей довіри і безпеки.

У той час, коли шифрування розвивається, виникає потреба в забезпеченні ширшої публічної обізнаності та розуміння цих технологій. Зростання числа інцидентів, пов'язаних з витоками даних та кібератаками, підкреслює необхідність вищого рівня освіти з питань кібербезпеки серед звичайних користувачів і професіоналів. Широке застосування шифрування на особистому та корпоративному рівнях може значно покращити загальний стан кібербезпеки, знижуючи вразливість систем до несанкціонованих втручань.

Значні інвестиції в дослідження та розробку нових методів шифрування відкривають шлях до більш безпечного майбутнього. Наприклад, розвиток криптографії, що заснована на основі апаратної

безпеки, такої як технології HSM (Hardware Security Modules), забезпечує високий рівень захисту ключів шифрування і транзакцій. Ці технології мінімізують ризики атак, заснованих на викраденні ключів, а також забезпечують контрольоване зберігання та обробку чутливих даних.

Однак, разом із прогресом шифрування та його інтеграцією у все більше аспектів цифрового життя, виникають складнощі, пов’язані з управлінням ключами та політиками доступу. Системи управління ключами (Key Management Systems) стають складнішими, що вимагає від організацій наявності спеціалізованих знань для ефективного адміністрування. Важливість комплексного підходу до управління криптографічними ключами не може бути недооцінена, оскільки від цього залежить загальний рівень безпеки інформаційних систем.

З поширенням облачних технологій виникає потреба в розробці і застосуванні шифрування в масштабі хмари. Це стосується не тільки зберігання даних, але й обробки та передачі інформації між розподіленими середовищами. Шифрування "end-to-end" в хмарних архітектурах забезпечує, що дані зашифровані на всіх етапах їхнього життєвого циклу, від відправлення до прийому, знижуючи ризики несанкціонованого доступу або маніпуляцій.

В цьому контексті також актуальним є розвиток стандартів і протоколів, які визначають, як і коли має використовуватися шифрування. Міжнародні стандарти, такі як ISO/IEC 27001, відіграють важливу роль у формуванні глобальних практик з кібербезпеки. Вони сприяють розробці загальноприйнятих методик шифрування, що спрощує міжнародну співпрацю та забезпечує високий рівень захисту у глобальних масштабах.

Крім технічних аспектів, важливо звертати увагу на правові рамки, що регулюють використання шифрування. В умовах різних юрисдикцій, політика використання шифрування може значно відрізнятися, що створює додаткові виклики для міжнародних компаній. Забезпечення відповідності

криптографічних методів законодавчим вимогам в кожній країні є критично важливим для забезпечення легальності та ефективності захисних заходів.

Виходячи з цього, необхідність адаптації криптографічних рішень до національних та міжнародних норм і законів стає ще одним пріоритетним напрямком у розвитку шифрування. Створення гнучких криптографічних систем, що можуть бути легко налаштовані відповідно до юридичних вимог різних країн, дозволить компаніям уникнути правових ризиків та сприятиме забезпеченню глобальної безпеки.

Наразі активно розвиваються технології, що дозволяють використовувати шифрування не тільки для забезпечення конфіденційності, але й для гарантування цілісності та автентичності даних. Такі технології, як цифрові підписи та блокчейн, використовують криптографічні алгоритми для створення надійних і верифікованих записів, що мають важливе значення в багатьох галузях, включаючи фінанси, логістику та управління документообігом.

Цифрові підписи, які використовують комбінацію приватного та публічного ключів для перевірки автентичності та незмінності документів, стали стандартом у сфері електронного документообігу. Вони дозволяють з упевненістю ідентифікувати особу, яка підписала документ, і переконатися, що документ не був змінений після підписання. Така технологія забезпечує високий рівень довіри та юридичну значимість електронних документів, що є важливим для бізнесу та урядових організацій.

Використання блокчейну пропонує ще один рівень захисту, дозволяючи розподілити зберігання даних по мережі та автоматично перевіряти цілісність інформації за допомогою криптографічних алгоритмів. Це знижує ризики централізованих атак та маніпуляцій з даними, оскільки змінити інформацію в одному блоку вимагає змін у всіх попередніх блоках ланцюжка, що практично неможливо без виявлення.

Інновації в шифруванні також включають розробку технологій, які забезпечують «шифрування на основі політик», де правила доступу та

обробки даних визначаються динамічно, залежно від контексту. Такий підхід дозволяє більш гнучко керувати конфіденційністю інформації в різних умовах і забезпечувати її захист відповідно до внутрішніх та зовнішніх політик безпеки.

З огляду на зростання кількості застосувань Інтернету речей (IoT), шифрування стає ще більш важливим для захисту великої кількості даних, що генеруються та обмінюються між пристроями. Забезпечення безпеки цих даних є критично важливим, адже IoT-пристрої часто залучені до управління критично важливими системами, такими як медичне обладнання, системи управління енергетичними ресурсами та транспортні системи.

Шифрування є не просто технологічною необхідністю; це стратегічний елемент, що дозволяє компаніям, урядам та індивідуальним користувачам захищати свою приватність, забезпечувати цілісність та доступність інформації в умовах зростаючих загроз у кіберпросторі. Континуальний розвиток криптографічних технологій, постійне оновлення політик і стандартів, а також міжнародне співробітництво в області кібербезпеки є ключовими для гарантування надійного захисту в інформаційну еру.

Шифрування продовжує еволюціонувати, реагуючи на зміни у технологічному ландшафті і суспільних очікуваннях. Ця динаміка підкреслює необхідність постійного наукового дослідження, інновацій та освітніх ініціатив, щоб гарантувати, що шифрування залишиться ефективним інструментом у захисті цифрового світу.

Розвиток DDoS захисту. З розвитком інтернету стало зрозуміло, що традиційні методи забезпечення безпеки вже не в змозі ефективно протистояти новим загрозам, таким як DDoS-атаки (розподілені відмови у обслуговуванні), які можуть знеструмити сервери та зупинити бізнес-процеси на невизначений термін. У відповідь на це, індустрія безпеки почала шукати шляхи ефективнішої боротьби з такими атаками, що призвело до розробки нових, більш складних технологій захисту.

В перші роки розвитку Інтернету DDoS-захист був мінімальним або його взагалі не було, що дозволяло хакерам легко використовувати ці вразливості. Однак, з часом, коли стало ясно, що захист від DDoS повинен стати пріоритетом, почали з'являтися рішення, спрямовані на мінімізацію впливу таких атак. Серед них – розподілені мережі доставки контенту (CDN), які не тільки прискорюють завантаження веб-сторінок для користувачів по всьому світу, але й допомагають розподіляти навантаження на мережу, роблячи менш вразливими до атак окремі сервери.

З появою технологій обробки великих даних стало можливим аналізувати трафік в реальному часі, що дозволило ідентифікувати і блокувати DDoS-атаки на ранніх стадіях. Сучасні системи DDoS-захисту використовують складне програмне забезпечення, яке аналізує моделі трафіку та виявляє ненормальну поведінку, що може вказувати на початок атаки.

Ще однією інновацією в області DDoS-захисту стало створення спеціалізованого обладнання, такого як анти-DDoS апаратні рішення, які можуть масштабуватися для обробки величезної кількості трафіку та ефективно відсіювати шкідливі запити. Ці рішення включають апаратні фільтри, що швидко розпізнають і блокують трафік від відомих джерел DDoS-атак, надаючи організаціям додатковий шар захисту.

Адаптивність системи є найважливішим аспектом у боротьбі з DDoS-атаками, оскільки зловмисники постійно змінюють тактику. Впровадження машинного навчання та штучного інтелекту у системи DDoS-захисту дозволяє їм "вчитися" на попередніх атаках і передбачати потенційні майбутні загрози, автоматично адаптуючи захисні механізми.

Управління реакцією на інциденти також важливо для ефективного DDoS-захисту. Це включає розробку та впровадження процедур реагування, які мають бути швидкими, координованими та ефективними, щоб забезпечити неперервність бізнес-операцій навіть під час масштабної атаки.

Окрім технічних засобів, важливо також розвивати корпоративну культуру безпеки, яка передбачає постійне навчання персоналу методам виявлення та реагування на DDoS-атаки. Це дозволить компаніям бути краще підготовленими до неминучих кіберзагроз і забезпечити стійкість своїх веб-інфраструктур.

Застосування облачних технологій. Поширення облачних технологій внесло значні зміни у пейзаж кібербезпеки, відкривши нові можливості та виклики для захисту даних. Облачні сервіси, які використовують дистанційно розташовані сервери для зберігання, обробки та управління даними, пропонують велику гнучкість і масштабованість, але також створюють нові вразливості, оскільки дані тепер перебувають поза корпоративним фізичним периметром.

Однією з переваг облачних технологій є те, що вони дозволяють компаніям швидко адаптуватися до змінюваних умов ринку та технологічних інновацій без необхідності інвестувати в дорогу інфраструктуру. Однак, з іншого боку, централізація даних в одному місці або в декількох дата-центрах, які управляються третіми сторонами, створює потенційні ризики витоку даних, злому, втрати даних або їхньої пошкодженості через кібератаки.

Для забезпечення безпеки в облачних середовищах компанії повинні використовувати різноманітні стратегії та технології. Шифрування даних на стороні клієнта перед їх відправленням у хмару є одним із найефективніших способів забезпечення конфіденційності інформації. Це гарантує, що навіть у разі витоку даних вони будуть безпечні, оскільки шифрування робить їх незрозумілими без відповідного ключа.

Іншим важливим аспектом захисту в облачних середовищах є сегментація мережі та застосування принципу найменших привілеїв. Це включає створення віртуальних приватних мереж (VPN), які ізолюють чутливі частини мережі від загальнодоступних ресурсів, а також

забезпечення, що користувачі мають доступ тільки до тих ресурсів, які необхідні для виконання їхніх робочих завдань.

Розвиток технологій управління ідентифікацією та доступом (IAM) відіграє ключову роль в забезпеченні безпеки облачних середовищ. Сучасні IAM-системи дозволяють централізовано керувати ідентифікаційними даними користувачів, їхніми правами доступу до ресурсів та виконувати аудит безпеки. Ці системи використовують складні політики безпеки, що включають багаторівневу автентифікацію та контекстну перевірку автентичності, що дозволяє підвищити рівень захисту і знизити ризик несанкціонованого доступу.

Також важливим елементом захисту облачних систем є постійний моніторинг та аналіз поведінки користувачів і трафіку у мережі. Це дозволяє виявляти незвичну поведінку, що може бути індикатором спроби злому або іншої шкідливої діяльності. Системи виявлення і запобігання вторгнень (IDS/IPS) та системи управління інформацією про події безпеки (SIEM) є стандартними інструментами, які використовуються для цих цілей.

Застосування облачних технологій вимагає також забезпечення фізичної безпеки дата-центрів, де фізично розміщені сервери. Це включає в себе не тільки контроль доступу на територію, але й заходи щодо захисту від природних катастроф, пожежі, та інших нештатних ситуацій.

Впровадження політик безпеки. У світлі постійної еволюції кіберзагроз, впровадження ефективних політик безпеки стало необхідністю для організацій всіх розмірів. Від ефективності цих політик залежить не лише захист конфіденційної інформації, але й спроможність компанії підтримувати довіру клієнтів та партнерів. Політики безпеки повинні охоплювати всі аспекти IT-інфраструктури, включно з фізичними та логічними заходами захисту, а також процедурами реагування на інциденти.

Першим кроком у впровадженні політик безпеки є визначення поточного рівня ризику та вразливостей в IT-системах компанії. Це вимагає проведення детального аудиту систем, включаючи аналіз програмного

забезпечення, обладнання, мережевих налаштувань та використання даних. На основі отриманих даних розробляються специфічні рекомендації, спрямовані на зміцнення захисту.

Однією з складових політик безпеки є регулярне оновлення та підтримка програмного забезпечення. Встановлення патчів безпеки та оновлень системи необхідне для захисту від відомих вразливостей, які можуть бути використані зловмисниками для втручання в системи або викрадення даних. Також важливою є належна конфігурація захисних систем, таких як файрволи, антивірусне програмне забезпечення та інші інструменти безпеки.

Управління доступом до ресурсів є ще однією важливою складовою політик безпеки. Застосування принципу найменшого привілею, де користувачам надаються мінімально необхідні права для виконання їхніх робочих завдань, може значно знизити ризик внутрішніх та зовнішніх загроз. Крім того, двофакторна аутентифікація та сильні парольні політики забезпечують додатковий рівень захисту.

Процедури реагування на інциденти є критично важливими для забезпечення оперативності дій в умовах безпекових порушень. Розроблення чітких кроків дій для різних типів інцидентів, навчання персоналу їх застосуванню, а також регулярні тренування та випробування готовності можуть значно знизити вплив кібератак на ресурси компанії.

Крім технічних і процедурних заходів, важливу роль у політиках безпеки відіграє корпоративна культура. Постійне навчання та підвищення обізнаності співробітників щодо кібербезпеки забезпечує, що вони знають про потенційні загрози та вміють діяти, щоб запобігти порушенням безпеки. Регулярні інструктажі, тренінги та внутрішні кампанії з підвищення обізнаності відіграють ключову роль у формуванні культури безпеки в організації.

У цілому, реалізація комплексних та ефективних політик безпеки вимагає поєднання технічних, процедурних та культурних підходів, які разом

формують міцний фундамент для захисту від сучасних кіберзагроз. Тільки через постійне оновлення політик, технологій та практик можна досягти реального зниження ризиків і підвищення рівня кібербезпеки в компанії.

Таблиця 2.1

Як змінювалися методи шифрування від кібератак 2000-2024 роки

2000-2010 роки	2010-2020 роки	2020-2024 роки
AES (Advanced Encryption Standard)	ECC (Elliptic Curve Cryptography)	Post-Quantum Cryptography (PQC)
RSA (Rivest–Shamir–Adleman)	TLS 1.3	Blockchain і криптовалюти
3DES (Triple Data Encryption Standard)	SHA-256	Advanced Encryption Standard (AES)
Diffie-Hellman key exchange	Homomorphic Encryption	Quantum Key Distribution (QKD)
PGP (Pretty Good Privacy)	Quantum Key Distribution (QKD)	Enhanced Privacy ID (EPID)

2000-2010 роки:

*AES (Advanced Encryption Standard***).** AES став новим стандартом шифрування після затвердження Національним інститутом стандартів і технологій (NIST) у 2001 році, замінивши DES. Він підтримує довжини ключів 128, 192 та 256 біт і забезпечує високий рівень безпеки, що робить його вибором для багатьох урядових і комерційних систем по всьому світу. AES використовує симетричне блочне шифрування, що дозволяє ефективно обробляти великі обсяги даних. Його міцність та ефективність забезпечили широке прийняття в індустрії безпеки.

RSA (Rivest–Shamir–Adleman). RSA залишається однією з найбільш використовуваних асиметричних криптографічних систем, особливо для забезпечення безпеки цифрових підписів та шифрування даних. Використовуючи пару ключів, публічний та приватний, RSA дозволяє безпечно обмінюватися інформацією через незахищені канали. Цей метод

широко використовується в системах електронної комерції та фінансових транзакціях завдяки його надійності та міцності.

3DES (Triple Data Encryption Standard). 3DES є розширенням DES, яке забезпечує вищий рівень безпеки шляхом тричі повторного шифрування блоку даних. Незважаючи на свою меншу популярність порівняно з AES, 3DES продовжував використовуватися у фінансових інституціях та інших застосуваннях, де потрібен додатковий рівень захисту. Його продуктивність може бути нижчою в порівнянні з AES через більшу обчислювальну вимогливість.

Diffie-Hellman key exchange. Метод обміну ключами Diffie-Hellman був розроблений для безпечного обміну криптографічними ключами через публічний канал. Він дозволяє двом сторонам мати спільний секретний ключ, не передаючи його явно, що робить його особливо корисним у створенні захищених приватних з'єднань, таких як VPN та інші мережеві протоколи.

PGP (Pretty Good Privacy). PGP є програмним забезпеченням для шифрування та цифрового підпису електронних комуніка### PGP (Pretty Good Privacy) (2000-2010) PGP є програмним забезпеченням для шифрування та цифрового підпису електронних комунікацій, яке забезпечує конфіденційність та автентичність передачі інформації. Воно використовує комбінацію симетричного шифрування, асиметричного шифрування та стиснення даних для захисту електронних повідомлень. PGP також включає систему управління ключами, що дозволяє користувачам легко та безпечно обмінюватися ключами. Його широке застосування в індустрії безпеки обумовлене високим рівнем надійності та зручністю у використанні

2010-2020 роки:

ECC (Elliptic Curve Cryptography). ECC відоме своєю здатністю забезпечувати той же рівень безпеки, що й інші методи шифрування, але з використанням менших ключів, що робить його ідеальним для використання в мобільних пристроях та IoT, де обчислювальні ресурси та пам'ять обмежені. Його ефективність і швидкість роблять ECC важливим

інструментом у сучасних криптографічних протоколах, включаючи ті, що використовуються для захисту фінансових транзакцій та обміну даними в хмарних системах

TLS 1.3. Оновлення протоколу TLS до версії 1.3 принесло значні покращення в швидкості та безпеці. Зменшення часу рукостискання, вдосконалення криптографічних методів та виключення застарілих функцій забезпечили кращий захист від атак та зниження затримки. TLS 1.3 широко прийнятий у веб-браузерах та інтернет-серверах, забезпечуючи безпечне з'єднання між користувачами та сайтами.

SHA-256. SHA-256 є частиною сімейства хеш-функцій SHA-2, яке використовується для створення унікального цифрового відбитку файлів, повідомлень або будь-яких інших даних. Ця хеш-функція забезпечує стійкість до колізій, що робить її надійним інструментом для систем безпеки, блокчейн-технологій та цифрових сертифікатів.

Homomorphic Encryption. Homomorphic encryption дозволяє виконувати обчислення безпосередньо на зашифрованих, забезпечуючи конфіденційність обробки даних у хмарних обчисленнях, без необхідності доступу до незашифрованої інформації.

Quantum Key Distribution (QKD). QKD використовує принципи квантової механіки для забезпечення надзвичайно безпечної передачі криптографічних ключів. Ця технологія, невразлива до всіх відомих методів криптоаналізу, зокрема, вважається стійкою до атак з використанням квантових комп'ютерів. QKD вже використовується у військових та фінансових застосуваннях, де потреба у високій конфіденційності є критичною.

2020-2024 роки:

Post-Quantum Cryptography. З розвитком квантових технологій, зростає потреба в алгоритмах, які можуть протистояти майбутнім квантовим комп'ютерам. Post-Quantum Cryptography (PQC) включає розробку нових криптографічних систем, здатних витримати атаки, що використовують

квантові обчислення, тим самим забезпечуючи довгострокову безпеку цифрових даних.

Blockchain і криптовалюти. Застосування криптографії в блокчейн технологіях і криптовалютах продовжує збільшуватися, надаючи високий рівень безпеки і анонімності в транзакціях. Blockchain використовує поєднання хешування, шифрування і консенсусних алгоритмів для забезпечення незмінності та прозорості даних.

Advanced Encryption Standard (AES). AES продовжує бути важливою частиною криптографічних рішень, забезпечуючи основу для безпечного шифрування в урядових установах, комерційних компаніях і особистих застосуваннях. Його роль як надійного стандарту для шифрування сучасних даних залишається критичною у забезпеченні конфіденційності та цілісності інформації.

Quantum Key Distribution (QKD). Технологія QKD продовжує розвиватися, надаючи ще більш безпечні методи передачі криптографічних ключів. Завдяки своїй спроможності гарантувати безпеку комунікацій, навіть у світлі потенційних майбутніх квантових загроз, QKD вває новаторські підходи до безпеки даних у надзвичайно важливих застосуваннях, зокрема в урядовому та оборонному секторах.

Enhanced Privacy ID (EPID). EPID стає ключовим інструментом у забезпеченні анонімності у сферах, де це критично важливо, таких як IoT і розумні міста. Технологія дозволяє зберігати конфіденційність користувачів під час взаємодії з різними цифровими сервісами, забезпечуючи при цьому високий рівень безпеки та управління доступом. Розвиток EPID відкриває нові можливості для захисту персональних даних у глобальних мережах.

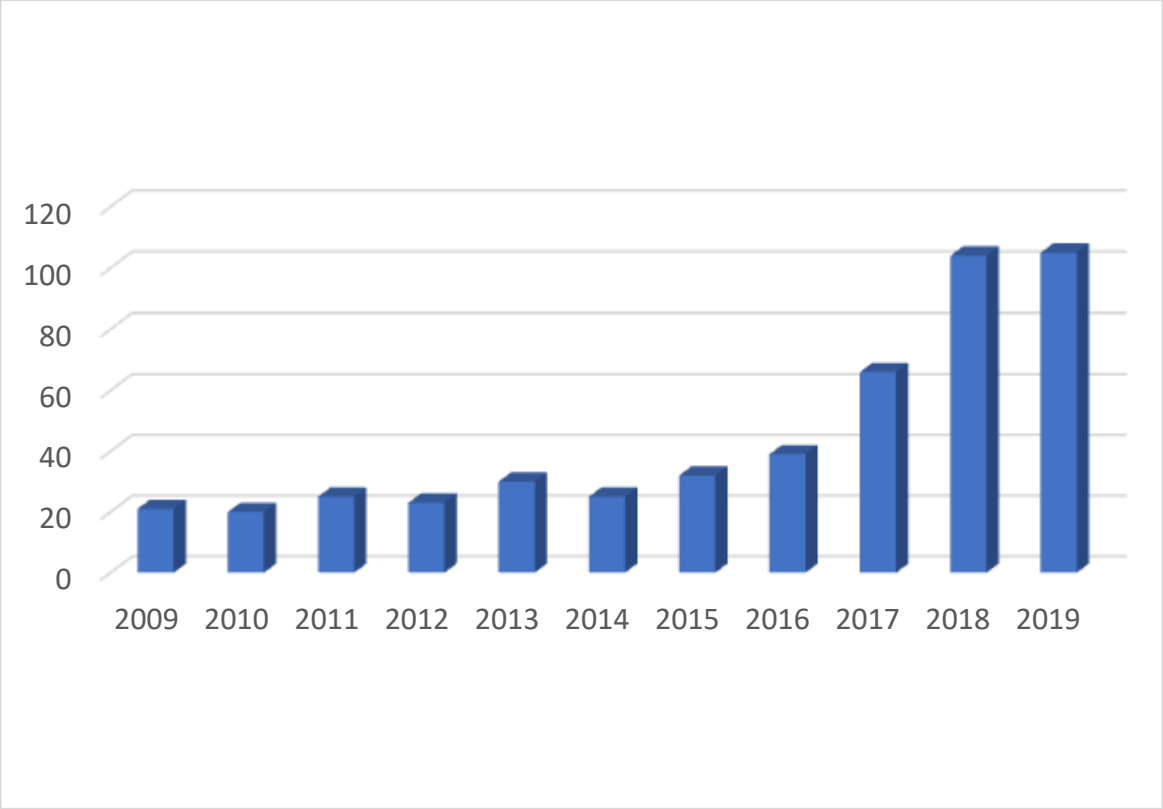

Рис. 2.1 Кібератаки зі збитками понад $1 000 000 (джерело [28])

2.2 Порівняння технологій за рівнями захисту та вартістю

Порівняння технологій захисту вимагає глибокого аналізу не тільки з точки зору їхньої ефективності але й з урахуванням вартості їх впровадження та подальшої експлуатації. Ринок пропонує широкий спектр рішень від простих антивірусних програм до складних інтегрованих систем кібербезпеки, які включають захист даних, шифрування, виявлення вторгнень і управління доступом. Розглянемо три основні категорії технологій захисту:

Базовий рівень. Базовий рівень захисту є фундаментом кібербезпеки будь-якої організації. Він включає антивірусне програмне забезпечення та персональні фаєрволи, які захищають кінцеві точки та мережі від загальновідомих загроз. Антивіруси сканують файли та програми на наявність шкідливого коду та видаляють його перед тим, як він зможе завдати шкоди. Фаєрволи контролюють вхідний та вихідний трафік в мережі,

блокуючи несанкціоновані спроби доступу та обмежуючи потоки даних, які можуть містити потенційні загрози. Ці інструменти є досить доступними та простими у використанні, що робить їх популярним вибором для малого та середнього бізнесу. Незважаючи на свою простоту, базовий рівень захисту ефективно відвертає більшість автоматизованих атак, таких як віруси та шпигунське програмне забезпечення. Однак, він не здатен впоратися з більш складними та цілеспрямованими загрозами, такими як фішинг або атаки нульового дня, для яких потрібні більш складні заходи захисту.

Середній рівень. Середній рівень захисту розширює базові можливості захисту, інтегруючи системи виявлення та запобігання вторгненням (IDS/IPS), рішення для управління шифруванням та контроль доступу. Ці системи використовуються для моніторингу мережевого трафіку на предмет аномалій, які можуть вказувати на спробу несанкціонованого доступу або інші підозрілі дії. IDS здатні ідентифікувати потенційні загрози за певними сигнатурами або аномаліями в трафіку, тоді як IPS може активно блокувати такі спроби, перш ніж вони завдадуть шкоди. Управління шифруванням гарантує, що всі чутливі дані зашифровані, знижуючи ризики витоку інформації в разі злому. Системи контролю доступу гарантують, що лише уповноважені користувачі мають доступ до важливих ресурсів, обмежуючи можливості внутрішніх і зовнішніх загроз. Впровадження цих технологій вимагає більш високих початкових інвестицій і складніше в налаштуванні, але надає значно кращий захист від розширеного спектру загроз.

Високий рівень. На високому рівні захисту використовуються найсучасніші технології, такі як аналітика великих даних, штучний інтелект (ШІ) для прогнозування загроз, автоматизоване реагування на інциденти, а також інтегровані платформи безпеки, які об'єднують всі аспекти захисту в єдину систему. Ці технології дозволяють не тільки виявляти та блокувати атаки, але й прогнозувати потенційні загрози на основі моделювання поведінки та інших складних алгоритмів. ШІ може аналізувати великі обсяги даних для ідентифікації складних патернів, що можуть вказувати на нові

види загроз. Автоматизовані системи реагування здатні миттєво реагувати на виявлені загрози, мінімізуючи потенційні збитки. Високий рівень захисту вимагає значних інвестицій у технології та їхнє утримання, але забезпечує найкращий можливий захист для організацій, чиї операції критично залежать від цифрової безпеки.

Можливі рішення безпеки можна умовно поділити на наступні категорії:

Низька вартість. Антивіруси та фаєрволи можна придбати за низькою ціною, а їх впровадження не вимагає значних зусиль, що робить їх доступними для малого та середнього бізнесу.

Середня вартість. Рішення середнього рівня, такі як IDS/IPS, вимагають більших інвестицій у ліцензування та налаштування, що може бути виправданим для компаній, що мають вищі вимоги до захисту даних.

Висока вартість. Інтегровані системи, які включають передові технології, зазвичай мають високу вартість впровадження і обслуговування, але їх ефективність в захисті від найсучасніших кіберзагроз може значно знизити потенційні втрати від інцидентів.

Порівняння технологій за рівнями захисту та вартості дозволяє компаніям знаходити баланс між вартістю та ефективністю. Під час вибору технологій необхідно враховувати як безпосередні, так і довгострокові потреби організації у захисті її цифрових активів.

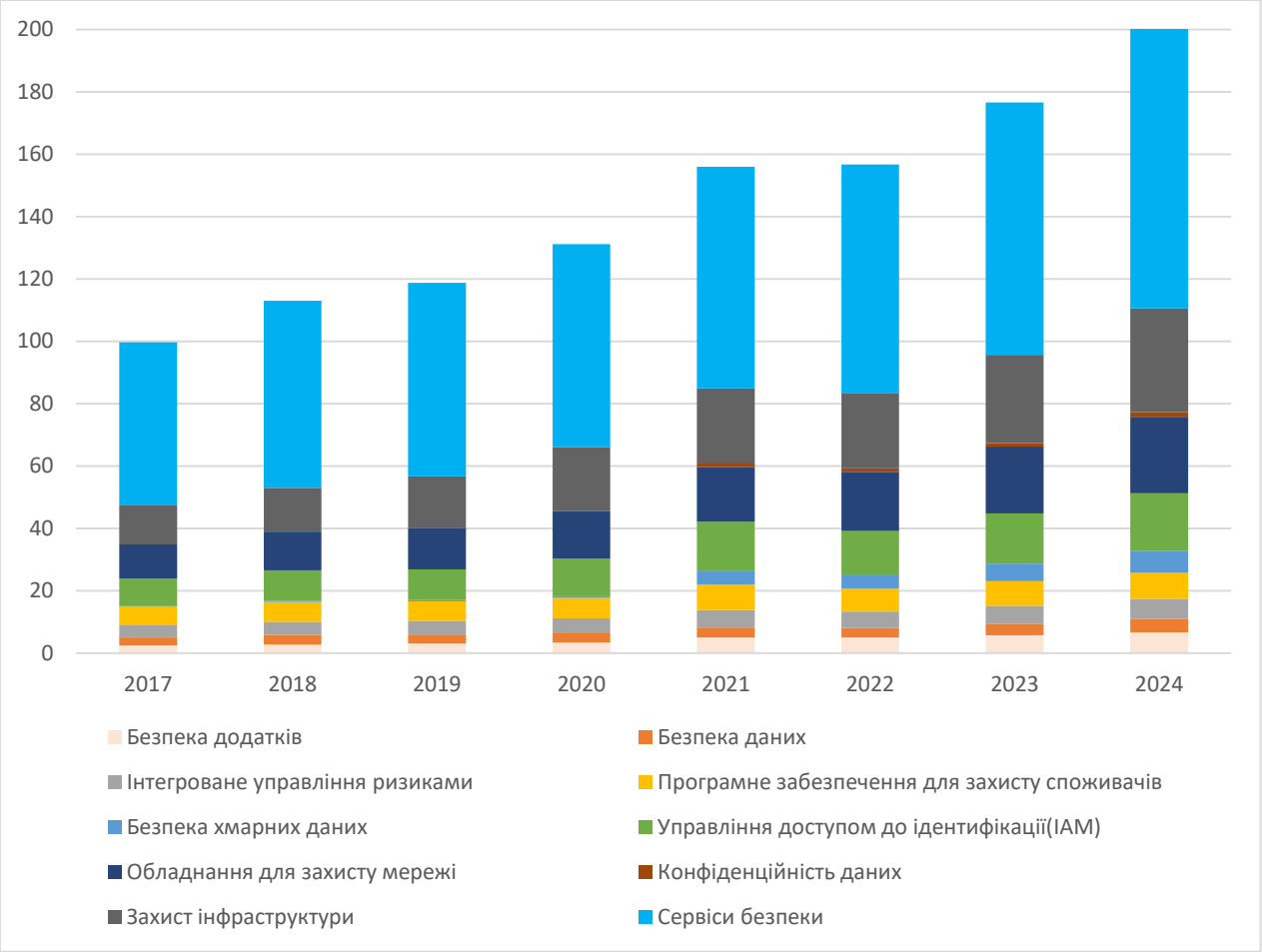

Рис. 2.2 Витрати на інформаційну безпеку у світі з 2017 по 2024 рік, за сегментами (у мільйонах доларів США) (джерело [30])

2.3 Аналіз змін у законодавстві та стандартах безпеки

З ростом кіберзагроз і значними порушеннями даних, було введено більш жорсткі законодавчі норми, такі як GDPR у Європі, що вимагають від компаній значно більші витрати на захист даних. Важливими аспектами є:

Захист персональних даних. Компанії тепер зобов'язані забезпечувати вищий рівень захисту особистих даних своїх клієнтів, що включає в себе шифрування даних і застосування багаторівневої автентифікації.

Звітність та відповідальність. Закони вимагають, щоб компанії вели детальні журнали їхніх операцій з даними, що включає в себе як збір так і обробку інформації. Підвищені вимоги до прозорості ведуть до необхідності

використання більш складних технологічних рішень для забезпечення дотримання цих вимог.

Штрафи та відповідальність. Недотримання вимог GDPR може призвести до значних штрафів, які можуть досягати до 4% від світового обороту компанії. Такі вимоги мотивують компанії більше інвестувати в кібербезпеку, щоб уникнути фінансових втрат.

2.4 Вивчення випадків та найефективніших практик

Використання передових практик і кейс-стадіїв великих компаній, таких як Google та Amazon, може надати цінні уроки у захисті веб-інфраструктур:

Застосування штучного інтелекту для прогнозування загроз. Штучний інтелект допомагає автоматизувати виявлення і відповідь на загрози, значно підвищуючи ефективність захисних систем. Великі дані, що аналізуються з допомогою ШІ, дозволяють ідентифікувати потенційні атаки набагато раніше, ніж вони стануть загрозою.

Використання хмарних технологій для масштабування захисту. Хмарні рішення дозволяють швидко масштабувати інфраструктуру безпеки в залежності від поточних потреб компанії. Моделі безпеки хмарних сервісів, які включають еластичне логування і аналіз, стають нормою для забезпечення постійного моніторингу.

Політики нульового довіряння. Політики "нульового довіряння" передбачають, що будь-який доступ до ресурси потрібно ретельно перевіряти, незалежно від того, наскільки користувач або пристрій може здаватися надійним. Це включає постійну валідацію користувачів та їхніх пристроїв перед наданням доступу до критичних ресурсів.

Аудит та відповідність стандартам. Компанії інтенсивно використовують внутрішні та зовнішні аудити для забезпечення дотримання політик безпеки і законодавчих вимог. Регулярні перевірки допомагають

ідентифікувати потенційні вразливості і забезпечують можливість швидко реагувати на будь-які виявлені проблеми.

2.5 Роль штучного інтелекту та машинного навчання в захисті веб-інфраструктур

Штучний інтелект (ШІ) та машинне навчання (МН) відіграють важливу роль у модернізації кібербезпеки, пропонуючи нові можливості для підвищення ефективності захисних систем:

Автоматизація виявлення загроз. Системи на базі ШІ можуть автоматично аналізувати великі обсяги даних для ідентифікації потенційних загроз в реальному часі. Це значно знижує час, необхідний для виявлення та реагування на інциденти, що підвищує загальний рівень безпеки.

Покращення точності прогнозів. Машинне навчання дозволяє системам безпеки "вчитися" з попередніх атак, що покращує їх здатність передбачати та блокувати подібні спроби в майбутньому. Такий підхід допомагає зменшити кількість помилкових спрацьовувань і забезпечує більш цілеспрямовану відповідь на загрози.

Оптимізація ресурсів безпеки. ШІ може допомогти автоматизувати рутинні задачі, звільшаючи навантаження на персонал безпеки та дозволяючи їм зосередитися на більш складних задачах. Завдяки цьому збільшується загальна ефективність команд безпеки і покращується їхнє реагування на інциденти.

Аналіз і адаптація до нових загроз. ШІ здатний швидко аналізувати нові види кібератак і адаптувати захисні механізми відповідно до поточних загроз. Ця гнучкість є критично важливою у світі, де методи кібератак постійно еволюціонують і стають складнішими.

2.6 Проблеми та перспективи розвитку систем захисту веб-інфраструктур

Останні розробки в технологіях і методологіях кібербезпеки відкривають нові можливості для захисту веб-інфраструктур, але також пропонують ряд викликів:

Інтеграція нових технологій. Впровадження нових рішень може бути складним через несумісність із існуючими системами і потребує значних інвестицій у час і ресурси. Потрібна постійна координація між командами розробників та безпеки для ефективного впровадження та управління новими технологіями.

Забезпечення приватності та дотримання законодавства. Зростання обсягів даних і більш строгі вимоги до приватності викликають потребу у розробці більш досконалих систем управління приватністю і даними. Організації повинні не тільки захищати дані від зовнішніх загроз, але й забезпечувати їх використання у відповідності з законодавчими і регулятивними вимогами.

Залучення і навчання фахівців з кібербезпеки. З огляду на швидкий розвиток кіберзагроз, існує нестача кваліфікованих фахівців у галузі кібербезпеки. Ця проблема зберігається, незважаючи на зусилля університетів та приватних компаній збільшувати кількість програм для підготовки фахівців. Важливим є також підвищення рівня освіти та навчання діючих спеціалістів для оновлення їх знань з новітніх технологій і методик.

Забезпечення резистентності до майбутніх загроз. Передові методи та технології, що з'являються сьогодні, мають бути адаптовані таким чином, щоб захистити інфраструктури від непередбачених майбутніх загроз, які можуть бути набагато складнішими. Підходи, які добре працюють сьогодні, можуть стати неефективними в майбутньому, тому важливо вести постійний розвиток захисних систем і методів.

Рис. 2.3 Модель безпеки Zero-Trust (джерело [32])

2.7 Задача розділення ринку хостингових послуг на зони впливу компаній

2.7.1 Постановка задачі

Припустимо, що є певна кількість хостингових компаній, послуг та клієнтів. Компанії можуть оказувати послуги: веб-сервери, e-mail сервіси, shared сервери з вбудованою панеллю керування, SSL/TLS сертифікати, dedicated сервери, serverless архітектура та E-commerce.

Веб-сервери надають хостинг та обробку веб-запитів. E-mail сервіси забезпечують роботу електронної пошти. Shared сервери з вбудованою панеллю керування дозволяють користувачам легко керувати веб-ресурсами. SSL/TLS сертифікати забезпечують захищене з'єднання між користувачами і веб-сайтами. Dedicated сервери пропонують фізичний сервер для ексклюзивного використання. Serverless архітектура автоматично керує

ресурсами для виконання задач. E-commerce сервіси підтримують фінансові та торгові транзакції в онлайн-середовищі.

Існує певний перелік клієнтів: новачки, програмісти, системні адміністратори, безпекові менеджери, власники бізнесу.

Новачки - це особи, які тільки починають працювати з веб-технологіями і потребують базових знань та навичок. Новачкам потрібен дуже юзер-френдлі інтерфейс та зручні засоби для побудови вебсайту. Програмісти - це особи, які вже мають досвід розробки веб-додатків і можуть створювати прості веб-рішення. Системні адміністратори - це фахівці, що відповідають за налаштування та обслуговування веб-серверів, забезпечуючи їх стабільну роботу. Системним адміністраторам необхідні потужні інструменти для керування серверами та оптимізації ресурсів. Безпекові менеджери - це фахівці, які спеціалізуються на кібербезпеці та захисті даних, захищаючи інформаційні системи від загроз. Безпековим менеджерам потрібні надійні засоби захисту даних і кібербезпеки для забезпечення безпеки інформаційних систем. Власники бізнесу - це люди, що відповідають за веб-інфраструктуру своїх компаній, забезпечуючи її ефективність і безпеку. Власникам бізнесу потрібні ефективні e-commerce рішення та надійні сервери для підтримки фінансових і торгових транзакцій.

Є визначений список компаній: Namecheap, GoDaddy, Shopify, Amazon Web Services, Hostinger.

Namecheap - це компанія, що надає послуги доменних імен, хостингу та інших сервісів для онлайн-присутності. Вони відомі своєю доступністю та простотою використання. GoDaddy - провідний постачальник доменних імен, хостингу та інших послуг для онлайн-бізнесу. Компанія відома своєю широкою пропозицією та зручними інструментами для керування веб-проектами. Shopify - це платформа для створення інтернет-магазинів, яка дозволяє швидко створити та запустити електронний бізнес. Amazon Web Services (AWS) - це провідний хмарний сервіс, що надає широкий спектр послуг для розробки та запуску веб-проектів. AWS відома своєю надійністю

та масштабованістю для будь-яких потреб бізнесу. Hostinger - це постачальник хостингу, що пропонує доступні та надійні веб-хостингові рішення. Компанія відома своєю привабливою ціновою політикою та добре розвиненою підтримкою клієнтів.

Для кожної категорії клієнтів значення певної послуги відрізняється, а різні хостингові компанії відповідають вимогам різних груп клієнтів на певному рівні. Тому потрібно встановити сфери впливу кожної компанії серед набору клієнтів.

2.7.2 Побудова математичної моделі

Клієнти $X = \{x_1, x_2, \dots x_n\}$:

x_1 – Новачки

x_2 – Програмісти

x_3 – Системні адміністратори

x_4 – Безпекові менеджери

x_5 – Власники бізнесу

Множина послуг, які надають компанії, $Y = \{y_1, y_2, \dots y_p\}$:

y_1 – Веб-сервери

y_2 – E-mail сервіси

y_3 – Shared сервери з вбудованою панеллю керування

y_4 – SSL/TLS сертифікати

y_5 – Dedicated сервери

y_6 – Serverless архітектура

y_7 – E-commerce

Множина компаній, $Z = \{z_1, z_2 \dots z_m\}$

z_1 – Namecheap

z_2 – GoDaddy

z_3 - Shopify

z_4 – Amazon Web Services

z_5 - Hostinger

Для кожної категорії клієнтів значення певної послуги відрізняється, а різні хостингові компанії відповідають вимогам різних груп клієнтів на певному рівні. Тому потрібно встановити сфери впливу кожної компанії серед набору клієнтів.

2.7.3 Розв'язування задачі за допомогою нечітких множин

Для розв'язування поставленої задачі скористаємось методом, описаним у літературі [33].

Опишемо за допомогою функції належності $\Phi_R : X \times Y \to [0;1]$ нечітке бінарне відношення R , яке представляє ступінь значущості послуги y в оцінці клієнта x при його виборі компанії. Вище значення функції належності вказує на більшу важливість цієї характеристики.

Відношення R може бути представлене наступним чином:

$$R = \begin{array}{c} \\ x_1 \\ x_2 \\ \dots \\ x_n \end{array} \begin{array}{c} \begin{array}{cccc} y_1 & y_2 & \dots & y_p \end{array} \\ \begin{bmatrix} \Phi_R(x_1, y_1) & \Phi_R(x_1, y_2) & \dots & \Phi_R(x_1, y_p) \\ \Phi_R(x_2, y_1) & \Phi_R(x_2, y_2) & \dots & \Phi_R(x_2, y_p) \\ \dots & \dots & \dots & \dots \\ \Phi_R(x_n, y_1) & \Phi_R(x_n, y_2) & \dots & \Phi_R(x_n, y_p) \end{bmatrix} \end{array}$$

Ступінь належності або сумісності компанії з певними критеріями представлений матрицею $\pi : Y \times Z \to [0;1]$, що є функцією належності нечіткого бінарного відношення S. Для кожного елемента з множин $y \in Y$ і $z \in Z$, значення $\pi_s(y,z)$ вказує на ступінь сумісності компанії Z з відповідною послугою Y.

У формі матриці це відношення виглядає наступним чином:

$$S = \begin{array}{c} \\ y_1 \\ y_2 \\ \dots \\ y_p \end{array} \begin{array}{c} \begin{array}{cccc} z_1 & z_2 & \dots & z_m \end{array} \\ \begin{bmatrix} \pi_s(y_1, z_1) & \pi_s(y_1, z_2) & \dots & \pi_s(y_1, z_m) \\ \pi_s(y_2, z_1) & \pi_s(y_2, z_2) & \dots & \pi_s(y_2, z_m) \\ \dots & \dots & \dots & \dots \\ \pi_s(y_p, z_1) & \pi_s(y_p, z_2) & \dots & \pi_s(y_p, z_m) \end{bmatrix} \end{array}$$

Складемо матрицю T, яка описує ступінь відповідності компанії z_i вимогам клієнта x_j, а саме:

$$T = \begin{array}{c} \\ x_1 \\ x_2 \\ \dots \\ x_n \end{array} \begin{array}{c} \begin{array}{cccc} z_1 & z_2 & \dots & z_m \end{array} \\ \begin{bmatrix} \mu_{A_1}(x_1, z_1) & \mu_{A_2}(x_1, z_2) & \dots & \mu_{A_m}(x_1, z_m) \\ \mu_{A_1}(x_2, z_1) & \mu_{A_2}(x_2, z_2) & \dots & \mu_{A_m}(x_1, z_m) \\ \dots & \dots & \dots & \dots \\ \mu_{A_1}(x_n, z_1) & \mu_{A_2}(x_n, z_2) & \dots & \mu_{A_m}(x_n, z_m) \end{bmatrix} \end{array}$$

Елементи цієї матриці визначені за допомогою функції належності, яка має такий вигляд:

$$\mu_A(x, z_i) = \frac{\sum_y \Phi_R(x, y)\pi_s(y, z_i)}{\sum_y \Phi_R(x, y)}, \qquad (2.7.1)$$

для всіх елементів $x \in X$, $y \in Y$ та $z \in Z$.

Сума $\sum_y \Phi_R(x, y)$ відображає ступінь належності нечіткій підмножині, яка демонструє кількість ключових послуг y, використаних клієнтом x для оцінки компанії, тоді як кожен елемент $\mu_{A_i}(x, z_i)$ можна розглядати як зважений ступінь переваги, який клієнт x надає компанії z_i. Функція переваги, описана у рівнянні (3.1), відповідає критеріям опуклої нечіткої підмножини, тобто

$$\mu_{A_i}[\lambda(x_1, z_i) + (1-\lambda)(x_2, z_i)] \geq \min[\mu_{A_i}(x_1, z_i), \mu_{A_i}(x_2, z_i)] \qquad (2.7.2)$$

для всіх елементів x_1 і x_2, всіх $z_i \in Z$ і всіх $\lambda \in [0;1]$.

Оскільки всі функції $\mu_{A_i}(x, z_i)$ опуклі, їх перерізи також будуть опуклими функціями. Отже, можна побудувати матрицю *W*, елементами якої будуть всі можливі перерізи, а саме:

$$W = \begin{bmatrix} \mu_{A_1}(x_1, z_1) \wedge \mu_{A_2}(x_1, z_2) & & \mu_{A_{m-1}}(x_1, z_{m-1}) \wedge \mu_{A_m}(x_1, z_m) \\ \mu_{A_1}(x_2, z_1) \wedge \mu_{A_2}(x_2, z_2) & & \mu_{A_{m-1}}(x_2, z_{m-1}) \wedge \mu_{A_m}(x_2, z_m) \\ \cdots & \cdots & \cdots \\ \mu_{A_1}(x_n, z_1) \wedge \mu_{A_2}(x_n, z_2) & & \mu_{A_{m-1}}(x_2, z_{m-1}) \wedge \mu_{A_m}(x_2, z_m) \end{bmatrix}$$

(2.7.3)

Перехрещення сфер впливу різних хостингових компаній, ймовірно, є більш загальним явищем, аніж винятком у цій моделі. Умову для визначення межі розділення цих зон можна встановити наступним чином:

$$l > \min_{ij} \max_{x} \min[\mu_{A_i}(x, z_i), \mu_{A_j}(x, z_j)] \qquad (2.7.4)$$

Якщо поріг l вибраний, то зона впливу альтернативних компаній $M_i, i = 1,2,...,m$ описується такою рівневою множиною:

$$M_i = \{x \mid \mu_{A_i}(x) \geq \min_{ij} \max_{x} \min[\mu_{A_i}(x, z_i), \mu_{A_j}(x, z_j)]\} \qquad (2.7.5)$$

для всіх елементів $x \in M_i$.

Тепер застосуємо зазначену методику для вирішення задачі, що перед нами. Функція належності для нечіткого бінарного відношення R, яка відображає важливість послуги y_j з точки зору клієнта хі при його виборі компанії, була встановлена за допомогою експертних оцінок та представлена у формі матриці відповідно до категорій клієнтів (див. табл. 2.2).

Таблиця 2.2

Функція належності нечіткого бінарного відношення *R*

Клієнт	Послуга						
	y_1	y_2	y_3	y_4	y_5	y_6	y_7
x_1	0,1	0,4	0,4	1	0	1	0,5
x_2	0,4	0,6	0,6	1	0,2	0,5	0,6

Продовження табл. 2.2

x_3	0,8	0,6	0,3	1	0,5	0	0,7
x_4	0,7	0,3	0,2	1	1	0	0,4
x_5	0,8	1	0,2	1	1	0	1

Функція належності нечіткого бінарного відношення S, яка показує ступінь сумісності компанії z_j з окремими критеріями (послугами) y_j, була встановлена та представлена у формі, зазначеній у таблиці 2.3.

Таблиця 2.3

Функція належності нечіткого бінарного відношення *S*

Критерій (послуга)	Хостингова компанія				
	z_1	z_2	z_3	z_4	z_5
y_1	0	0	0	1	0
y_2	0,8	0,5	0.1	0.2	0.7
y_3	0,9	0.8	0	0	0.7
y_4	1	0.7	0.8	0.6	0.8
y_5	1	0	0	0.8	0
y_6	0.3	0.4	1	0	0.4
y_7	0.4	0.6	0.7	0.2	0.7

Тепер за формулами (3.1) обчислимо матрицю T – ступінь відповідності хостингової компанії z_j вимогам клієнта x_i. Результати обчислень зведено в табл. 2.4.

Таблиця 2.4

Ступінь відповідності компанії z_j вимогам клієнта x_i (матриця *T*)

Клієнт	Компанія				
	z_1	z_2	z_3	z_4	z_5
x_1	0,641	0,565	0,644	0,259	0,621
x_2	0,669	0,523	0,456	0,359	0,579

x_3	0,649	0,426	0,346	0,528	0,492

Продовження табл. 2.4

x_4	0,717	0,347	0,308	0,622	0,397
x_5	0,676	0,392	0,32	0,52	0,468

Далі обчислимо матрицю *W*.

Таблиця 2.5

Перекривання зон впливу хостингових компаній (матриця W)

0,565	0,641	**0,259**	0,621	0,565	**0,259**	0,565	**0,259**	0,621	**0,259**
0,523	0,456	0,359	0,579	0,456	0,359	0,523	0,359	0,456	0,359
0,426	0,346	0,528	0,492	0,346	0,426	0,426	0,346	0,346	0,492
0,347	0,308	0,622	0,397	0,308	0,347	0,347	0,308	0,308	0,397
0,392	0,320	0,520	0,468	0,320	0,392	0,392	0,320	0,320	0,468

З огляду на дані табл. 2.5 визначимо мінімальний поріг розділення множини клієнтів на зони впливу компаній. Він дорівнює 0,259.

Враховуючи інформацію з матриці T (таблиця 2.4), давайте визначимо та запишемо зони впливу для кожної з компаній наступним чином:

$M_1 = \{x_1, x_2, x_3, x_4, x_5\}, M_2 = \{x_1, x_2, x_3, x_4, x_5\}, M_3 = \{x_1, x_2, x_3, x_4, x_5\},$
$M_4 = \{x_2, x_3, x_4, x_5\}, M_5 = \{x_1, x_2, x_3, x_4, x_5\}$

Виходячи з умови (2.7.4), виберемо поріг $l = 0{,}5$. Отже, зони впливу компаній визначатимуться наступним чином:

$M_1 = \{x_1, x_2, x_3, x_4, x_5\}\ M_2 = \{x_1, x_2\}\ M_3 = \{x_1\}$
$M_4 = \{x_3, x_4, x_5\}\ M_5 = \{x_1, x_2\}$

Якщо використати інше значення, наприклад, l = 0,6, то результат буде наступним:

$M_1 = \{x_1, x_2, x_3, x_4, x_5\}, M_2 = \{\}, M_3 = \{x_1\}, M_4 = \{x_4\}, M_5 = \{x_1\}$

Таким чином, розрахунки демонструють, що з усіх компаній, враховуючи підвищення порогових значень для розділення множин, лише

одна залишається конкурентоздатною, адже її вплив на ринок споживачів хостингових послуг є найвищим. Зазначимо, що відповідність компанії до потреб споживача була визначена на основі множини характеристик і виражена у формі нечіткої оцінки.

Висновок за розділом 2

У другому розділі було проведено детальний аналіз сучасних підходів до забезпечення безпеки веб-інфраструктур. Особлива увага була приділена криптографічним методам, зокрема SSL/TLS, що забезпечують захист даних під час передачі через Інтернет. Криптографія є одним з компонентів сучасної веб-безпеки, оскільки вона дозволяє захистити конфіденційність та цілісність даних. Протоколи SSL/TLS широко використовуються для шифрування інформації, що передається між веб-серверами та клієнтами. Це значно зменшує ризик перехоплення та модифікації даних третіми сторонами. Також було розглянуто технології блокчейну, які забезпечують надійний захист даних та транзакцій завдяки децентралізованому характеру. Блокчейн має унікальну властивість, яка дозволяє забезпечити високий рівень безпеки та прозорості для зберігання та передачі даних. Застосування блокчейну у веб-інфраструктурах може допомогти запобігти фальсифікації даних та забезпечити їх цілісність.

Застосування штучного інтелекту та машинного навчання у веб-безпеці також було детально досліджено. Штучний інтелект та машинне навчання надають нові можливості для виявлення та запобігання кіберзагрозам у реальному часі. Ці технології можуть аналізувати великі обсяги даних, виявляти аномалії та прогнозувати потенційні загрози. Використання машинного навчання дозволяє створювати адаптивні системи захисту, які постійно вдосконалюються та підлаштовуються під нові типи загроз.

Було проведено аналіз ефективності різних підходів та методів захисту. Це дозволило визначити їхні сильні та слабкі сторони. Наприклад, криптографічні методи забезпечують високий рівень захисту даних, але

можуть бути вразливими до певних типів атак, таких як атаки на протоколи. Блокчейн забезпечує високий рівень прозорості та незмінності даних, але його інтеграція може бути складною та затратною. Штучний інтелект та машинне навчання надають адаптивні та динамічні системи захисту, але можуть вимагати значних обчислювальних ресурсів.

Розглянуті підходи та методи показують високу ефективність у різних умовах, що підтверджує їх доцільність для впровадження в сучасні веб-інфраструктури.

Це дозволяє забезпечити захист на всіх рівнях веб-інфраструктури, від аутентифікації користувачів до захисту даних. Проведений аналіз також підкреслив важливість регулярного оновлення та вдосконалення захисних механізмів. Веб-інфраструктури повинні бути гнучкими та адаптивними, щоб ефективно протистояти новим загрозам.

Також було розв’язано задачу розділення ринку на зони впливу за допомогою нечітких множин.

Таким чином, другий розділ дипломної роботи показав, що сучасні підходи до забезпечення безпеки веб-інфраструктур є ефективними та надійними. Впровадження цих підходів дозволить значно підвищити рівень захисту та забезпечити безпеку даних у сучасних веб-інфраструктурах.

ВИСНОВКИ

У дипломній роботі було зроблено загальний аналіз та оцінка ефективності сучасних підходів до забезпечення безпеки веб-інфраструктур. Робота показала, що забезпечення безпеки веб-інфраструктур є складним та багатогранним завданням, яке вимагає застосування різних методів та технологій. Проведений аналіз виявив основні проблеми та виклики, що стоять перед підприємствами у сфері веб-безпеки. Дослідження сучасних підходів, таких як криптографія, блокчейн, штучний інтелект та машинне навчання, показало їх високу ефективність у захисті веб-інфраструктур. Зокрема, було розглянуто приклади успішного впровадження цих технологій у різних галузях, що демонструють їхню практичну цінність. Також було з’ясовано, що криптографічні методи, такі як SSL/TLS, забезпечують надійний захист даних під час їх передачі. Використання блокчейну дозволяє забезпечити надійність і незмінність даних завдяки децентралізованій структурі. Окрім того, блокчейн-технологія може використовуватися для створення безпечних смарт-контрактів, що автоматизують бізнес-процеси. Штучний інтелект та машинне навчання допомагають у виявленні та запобіганні кіберзагрозам у реальному часі, що значно підвищує рівень безпеки. Ці технології здатні швидко адаптуватися до нових типів атак, що робить їх незамінними в умовах динамічного кіберпростору. Було розглянуто рекомендації щодо впровадження цих методів для підвищення рівня безпеки. Робота також підкреслила важливість дотримання регуляторних вимог та стандартів, що є невід'ємною частиною забезпечення безпеки. Виконання вимог таких стандартів, як GDPR та ISO/IEC 27001, сприяє покращенню загальної безпеки веб-інфраструктур. Встановлено, що дотримання стандартів та регуляторних вимог допомагає уніфікувати підходи до забезпечення безпеки та зменшити ризики. Загальні висновки підтверджують, що комплексний підхід до веб-безпеки, що включає комбінацію різних методів та технологій, є найбільш ефективним.

Впровадження таких підходів дозволить підприємствам значно підвищити захист своїх веб-інфраструктур від різноманітних загроз. Отже, комплексне застосування криптографії, блокчейну, штучного інтелекту та машинного навчання є вагомим досягненням у підвищенні рівня безпеки веб-інфраструктур. Впровадження таких підходів сприяє підвищенню конкурентоспроможності підприємств на ринку. Інноваційні підходи дозволяють підприємствам адаптуватися до нових загроз та ефективно їм протистояти. Загальний підхід, що включає використання різних технологій, допомагає створити багаторівневу систему захисту. Це дозволяє забезпечити цілісність, конфіденційність та доступність даних. Впровадження сучасних методів захисту також сприяє підвищенню довіри користувачів до веб-інфраструктур. У результаті, підприємства отримують можливість ефективніше захищати свої ресурси та дані від кіберзагроз.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Cybersecurity Stats: Facts And Figures You Should Know. Вебсайт. URL: https://www.forbes.com/advisor/education/it-and-tech/cybersecurity-statistics/ (Дата звернення 15.04.2024)

2. Статистика кіберзлочинності за 2014-2023 роки. Вебсайт. URL: https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/ (Дата звернення 15.04.2024)

3. Виплати викупів по кварталах за 2018-2023 роки. Вебсайт. URL: https://www.coveware.com/blog/2024/4/17/raas-devs-hurt-their-credibility-by-cheating-affiliates-in-q1-2024 (Дата звернення 15.04.2024)

4. Types of SSL certificates: SSL certificate types explained. Вебсайт. URL: https://www.cloudflare.com/learning/ssl/types-of-ssl-certificates/ (Дата звернення 12.05.2024)

5. І. С. Зоря, А. В. Марущак. Застосування штучного інтелекту для виявлення та реагування на кіберзагрози. Вінницький національний технічний університет. Доступно на: https://ir.lib.vntu.edu.ua/bitstream/handle/123456789/42057/20610.pdf (Дата звернення 12.05.2024)

6. Двофакторна автентифікація для безпеки облікового запису — що це, її види та як використовувати. Вебсайт. URL: https://ssl.com.ua/blog/ukr/what-is-2fa/ (Дата звернення 12.05.2024)

7. Інна З. Для чого потрібен комплаєнс на підприємстві. 2023. Вебсайт. URL: https://biz.ligazakon.net/analitycs/217068_dlya-chogo-potrben-komplans-na-pdprimstv (Дата звернення 27.05.2024)

8. Скіцько О., Складний П., Ширшов Р., Гуменюк М., Ворохоб М. Загрози та ризики використання штучного інтелекту. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка» - Том 2 (22). 2023, С. 6-18.

9. Що таке безпека блокчейну: приклади, проблеми та рішення. Вебсайт. URL: https://www.h-x.technology/ua/blog-ua/what-is-blockchain-security-examples-issues-and-solutions-ua (Дата звернення 12.05.2024)

10. Квантова криптографія. Вебсайт. URL: https://uk.wikipedia.org/wiki/Квантова_криптографія (Дата звернення 12.05.2024)

11. Оновлення освітніх програм у сфері кібербезпеки згідно з новими профстандартами: досвід та плани. Вебсайт. URL: https://cip.gov.ua/ua/news/onovlennya-osvitnikh-program-u-sferi-kiberbezpeki-zgidno-z-novimi-profstandartami-dosvid-ta-plani (Дата звернення 27.05.2024)

12. Дмитренко Т. Л., Терещенко Г. М. Підвищення рівня освіти у сфері кібербезпеки, фінансової та цифрової грамотності як чинник зниження ризиків на крипторинку. “Освітня аналітика України”. 2023. Доступно на: https://science.iea.gov.ua/wp-content/uploads/2023/05/3_Dmytrenko_Tereschenko_122_2023_38-50.pdf (Дата звернення 15.05.2024)

13. Види шифрування інформації. Вебсайт. URL: https://ua5.org/protect/395-vidi-shifruvannya-informaciyi.html (Дата звернення 19.04.2024)

14. Chidimma L.O., Mercy Benson-Emenike. Secured and Encrypted Data Transmission over the Web Using Cryptography of the Creative Commons Attribution License (CC BY 4.0). International Journal of Sustainable Development Volume. 2022. Доступно на: https://www.researchgate.net/publication/366589178_Secured_and_Encrypted_Data_Transmission_over_the_Web_Using_Cryptography_of_the_Creative_Commons_Attribution_License_CC_BY_40 (Дата звернення 06.05.2024)

15. What is TLS (Transport Layer Security)? Вебсайт. URL: https://www.cloudflare.com/learning/ssl/transport-layer-security-tls/ (Дата звернення 12.05.2024)

16. SSL/TLS Demystified: Your Ultimate Guide to Web Security. Вебсайт. URL: https://emudhra.com/blog/ssltls-demystified-your-ultimate-guide-to-web-security (Дата звернення 12.05.2024)

17. What is SSL? Вебсайт. URL: https://www.entrust.com/resources/learn/what-is-ssl (Дата звернення 12.05.2024)

18. How does SSL work? Вебсайт. URL: https://www.cloudflare.com/learning/ssl/how-does-ssl-work/ (Дата звернення 12.05.2024)

19. Best Practices for Protecting SSL/TLS Certificates and Keys. Вебсайт. URL: https://cybersecuritynews.com/protecting-ssl-tls-certificates/ (Дата звернення 12.05.2024)

20. IDS vs. IPS: Definitions, Comparisons & Why You Need Both. Вебсайт. URL: https://www.okta.com/identity-101/ids-vs-ips/ (Дата звернення 16.05.2024)

21. IDS and IPS: Understanding Similarities and Differences. Вебсайт. URL: https://www.eccouncil.org/cybersecurity-exchange/network-security/ids-and-ips-differences/ (Дата звернення 16.05.2024)

22. Intrusion Protection System (IPS) and Intrusion Detection System (IDS). Вебсайт. URL: https://www.sophos.com/en-us/cybersecurity-explained/ips-and-ids (Дата звернення 16.05.2024)

23. What's an electronic signature? Вебсайт. URL: https://www.adobe.com/sign/electronic-signatures.html (Дата звернення 05.05.2024)

24. What is a DDoS attack? Вебсайт. URL: https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/ (Дата звернення 13.05.2024)

25. What is a DDOS Attack & How to Protect Your Site. Вебсайт. URL: https://aws.amazon.com/en/shield/ddos-attack-protection/ (Дата звернення 13.05.2024)

26. What is cloud security? Вебсайт. URL: https://www.ibm.com/topics/cloud-security (Дата звернення 21.05.2024)

27. How does cloud security work? Вебсайт. URL: https://www.cloudflare.com/learning/cloud/what-is-cloud-security/ (Дата звернення 23.05.2024)

28. Cyber Attack Incidents with $1M+ in Reported Losses. Вебсайт. URL: https://sectigostore.com/blog/42-cyber-attack-statistics-by-year-a-look-at-the-last-decade/ (Дата звернення 27.05.2024)

29. A Comparison of Different Security Technologies. Вебсайт. URL: https://www.aisecuredata.com/ai-data-security-comparison-different/ (Дата звернення 27.05.2024)

30. Information security spending worldwide from 2017 to 2024, by segment. Вебсайт. URL: https://www.statista.com/statistics/790834/spending-global-security-technology-and-services-market-by-segment/ (Дата звернення 27.05.2024)

31. Security and Privacy Law. Вебсайт. URL: https://www.sciencedirect.com/topics/computer-science/security-and-privacy-law

32. Top 10 Cyber Security Benefits For Small Business. Lack Of A Security Strategy. Вебсайт. URL: https://purplesec.us/learn/cyber-security-benefits/ (Дата звернення 20.05.2024)

33. Желдак Т.А. Нечіткі множини в системах управління та прийняття рішень: навч. посіб. / Т.А. Желдак, Л.С. Коряшкіна, С.А. Ус; М-во освіти і науки України, Нац. техн. ун-т «Дніпровська політехніка». – Дніпро : НТУ «ДП», 2020, - 287-292с.

Додаток А. Відомість матеріалів кваліфікаційної роботи

№ з/п	Позначення	Найменування	Кількість аркушів	Примітки
1				
2		Документація		
3				
4	124.КР.24.09.ПЗ	Пояснювальна записка	68	Формат А4
5				
6	124.КР.24.09.ДМ	Демонстраційний матеріал		Презентація на CD-R
7				
8	124.КР.24.09.КР	Копія роботи	1	Диск CD-R
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				

					124.КР.24.09.ПЗ.			
Змін.	Аркуш	№ докум.	Підпис	Дата				
Розроб.		Степанов			**Матеріали кваліфікаційної роботи**	Літ.	Аркуш	Аркушів
К. розд.		Ус						
Керівн.		Ус				НТУ «ДП», 12; 124-21ск-1		
Н.контр.		Хом’як						
Зав. каф.		Желдак						