НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»
ФАКУЛЬТЕТ КІБЕРБЕЗПЕКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«ВДОСКОНАЛЕННЯ ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ІНТЕРНЕТ-ПРОВАЙДЕРІВ»

Виконав: здобувач 4 курсу

Рівень бакалавр

Галузь знань 12 Інформаційні технології»,

спеціальність 125 «Кібербезпека»

Марюха Віталій Григорович

Керівник: доцент, к.ф.-м.н.

Чепурна Олена Євгенівна

Рецензент: доцент, к.т.н.

Бойко Віктор Дмитрович

Одеса – 2024

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»

Факультет **кібербезпеки та інформаційних технологій**
Кафедра **кібербезпеки**
Галузь знань: **12 Інформаційні технології**
Спеціальність: **125 Кібербезпека**
Назва освітньої програми: **Кібербезпека**

ЗАТВЕРДЖУЮ
Завідувач кафедри кібербезпеки
професор С.А. Горбаченко
_____ «____ »_____ 2024 року

З А В Д А Н Н Я
на кваліфікаційну (бакалаврську) роботу
здобувачу Марюсі Віталієві Григоровичу

1. Тема роботи: «Оцінка інтелектуальних систем виявлення загроз кібербезпеки»
Керівник роботи: к.ф-м.н, доцент Чепурна Олена Євгенівна
затверджені наказом НУ ОЮА від «02» квітня 2024 року № 809-06
2. Строк подання здобувачем роботи «20» травня 2024 року
3. Дата видачі завдання«15» вересня 2024 року

КАЛЕНДАРНИЙ ПЛАН

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

Здобувач _____
(підпис) (прізвище та ініціали)

Керівник роботи _____
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Кваліфікаційна робота на тему «Вдосконалення політики інформаційної безпеки інтернет-провайдерів» на здобуття першого (бакалаврського) рівня вищої освіти за спеціальністю 125 Кібербезпека, освітньою програмою: Кібербезпека.

Містить 4 рисунків, 20 літературних джерел за переліком посилань. Робота виконана на 48 сторінках загального тексту і 41 сторінках основного тексту.

Метою роботи є розробка і впровадження ефективних заходів та стратегій для вдосконалення політики інформаційної безпеки інтернет-провайдерів.

Об’єктом дослідження є системи та інфраструктура інформаційної безпеки, які використовуються інтернет-провайдерами для захисту даних і забезпечення безперебійного функціонування мережевих сервісів.

Предмет дослідження є політика інформаційної безпеки інтернет-провайдерів, включаючи існуючі методи і засоби захисту, нормативно-правову базу, а також процеси та процедури, які впливають на рівень захищеності інформаційних ресурсів.

Результати дослідження допоможуть інтернет-провайдерам відповідати вимогам міжнародних стандартів та нормативних документів у сфері інформаційної безпеки. Забезпечення високого рівня інформаційної безпеки безпосередньо вплине на якість надання послуг користувачам, зменшення кількості інцидентів покращить загальний досвід користувачів, сприяючи зростанню їх довіри та задоволеності.

Можливі напрями подальших досліджень щодо вдосконалення політики інформаційної безпеки інтернет-провайдерів можуть охоплювати вивчення ефективності технічних засобів захисту мережевих інфраструктур, аналіз інноваційних стратегій захисту від кіберзагроз, дослідження ролі регулювальних органів у забезпеченні безпеки мережевих послуг.

ІНФОРМАЦІЙНА БЕЗПЕКА, ІНТЕРНЕТ-ПРОВАЙДЕРИ, КІБЕРЗАХИСТ, ТЕХНІЧНІ ЗАСОБИ ЗАХИСТУ, РЕГУЛЮВАЛЬНІ ОРГАНИ

ABSTRACT

Qualification work on the topic ‘Improving the information security policy of Internet providers’ for the first (bachelor's) level of higher education in the specialty 125 Cybersecurity, educational programme: Cybersecurity.

Contains 4 figures, 20 references according to the list of references. The work is executed on 48 pages of the general text and 41 pages of the main text.

The purpose of the work is to develop and implement effective measures and strategies to improve the information security policy of Internet service providers.

The object of the study is the information security systems and infrastructure used by Internet service providers to protect data and ensure the smooth operation of network services.

The subject of the study is the information security policy of Internet service providers, including existing methods and means of protection, the regulatory framework, as well as processes and procedures that affect the level of security of information resources.

The results of the study will help Internet service providers to meet the requirements of international standards and regulations in the field of information security. Ensuring a high level of information security will directly affect the quality of service provided to users, while reducing the number of incidents will improve the overall user experience, contributing to the growth of their trust and satisfaction.

Possible areas for further research on improving the information security policy of ISPs may include studying the effectiveness of technical means of protecting network infrastructures, analysing innovative strategies for protecting against cyber threats, and investigating the role of regulatory authorities in ensuring the security of network services.

INFORMATION SECURITY, INTERNET PROVIDERS, CYBER DEFENCE, TECHNICAL MEANS OF PROTECTION, REGULATORY AUTHORITIES

ЗМІСТ

ВСТУП

Актуальність теми. У сучасному світі, де інформація є одним з найбільш цінних ресурсів, забезпечення її безпеки стає першочерговим завданням для будь-якої організації. Інтернет-провайдери відіграють ключову роль у забезпеченні доступу до інформації, тому їх політика інформаційної безпеки має бути максимально ефективною. Останні роки свідчать про зростання кількості кіберзагроз, атак на інфраструктуру провайдерів, витоків конфіденційних даних, що робить тему вдосконалення політики інформаційної безпеки надзвичайно важливою.

Незадовільний рівень інформаційної безпеки може призвести до значних фінансових втрат для провайдерів та їх клієнтів, підриву репутації компаній та втрати довіри споживачів. Захист інформаційних ресурсів є важливою складовою національної безпеки, оскільки відсутність належних заходів може призвести до дестабілізації критичної інфраструктури, включаючи фінансову, енергетичну та комунікаційну галузі.

Дослідження в галузі вдосконалення політики інформаційної безпеки інтернет-провайдерів сприяють розробці нових методик та підходів до захисту інформації. Це може включати впровадження сучасних технологій шифрування, розробку політик щодо захисту від DDoS-атак, систем виявлення та запобігання вторгненням, а також підвищення рівня обізнаності персоналу щодо загроз інформаційної безпеки.

Мета дослідження є розробка і впровадження ефективних заходів та стратегій для вдосконалення політики інформаційної безпеки інтернет-провайдерів з метою забезпечення надійного захисту інформаційних ресурсів та мінімізації ризиків кіберзагроз.

Для досягнення поставленої мети в роботі було визначено **завдання**, які потрібно виконати:

- дослідити сутність та значення інформаційної безпеки;
- визначити сучасні методи та технології захисту інформації;

- виявити недоліки та проблеми в існуючих політиках інформаційної безпеки провідних інтернет-провайдерів;
- розробити заходи та стратегї для підвищення рівня захисту інформаційних систем;
- скласти методи впровадження сучасних технологій захисту інформації.

Об'єктом дослідження є системи та інфраструктура інформаційної безпеки, які використовуються інтернет-провайдерами для захисту даних і забезпечення безперебійного функціонування мережевих сервісів.

Предмет дослідження є політика інформаційної безпеки інтернет-провайдерів, включаючи існуючі методи і засоби захисту, нормативно-правову базу, а також процеси та процедури, які впливають на рівень захищеності інформаційних ресурсів.

Практичне значення отриманих результатів. провадження розроблених у рамках дослідження заходів та стратегій дозволить значно зменшити ймовірність успішних кібер-атак, витоків конфіденційних даних та інших інцидентів, пов'язаних з інформаційною безпекою.

Оптимізація ресурсів є ще одним важливим аспектом, оскільки розроблені методи та засоби сприятимуть більш ефективному використанню як технічних (сервери, мережеве обладнання), так і людських (персонал, відповідальний за інформаційну безпеку) ресурсів інтернет-провайдерів. Це забезпечить краще управління ресурсами та зменшить витрати на їхнє обслуговування.

Також результати дослідження допоможуть інтернет-провайдерам відповідати вимогам міжнародних стандартів та нормативних документів у сфері інформаційної безпеки. Це, в свою чергу, відкриє нові можливості для міжнародного співробітництва та залучення іноземних клієнтів, що підвищить їх конкурентоспроможність на ринку. Забезпечення високого рівня інформаційної безпеки безпосередньо вплине на якість надання послуг користувачам, зменшення кількості інцидентів покращить загальний досвід користувачів, сприяючи зростанню їх довіри та задоволеності..

1 ТЕОРЕТИЧНІ ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1 Сутність та значення інформаційної безпеки

У цифрову епоху, коли інформація безперешкодно поширюється по всьому світу, безпека даних стала першочерговим завданням. Безмежні простори кіберпростору, пропонуючи безпрецедентні можливості для інновацій та зв'язку, водночас представляють собою ландшафт, сповнений ризиків та вразливостей. Загрози інформаційній безпеці всюдисущі та постійно змінюються - від витончених кібератак, організованих зловмисниками, до ненавмисного витоку даних, спричиненого людською помилкою.

Сьогодні організації стоять на перехресті величезного технологічного прогресу і складних викликів у сфері безпеки. Захист конфіденційної інформації є не просто технічною необхідністю, а критично важливим компонентом підтримки довіри, дотримання нормативних вимог та безперервності роботи. Оскільки бізнес, уряди та приватні особи все більше покладаються на цифрову інфраструктуру, необхідність захисту інформаційних активів є як ніколи актуальною.

Цей розділ заглиблюється в суть і важливість інформаційної безпеки, надаючи всебічне дослідження її основних принципів, багатогранних викликів, які вона вирішує, та її незамінної ролі в сучасному суспільстві. Він слугує життєво важливим дискурсом про те, чому інформаційна безпека має бути пріоритетом і як організації можуть стратегічно зміцнити свій захист у взаємопов'язаному світі [1].

Інформаційна безпека є критично важливим аспектом сучасного цифрового суспільства, слугуючи наріжним каменем захисту цілісності, конфіденційності та доступності даних. В епоху, що характеризується безпрецедентною цифровою трансформацією, захист інформаційних систем від несанкціонованого доступу, збоїв і порушень набуває першочергового значення. Цей розділ заглиблюється в суть і значення інформаційної безпеки, досліджуючи

її фундаментальні принципи, виклики, які вона вирішує, і її незамінну роль в сучасних організаціях.

Інформаційна безпека охоплює широкий спектр практик, технологій і політик, спрямованих на захист інформаційних активів від різних загроз. Вона передбачає реалізацію заходів, спрямованих на запобігання несанкціонованому доступу, використанню, розголошенню, порушенню, модифікації або знищенню інформації. Основні цілі інформаційної безпеки часто описують у вигляді тріади ЦРУ: Конфіденційність, Цілісність і Доступність.

1. Конфіденційність - забезпечує доступ до інформації лише тим, хто має на це право. Заходи для досягнення конфіденційності включають шифрування, контроль доступу та протоколи автентифікації.
2. Цілісність - передбачає збереження точності та повноти даних. Це досягається за допомогою таких механізмів, як хешування, цифрові підписи та надійні процеси аудиту, які допомагають виявляти та запобігати несанкціонованим змінам.
3. Доступність - гарантує, що інформація та ресурси будуть доступні авторизованим користувачам у разі потреби. Резервування, відмовостійкість та плани аварійного відновлення є важливими компонентами для забезпечення безперервного доступу до критично важливої інформації [2].

Значення інформаційної безпеки неможливо переоцінити, враховуючи її критичну роль у захисті активів окремих осіб, організацій та держав. Ключові причини, які підкреслюють важливість інформаційної безпеки описано в таблиці 1.1.

Таблиця 1.1 – Ключові аспекти важливості інформаційної безпеки [3]

№	Аспект	Опис
1.	Захист чутливої інформації	організації в різних секторах, включаючи охорону здоров'я, фінанси та уряд, працюють з конфіденційними даними, такими як особиста інформація, фінансова звітність та інтелектуальна власність. Ефективні заходи інформаційної безпеки є життєво важливими для запобігання

		витоку даних, що може призвести до крадіжки особистих даних, фінансових втрат та шкоди репутації.
2.	Відповідність та юридичні зобов'язання	багато галузей підпадають під дію суворих регуляторних вимог щодо захисту даних. Дотримання таких стандартів, як Загальний регламент про захист даних (GDPR), Закон про переносимість і підзвітність у сфері медичного страхування (HIPAA) та Стандарт безпеки даних індустрії платіжних карток (PCI DSS), має важливе значення для уникнення юридичних санкцій і збереження довіри клієнтів.
3.	Безперервність та стійкість бізнесу	інформаційна безпека є невід'ємною частиною забезпечення безперервності бізнесу. Кібератаки, стихійні лиха та інші непередбачувані події можуть серйозно вплинути на діяльність. Впроваджуючи комплексні заходи безпеки, організації можуть підвищити свою стійкість і здатність швидко відновлюватися після інцидентів, тим самим мінімізуючи час простою і фінансові втрати.
4.	Захист інтелектуальної власності	для багатьох підприємств інтелектуальна власність (ІВ) становить значну частину їхньої вартості. Захист ІВ від кібершпигунства та крадіжок має вирішальне значення для збереження конкурентної переваги та сприяння інноваціям.
5.	Управління довірою та репутацією	довіра є фундаментальним елементом відносин з клієнтами. Порушення безпеки може підірвати довіру клієнтів і зашкодити репутації організації. Демонстрація прихильності до надійних практик інформаційної безпеки допомагає будувати та підтримувати довіру з клієнтами, партнерами та зацікавленими сторонами.

Незважаючи на свою важливість, інформаційна безпека стикається з численними викликами в сучасному складному цифровому ландшафті, що швидко розвивається.

Еволюція ландшафту загроз – кіберзагрози постійно розвиваються, а зловмисники застосовують все більш витончені методи. Щоб бути на крок попереду цих загроз, потрібна постійна пильність, регулярне оновлення протоколів безпеки та інвестиції в передові технології виявлення загроз і реагування на них.

Людський фактор – людські помилки залишаються значною вразливістю в інформаційній безпеці. Фішингові атаки, слабкі паролі та ненавмисні витоки даних через недбалість є поширеними проблемами. Безперервна освіта та

навчальні програми мають важливе значення для підвищення обізнаності та формування культури безпеки.

Технологічна складність – поширення взаємопов'язаних пристроїв і систем, в тому числі Інтернету речей (IoT), хмарних обчислень і мобільних технологій, розширило поле для атак. Управління безпекою в різноманітних і складних середовищах створює значні виклики.

Обмеженість ресурсів – багато організацій, особливо малі та середні підприємства (МСП), стикаються з обмеженими ресурсами з точки зору бюджету та експертизи. Баланс між потребою в комплексних заходах безпеки та обмеженими ресурсами вимагає стратегічного планування та визначення пріоритетів.

Дотримання нормативних вимог – орієнтуватися в складному ландшафті регуляторних вимог може бути непросто. Організації повинні забезпечити дотримання різних законів і стандартів, що часто вимагає значних інвестицій в інфраструктуру та процеси безпеки.

Щоб вирішити ці проблеми та захистити інформаційні активи, організації повинні прийняти цілісний та проактивний підхід до інформаційної безпеки. Стратегії такого підходу включають наступні пункти з зображення 1.1.

1. Оцінка та управління ризиками - проводьте регулярну оцінку ризиків для виявлення вразливостей та потенційних загроз. Розробляти та впроваджувати плани управління ризиками для пом'якшення виявлених ризиків.

2. Політика та процедури безпеки - розробити комплексну політику та процедури безпеки, які визначають ролі, обов'язки та інструкції щодо захисту інформації. Регулярно переглядайте та оновлюйте ці політики, щоб адаптуватися до мінливих загроз і потреб бізнесу.

3. Передові технології безпеки - інвестуйте в передові технології безпеки, такі як брандмауери, системи виявлення вторгнень, шифрування та багатофакторна автентифікація. Використовуйте штучний інтелект і машинне навчання для покращення виявлення загроз і реагування на них.

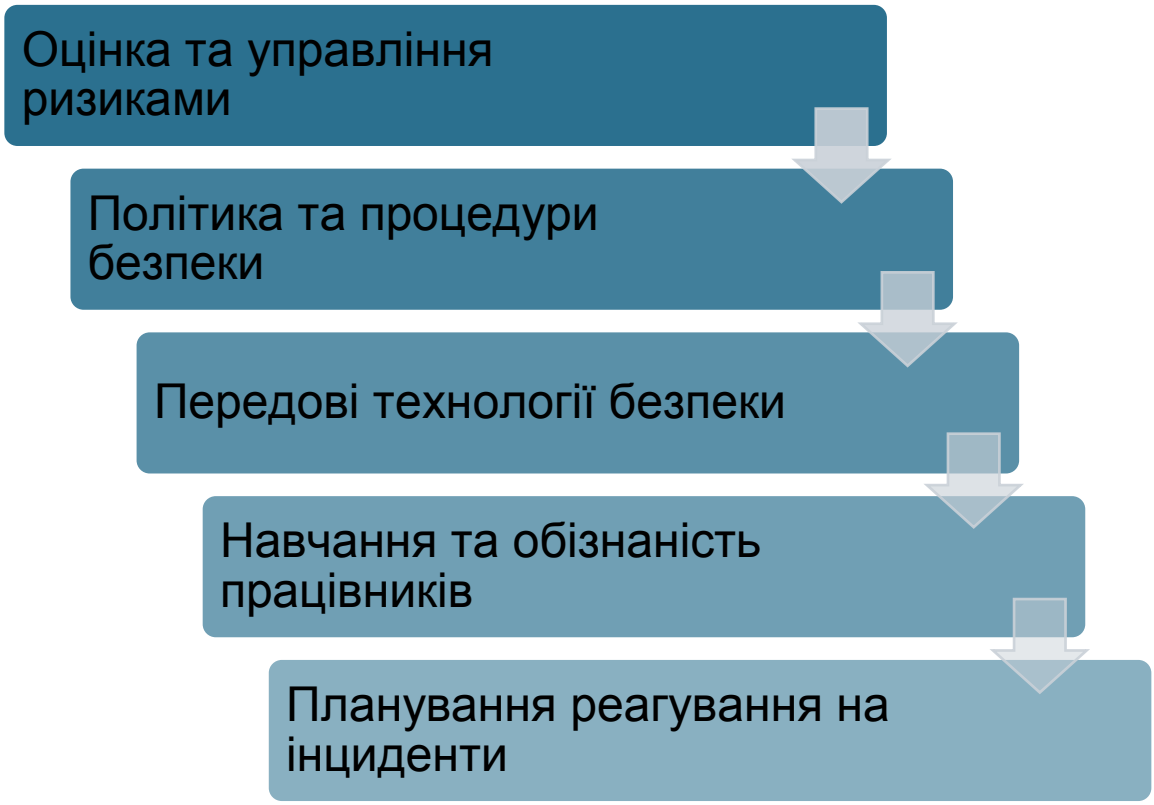

Рисунок 1.1 Стратегії вирішення проблем безпеки інформації [4]

4. Навчання та обізнаність працівників - впроваджуйте безперервні навчальні програми для ознайомлення працівників з найкращими практиками безпеки, загрозами соціальної інженерії та важливістю дотримання політик безпеки. Сприяти формуванню організаційної культури, орієнтованої на безпеку.

5. Планування реагування на інциденти - розробити та регулярно тестувати плани реагування на інциденти для забезпечення швидкого та ефективного реагування на інциденти безпеки. Встановіть чіткі канали зв'язку та розподіліть ролі для управління інцидентами.

Співпраця та обмін інформацією - співпрацюйте та обмінюйтеся інформацією з колегами по галузі, державними установами та організаціями з кібербезпеки. Обмін розвідданими про загрози та найкращими практиками може посилити колективні зусилля з безпеки.

Інформаційна безпека є фундаментальним компонентом сучасної організаційної стратегії, необхідним для захисту конфіденційних даних, забезпечення відповідності нормативним вимогам і підтримки безперервності

бізнесу. Оскільки кіберзагрози продовжують розвиватися, організації повинні застосовувати проактивний і комплексний підхід до безпеки, використовуючи передові технології, надійні політики і безперервну освіту. Надаючи пріоритет інформаційній безпеці, організації можуть захистити свої активи, зберегти довіру та забезпечити довгострокову стійкість у світі, що стає все більш цифровим.

Інформаційна безпека є важливим стовпом сучасного цифрового суспільства, що захищає цілісність, конфіденційність і доступність життєво важливих даних. Оскільки кіберзагрози продовжують розвиватися, а цифровий ландшафт стає все більш складним, організації повинні вживати проактивних і комплексних заходів безпеки. Надаючи пріоритет управлінню ризиками, використовуючи передові технології, розвиваючи культуру безпеки та забезпечуючи відповідність нормативним стандартам, організації можуть захистити свої інформаційні активи, зберегти довіру та забезпечити безперервність бізнесу. У світі, де дані є критично важливим активом, надійні практики інформаційної безпеки є незамінними для довгострокової стійкості та успіху.

1.2 Огляд сучасних методів та технологій захисту інформації

Забезпечення безпеки конфіденційних даних і збереження цілісності інформаційних систем вимагає застосування складних методів і новітніх технологій. У цьому розділі ми детально розглянемо сучасні методи та технології інформаційної безпеки, висвітлимо їх значення, функціональність та застосування у захисті даних і систем.

Криптографія є основою інформаційної безпеки, забезпечуючи захист даних за допомогою різних методів шифрування та безпечних протоколів зв'язку. Сучасна криптографія забезпечує конфіденційність, цілісність даних та автентифікацію, що робить її незамінною для захисту конфіденційної інформації [5].

Симетричне шифрування, таке як Advanced Encryption Standard (AES), використовує один і той самий ключ для шифрування і розшифрування, що робить його високоефективним для шифрування великих обсягів даних. Наприклад, наступний код на Python демонструє використання шифрування AES за допомогою бібліотеки `pycryptodome`[6]:

```python
з Crypto.Cipher import AES
from Crypto.Random import get_random_bytes
Згенерувати випадковий 16-байтовий ключ
key = get_random_bytes(16)
# Створити об'єкт шифру з використанням ключа
cipher = AES.new(key, AES.MODE_EAX)
# Зашифрувати дані
data = b'Secret Data'
nonce = cipher.nonce
ciphertext, tag = cipher.encrypt_and_digest(data)
print(f «Ключ: {key.hex()}»)
print(f «Nonce: {nonce.hex()}»)
print(f «Ciphertext: {ciphertext.hex()}»)
print(f «Тег: {tag.hex()}»)```
```

Асиметричне шифрування передбачає використання пари ключів - відкритого ключа для шифрування і закритого ключа для розшифрування, що забезпечує надійне рішення для безпечного обміну ключами і цифрових підписів. RSA є широко використовуваним асиметричним алгоритмом. Наступний код на Python демонструє використання шифрування RSA за допомогою бібліотеки `PyCryptodome`:

```python
from Crypto.PublicKey import RSA
from Crypto.Cipher import PKCS1_OAEP
# Згенерувати RSA-ключі
key = RSA.generate(2048)
public_key = key.publickey()
# Зашифрувати дані
cipher = PKCS1_OAEP.new(public_key)
ciphertext = cipher.encrypt(b'Secret Data')
```

```
    # Розшифрувати дані
    decipher = PKCS1_OAEP.new(key)
    plaintext = decipher.decrypt(ciphertext)
    print(f «Шифротекст: {ciphertext.hex()}»)
    print(f «Відкритий текст: {відкритий.розшифрувати()}»)```
```

Хеш-функції, такі як SHA-256, генерують хеш-значення фіксованого розміру з вхідних даних, забезпечуючи цілісність даних шляхом виявлення будь-яких змін. Наступний код на Python демонструє використання SHA-256 з бібліотекою `hashlib`:

```
    ```python
    import hashlib
    data = b'Secret Data'
    hash_object = hashlib.sha256(data)
    hex_dig = hash_object.hexdigest()
    print(f «SHA-256 Хеш: {hex_dig}»)```
```

На зображені 1.2 можливо побачити роботу алгоритму SHA-256. Цифрові підписи, створені за допомогою асиметричних алгоритмів шифрування, забезпечують автентифікацію і неспростування, гарантуючи, що походження і цілісність повідомлення або документа можуть бути перевірені [7].

Мережева безпека має вирішальне значення для запобігання несанкціонованому доступу та забезпечення безпечної передачі даних через мережі. Для захисту мережевої інфраструктури від широкого спектру загроз використовуються різні технології та методології.
```

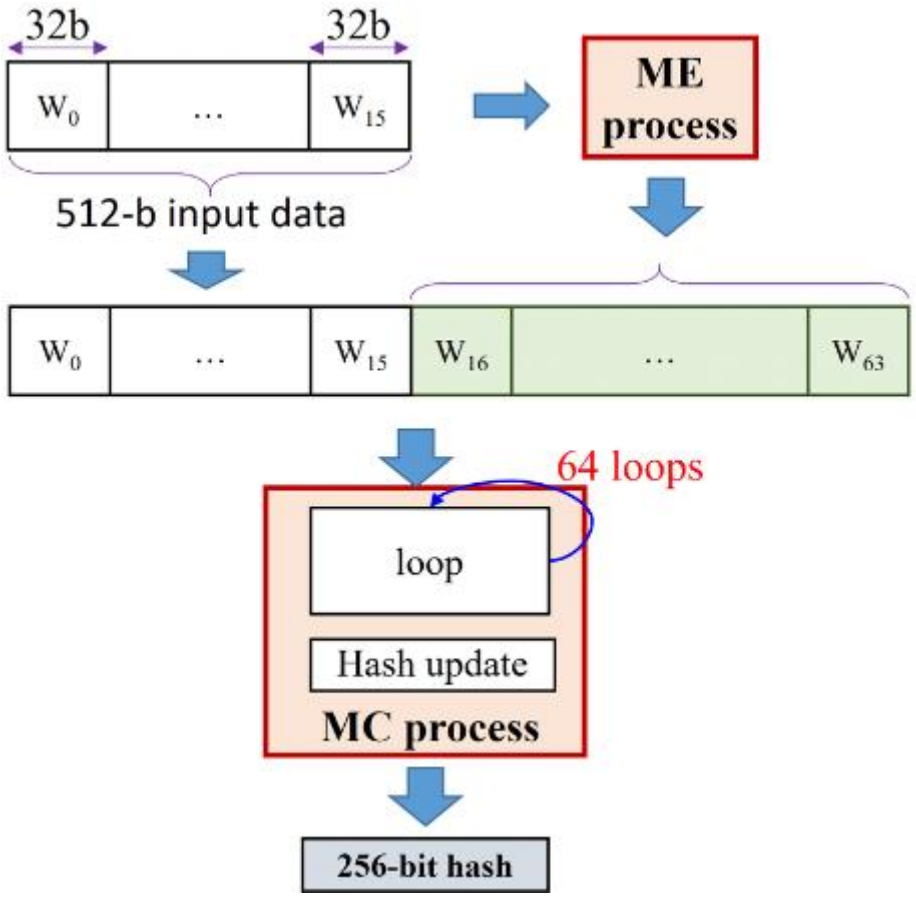

Рисунок 1.2 – Принцип роботи алгоритму SHA-256

Брандмауери слугують бар'єрами між довіреними та недовіреними мережами, регулюючи трафік на основі заздалегідь визначених правил безпеки. Вони можуть бути апаратними, програмними або комбінованими, і мають важливе значення для захисту внутрішніх мереж від зовнішніх загроз.

Системи виявлення та запобігання вторгнень (IDPS) відіграють ключову роль у моніторингу мережевого трафіку на предмет підозрілих дій. Нижче наведено приклад налаштування Snort, системи виявлення мережевих вторгнень з відкритим вихідним кодом [8]:

```hell
# Встановлення Snort
sudo apt-get install snort
# Налаштування Snort
sudo vi /etc/snort/snort.conf
# Додайте діапазон мережі для моніторингу
ipvar HOME_NET 192.168.1.0/24
```

```
    # Запустіть Snort в режимі IDS
    sudo snort -A console -i eth0 -c
/etc/snort/snort.conf```
```

Віртуальні приватні мережі (VPN) створюють безпечні, зашифровані з'єднання через загальнодоступні мережі, надаючи віддалений доступ до ресурсів організації, забезпечуючи при цьому конфіденційність і цілісність даних. Наступний приклад демонструє, як налаштувати сервер OpenVPN:

```
```hell
# Встановлення OpenVPN
sudo apt-get install openvpn easy-rsa
# Налаштуйте каталог центрів сертифікації
make-cadir ~/openvpn-ca
cd ~/openvpn-ca
# Створіть центр сертифікації
вихідні параметри
./clean-all
./build-ca
# Згенеруйте ключ і сертифікат сервера
./build-key-server server
# Згенеруйте клієнтський ключ і сертифікат
./build-key client1
# Згенерувати параметри Діффі-Хеллмана
./build-dh
# Запуск сервера OpenVPN
sudo openvpn --config /etc/openvpn/server.conf```
```

Кінцеві пристрої, включаючи ноутбуки, смартфони та планшети, часто стають мішенню кіберзагроз через їх широке використання та різний рівень захисту. Сучасні рішення для захисту кінцевих точок покликані захистити ці пристрої від безлічі загроз.

Антивірусні та антишкідливі програми виявляють і видаляють шкідливе програмне забезпечення з кінцевих точок. Передові рішення використовують евристичні та поведінкові методи виявлення раніше невідомих загроз, пропонуючи комплексний захист від шкідливого програмного забезпечення.
```

Endpoint Detection and Response (EDR) забезпечує безперервний моніторинг та аналіз активності кінцевих точок, виявляючи та реагуючи на сучасні загрози. Приклад налаштування інструменту EDR з відкритим вихідним кодом, OSSEC, наведено нижче [9]:

```командний рядок
# Встановлення OSSEC
sudo apt-get install ossec-hids
# Налаштуйте OSSEC
sudo vi /var/ossec/etc/ossec.conf
# Запуск OSSEC
sudo /var/ossec/bin/ossec-control start```

Керування мобільними пристроями (MDM) забезпечує захист, моніторинг і керування мобільними пристроями в організації. Рішення MDM застосовують політики безпеки, керують конфігураціями пристроїв і забезпечують захист даних на мобільних кінцевих точках, що робить їх необхідними в епоху віддаленої роботи і політики BYOD (Bring Your Own Device).

Білі списки додатків обмежують запуск на кінцевих точках лише попередньо схвалених додатків, що значно знижує ризик зараження шкідливим програмним забезпеченням і несанкціонованого встановлення програмного забезпечення. Контролюючи, які програми можна запускати, організації можуть краще захистити свої системи від небажаного або шкідливого програмного забезпечення.

Ефективне управління ідентифікацією користувачів і правами доступу має вирішальне значення для забезпечення доступу до конфіденційної інформації та систем лише уповноваженим особам. Управління ідентифікацією та доступом (IAM) охоплює низку технологій і практик, призначених для захисту та управління цифровими ідентифікаційними даними.

Багатофакторна автентифікація (MFA) підвищує безпеку, вимагаючи від користувачів надання двох або більше факторів перевірки для отримання доступу до системи. До загальних факторів належать: те, що користувач знає
```

(пароль), те, що користувач має (маркер безпеки), і те, ким є користувач (біометрична перевірка). MFA значно знижує ризик несанкціонованого доступу, додаючи кілька рівнів перевірки.

Єдиний вхід (Single Sign-On, SSO) покращує користувацький досвід і безпеку, дозволяючи користувачам автентифікуватися один раз і отримати доступ до декількох систем без необхідності входити в кожну з них окремо. Це зменшує навантаження на управління декількома паролями та мінімізує проблеми безпеки, пов'язані з паролями [10].

Контроль доступу на основі ролей (RBAC) надає права доступу на основі ролей користувачів в організації, гарантуючи, що користувачі мають мінімальний рівень доступу, необхідний для виконання своїх робочих функцій. Це відповідає принципу найменших привілеїв, зменшуючи ризик внутрішніх загроз і випадкового витоку даних.

Identity Governance and Administration (IGA) забезпечує нагляд і управління ідентифікаційними даними користувачів і правами доступу в організації. Рішення IGA полегшують управління життєвим циклом ідентичностей, перевірку доступу та звітність про відповідність, гарантуючи, що права доступу призначаються та управляються належним чином.

З широким розповсюдженням хмарних обчислень захист хмарних середовищ став критично важливим аспектом інформаційної безпеки. Хмарна безпека охоплює цілий ряд технологій і практик, призначених для захисту даних і додатків у хмарі.

Брокери безпеки хмарного доступу (CASB) виступають посередниками між користувачами хмарних сервісів і провайдерами, забезпечуючи дотримання політик безпеки та прозорість використання хмарних сервісів. CASB пропонують такі функції, як запобігання втраті даних (DLP), захист від загроз і моніторинг відповідності, допомагаючи організаціям захистити свої хмарні середовища.

Шифрування в хмарі захищає дані, що зберігаються та обробляються в хмарних середовищах. Хмарне шифрування можна застосовувати до даних у

стані спокою, під час передачі та використання, забезпечуючи комплексний захист даних. Шифруючи конфіденційну інформацію, організації можуть зменшити ризик витоку даних і забезпечити відповідність нормативним вимогам.

Платформи захисту хмарних робочих навантажень (CWPP) захищають хмарні робочі навантаження, включаючи віртуальні машини, контейнери та безсерверні функції. Рішення CWPP пропонують такі функції, як управління вразливостями, захист під час виконання та контроль додатків, забезпечуючи безпеку та стійкість хмарних додатків до атак.

Управління ідентифікацією та доступом (IAM) у хмарі поширює традиційні практики IAM на хмарні середовища, забезпечуючи безпечний доступ до хмарних ресурсів. Хмарні рішення IAM інтегруються з локальними системами IAM і підтримують об'єднане управління ідентичностями, забезпечуючи безперебійну та безпечну роботу користувачів.

Швидкий темп технологічних інновацій продовжує впроваджувати нові методи і технології для посилення інформаційної безпеки. Нові технології відкривають великі перспективи для розвитку сфери кібербезпеки та протидії новим загрозам.

Штучний інтелект (ШІ) і машинне навчання (МН) все частіше використовуються в кібербезпеці для виявлення загроз і реагування на них. Ці технології аналізують величезні обсяги даних для виявлення закономірностей і аномалій, що дозволяє проактивно виявляти загрози і автоматично реагувати на них. Безпекові рішення на основі AI/ML можуть адаптуватися до нових загроз у режимі реального часу, пропонуючи динамічний і стійкий захист.

Технологія блокчейн пропонує децентралізовані та захищені від несанкціонованого доступу реєстри для безпечного зберігання даних і перевірки транзакцій. Блокчейн досліджується для таких застосувань, як безпечне управління ідентифікацією та цілісність ланцюгів поставок, забезпечуючи прозорі та незмінні записи, що підвищують безпеку та довіру.

Архітектура нульової довіри виступає за модель безпеки, в якій жодному об'єкту, як всередині, так і поза мережею, не довіряють за замовчуванням. Принципи Zero Trust включають безперервну перевірку, доступ з найменшими привілеями та мікросегментацію, щоб зменшити поверхню атаки та обмежити бічний рух. Припускаючи, що загрози можуть існувати як всередині, так і поза мережею, архітектура нульової довіри забезпечує надійну основу для сучасної кібербезпеки.

Квантова криптографія використовує принципи квантової квантової механіки для розробки нових криптографічних методів, які теоретично стійкі до квантових комп'ютерних атак. Квантовий розподіл ключів (QKD) є одним з найбільш перспективних застосувань квантової криптографії, що дозволяє безпечно обмінюватися криптографічними ключами з високим рівнем захисту [11].

Сучасні методи і технології інформаційної безпеки необхідні для захисту конфіденційних даних і забезпечення цілісності, конфіденційності та доступності інформаційних систем. Використовуючи поєднання передових криптографічних методів, надійних заходів захисту мережі та кінцевих точок, комплексних практик IAM та інноваційних рішень для захисту хмарних технологій, організації можуть ефективно знизити ризики, пов'язані з постійно мінливим ландшафтом загроз. Оскільки нові технології, такі як штучний інтелект, блокчейн і квантова криптографія, продовжують з'являтися, відстеження цих досягнень буде мати вирішальне значення для підтримки стійкої системи безпеки в цифрову епоху.

2 АНАЛІЗ ІСНУЮЧИХ ПІДХОДІВ ДО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ІНТЕРНЕТ-ПРОВАЙДЕРІВ

2.1 Виявлення недоліків та проблем в існуючих політиках інформаційної безпеки

Незважаючи на свою важливість, багато існуючих політик інформаційної безпеки мають недоліки, які ставлять під загрозу їхню ефективність. Ці прогалини можуть зробити організації вразливими до безлічі загроз - від кібератак і витоків даних до інсайдерських загроз і збоїв у дотриманні нормативних вимог. Швидка еволюція ландшафту загроз у поєднанні зі складною взаємодією технологій, людської поведінки та організаційних процесів вимагає постійної переоцінки та вдосконалення цих політик.

Розпочинаючи це дослідження, важливо визнати, що ефективність політики інформаційної безпеки залежить не лише від її розробки, але й від її впровадження та дотримання. Цей комплексний аналіз має на меті надати ідеї та рекомендації, які сприятимуть розробці більш цілісних, динамічних та ефективних політик безпеки, що в кінцевому підсумку підвищить здатність організації захищатися від загроз цифрового світу, які постійно змінюються [12].

Політика інформаційної безпеки є життєво важливою для захисту конфіденційності, цілісності та доступності даних в організації. Однак, незважаючи на їхню важливість, багато існуючих політик мають прогалини та проблеми, які можуть поставити під загрозу їхню ефективність. Дослідження цих недоліків та надання всебічного аналізу допоможуть розробити більш надійні та ефективні політики інформаційної безпеки. Розглянемо основні проблеми політик інформаційної безпеки в рисунку 2.1.

Однією з найбільш значних прогалин в існуючих політиках інформаційної безпеки є відсутність всебічного охоплення. Багато політик зосереджуються переважно на певних аспектах безпеки, таких як мережева безпека або шифрування даних, нехтуючи при цьому іншими критично важливими сферами. Наприклад, фізична безпека, безпека персоналу та реагування на інциденти часто

залишаються без належної уваги. Такий вузький фокус може зробити організації вразливими до різних загроз, які не охоплюються існуючими політиками.

Рисунок 2.1 Основні проблеми політик інформаційної безпеки [13]

Ще однією поширеною проблемою є недостатня увага до навчання та обізнаності працівників. Навіть найбільш ретельно розроблені політики можуть виявитися неефективними, якщо працівники не мають достатньої підготовки для їх розуміння та впровадження. Багато організацій не проводять регулярних, актуальних тренінгів або не створюють культуру обізнаності з питань безпеки серед персоналу. Такий брак навчання може призвести до людських помилок, які є значним джерелом порушень безпеки.

Швидкі темпи технологічного прогресу означають, що загрози інформаційній безпеці постійно розвиваються. Однак багато організацій не оновлюють свої політики безпеки достатньо часто, щоб встигати за цими змінами. Застарілі політики можуть не протидіяти новим типам загроз, таким як сучасні постійні загрози (APT) або вразливості «нульового дня», залишаючи організації вразливими до сучасних кіберризиків.

Ефективне реагування на інциденти та управління ними мають вирішальне значення для пом'якшення наслідків порушень безпеки. На жаль, багато політик інформаційної безпеки не містять детальних, дієвих планів реагування на

інциденти. Така непідготовленість може призвести до запізнілого реагування, що посилює шкоду, завдану інцидентами безпеки. Політики часто не визначають чітких ролей та обов'язків щодо реагування на інциденти, що призводить до плутанини та неефективності у критичні моменти.

Політика інформаційної безпеки повинна бути узгоджена із загальними бізнес-цілями організації. Однак, часто існує розрив між політиками безпеки та бізнес-цілями. Така невідповідність може призвести до того, що заходи безпеки будуть або занадто слабкими, або занадто обмежувальними, що перешкоджатиме бізнес-операціям та інноваціям. Збалансований підхід, який інтегрує безпеку з бізнес-цілями, має важливе значення для досягнення оптимального захисту без шкоди для продуктивності.

Управління ризиками є фундаментальним компонентом інформаційної безпеки, проте багато політик не приділяють йому належної уваги. Ефективне управління ризиками передбачає виявлення, оцінку та визначення пріоритетності ризиків з подальшим впровадженням відповідних засобів контролю. Однак багатьом організаціям бракує системного підходу до управління ризиками, що призводить до невиявлених вразливостей і недостатніх стратегій зменшення ризиків.

Контроль доступу є критично важливим аспектом інформаційної безпеки, який гарантує, що лише уповноважені особи мають доступ до конфіденційних даних та систем. Незважаючи на його важливість, багато політик мають слабкі заходи контролю доступу, такі як неадекватні методи автентифікації або недостатньо деталізовані дозволи на доступ. Слабкий контроль доступу може призвести до несанкціонованого доступу, витоку даних та внутрішніх загроз.

Організації часто покладаються на сторонніх постачальників різних послуг, що може створювати додаткові ризики для безпеки. Багато політик інформаційної безпеки не приділяють належної уваги управлінню безпекою сторонніх постачальників, не гарантуючи, що вони дотримуються стандартів безпеки організації. Такий недогляд може призвести до вразливостей у

ланцюжку постачання, що потенційно може поставити під загрозу загальну систему безпеки організації.

Навіть добре розроблені політики безпеки можуть зазнати невдачі, якщо їх послідовно не впроваджувати. Непослідовне впровадження може статися через відсутність механізмів моніторингу та аудиту або через відсутність наслідків за порушення політики. Така непослідовність може призвести до хибного відчуття безпеки та підвищеного ризику інцидентів безпеки [13].

Політика інформаційної безпеки повинна бути адаптована до конкретних потреб і контексту організації. Однак, багато політик є загальними і не адаптовані до унікальних ризиків та вимог організації. Відсутність кастомізації може призвести до неефективних заходів безпеки, які не захищають належним чином активи організації.

Усунення прогалин і проблем в існуючих політиках інформаційної безпеки має важливе значення для посилення захищеності організації. Забезпечуючи всебічне охоплення, регулярно оновлюючи політики, проводячи належне навчання та узгоджуючи безпеку з бізнес-цілями, організації можуть розробити більш ефективні політики безпеки. Крім того, надійне управління ризиками, суворі заходи контролю доступу, ефективне реагування на інциденти та послідовне дотримання законодавства мають вирішальне значення для захисту від загроз, що еволюціонують. Усунувши ці недоліки, організації зможуть краще захистити свої дані та системи в умовах дедалі складнішого ландшафту загроз.

В умовах невпинного технологічного прогресу сфера інформаційної безпеки продовжує розвиватися безпрецедентними темпами. Оскільки організації прагнуть використати можливості цифрової трансформації, потреба в надійних, комплексних та адаптивних політиках інформаційної безпеки ніколи не була такою гострою, як зараз. Це дослідження прогалин і проблем в існуючих політиках інформаційної безпеки підкреслює складність і виклики, з якими стикаються сучасні організації у своєму прагненні захистити конфіденційні дані та підтримати операційну цілісність.

В ході цього аналізу ми виявили численні недоліки, які ставлять під загрозу ефективність існуючих політик безпеки. Від відсутності комплексного покриття до неналежного навчання співробітників, від застарілих політик до недостатніх механізмів реагування на інциденти - слабкі місця є різноманітними та різноманітними. Ці прогалини наражають організації на цілий спектр ризиків, включаючи кібератаки, витоки даних та порушення нормативних вимог, кожен з яких може завдати значної шкоди репутації, фінансовому стану та безперервності роботи організації.

Однак визнання цих прогалин - це лише перший крок. Справжній виклик полягає в усуненні цих недоліків за допомогою стратегічних, добре обґрунтованих заходів. Це вимагає цілісного підходу, який об'єднує технологічні досягнення, людський фактор і організаційні процеси в єдину систему безпеки. Це передбачає не лише оновлення та розширення сфери дії політик безпеки, але й формування культури обізнаності з питань безпеки, забезпечення послідовного дотримання законодавства та узгодження заходів безпеки з бізнес-цілями.

Крім того, динамічний характер ландшафту загроз вимагає постійного моніторингу, оцінки та адаптації політик безпеки. Те, що сьогодні може вважатися надійним і всеосяжним, завтра може стати застарілим. Тому організації повинні займати проактивну позицію, регулярно переглядаючи та вдосконалюючи свої політики безпеки, щоб випереджати нові загрози. Це передбачає використання останніх досягнень у сфері кібербезпеки, таких як штучний інтелект, машинне навчання та передова аналітика, для покращення можливостей виявлення загроз та реагування на них.

Не менш важливим є акцент на людському факторі в організації. Ефективна інформаційна безпека - це не лише сфера діяльності IT-відділів, а колективна відповідальність, яка охоплює всі рівні організації. Комплексні навчальні програми, регулярні навчання з безпеки та чітке інформування про політику безпеки мають важливе значення для виховання пильної та обізнаної робочої сили. Надаючи працівникам знання та інструменти для розпізнавання та

реагування на загрози безпеці, організації можуть значно зменшити ризик людських помилок, які залишаються основною вразливістю.

Усуваючи ці прогалини, організації також повинні визнати важливість управління безпекою з боку третіх сторін. У взаємопов'язаній цифровій екосистемі стан безпеки сторонніх постачальників і партнерів може безпосередньо впливати на організацію.

Тому суворі процеси перевірки, чіткі вимоги до безпеки та постійний моніторинг дотримання вимог третіми сторонами є критично важливими компонентами надійної стратегії безпеки.

Підсумовуючи це дослідження, стає очевидним, що шлях до надійної інформаційної безпеки – це безперервна подорож, яка вимагає пильності, адаптивності та далекоглядного мислення. Уроки, винесені з цього аналізу, слугують дорожньою картою для організацій для зміцнення їхніх систем безпеки, зменшення ризиків та захисту цифрових активів в умовах дедалі більш мінливого кібер-ландшафту [14].

Майбутнє інформаційної безпеки, безсумнівно, принесе нові виклики та можливості. Оскільки нові технології, такі як квантові обчислення, блокчейн та Інтернет речей (IoT), змінюють цифрове середовище, організації повинні бути готовими до відповідної еволюції своїх стратегій безпеки. Застосовуючи проактивний і комплексний підхід до інформаційної безпеки, організації можуть не лише захистити себе від поточних загроз, але й побудувати стійкий фундамент для подолання невизначеностей майбутнього.

На завершення, давайте визнаємо, що хоча шлях до досконалої інформаційної безпеки може бути недосяжною метою, постійне прагнення до досконалості в практиці безпеки є необхідним і благородним прагненням.

Завдяки невпинній пильності, постійному навчанню та непохитному прагненню до вдосконалення організації можуть створити безпечне та надійне цифрове середовище, яке підтримує їхню місію та забезпечує їхній успіх у цифрову епоху.

2.2 Дослідження політик інформаційної безпеки провідних інтернет-провайдерів

Сучасна цифрова епоха значною мірою покладається на інтернет-провайдерів (ISP) у забезпеченні безпечного та надійного з'єднання. Політика інформаційної безпеки має вирішальне значення для провайдерів, оскільки вона захищає від безлічі кіберзагроз і витоків даних. У цьому розділі розглядаються політики інформаційної безпеки провідних інтернет-провайдерів, їхні сильні та слабкі сторони, а також напрямки для вдосконалення [15].

Політика інформаційної безпеки інтернет-провайдерів зазвичай охоплює кілька основних сфер: захист даних, конфіденційність користувачів, мережева безпека, реагування на інциденти та відповідність нормативним вимогам. Ці політики покликані захистити як інфраструктуру провайдерів, так і дані їхніх користувачів. Опис захисту в кожній сфері складено в таблиці 2.1.

Таблиця 2.1 Захист інформаційної безпеки інтернет-провайдерів в різних сферах [16]

Сфера	Склад	Опис
Захист даних	Шифрування	провідні провайдери використовують передові методи шифрування для захисту даних під час передачі та у стані спокою. Наприклад, Verizon використовує захист на транспортному рівні (TLS) та вдосконалений стандарт шифрування (AES) для забезпечення конфіденційності даних.
	Контроль доступу	такі провайдери, як AT&T, впроваджують суворий контроль доступу, гарантуючи, що лише уповноважений персонал має доступ до конфіденційної інформації. Це включає багатофакторну автентифікацію (MFA) та контроль доступу на основі ролей (RBAC).
Конфіденційність користувачів	Політики конфіденційності	comcast та інші великі провайдери підтримують комплексну політику конфіденційності, яка визначає, як збираються, використовуються та поширюються дані користувачів. Ці політики часто є прозорими та відповідають таким нормативним актам, як Загальний регламент про захист даних (GDPR).

	Анонімізація даних	щоб підвищити рівень конфіденційності користувачів, деякі інтернет-провайдери анонімізують дані користувачів, що ускладнює відстеження інформації до окремих користувачів.
Мережева безпека	-Брандмауери та системи виявлення вторгнень (IDS)	такі провайдери, як CenturyLink, розгортають надійні брандмауери та IDS для виявлення та запобігання несанкціонованому доступу до своїх мереж.
	Захист від DDoS-атак	розподілені атаки на відмову в обслуговуванні (DDoS) є значною загрозою. Такі провайдери, як «Чартерні комунікації», використовують передові методи захисту від DDoS-атак для підтримки доступності послуг.
Реагування на інциденти	Плани реагування на інциденти (IRP)	провідні інтернет-провайдери мають детальні плани реагування на інциденти, які визначають процедури виявлення, реагування та відновлення після інцидентів, пов'язаних з безпекою. Ці плани часто включають регулярні навчання та оновлення для адаптації до нових загроз.
	Операційні центри безпеки (SOC)	такі провайдери, як British Telecom, використовують SOC, які відстежують мережевий трафік і реагують на інциденти безпеки в режимі реального часу.
Регуляторна відповідність	Законодавчі та регуляторні вимоги	інтернет-провайдери повинні дотримуватися різних національних та міжнародних нормативних актів. Наприклад, європейські провайдери дотримуються Загального регламенту про захист даних (GDPR), а американські - правил Федеральної комісії з питань зв'язку (FCC).
	Аудити та сертифікація	регулярні аудити та сертифікації, такі як ISO/IEC 27001, проводяться для забезпечення відповідності та підвищення рівня безпеки.

Незважаючи на надійні заходи безпеки, в політиці інформаційної безпеки провідних інтернет-провайдерів є кілька прогалин і проблем:

1. Недостатня прозорість:

- Недостатня обізнаність користувачів - багато провайдерів не інформують користувачів належним чином про свою політику і практику безпеки. Така

непрозорість може підірвати довіру та залишити користувачів в невіданні щодо того, як захищаються їхні дані.

- Оновлення політики - часті оновлення політик безпеки необхідні для протидії новим загрозам, але провайдери часто не повідомляють про ці зміни своїм користувачам.

2. Непослідовне впровадження політик:

- Географічні відмінності - застосування політик безпеки може суттєво відрізнятися в різних регіонах. Наприклад, інтернет-провайдер може впроваджувати суворі заходи безпеки в Європі через GDPR, але мати слабкіше правозастосування в інших регіонах.

- Внутрішній комплаєнс - забезпечити, щоб усі внутрішні відділи та працівники дотримувалися політики безпеки, є складним завданням. Існують випадки, коли протоколи безпеки обходять, що призводить до вразливостей.

3. Розширений захист від загроз:

- Нові загрози - швидко еволюціонуючий характер кіберзагроз, таких як програми-вимагачі та експлойти нульового дня, вимагає від провайдерів постійно оновлювати свої засоби захисту. Однак деякі провайдери намагаються не відставати від цих нових загроз.

- Обмін розвідданими про загрози - хоча деякі провайдери беруть участь в обміні розвідданими про загрози, інші роблять це неохоче через побоювання щодо конкуренції або юридичні наслідки. Таке небажання перешкоджає колективному підходу до захисту від кіберзагроз.

4. Захист даних користувачів

- Витоки даних - незважаючи на надійні заходи, витоки даних все ще трапляються. Наприклад, у 2020 році один з найбільших провайдерів зазнав витоку даних, в результаті якого були розкриті мільйони записів користувачів, що підкреслило необхідність постійного вдосконалення стратегій захисту даних.

- Ризики третіх сторін - інтернет-провайдери часто співпрацюють зі сторонніми постачальниками, які можуть не дотримуватися тих самих

стандартів безпеки. Це створює ризики, які можуть скомпрометувати дані користувачів.

5. Занепокоєння щодо конфіденційності:

- Монетизація даних - деякі Інтернет-провайдери піддаються критиці за монетизацію даних користувачів, що викликає значні занепокоєння щодо конфіденційності. Користувачі часто не мають контролю над тим, як використовуються та поширюються їхні дані.

- Державний нагляд - виконання урядових запитів на нагляд може суперечити конфіденційності користувачів. Інтернет-провайдери повинні балансувати між юридичними зобов'язаннями та необхідністю захищати конфіденційність користувачів [16].

Щоб усунути ці прогалини та вдосконалити свою політику інформаційної безпеки, провідні провайдери повинні розглянути наступні рекомендації з рисунку 2.2.

Рисунок 2.2 Рекомендації вдосконалення політики інформаційної безпеки [17]

Для підвищення прозорості, провайдери повинні чітко інформувати користувачів про свою політику безпеки та будь-які її зміни, регулярно оновлюючи інформацію на своїх веб-сайтах та проводячи освітні кампанії. Це дозволить користувачам краще розуміти методи безпеки та способи захисту їх даних. Щодо послідовного впровадження політики, важливо втілювати узгоджені стандарти безпеки в усіх регіонах і проводити регулярні внутрішні аудити для перевірки дотримання політики безпеки серед співробітників.

Удосконалення захисту від загроз можна здійснити за рахунок інвестицій у передові технології, такі як машинне навчання і рішення на основі штучного інтелекту, а також за допомогою участі у галузевих ініціативах з обміну даними про загрози. Для посилення захисту даних користувачів, необхідно забезпечити наскрізне шифрування всіх даних і регулярно проводити аудити третіх сторін для перевірки дотримання стандартів безпеки.

Нарешті, для покращення конфіденційності, важливо впровадити строгі механізми згоди користувачів на збір і передачу даних, а також дотримуватись принципів мінімізації даних, збираючи лише необхідні дані та безпечно видаляючи їх, коли вони більше не потрібні.Політика інформаційної безпеки провідних інтернет-провайдерів має вирішальне значення для захисту як їхньої інфраструктури, так і даних користувачів. Незважаючи на значний прогрес, все ще існують прогалини та сфери, які потребують вдосконалення. Підвищуючи прозорість, забезпечуючи послідовне дотримання політики, випереджаючи нові загрози, посилюючи захист даних і вирішуючи проблеми конфіденційності, інтернет-провайдери можуть побудувати більш надійні та стійкі системи безпеки. Ці зусилля не лише захистять їхніх користувачів, але й підвищать довіру до них у все більш взаємопов'язаному цифровому

Політика інформаційної безпеки провідних інтернет-провайдерів відіграє ключову роль у захисті цифрової інфраструктури та даних користувачів у світі, який стає все більш взаємопов'язаним. Оскільки залежність від інтернет-послуг продовжує зростати, зростає і відповідальність інтернет-провайдерів за захист своїх мереж і користувачів від безлічі кіберзагроз. Незважаючи на значний

прогрес у сфері інформаційної безпеки, залишається кілька прогалин і викликів, які потребують постійної уваги та вдосконалення.

Інтернет-провайдери досягли значних успіхів у захисті даних, конфіденційності користувачів, мережевій безпеці, реагуванні на інциденти та дотриманні нормативних вимог. Передові методи шифрування, суворий контроль доступу, комплексні політики конфіденційності, надійні брандмауери та проактивні плани реагування на інциденти є одними з ключових заходів, впроваджених для забезпечення безпеки. Однак ландшафт загроз, що швидко змінюється, та різноманітне регуляторне середовище в різних регіонах створюють постійні виклики.

Прозорість залишається найважливішою сферою для вдосконалення. Користувачі повинні бути адекватно поінформовані про те, як захищені їхні дані і як провайдери реагують на інциденти, пов'язані з безпекою. Чітке інформування та навчання користувачів може підвищити довіру та обізнаність, надаючи їм можливість відігравати активну роль у забезпеченні власної безпеки. Крім того, провайдери повинні забезпечити послідовне дотримання політики безпеки на глобальному рівні, мінімізуючи географічні відмінності та внутрішні проблеми з дотриманням вимог.

Потребу в передовому захисті від загроз неможливо переоцінити. Інтернет-провайдери повинні інвестувати в передові технології та брати участь у галузевих ініціативах з обміну інформацією про загрози, щоб бути на крок попереду нових загроз. Захист даних користувачів також потребує постійного вдосконалення. Наскрізне шифрування, регулярний аудит сторонніх постачальників і суворий контроль доступу є важливими для зменшення ризиків і запобігання витоку даних.

Занепокоєння щодо конфіденційності, особливо щодо монетизації даних та урядового нагляду, підкреслюють делікатний баланс, який провайдери повинні підтримувати між юридичними зобов'язаннями та конфіденційністю користувачів. Впровадження надійних механізмів згоди користувачів і

дотримання принципів мінімізації даних може вирішити ці проблеми і зміцнити довіру користувачів.

Зрештою, шлях до надійної інформаційної безпеки триває. Інтернет-провайдери повинні залишатися пильними, адаптивними і прагнути до постійного вдосконалення. Усуваючи виявлені прогалини та вдосконалюючи свої системи безпеки, провайдери можуть краще захищати свої мережі та користувачів, сприяючи створенню безпечнішого та надійнішого цифрового середовища. Таке прагнення до досконалості у сфері інформаційної безпеки не лише зменшує ризики, але й зміцнює довіру та авторитет провайдерів в очах користувачів, регуляторних органів та ширшої цифрової спільноти.

Динамічний характер кіберзагроз вимагає проактивного підходу, заснованого на співпраці. Використовуючи передові технології, сприяючи прозорості, забезпечуючи послідовне дотримання політики та надаючи пріоритет конфіденційності користувачів, інтернет-провайдери можуть побудувати стійку та надійну цифрову екосистему. Це не лише захистить критично важливу інфраструктуру Інтернету, але й сприятиме загальній стабільності та безпеці нашого взаємопов'язаного світу.

3 РОЗРОБКА ТА ОБҐРУНТУВАННЯ ВДОСКОНАЛЕНОЇ ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

3.1 Розробка заходів та стратегій для підвищення рівня захисту інформаційних систем

Підвищення рівня захисту інформаційних систем передбачає комплексний підхід, який охоплює різні аспекти безпеки, від розробки політики до технічної реалізації та постійного моніторингу. У цьому тексті викладено детальну стратегію підвищення рівня інформаційної безпеки в організації.

Основою будь-якої ефективної стратегії безпеки є ретельна оцінка ризиків. Цей процес починається з ідентифікації всіх активів організації, включаючи обладнання, програмне забезпечення, дані та персонал. Розуміючи, що потребує захисту, організація може визначити потенційні загрози, такі як кібератаки, інсайдерські загрози, стихійні лиха та системні збої. Оцінка вразливостей системи, таких як застаріле програмне забезпечення, слабкі паролі та невиправлені недоліки безпеки, має вирішальне значення. Вплив кожної потенційної загрози на діяльність, репутацію та фінанси організації необхідно оцінити, щоб розрахувати загальний ризик. Використання систем оцінки ризиків, таких як NIST або ISO 27005, може забезпечити структурований підхід до цього процесу.

Надійна політика безпеки має важливе значення для створення фундаменту системи безпеки організації. Ця політика повинна чітко визначати цілі та завдання безпеки, які узгоджуються з пріоритетами організації. Вона повинна визначати ролі та обов'язки щодо інформаційної безпеки, гарантуючи, що кожен член організації розуміє свою роль у підтримці безпеки. Повинні бути встановлені та задокументовані детальні процедури управління та реагування на інциденти безпеки. Сюди входять протоколи для виявлення, звітування та усунення порушень безпеки.

Ефективний контроль доступу має вирішальне значення для захисту інформаційних систем. Багатофакторна автентифікація (MFA) повинна

використовуватися, щоб гарантувати, що тільки авторизовані користувачі можуть отримати доступ до конфіденційних систем. Контроль доступу на основі ролей (RBAC) допомагає, призначаючи дозволи на основі ролей користувачів, тим самим обмежуючи доступ лише тим, кому він потрібен для виконання їхніх робочих функцій. Регулярний моніторинг журналів доступу необхідний для виявлення та оперативного реагування на будь-які спроби несанкціонованого доступу [18].

Безпека мережі може бути посилена за допомогою розгортання та належного налаштування брандмауерів для фільтрації вхідного та вихідного трафіку. Системи виявлення вторгнень (IDS) повинні бути впроваджені для виявлення та оповіщення про потенційні порушення безпеки [19]. Для захисту віддаленого доступу до мережі організації необхідні віртуальні приватні мережі (VPN).

Безпека даних має першорядне значення, а шифрування конфіденційних даних як у стані спокою, так і під час передачі захищає їх від несанкціонованого доступу. Регулярне резервне копіювання даних гарантує, що інформацію можна буде відновити у випадку злому або втрати даних. Практики мінімізації даних, які передбачають збір і збереження лише тих даних, які необхідні для бізнес-операцій, зменшують ризик розголошення непотрібної інформації.

Оновлення програмного забезпечення, включаючи операційні системи та додатки, найновішими патчами безпеки є життєво важливим для захисту від відомих вразливостей. Повинен бути впроваджений ефективний процес управління вразливостями з використанням автоматизованих інструментів для регулярного пошуку та оперативного усунення вразливостей.

Людські помилки часто є значним фактором ризику для інформаційної безпеки. Регулярне навчання працівників з питань безпеки гарантує, що вони розуміють політику та процедури безпеки. Моделювання фішингових атак може навчити працівників розпізнавати спроби фішингу та реагувати на них, а постійні кампанії з підвищення обізнаності про безпеку сприяють формуванню культури безпеки.

Ефективний план реагування на інциденти має вирішальне значення для мінімізації шкоди від порушень безпеки. Цей план повинен передбачати створення групи реагування на інциденти з чітко визначеними ролями та обов'язками. Детальні процедури виявлення, реагування та відновлення після інцидентів безпеки повинні бути задокументовані. План комунікації також необхідний для координації зусиль з реагування та інформування зацікавлених сторін під час інциденту.

Регулярне тестування та аудит заходів безпеки гарантує, що вони залишатимуться ефективними. Тестування на проникнення може виявити та усунути слабкі місця в системі безпеки до того, як вони будуть використані. Аудит безпеки слід проводити регулярно, щоб забезпечити відповідність політикам і правилам безпеки. Інструменти безперервного моніторингу забезпечують виявлення та реагування на загрози безпеці в режимі реального часу.

Таблиця 3.1 з основними заходами та стратегіями для підвищення рівня захисту інформаційних систем.

Таблиця 3.1 – Заходи і стратегії для підвищення рівня захисту інформаційних систем

Захід/Стратегія	Опис
Комплексна оцінка ризиків	Ідентифікація активів, загроз, вразливостей та оцінка впливу на організацію для розрахунку ризику.
Розробка надійної політики безпеки	Визначення цілей безпеки, ролей та відповідальностей, а також процедур для управління інцидентами.
Впровадження контролю доступу	Використання багатофакторної аутентифікації, контроль доступу на основі ролей, моніторинг доступу.
Покращення мережевої безпеки	Розгортання та налаштування міжмережевих екранів, систем виявлення вторгнень та VPN.
Забезпечення безпеки даних	Шифрування даних, регулярне резервне копіювання, мінімізація збирання та зберігання даних.
Регулярні оновлення та виправлення	Оновлення програмного забезпечення, управління вразливостями за допомогою автоматизованих інструментів.

Навчання та підвищення обізнаності	Регулярне навчання співробітників, симуляції фішингових атак, кампанії підвищення обізнаності.
План реагування на інциденти	Створення команди реагування на інциденти, розробка процедур та плану комунікацій під час інцидентів.
Регулярні тести та аудити	Проведення тестів на проникнення, регулярні аудити безпеки, впровадження інструментів безперервного моніторингу.
Співпраця з зовнішніми організаціями	Участь у мережах обміну інформацією, забезпечення відповідності стандартам безпеки сторонніх постачальників.

Співпраця із зовнішніми організаціями може посилити безпеку організації. Участь у мережах обміну інформацією допомагає залишатися в курсі останніх загроз і найкращих практик. Важливо також переконатися, що сторонні постачальники та партнери дотримуються стандартів безпеки організації.

Впроваджуючи ці комплексні заходи та стратегії, організації можуть значно посилити захист своїх інформаційних систем. Такий проактивний підхід знижує ризик порушень безпеки, забезпечуючи конфіденційність, цілісність і доступність критично важливих даних.

3.2 Впровадження сучасних технологій захисту інформації

За останні кілька десятиліть сфера інформаційної безпеки зазнала значних змін, зумовлених зростаючою складністю та витонченістю кіберзагроз. Сучасні технології інформаційної безпеки охоплюють широкий спектр інструментів і методологій, призначених для захисту даних, систем і мереж від несанкціонованого доступу, атак і пошкоджень. У цьому тексті розглядаються деякі з ключових технологій у цій галузі та наводяться приклади фрагментів коду, що ілюструють їхню реалізацію.

Шифрування - це процес перетворення відкритого тексту в зашифрований для запобігання несанкціонованому доступу [20]. Сучасні алгоритми

шифрування, такі як AES (Advanced Encryption Standard), широко використовуються для захисту конфіденційних даних.

Приклад коду: Шифрування AES у Python

```python
з Crypto.Cipher імпортувати AES
from Crypto.Random import get_random_bytes
import base64
# Згенерувати випадковий 16-байтовий ключ
key = get_random_bytes(16)
# Створити новий шифр AES
cipher = AES.new(key, AES.MODE_EAX)
# Зашифрувати дані
data = b'Конфіденційні дані'
ciphertext, tag = cipher.encrypt_and_digest(data)
# Кодуємо шифрований текст для безпечного зберігання/передачі
encoded_ciphertext = base64.b64encode(cipher.nonce + tag + ciphertext)
print(f'Зашифровані дані: {encoded_ciphertext}')
```

MFA підвищує безпеку, вимагаючи декількох форм перевірки перед наданням доступу. Це може включати щось, що користувач знає (пароль), щось, що користувач має (маркер безпеки), і щось, чим користувач є (біометрична перевірка).

Приклад коду: MFA на основі Google Authenticator в Python

```python
import pyotp
# Згенерувати base32 секрет
secret = pyotp.random_base32()
print(f'Secret: {secret}')
# Створити об'єкт TOTP
totp = pyotp.TOTP(secret)
# Згенерувати поточний OTP
otp = totp.now()
print(f'Поточний OTP: {otp}')
# Перевірити OTP
verification = totp.verify(otp)
```

```
print(f'Перевірка OTP: {verification}')```
```

IDS призначені для моніторингу мережевого трафіку на предмет підозрілої активності та потенційних загроз. Існує два основних типи: на основі сигнатур, які шукають відомі шаблони атак, і на основі аномалій, які виявляють відхилення від нормальної поведінки.

Приклад коду: Проста IDS з використанням Scapy в Python

```
```python
from scapy.all import *
def detect_intrusion(packet):
    # Приклад правила: Виявити TCP-пакети на порт 80 (HTTP)
    if packet.haslayer(TCP) and packet[TCP].dport == 80:
        print(f'HTTP пакет виявлено: {packet.summary()}')
# Обнюхуємо мережевий інтерфейс на наявність пакетів
sniff(prn=detect_intrusion, filter=«tcp», store=0)```
```

Безпечне кодування є важливим для запобігання таким вразливостям, як SQL-ін'єкції, міжсайтовий скриптинг (XSS) та переповнення буферу. Це передбачає перевірку вхідних даних, використання параметризованих запитів та уникнення небезпечних функцій.

Приклад коду: Запобігання SQL-ін'єкціям у Python

```
```python
import sqlite3
# Підключення до бази даних
conn = sqlite3.connect('example.db')
cursor = conn.cursor()
# Введення даних користувача
user_id = '1 OR 1=1' # Шкідливе введення
# Небезпечний запит (вразливий до SQL-ін'єкції)
unsafe_query = f «SELECT * FROM users WHERE id = {user_id}»
cursor.execute(unsafe_query)
print(cursor.fetchall())
```
```
```

```
    # Безпечний запит з використанням параметризованих
запитів
    safe_query = «SELECT * FROM users WHERE id = ?»
    cursor.execute(safe_query, (user_id,))
    print(cursor.fetchall())```
```

Рішення EDR забезпечують безперервний моніторинг і реагування на сучасні загрози на кінцевих точках. Вони збирають і аналізують дані для виявлення підозрілих дій і автоматично реагують на потенційні загрози.

Приклад коду: Простий моніторинг кінцевих точок за допомогою Python

```
    ```python
    import psutil
    import time
    def monitor_endpoints():
        while True:
            for proc in psutil.process_iter(['pid',
'name', 'username']):
                print(proc.info)
            time.sleep(10) # Перевірка кожні 10 секунд
    monitor_endpoints()```
```

Впровадження сучасних технологій інформаційної безпеки має вирішальне значення для захисту даних і систем від нових кіберзагроз. Впроваджуючи шифрування, багатофакторну автентифікацію, системи виявлення вторгнень, безпечне кодування, а також виявлення кінцевих точок і реагування на них, організації можуть значно підвищити рівень своєї безпеки.

3.3 Опис захисту від загроз за НД ТЗІ 2.5-010-03

Рекомендації по захисту веб-додатків описані в НД ТЗІ 2.5-010-03. Цей документ встановлює різні норми щодо захисту від загроз. Під час створення веб-сторінки та визначення операторів, вузли яких використовуватимуться для підключення до мережі Інтернет, установи повинні керуватися законами України
```

та іншими нормативно-правовими актами, що встановлюють вимоги з технічного захисту інформації.

Веб-сторінка установи може бути розміщена як на власному сервері, так і на сервері оператора. Власник сервера зобов'язаний гарантувати рівень захисту відповідно до вимог НД ТЗІ 2.5-010-03. Функціонування веб-сторінки забезпечується автоматизованою системою (АС), яка здійснює актуалізацію розміщених на ній інформаційних ресурсів та керування доступом до них. Для забезпечення захисту інформації в цій АС створюється комплексна система захисту інформації (КСЗІ), що складається з організаційних, інженерно-технічних заходів та програмно-апаратних засобів.

Перелік інформації для публічного розміщення на веб-сторінці визначається з урахуванням вимог чинного законодавства і затверджується керівником установи. Організація робіт із захисту інформації та контроль за її станом на веб-сторінці здійснюються відповідальним підрозділом або відповідальною особою (службою захисту інформації, СЗІ).

Захист інформації на всіх етапах створення та експлуатації веб-сторінки здійснюється згідно з планом захисту інформації, розробленим установою. Цей план затверджується керівником установи, а у випадку використання сервера оператора - погоджується з власником сервера.

До складу АС, що забезпечує функціонування веб-сторінки, входять операційна система, фізичне середовище, середовище користувачів та оброблювана інформація. Під час забезпечення захисту інформації враховуються всі характеристики зазначених складових, що впливають на реалізацію політики безпеки веб-сторінки.

Політика безпеки інформації в АС поширюється на об'єкти комп'ютерної системи, що безпосередньо чи опосередковано впливають на безпеку інформації. До них належать адміністратори безпеки та співробітники СЗІ, користувачі з повноваженнями щодо управління АС, користувачі з доступом до загальнодоступної інформації, інформаційні об'єкти, системне та функціональне

програмне забезпечення, технологічна інформація КСЗІ, засоби адміністрування та обчислювальні ресурси АС.

Враховуючи особливості надання доступу до інформації веб-сторінки, типові характеристики середовищ функціонування та особливості технологічних процесів оброблення інформації, в НД ТЗІ 2.5-010-03 визначаються мінімально необхідні рівні послуг безпеки для захисту інформації від загроз. Наприклад, якщо веб-сервер і робочі станції знаходяться на території установи або оператора (технологія Т1), мінімально необхідний функціональний профіль включає різні компоненти безпеки, такі як КА-2, ЦА-1, ДВ-1, НР-2, та інші.

У випадку, коли веб-сервер знаходиться у оператора, а робочі станції - на території власника веб-сторінки, і взаємодія між ними здійснюється через мережі передачі даних (технологія Т2), мінімально необхідний функціональний профіль також включає додаткові компоненти безпеки, враховуючи незахищене середовище передачі інформації.

Власник веб-сторінки має право реалізувати окремі послуги безпеки з вищим рівнем, доповнювати профілі іншими послугами або реалізувати послуги безпеки з більш високим рівнем гарантій у разі необхідності.

Захист веб-додатків відповідно до НД ТЗІ 2.5-010-03 є комплексним процесом, який включає дотримання законодавчих вимог, правильне розміщення серверів, організацію робіт із захисту інформації, а також розробку і виконання плану захисту. Ключовими аспектами є забезпечення відповідного рівня захисту інформації, створення комплексної системи захисту, а також контроль за станом її захищеності. Політика безпеки повинна охоплювати всі компоненти автоматизованої системи, включаючи фізичне середовище, програмне забезпечення, користувачів та обчислювальні ресурси.

Особлива увага приділяється розробці функціонального профілю захисту залежно від умов розміщення веб-сервера і робочих станцій. При використанні технології Т1, де сервер і робочі станції знаходяться на одній території, вимоги до захисту дещо відрізняються від технології Т2, де передача даних відбувається через незахищене середовище. Усі ці заходи спрямовані на мінімізацію ризиків

втрати або компрометації інформації, що обробляється або зберігається у веб-додатках.

Таким чином, дотримання вимог НД ТЗІ 2.5-010-03 забезпечує високий рівень захисту інформації на всіх етапах створення та експлуатації веб-сторінок, дозволяючи установам ефективно протистояти сучасним кіберзагрозам.

ВИСНОВКИ

В даній дипломній роботі було проведено ґрунтовне дослідження теоретичних основ інформаційної безпеки, проаналізовано сучасні методи та технології захисту інформації, а також розглянуто існуючі підходи до забезпечення інформаційної безпеки інтернет-провайдерів.

У першому розділі роботи розкрито сутність та значення інформаційної безпеки в сучасному світі. Проаналізовано основні принципи та концепції, що лежать в основі захисту інформації, визначено ключові загрози та ризики, що виникають в інформаційних системах. Також проведено огляд сучасних методів та технологій захисту інформації, включаючи криптографічні засоби, системи управління доступом, антивірусні програми та інші технології.

Другий розділ був присвячений аналізу існуючих підходів до забезпечення інформаційної безпеки інтернет-провайдерів. У ході дослідження було виявлено низку недоліків та проблем в існуючих політиках інформаційної безпеки. Основними з них є недостатня комплексність заходів безпеки, відсутність систематичного підходу до управління інформаційною безпекою, низький рівень обізнаності персоналу щодо актуальних загроз та методів їх нейтралізації, а також недосконаліть технічних засобів захисту. Було проведено дослідження політик інформаційної безпеки провідних інтернет-провайдерів, що дозволило виділити найбільш ефективні практики та підходи до забезпечення захисту інформаційних систем.

Третій розділ роботи присвячено розробці та обґрунтуванню вдосконаленої політики інформаційної безпеки. Розроблено комплекс заходів та стратегій для підвищення рівня захисту інформаційних систем інтернет-провайдерів. Запропоновано впровадження сучасних технологій захисту інформації, таких як використання багатофакторної аутентифікації, застосування систем виявлення та попередження вторгнень, регулярне оновлення програмного забезпечення, проведення навчань та тренінгів для персоналу.

Запропоновані заходи та стратегії мають на меті забезпечення високого рівня захисту інформаційних систем інтернет-провайдерів, зменшення ризиків витоку конфіденційної інформації, підвищення стійкості до кібератак та забезпечення безперервності надання послуг. Впровадження сучасних технологій захисту інформації сприятиме підвищенню рівня довіри користувачів до інтернет-провайдерів та зміцненню їх позицій на ринку.

У результаті проведеного дослідження були розроблені рекомендації щодо вдосконалення політик інформаційної безпеки інтернет-провайдерів, що включають як організаційні, так і технічні заходи. Застосування цих рекомендацій дозволить значно підвищити рівень захисту інформаційних систем та забезпечити надійний захист конфіденційної інформації користувачів.

ПЕРЕЛІК ПОСИЛАНЬ

1. Сопілко І. М. Інформаційна безпека та кібербезпека: порівняльно-правовий аспект// Юридичний вісник Повітряне і космічне право. – Київ: НАУ, 2021. – № 2(59). С. 110-115.
2. Диджиталізація (цифровізація) суспільства: інституційні, економічні, соціально-психологічні та правові аспекти : матеріали факульт. наук.-практ. конф. докторантів, аспірантів, молодих вчених і студентів, м. Харків, 24 листопада 2023 р. Харків: Харківський національний економічний університет імені Семена Кузнеця, 2023. 110 с.
3. Галіпчак В. Інформаційна війна як складова гібридної війни в умовах російської агресії. *Вісник Прикарпатського університету*, 2023. Вип. 15. 26-32.
4. Чмир Я. Сучасні проблеми інформаційної безпеки України та перспективні напрями їх вирішення». *Наукові праці Міжрегіональної Академії управління персоналом. Політичні науки та публічне управління*, 2022. №2(62). С. 149-154.
5. Циріна М. Сучасні технології захисту й опрацювання конфіденційної докуметної інформації в організаціях і установах різних форм власності. Національна академія керівних кадрів культури і мистецтв. *Бібліотекознавство. Документознавство. Інформологія*, 2021. №4. С. 15-23.
6. Azhari M., Perwitosari F. J. Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES). *Jurnal Pendidikan Sains dan Komputer*, 2022. Vol. 2 No. 01. C. 163-171.
7. Chen Y., Li S. A High-Throughput Hardware Implementation of SHA-256 Algorithm. IEEE International Symposium on Circuits and Systems (ISCAS), Spain, 2020, PP. 1-4.
8. Очеретний С.О., Крижановський В.Г. Системи виявлення та запобігання вторгнень, найбільш успішні практики. *Прикладні аспекти сучасних міждисциплінарних досліджень*, 2024. С. 236-238.
9. Arfeen A., Ahmed S., Khan M. A., Jafri S. F. A. Endpoint Detection & Response: A Malware Identification Solution. *International Conference on Cyber Warfare and Security (ICCWS)*, Islamabad, Pakistan, 2021, PP. 1-8.
10. SSO: що таке система єдиного входу? Універсальна служба SSO для підприємств. URL: https://hideez.com/uk/pages/sso-service
11. Романюк О. Н., Нечипорук М. Л., Ціхановська О. М. Автоматизація та комп’ютерно-інтегровані технології у виробництві та освіті: стан,

досягнення, перспективи розвитку: матеріал. Всеукр. наук.-практ. Internet-конф. м. Черкаси, 11-17 березн. 2024 р. Чорноморський державний університет імені Петра Могили, 2024. 384 с.

12. Рубан А. О. Інформаційна політика держави в сучасному глобалізованому суспільстві. Теоретичні та наукові засади розвитку наукової думки : матеріали V Міжнар. наук. конф. м. Рим, 16-19 лют. 2021 р. Італія. С. 534-538.
13. Копілка М. В. Модернізація політики міжнародних організацій у сфері інформаційної безпеки. Політичні проблеми міжнародних систем та глобального розвитку. *Політичне життя*, 2020. №1. С. 102-109.
14. Маковський, І. Ю. Аналіз вихідних даних для формування політики інформаційної безпеки на підприємстві. *Економіка, управління та адміністрування*, 2020. №1(91). С. 38–42.
15. Поліняка П. В. Інформаційна система обліку мережевого обладнання Інтернет-провайдера. Поліський нац. ун-т, каф. комп'ют. технологій і моделювання систем. Житомир, 2021. 35 с.
16. Гаврилюк Б. В., Зоріло В. В., Кушніренко Н. І. Розробка програмного забезпечення зберігання та захисту даних для приватного та корпоративного застосування. Інформатика та математичні методи в моделюванні, 2022 . Т. 12 № 1-2. С. 15-22.
17. Шевченко, С. М., Жданова Ю. Д., Кравчук К. В. Модель захисту інформації на основі оцінки ризиків інформаційної безпеки для малого та середнього бізнесу. *Кібербезпека: освіта, наука, техніка*, 2021. №2 (14). С.. 158-175.
18. Керусов М. В. Політика інформаційної безпеки інтернет провайдерів. *Кібербезпека в сучасному світі* : матеріали II Всеукр. наук.-практ. конф. м. Одеса, 20 листоп. 2020 р. Одеса : Видавничий дім «Гельветика», 2020. С.27-30.
19. Бондаренко А., Стаценко В. Використання методів та моделей штучного інтелекту для покращення експертних систем виявлення вторгнень. Вісник Хмельницького національного університету. Серія: Технічні науки, 2024. Т. 333(2), С. 99–106.
20. Бабінська, С. Ведення бухгалтерського обліку в умовах впровадження сучасних інформаційних технологій. *Економіка та суспільство*, 2021. №26. URL: https://economyandsociety.in.ua/index.php/journal/article/view/323/309