МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ІВАНА ФРАНКА

Факультет прикладної математики та інформатики
(повне найменування назва факультету)

кібербезпеки
(повна назва кафедри)

Дипломна робота

Стандарти та контролі інформаційної безпеки для хмарних сервісів (GCP, Azure, AWS)

Виконав:

студент групи ПМК-41

спеціальності 125 «Кібербезпеки»
(шифр і назва спеціальності)

Гранатир С. І.
(підпис) (прізвище та ініціали)

Керівник Кропива М. В.
(підпис) (прізвище та ініціали)

Рецензент Клаковичч Л.М.
(підпис) (прізвище та ініціали)

2023

ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ІВАНА ФРАНКА

Факультет Прикладної математики та інформатики

Кафедра Кібербезпеки

Спеціальність 125 «Кібербезпека»
(шифр і назва)

«ЗАТВЕРДЖУЮ»

Завідувач кафедри _____

"31" серпня 2022 року

З А В Д А Н Н Я

НА ДИПЛОМНУ РОБОТУ СТУДЕНТУ

Гранатира Святослава Ігоровича
(прізвище, ім'я, по батькові)

1. Тема роботи Стандарти та контролі інформаційної безпеки для хмарних сервісів (GCP, Azure, AWS)

керівник роботи Кропива Михайло Вікторович, асистент кафедри кібербезпеки
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені Вченою радою факультету від **"13" вересня 2022 року № 15**

2. Строк подання студентом роботи **13.06.2023р.**

3. Вихідні дані до роботи Розглянути та проаналізувати стандарти та контролі інформаційної безпеки застосовні для хмарних сервісів. Розглянути інстурменти забезпечення відповідності та продемонструвати їх роботу на прикладі одного з відомих хмарних сервісів

4. Зміст дипломної роботи (перелік питань, які потрібно розробити)

1. Теоретичні основи інформаційної безпеки та хмарних сервісів.
2. Дослідження відомих стандартів та контролів інформаційної безпеки.
3. Практична застосування стандартів та контролів інформаційної безпеки.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень) Презентація доповіді, виконана в Microsoft PowerPoint

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Вступ	Кропива М. В. Асистент кафедри кібербезпеки	22.03	23.03
Розділ 1	Кропива М. В. Асистент кафедри кібербезпеки	24.03	04.04
Розділ 2	Кропива М. В. Асистент кафедри кібербезпеки	04.04	14.04
Розділ 3	Кропива М. В. Асистент кафедри кібербезпеки	14.04	10.05
Розділ 4	Кропива М. В. Асистент кафедри кібербезпеки	10.05	20.05
Розділ 5	Кропива М. В. Асистент кафедри кібербезпеки	20.05	30.05

7. Дата видачі завдання **31 серпня 2022 р.**

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломної роботи	Строк виконання етапів роботи	Примітка
1	Уточнення постановки завдання	21.03.2023	
2	Аналіз літератури	28.03.2023	
3	Обґрунтування вибору рішення	31.03.2023	
4	Збір даних	07.04.2023	
5	Теоретичні основи інформаційної безпеки та хмарних сервісів	18.04.2023	
6	Дослідження стандартів та контролів інформаційної безпеки	12.05.2023	
7	Дослідження щодо практичного застосування стандартів та контролів інформаційної безпеки у хмарних сервісах	25.05.2023	
8	Оформлення та друк пояснювальної записки	03.06.2023	
9	Оформлення презентації	06.06.2023	
10	Отримання рецензій	10.06.2023	
11	Подання роботи на кафедру	12.06.2023	
12	Захист в ЕК	15.06.2023	

Студент _____ Гранатир С. І.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Кропива М. В.
(підпис) (прізвище та ініціали)

Реферат

Пояснювальна записка дипломного проекту складається зі вступу, трьох розділів, що містять 9 рисунків, висновків та списку використаних джерел з 84 найменувань. Загальний обсяг роботи становить 83 сторінок.

Об'єкт дослідження: стандарти та контролі інформаційної безпеки для хмарних сервісів (GCP, Azure, AWS)

Метою даної роботи є дослідження стандартів та контролів інформаційної безпеки для хмарних сервісів. Дослідження практичного застосування стандартів та контролів для хмарного сервісу AWS.

У першому розділі розглядається поняття інформаційної безпеки, її історія, головні принципи, відмінності від кібер-безпеки, та перелік найвідоміших загроз.

У другому розділі розглядається поняття хмарних сервісів та історія їх виникнення. Крім того аналізуються характеристики та типи хмарних сервісів.

У третьому розділі розглядається поняття політики інформаційної безпеки, їх типи та ключові аспекти.

У Четвертому розділі аналізується стандарт інформаційної безпеки NIST 800-53, та його контролі. Також у цьому розділі проводиться огляд та аналіз CIS контролів.

У п'ятому розділі аналізується інструменти аналізу відповідності контролям NIST 800-53 та CIS. Проводиться практичне застосування з аналізу відповідності контролям сервісів AWS.

Галузь застосування: Матеріали роботи можуть бути використанні при побудові інформаційної безпеки у хмарних сервісах відповідно до стандарту NIST 800-53, а також при впровадженні CIS контролів у хмарні сервіси.

Ключові слова: AWS, ІНФОРМАЦІЙНА БЕЗПЕКА, СТАНДАРТ, КОНТРОЛЬ, ТЕХНОЛОГІЇ, ХМАРНІ СЕРВІСИ, NIST 800-53, CIS.

ABSTRACT

The explanatory note of the diploma project consists of an introduction, three sections containing 9 figures, conclusions and a list of used sources of 84 items. The total volume of the work is 83 pages

Object of research: Information security standards and controls for cloud services (GCP, Azure, AWS)

The purpose of the diploma project research on information security standards and controls for cloud services. A study of the practical application of standards and controls for the AWS cloud service.

The first section examines the concept of information security, its history, main principles, differences from cyber security, and a list of the most well-known information security threats.

The second section examines the concept of cloud services and its history. In addition, the characteristics and types of cloud services are analyzed.

The third section examines information security policies, their types, and key aspects.

The fourth section analyzes NIST 800-53 information security standard and its controls. This section also provides an overview and analysis of CIS controls.

Field of application: The materials of the work can be used to build the information security in cloud services following the NIST 800-53 information security standard, as well as to implement CIS controls in cloud services.

Keywords: AWS, INFORMATION SECURITY, STANDARD, CONTROL, TECHNOLOGIES, CLOUD SERVICES, NIST 800-53, CIS.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ІБ	Інформаційна безпека
NIST	National Institute of Standards and Technology
CIS	Center of Internet Security
AWS	Amazon Web Services
GCP	Google Cloud Platform
IT	Інформаційні технології
ARPANET	Advanced Research Projects Agency Network
CFAA	Computer Fraud and Abuse Act
CIA	Confidentiality, Integrity, Availability
ПЗ	Програмне забезпечення
СКБД	Система Керування Базами Даних
EDR	Endpoint Detection and Response
SANS	SysAdmin, Audit, Network and Security
IG	Implementation Group
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
MFA	Multi-Factor Authentication
URL	Uniform Resource Locator
DMARC	Domain-based Message Authentication, Reporting, and Conformance
VPN	Virtual Private Network
AAA	Authentication, Authorization and Accounting
ЦЗОД	Центр зберігання та обробки даних
SSH	Secure Shell
EBS	Elastic Block Store
VPC	Virtual Private Cloud
EC2	Elastic Compute Cloud
S3	Simple Storage Service
IMDSv2	Instance Metadata Service Version 2

ECR Elastic Container Registry

IAM Identity and Access Management

ВСТУП

Хмарні сервіси з кожним роком набувають все більшої популярності. За приблизними підрахунками, у 2022 році близько 60% корпоративних даних зберігались та оброблялись у хмарах. До прикладу у 2015 році це число складало лише 30%, тобто використання хмарних сервісів зросло вдвічі за останні 7 років, що підкреслює їхню користь для бізнесу у світі інформаційних технологій.

Хмарні сервіси надають можливість зберігати, обробляти та обмінюватись даними у віртуальних оточеннях, що забезпечує гнучкий та ефективний доступ до інформації. Однак не дивлячись на усі переваги, організації, які використовують хмарні сервіси рано чи пізно стикаються з викликами інформаційної безпеки. Стандарти та контролі інформаційної безпеки покликані допомогти організаціям у забезпечені інформаційної безпеки. Стандарти та контролі ІБ впроваджуються як для захисту внутрішньої інфраструктури організації, так і інфраструктури наданої третіми сторонами, як от хмарні сервіси.

Метою даної роботи є дослідження існуючих стандартів та контролів інформаційної безпеки та їх застосування для хмарних сервісів. У цій роботі будуть проаналізовані відомі стандарти та контролі ІБ, такі як NIST SP 80-53 та CIS контролі. Аналіз цих стандартів та контролів дозволить визначити їхні переваги, недоліки та застосовність для найрозповсюдженіших хмарних сервісів, таких як AWS, GCP та AZURE.

Об’єкт дослідження: Стандарти та контролі інформаційної безпеки для хмарних сервісів.

Предмет Дослідження: Методи впровадження та контролю відповідності стандартам та контролям інформаційної безпеки в хмарних сервісах.

Результати даного дослідження можуть бути корисними для організацій, які мають намір, або вже активно використовують хмарні рішення. Розуміння

стандартів та контролів інформаційної безпеки може допомогти забезпечити високий рівень інформаційної безпеки хмарних середовищ, та знизити ризики пов’язані зі зберіганням та обробкою даних у хмарах.

Розділ 1

Поняття інформаційної безпеки

1.1 Історія інформаційної безпеки

Інформаційна безпека – це важлива та невід’ємна частина сфери інформаційних технологій. Історично проблема інформаційної безпеки росла паралельно з тим, як розвивався світ інформаційних технологій. Розглядаючи ретро перспективу розвитку ІТ, можна помітити, що проблема ІБ ставала щораз гострішою разом із приходом нових технологій.

До прикладу, в 1960-х роках комп’ютерна техніка використовувалась в обмеженій кількості галузей і була досить рідкісною, відповідно проблема інформаційної безпеки не стояла так гостро. Так як ані комп’ютерних мереж, ані тим паче інтернету ще не було, компанії в основному були сфокусовані на захисті фізичного доступу до комп’ютерів, та захисті збережених даних, наприклад, для обмеження доступу використовувались паролі безпосередньо на девайсах, а для захисту збережених даних впроваджувались банально правила пожежної безпеки.

В 1970-х, з появою на світ ARPANET з’явились і перші ентузіасти, які намагались знайти та використати вразливості цієї мережі, щоб викрасти дані, або банально заявити про себе. На приклад, ентузіаст Боб Томас у 70-х створив програму «CREEPER», яка гуляла просторами мережі ARPANET та залишала по собі жартівливе повідомлення: «I’m the creeper: Catch me if you can». Пізніше, уже інший ентузіаст Рей Томлінсон розвинув «CREEPER» та додав йому можливість самовідтворення, тим самим створивши першого в історії комп’ютерного хробака. Більше того, Томлінсон також написав іншу програму з

назвою «REEPER», яка виявляла попередньо згаданого “CREEPER” та видаляла його, простіше кажучи, це був приклад першого антивірусу.

Друга половина 1980-х та 1990-ті ознаменувалась активним розвитком комп’ютерних мереж. Комп’ютери університетів, різних компаній, державних структур, та навіть рядових користувачів почали спілкуватись між собою та об’єднуватись в глобальну мережу, сьогодні відому як інтернет. Разом з цим комп’ютерні віруси ставали все досконалішими та отримали змогу набагато швидше розповсюджуватись. У 1988 році аспірант факультету Обчислювальної техніки Корнельського університету Роберт Моріс розробив комп’ютерного хробака, який сьогодні відомий як «Хробак Моріса». Хробак розповсюджувався через мережу та вражав комп’ютери, використовуючи давно відому вразливість в поштовому сервері «Sendmail» та сервісах «Finger», і в результаті паралізував роботу близько шести тисяч інтернет-вузлів у США. Інцидент з Хробаком Моріса став однією з відправних точок в історії інформаційної безпеки. Більше того, Роберт Моріс став першою людиною по відношенню до якої було висунуте обвинувачення відповідно до закону про комп’ютерне шахрайство та зловживання (CFAA). А також з метою запобігання схожих інцидентів в майбутньому була створена Комп’ютерна група реагування на надзвичайні ситуації (CERT).

У подальші роки інтернет ставав все більш доступним для рядових користувачів, і, як наслідок, наповнювався їх особистими даними. Як наслідок, зловмисники отримали можливість викрадати конфіденційні дані користувачів, компаній та навіть урядів країн. Для запобігання та протидії зловмисникам активно почало розвиватись антивірусне ПЗ та брандмауери (Firewalls).

Далі у 2000-их роках, внаслідок експоненціального росту мережі інтернет, зловмисники почали удосконалювати методи та інструменти проникнення в комп’ютерні системи з метою викрадення або знищення даних, а паралельно з цим фахівці покращували та створювали нові інструменти інформаційної безпеки. У наш час можливості зловмисників сягнули нового та дуже небезпечного рівня. За останні десять років під приціл кібер-злодіїв підпали не

лише звичайні користувачі, а й корпорації, і навіть цілі країни. До прикладу, можна згадати, мабуть, одну з найвідоміших кібератак, яка була проведена у 2017 році і використовувала вірус вимагач «WannaCry», який уражав комп'ютери під управлінням операційної системи «Windows», шифрував дані, блокував систему та вимагав оплату у крипто валюті «Bitcoin» для отримання ключа розшифрування. Лише за один день вірус інфікував понад 230 000 комп'ютерів у 150 країнах світу.

1.2 Принципи інформаційної безпеки

Базові принципи інформаційної безпеки - це конфіденційність, цілісність та доступність. В купі вони утворюють так звану КЦД трійцю (CIA triad).

Рисунок 1.1 – КЦД трійця

1. Конфіденційність (Confidentiality) Ціль конфіденційності - забезпечення конфіденційності інформації, яка цього потребує, та гарантування, що вона доступна лише авторизованим користувачам, які її потребують.
2. Цілісність (Integrity) запобігає неавторизованим змінам даних. Мета цілісності - забезпечення точності, достовірності та захисту від несанкціонованої модифікації даних.

3. Доступність (Availablity) – це здатність системи бути готовою надавати доступ до даних за потреби.

1.3 Відмінності інформаційної та кібер- безпеки

Важливо розуміти різницю між інформаційною та кібер- безпекою. Загалом інформаційна безпека відрізняється від кібербезпеки як за об'ємом зони відповідальності, так і за призначенням. Можна сказати, що кібербезпека це частина ІБ. Інформаційна безпека це широке поняття, яке покриває багато сфер, таких як: фізична безпека, безпека кінцевих точок, шифрування даних та мережева безпека.

Кібербезпека в основному спрямована на захист від загроз в сфері ІТ. Для цього використовуються кращі практики та інструменти для їх попередження та запобігання. До прикладу, КБ відповідає за безпеку даних, які зберігаються або обробляються.

1.4 Топ загроз інформаційної безпеки

Існують сотні категорій загроз інформаційної безпеки і мільйони відомих векторів їх використання. З поміж них можна виділити основні, або пріоритетні для відділів інформаційної безпеки:

1. **Незахищені або погано захищені системи**

   Поспіх при розробці ПЗ часто приводить до компромісів у інформаційній безпеці, а інколи навіть до її повного ігнорування. Таке програмне забезпечення може використовуватись компанією протягом довгого часу. Компанія повинна виявляти такі системи і закривати вразливості оновленнями, або ж виводити їх з експлуатації.

2. **Соціальна інженерія**

   Під час використання соціальної інженерії зловмисники до прикладу можуть розсилати електроні смс або повідомлення інших типів і з допомогою обману змусити жертву до дій, які призведуть до компрометації систем безпеки, або розкриття конфіденційної інформації.

Зловмисники маніпулюють людьми використовуючи психологічні тригери, такі як: цікавість, терміновість чи залякування. Наприклад в електронному листі може бути сказано:

“Привіт, мене звуть Андрій, я новий аналітик у компанії. Я мушу зробити та подати звіт про наші прибутки до вечора інакше на нас чекають великі неприємності. Терміново відправ мені дані про доходи компанії за останній квартал. Дякую!”.

3. Шкідливе ПЗ

Як правило, у компаніях працівники користуються багатьма різноманітними «девайсами», такими як: персональні комп’ютери, ноутбуки та смартфони. Вони можуть бути як корпоративними, так і персональними, але часто усі вони підключені до спільної корпоративної мережі. Шкідливе програмне забезпечення є однією з головних загроз для комп’ютерної техніки, а як наслідок, і для всієї компанії. До прикладу, варто комп’ютерному хробаку потрапити на один пристрій в мережі, як він одразу може розповсюдитись на інші пристрої, які потенційно можуть зберігати та обробляти конфіденційну інформацію. Традиційні антивірусні системи не можуть захистити компанію від усіх видів шкідливого ПЗ, тому існують багато більш ефективних систем для захисту кінцевих точок, наприклад EDR, система виявлення загрози кінцевої точки та відповідь.

4. Недостатнє шифрування

Шифрування - це процес кодування інформації з метою запобігання несанкціонованого доступу та її компрометації. Шифрування захищає дані при втраті або крадіжці обладнання, на якому вони збережені, а також при компрометації інформаційних систем.

На жаль, часто шифруванню не надають достатньої уваги, тому що його імплементація вимагає досить багато зусиль, та часу, а також існують певні юридичні, та правові вимоги щодо його реалізації. Компанії часто

впроваджують шифрування шляхом використання систем збереження даних або використання хмарних сервісів з підтримкою шифрування.

5. **Неправильні налаштування систем безпеки**

Компанії користуються великим спектром сервісів, інструментів, та обладнанням, наприклад: хмарними, та веб-сервісами, мережевим, та серверним обладнанням. Як правило, такі системи мають вбудовані інструменти безпеки, які вимагають певних налаштувань.

Людський фактор, як от необачність, або нестача знань, може призвести до прогалин в безпеці тієї чи іншої системи, або сервісу. Також з плином часу конфігурації безпеки можуть застаріти і в результаті викликати проблеми з безпекою. Налаштування безпеки мусять контролюватись системами моніторингу, ідентифікації та оповіщення, які дозволяють виявляти або навіть автоматично виправляти неправильні налаштування безпеки.

Розділ 2

Поняття хмарних сервісів

2.1 Історія хмарних сервісів

У 1963 році Агентство Передових Оборонних Дослідницьких Проектів США (DARPA) надало Массачусетському технологічному інституту (MIT) грант у розмірі двох мільйонів доларів на дослідження у сфері математики та обрахунків. Однією з вимог до MIT була розробка технології, яка дозволить одночасно використовувати комп’ютер двома або більше людьми. Для опису такого підходу було введене поняття віртуалізації, яке пізніше значно розширилось. Поняття віртуалізації набуло свого сучасного визначення у 1970-ті роки, воно описує процес створення віртуальної машини, яка працює як справжній фізичний комп’ютер з повністю функціонуючою операційною системою. Концепція віртуалізації набула популярності разом з розвитком мережі інтернет, коли компанії почали орендувати цілі приватні віртуальні

мережі. Активне використання віртуальних комп'ютерів у 1990-их роках призвело до створення концепції сучасних хмарних сервісів.

Хмарні сервіси – це широкий спектр різноманітних комп'ютерних та мережевих сервісів, які надаються клієнтові, або компанії за потреби (on-demand) через мережу інтернет. Хмарні сервіси дозволяють легко та дешево створювати, масштабувати та отримувати доступ до комп'ютерних ресурсів без необхідності використання власного комп'ютерного/мережевого обладнання.

2.2 Характеристики хмарних сервісів

Існують три типи хмарних сервісів:

1. **Приватна хмара (Private cloud)** – хмарна інфраструктура призначена для використання в масштабі однієї організації.
2. **Публічна хмара (Public cloud)** – хмарна інфраструктура призначена для вільного використання ресурсів багатьма клієнтами або компаніями.
3. **Гібридна хмара (Hybrid cloud)** – це комбінація локальної інфраструктури з приватними та публічними хмарними сервісами.

Також хмарні сервіси різняться за своєю бізнес-моделлю та функціоналом. Наприклад, нижче наведені три основні моделі:

1. **Програмне забезпечення як послуга (SaaS)** – це модель надання хмарних обчислень де клієнт використовує ПЗ постачальника, запущене в хмарній інфраструктурі, яке доступне клієнту через веб, або програмний інтерфейс. Користувачі не можуть керувати та контролювати хмарну інфраструктуру, в тому числі і мережу, сервери, операційні системи, сховища даних, або навіть міняти параметри налаштування певного програмного забезпечення.
2. **Платформа як послуга (PaaS)** – це модель надання хмарних обчислень, при якій користувач отримує доступ до використання програмної платформи: операційних систем, СКБД, прикладного ПЗ, засобів розробки і тестування. Фактично клієнт орендує комп'ютерну платформу з

встановленою операційною системою та спеціалізованим засоби для розробки, розміщення та керування веб-аплікаціями. Клієнт не керує інфраструктурою, в тому числі мережею, серверами, операційною системою або сховищем даних, але керує розгорнутим програмним забезпеченням і параметрами налаштування робочого середовища

3. **Інфраструктура як послуга (IaaS)** – це модель надання хмарних обчислень, при якій клієнт отримує можливість керувати засобами обробки і зберігання, а також іншими обчислювальними ресурсами (віртуальними серверами та мережевою інфраструктурою), на яких він може самостійно встановлювати операційні системи та прикладні програми у власних цілях. По суті, клієнт орендує абстрактні обчислювальні ресурси (серверний час, дисковий простір та пропускну здатність мережевих каналів) або використовує послуги аутсорсингу IT-інфраструктури. Клієнт не керує основною інфраструктурою хмари, але керує операційними системами, сховищами та аплікаціями.

Порівняння моделей

Модель	Споживач	Налаштування
SaaS	Кінцеві користувачі	Мінімальні, або відсутні
PaaS	Власник додатку	Високий рівень налаштувань, але лише на рівні визначених провайдером операційних систем, та додатків.
IaaS	Власник додатку	Високий рівень гнучкості налаштувань, в тому числі можливість налаштування мереж, віртуальними серверами, тощо.

Таблиця 2.1

Розділ 3

Політики інформаційної безпеки

3.1 Визначення політики безпеки

Політика інформаційної безпеки - це набір правил, політик та процедур покликаних гарантувати, що всі кінцеві точки, працівники та мережі організації відповідають вимогам інформаційної безпеки.

3.2 Типи політик безпеки

Політики безпеки поділяються на три типи:

1. **Організаційні (Organizational)** - це основні політики безпеки, які розповсюджуються на всю організацію.
2. **Системно-залежні (System-specific)** - системно-залежні політики охоплюють інформаційні системи та мережу організації.
3. **Проблемно-залежні (Issue-specific)** - це політики, які створені на основі організаційних політик та містять в собі більш конкретні рекомендації щодо певних проблем.

3.3 Ключові аспекти політики безпеки

- **Мета**

  Організація створює політики інформаційної безпеки з різних причин:
  - Для встановлення основних підходів інформаційної безпеки
  - Для визначення та попередження компромісів інформаційної безпеки, наприклад, зловживання даними, мережами або комп’ютерними системами.
  - Для захисту репутації організації відповідно до етичних та правових норм.

- **Область застосування**

  В область застосування політики інформаційної безпеки повинні бути включені без виключень усі системи, обладнання, інформаційна інфраструктура, працівники та дані організації.

- **Цілі політики інформаційної безпеки**

  Для створення ефективної політики інформаційної безпеки організація повинна чітко визначити її цілі. Цілі політики ІБ мають бути погодженні вищим керівництвом, щоб уникнути неточностей, або розбіжностей, які можуть призвести до негативних наслідків.

- **Класифікація даних**

  Політика інформаційної безпеки повинна поділяти дані на категорії. Один з підходів - класифікація даних за п’ятьма рівнями відповідно до потреби в їх захисті:

  - **Рівень 1** - Загальнодоступна інформація
  - **Рівень 2** - Інформація, визначена організацією як конфіденційна, але її розкриття не призведе до матеріальних або репутаційних втрат.
  - **Рівень 3** - Інформація, розкриття якої може завдати незначної матеріальної або репутаційної шкоди окремим особам, або всій організації.
  - **Рівень 4** - Інформація, розкриття якої призведе до вагомої матеріальної, або репутаційної шкоди окремим особам, або всій організації.
  - **Рівень 5** - Інформація, розкриття якої може завдати сильної матеріальної або репутаційної шкоди окремим особам, або всій організації.

  При такій класифікації рівні 2 - 5 можуть класифікуватись як конфіденційна інформація і потребувати додаткового захисту

- **Повноваження та доступи**

  Зазвичай працівники різних рівнів, або відділів мають різні доступи до систем та інформації. Наприклад, розробник має доступ до вихідного коду, систем та інструментів розробки, в той час як проектний менеджер

має доступ до усієї проектної інформації. Працівники з різними рівнями доступів не підпадають під одні й ті ж умови політик інформаційної безпеки. Тобто політики повинні покривати усі базові посади організації зі специфікаціями пояснюючими їх повноваження та обов'язки в тій чи іншій сфері.

- **Навчання та освіченість персоналу**
  Поширення політик інформаційної безпеки серед персоналу є критичною та обов'язковою процедурою. Саме лише прочитання та ознайомлення з політиками не гарантує повного їх розуміння. Тому задля впевненості, що персонал повністю розуміє політики та описані в них процедури організація повинна організовувати тренінги та регулярно проводити тестування на розуміння політик ІБ.

- **Відповідальність, права, та обов'язку персоналу**
  Організація повинна визначити осіб відповідальних за впровадження, поширення, та регулярне оновлення політик інформаційної безпеки.

- **Посилання та відповідність законодавству**
  Існує низка різних законодавчих актів та законів, які можуть вплинути на процедури політик ІБ організації. Наприклад, в Україні перелік відповідних законів включатиме:
  - Закон України "Про інформацію" від 02.10.1992 №2657-XII
  - Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" від 05.07.1994 № 80/94-ВР
  - Закон України "Про державну таємницю" від 21.01.1994 № 3855-XII
  - Закон України "Про захист персональних даних" від 01.06.2010 № 2297-VI

Розділ 4
Стандарти та контролі інформаційної безпеки

4.1 NIST 800-53

4.1.1 Визначення стандарту

NIST SP 800-53 - це стандарт інформаційної безпеки, який складається з контролів ІБ та рекомендацій щодо їх впровадження. Розроблений для федеральних та комерційних організацій США, NIST SP 800-53 надає чіткі інструкції щодо покращення безпеки інформаційних систем. Це досягається за рахунок каталогу контролів, які підтримують створення безпечних та стійких інформаційних систем, та забезпечують три базові принципи ЦКД інформаційної безпеки.

4.1.2 Контролі стандарту

Контролі NIST SP 800-53 поділені на так звані сім'ї, кожна з яких відповідає за окрему сферу інформаційної безпеки. Далі наведена типова структура контролю NIST SP 800-53. Перш за все визначається код сімейства контролю та його номер, наприклад AU-3, де AU - це код сімейства Audit and Accountability (Аудит та звітність), а число 3, відповідно - це номер контролю. Далі вказується назва безпосередньо назва контролю, до прикладу «зміст записів аудиту», а після назви йдуть наступні розділи:

- **Контроль (Control)** – Опис дій та заходів, по відношенню до інформаційної безпеки, які потрібно виконати для впровадження контролю. Для деяких контролів передбачена можливість гнучкого налаштування, надаючи організації можливість самостійно визначати певні параметри контроля. Наприклад частота проведення аудиту, або термін зберігання логів може бути визначений організацією. Таким чином можна підганяти контроль під конкретні потреби, беручи до уваги вимоги бізнесу, результати оцінки ризиків, а також вимоги законів та регуляторів.

- **Додаткова інформація (Supplemental Guidance)** – Додаткова інформація для контролю. Містить в собі пояснювальну інформацію щодо впровадження контролю.
- **Покращення контролю (Control Enhancements)** – У цьому розділі представленні можливості з покращення контролю шляхом впровадження додаткового функціоналу, або покращення існуючого. Покращення описуються у вигляді під контролів.
- **Посилання (References)** – Тут зібрані посилання на законодавство, стандарти, вимоги регуляторів і т. д.
- **Пріоритет та базовий розподіл (Priority and Baseline Allocation)** – Інформація про рекомендований пріоритет при впорядкуванні в процесі прийняття рішення про реалізацію контролів.

Розгляньмо сімейства контролів стандарту NIST 800-52:

AC - Керування доступом

Сімейство керування доступом включає в себе контролі доступу до систем, мереж, та девайсів. Контролі надають інструкції щодо впровадження політик контролю доступу, політик керування обліковими записами, та привілеїв користувачів.

AT - Інформування та навчання

Контролі цього сімейства покликанні впевнитись, що усі користувачі, які мають доступ до інформаційних систем належним чином обізнані, щоб користуватись цими системами, а також самостійно ідентифікувати можливі загрози під час роботи з ними.

AU – Аудит та звітність

Сімейство аудиту та звітності пояснює, як організація повинна встановити процедури логування подій та аудиту. Воно охоплює базові параметри для записів аудиту, ємності зберігання журналів та вказівки, щодо моніторингу та перегляду журналів.

CA – Оцінка, Авторизація та моніторинг

Контролі цього сімейства націлені на постійне вдосконалення та моніторинг контролів інформаційної безпеки. Мета контролів – впевнитись, що контролі інформаційної безпеки залишаються ефективними з плином часу.

CM – Управління конфігурацією

Мета цього сімейства – це управління конфігурацією програмного забезпечення та мережі організації. Воно охоплює політки конфігурації, базові конфігурації систем, та управління авторизованим доступом до пристроїв. Впровадження цих контролів допомагає знизити ризик несанкціонованого встановлення програмного або апаратного забезпечення в системи організації.

CP – Планування неперервності

Контролі допомагають організації підготуватись до форс мажорних обставин. Сімейство включає в себе створення резервних сховищ даних, резервне копіювання систем, які допомагають зменшити та пом’якшити простій систем у випадку руйнування.

IA – Ідентифікація та автентифікація

Сімейство містить контролі, які допомагають ідентифікувати девайси та користувачів систем та мереж організації. Контролі сфокусовані на посиленні політик управління, та пониженні ризиків, пов’язаних з несанкціонованим доступом до систем організації.

IR – Реагування на інциденти

Сімейство контролів реагування на інциденти охоплює засоби контролю для конкретних подій, з якими може зіткнутись організація, зокрема зловмисного коду, витоків даних та збою в ланцюжках поставок.

MA – Обслуговування

Контролі сімейства обслуговування покривають технічне обслуговування систем, оновлення програмного забезпечення, та системи логування. Ціль контролів – впровадження політик та пониження ризиків пов’язаних з перебоями в роботі систем та мереж організації

MP – Захист носіїв інформації

Це сімейство включає в себе контролі націлені на захист медіа файлів, забезпечуючи безпечне використання, збереження та зниження всіх медіа файлів організації. Контролі допомагають впровадити базові засоби контролю пов’язані з пошкодженням та витоком інформації.

PE – Фізичний захист та захист від стихійних лих

Сімейство охоплює контролі пов’язані з фізичним доступом до об’єктів та пристроїв організації. Це допомагає організаціям впровадити політики контролю фізичного доступу, включаючи доступ відвідувачів та моніторинг пристроїв. Також контролі допомагають планувати та реагувати на такі загрози, як наприклад аварійне відключення живлення або екстрене переміщення організації у випадку стихійного лиха.

PL – Планування

Контролі сімейства планування відносяться до архітектури, планування безпеки, конфіденційності та управління системами організації.

PM – Програма управління

Сімейство контролів включає в себе елементи управління інформаційними технологіями та системами організації. Контролі допомагають впровадити плани, процеси та програми пов’язанні з системами організації. Це допомагає створити стратегію управління ризиками, план критичної інфраструктури, та план програми інформаційної безпеки.

PS – Безпека персоналу

Сімейство включає в себе політики та процедури управління персоналом. На приклад це допомагає організації визначити процедуру припинення контрактів, розуміти ризики, пов’язані з персоналом, який має відношення до інформаційної безпеки.

PT – Обробка та прозорість персональних даних

Контролі цього сімейства покликані на захист персональних даних. Це допомагає організаціям впровадити процеси управління, знищення даних, а також гарантувати наявність угод про обробку даних для захисту прав суб’єктів даних.

RA – Оцінка ризиків

Сімейство охоплює оцінку вразливостей та ризиків пов’язаних з системами організації. Контролі описують процедури реагування на ризики, процеси моніторингу вразливостей та інструменти оцінки ризиків.

SA – Придбання систем та сервісів

Контролі сімейства покривають процес розподілу ресурсів та політки життєвого циклу систем. Це допомагає організації безпечно придбати нові пристрої та системи, разом з тим захищаючи цілісність та безпеку існуючих систем та даних.

SC – Захист систем та комунікацій

Контролі включать в себе політики безпечного використання та обмеження для пристроїв спільного використання. Це допомагає організації впровадити контролі управління доступом та обмеження використання систем спільного використання.

SI – Цілісність систем та інформації

Це сімейство контролів охоплює такі теми, як захист від шкідливого коду, захист від спаму та процеси загальносистемного моніторингу. Контролі

сімейства впроваджуються для підтримки цілісності інформаційних систем організації.

SR – Управління ризиками ланцюжків поставок

Контролі цього сімейства пропонують політики для пониження ризиків у ланцюжку поставок. Сімейство включає в себе управління постачальниками, оцінку постачальників та перевірку елементів ланцюжка поставок.

Сімейства контролів NIST 800-53

Абревіатура	**Сім'я Контролів (EN)**	**Сім'я Контролів (UA)**
AC	Access Control	Керування доступом
AT	Awareness and Training	Інформування та навчання
AU	Audit and Accountability	Аудит та звітність
CA	Security Assessment and Authorization	Оцінка, авторизація та моніторинг
CM	Configuration Management	Управління конфігурацією
CP	Contingency Planning	Планування неперервності
IA	Identification and Authentification	Ідентифікація та автентифікація
IR	Incident Response	Реагування на інциденти
MA	Maintenance	Обслуговування
MP	Media Protection	Захист носіїв інформації
PE	Physical and Environmental Protection	Фізичний захист та захист від стихійних лих
PL	Planning	Планування
PM	Program Management	Керування програмою ІБ
PS	Personnel Security	Безпека персоналу
PT	PII Processing and Transparency	Обробка та прозорість персональних даних
RA	Risk Assessment	Оцінка ризиків

SA	System and Services Acquisition	Придбання систем та сервісів
SC	System and Communication Protection	Захист систем та комунікацій
SI	System and Information Integrity	Цілісність систем та інформації
SR	Supply Chain Risk Management	Управління ризиками ланцюжків поставок
PM	Program Management	Керування програмою ІБ

4.2 CIS контролі

4.2.1 Визначення CIS контролів

CIS контролі – це перелік заходів інформаційної безпеки, які допомагають організації пом’якшити ризики пов’язані з найбільш поширеними кібератаками. Головна перевага CIS контролів полягає в тому, що вони зосереджені на невеликій кількості дій, які в результаті допомагають організації значно знизити ризики кібербезпеки.

Загалом контролі були розроблені інститутом SANS і були відомі як SANS контролі, проте зараз вони керуються Центром Інтернет-безпеки і носять всім відому назву CIS контролі. Розробкою контролів займаються низка експертів з безпеки, з різноманітних сфер, до прикладу, кібербезпеки, освіти, державних установ та охорони здоров’я.

CIS контролі мають наступну структуру:

1. **Огляд (Overview)** – Короткий опис цілей контролю та його користі в якості захисної дії
2. **Чому цей контроль критичний? (Why is this control critical?)** – Опис важливості цього контролю для блокування, пом’якшення чи виявлення

кібератак, а також пояснення того, яким чином зловмисники можуть скористатися його відсутністю.

3. **Процедури та інструменти (Procedures and tools)** – Більш технічний опис процесів та технологій, які використовуються для впровадження та автоматизації контролю.
4. **Опис процедур захисту (Safeguard description)** – Перелік специфічних дій, які організація мусить зробити для впровадження контролю.

Також процедури захисту CIS контролів поділяються на три групи імплементації, відповідно до розмірів та структури організації:

1. **IG1** – Невелика або середніх розмірів організація, яка має невеликий досвід у сфері IT та інформаційної безпеки. Основним завданням таких компаній є забезпечення безперервної роботи бізнесу, оскільки вони є вразливими до простоїв. Як правило конфіденційні дані таких організацій обмежуються даними про співробітників та фінанси. Засоби захисту першої групи імплементації можуть бути впровадженні навіть з обмеженими знаннями та досвідом в сфері інформаційної безпеки. Вони спрямовані на запобігання загальним, нецільовим кібератакам.
2. **IG2** – Організація, яка має в своєму штаті людей, відповідальних за управління та захист IT-інфраструктури. Як правило такі організації мають поділ на відділи з різними профілями ризику, базованими на посадових функціях та завданнях. Організації другої групи імплементації часто зберігають і обробляють персональні дані клієнтів, та іншу конфіденційну інформацію, а також такі організації є стійкими до короткочасних простоїв бізнесу. Головна загроза для таких організацій – репутаційні та фінансові втрати при порушені інформаційної безпеки.
3. **IG3** – Організація великих розмірів, яка має в своєму штаті експертів з інформаційної та кібербезпеки. Організації третьої групи імплементації як правило зберігають та обробляють конфіденційну інформацію яка захищається нормативно-правовими актами тієї чи іншої країни. Головне

завдання такої організації – це турбота за доступність послуг та конфіденційність і цілісність даних.

4.2.2 Огляд контролів

CIS контролі складаються з 18 контролів, а контролі в свою чергу містять перелік запобіжних заходів:

1. **Інвентаризація та контроль апаратних активів (Inventory and Control of Hardware Assets)**

   Контроль містить в собі 5 запобіжних заходів:

   1. Створення та ведення детальної інвентаризації активів підприємства
   2. Виявлення неавторизованих активів
   3. Використання інструментів активного виявлення активів
   4. Використання протоколу динамічної конфігурації хоста (DHCP) для оновлення інвентарю активів підприємства.
   5. Використання інструментів пасивного виявлення активів

2. **Інвентаризація та контроль програмних активів (Inventory and Control of Software Assets)**

   Контроль складається з 7 запобіжних заходів:

   1. Створення та ведення детальної інвентаризації програмного забезпечення
   2. Впевнення, що авторизоване програмне забезпечення підтримується
   3. Виявлення неавторизованого програмного забезпечення
   4. Використання інструментів автоматизованої інвентаризації програмного забезпечення
   5. Білий список авторизованого програмного забезпечення
   6. Білий список авторизованих бібліотек
   7. Білий список авторизованих скриптів

3. **Захист даних (Data Protection)**

   Контроль містить 14 запобіжних заходів:

   1. Впровадження та підтримка процесу управління даними
   2. Впровадження та підтримка інвентаризації даних

3. Налаштування списків контролю доступу до даних
4. Примусове збереження даних
5. Безпечна утилізація даних
6. Шифрування даних на пристроях кінцевих користувачів
7. Впровадження та підтримка схеми класифікації даних
8. Документування потоків даних
9. Шифрування даних на знімних носіях
10. Шифрування конфіденційних даних під час передачі
11. Шифрування конфіденційних даних які знаходяться в спокої
12. Сегментування обробки та зберігання даних на основі конфіденційності
13. Розгортання рішень для запобігання втрати даних
14. Логування доступу до конфіденційних даних

4. **Безпечна конфігурація активів та програмного забезпечення організації (Secure Configuration of Enterprise Assets and Software)**

Контроль містить 12 запобіжних заходів:

1. Впровадження та підтримка безпечного процесу конфігурації
2. Впровадження та підтримка безпечного процесу конфігурації мережевої інфраструктури
3. Налаштування автоматичного блокування сеансів для активів організації
4. Впровадження та управління брандмауерами на серверах
5. Впровадження та управління брандмауерами на девайсах кінцевих користувачів
6. Безпечне управління корпоративними активами та програмним забезпеченням
7. Управління аккаунтами за замовчуванням корпоративних активів та програмного забезпечення
8. Видалення або відключення непотрібних сервісів корпоративних активів та програмного забезпечення
9. Налаштування довірених DNS-серверів на активах організації

10. Примусове автоматичне блокування портативних пристроїв кінцевих користувачів
11. Впровадження функції віддаленого стирання портативних пристроїв кінцевих користувачів
12. Відділення корпоративної робочої області на мобільних пристроях кінцевих користувачів

5. Управління аккаунтами

Контроль містить 6 запобіжних заходів:

1. Впровадження та підтримка інвентаризації аккаунтів
2. Використання унікальних паролів
3. Відключення неактивних аккаунтів
4. Обмеження адміністраторських прав для виділення окремих аккаунтів з адміністраторськими правами
5. Впровадження та підтримка інвентаризації сервісних аккаунтів
6. Централізоване управління акаунтами

6. Управління доступами

Контроль містить 8 запобіжних заходів:

1. Впровадження процесу надання доступів
2. Впровадження процесу скасування доступів
3. Впровадження MFA для зовнішніх додатків
4. Впровадження MFA для віддаленого доступу до мережі
5. Впровадження MFA для адміністративного доступу
6. Впровадження та підтримка інвентаризації систем автентифікації та авторизації
7. Централізоване управління доступами
8. Впровадження та підтримка управління доступами на основі ролей

7. Безперервне управління вразливостями

Контроль містить 7 запобіжних заходів:

1. Впровадження та підтримка процесу управління вразливостями
2. Впровадження та підтримка процесу відновлення
3. Виконання автоматичного оновлення операційних систем

4. Виконання автоматичного оновлення додатків
5. Виконання автоматичного сканування внутрішніх активів організації на наявність вразливостей
6. Виконання автоматичного сканування зовнішніх активів організації на наявність вразливостей
7. Усування виявлених вразливостей

8. Управління аудит-логами

Контроль містить 12 запобіжних заходів:

1. Впровадження та підтримка процесу управління аудит-логами
2. Збір аудит-логів
3. Забезпечення належного зберігання аудит-логів
4. Синхронізація часу
5. Детальний збір аудит-логів
6. Збір аудит-логів DNS запитів
7. Збір аудит-логів URL запитів
8. Збір аудит-логів командного рядка
9. Централізація аудит-логів
10. Збереження аудит-логів
11. Проведення перевірки аудит-логів
12. Збір логів постачальників послуг

9. Захист електронної пошти та веб-браузерів

Контроль містить 7 запобіжних заходів:

1. Використання лише повністю підтримуваних браузерів та клієнтів електронної пошти
2. Використання служб фільтрації DNS
3. Впровадження та підтримка мережевих URL-фільтрів
4. Обмеження використання непотрібних або несанкціонованих розширень браузерів та клієнтів електронної пошти
5. Впровадження DMARC
6. Блокування непотрібних типів файлів

7. Розгортання та підтримка системи захисту сервера електронної пошти від шкідливого програмного забезпечення

10. Захист від шкідливого програмного забезпечення

Контроль містить 7 запобіжних заходів:

1. Розгортання та підтримка систем захисту від шкідливого програмного забезпечення
2. Налаштування автоматичного оновлень сигнатур систем захисту від шкідливого ПЗ
3. Відключення автозапуску та автовідтворення для знімних носіїв даних
4. Налаштування автоматичного сканування знімних носіїв на наявність вразливого ПЗ
5. Увімкнення функції захисту експлуатації
6. Централізоване управління системами захисту від шкідливого ПЗ
7. Використання поведінкових систем захисту від шкідливого ПЗ

11. Відновлення даних

Контроль містить 5 запобіжних заходів:

1. Впровадження та підтримка процесу відновлення даних
2. Автоматичне резервне копіювання
3. Захист даних відновлення
4. Впровадження та підтримка ізольованої точки відновлення даних
5. Тестування відновлення даних

12. Управління мережевою інфраструктурою

Контроль містить 8 запобіжних заходів:

1. Впевнення, що мережева інфраструктура оновлена
2. Впровадження та підтримка безпечної мережевої інфраструктури
3. Безпечне управління мережевою інфраструктурою
4. Впровадження та підтримка діаграм архітектури
5. Централізація мережевої автентифікації, авторизації та аудиту.
6. Використання безпечного управління мережею та протоколів зв’язку

7. Впевнення, що віддалені пристрої використовують VPN та підключення до AAA інфраструктури організації
8. Визначення та підтримка виділених комп'ютерних ресурсів для всієї адміністративної роботи

13. Моніторинг та захист мережі

Контроль містить 11 запобіжних заходів:

1. Централізована система оповіщення про інциденти безпеки
2. Розгортання системи виявлення вторгнення на хостах
3. Розгортання системи виявлення вторгнення в мережах
4. Виконання фільтрації трафіку між сегментами мережі
5. Управління контролем доступу до віддалених активів
6. Збір логів мережевого трафіку
7. Розгортання системи запобігання вторгнення на хостах
8. Розгортання системи запобігання вторгнення в мережах
9. Впровадження контролю доступу на рівні порту
10. Виконання фільтрації прикладного рівня
11. Налаштування порогових значень для сповіщень про інциденти безпеки

14. Тренінги та підвищення обізнаності в безпеці

Контроль містить 9 запобіжних заходів:

1. Визначення та підтримка програми обізнаності безпеки
2. Навчання персоналу розпізнавати атаки з використанням соціальної інженерії
3. Навчання персоналу найкращим практикам автентифікації
4. Навчання персоналу найкращим практикам обробки даних
5. Навчання персоналу щодо причин ненавмисного розкриття даних
6. Навчання персоналу розпізнавати ти звітувати про інциденти безпеки
7. Навчання персоналу визначати та повідомляти про активи організації з відсутніми оновленнями

8. Навчання персоналу щодо небезпеки підключення та передачі корпоративних даних через незахищені мережі.
9. Проведення тренінгів з питань безпеки відповідно до специфіки позиції працівників

15. Управління сервіс-провайдерів

Контроль містить 7 запобіжних заходів:

1. Впровадження та підтримка інвентаризації сервіс-провайдерів
2. Впровадження та підтримка політики управління сервіс-провайдерами
3. Класифікація сервіс-провайдерів
4. Впевнення, що контракти з сервіс-провайдерами включають в себе вимоги безпеки
5. Оцінка сервіс-провайдерів
6. Моніторинг сервіс-провайдерів
7. Безпечне виведення з експлуатації сервіс-провайдерів

16. Безпека програмного забезпечення

Контроль містить 14 запобіжних заходів:

1. Впровадження та підтримка безпечного процесу розробки ПЗ
2. Впровадження та підтримка процесу прийняття та усунення вразливостей ПЗ
3. Виконання аналізу першопричин вразливостей безпеки
4. Впровадження та підтримка інвентаризації програмних компонентів сторонніх розробників
5. Використання оновлених та довірених програмних компонентів сторонніх розробників
6. Впровадження та підтримка системи та процесу оцінки важливості вразливостей ПЗ
7. Використання стандартних посилених шаблонів конфігурації для додатків інфраструктури
8. Розділення виробничих та невиробничих систем

9. Навчання розробників щодо концептів безпеки додатків та безпечного кодування
10. Застосування принципів безпечного проектування в архітектурі додатків
11. Використання перевірених модулів та сервісів для компонентів безпеки ПЗ
12. Впровадження перевірки безпеки на рівні коду
13. Проведення тестування додатків на проникнення
14. Проведення моделювання загроз

17. Управління реагуванням на інциденти

Контроль містить 9 запобіжних заходів:

1. Призначення персоналу відповідального за врегулювання інцидентів
2. Визначення та підтримка контактної інформації для повідомлення про інциденти безпеки
3. Впровадження та підтримка корпоративного процесу повідомлення про інциденти безпеки
4. Впровадження та підтримка процесу повідомлення про інциденти безпеки
5. Призначення ключових ролей та обов’язків
6. Визначення механізмів комунікації під час реагування на інциденти
7. Проведення регулярних навчань щодо реагування на інциденти
8. Проведення пост-перегляду інцидентів
9. Визначення та підтримка порогових значень інцидентів безпеки

18. Тестування на проникнення

Контроль містить 5 запобіжних заходів:

1. Визначення та підтримка програми тестування на проникнення
2. Періодичне проведення тестування на проникнення ззовні
3. Усунення результатів тесту на проникнення
4. Перевірка заходів безпеки
5. Періодичне проведення внутрішнього тестування на проникнення

Розділ 5
Застосування у AWS

5.1 Відповідність

Популярні хмарні сервіси, як правило, пройшли сертифікацію незалежними організаціями щодо відповідності відомим стандартам та контролям ІБ. Проте, беручи до уваги те, що з їх допомогою стороні організації будують власну інфраструктуру для досягнення бізнес цілей, відповідальність за відповідність стандартам та контролям інформаційної безпеки розповсюджуються на обидві сторони:

1. **Спільна відповідальність** – клієнт несе відповідальність за відповідність стандарту конфігурації ресурсів хмарного сервісу, а провайдер в свою чергу відповідальний за відповідність на стороні інфраструктури.
2. **Відповідальність клієнта** – клієнт несе повну відповідальність за налаштування безпеки гостьових операційних систем, розгорнутих додатків та мережевих ресурсів. Зокрема клієнт несе повну відповідальність за налаштування безпеки з точки зору конфігурації хмарних ресурсів.
3. **Відповідальність провайдера** - Провайдер відповідальний безпосередньо за інфраструктуру, тобто фізичні мережі, носії даних, системні ресурси, ЦЗОД, та фізичну безпеку.

Для нас особливо цікавою є відповідність з точки зору клієнта хмарних сервісів. Популярні хмарні провайдери надають вбудовані сервіси для управління безпекою. На приклад AWS Security Hub для AWS, Security Command Center для GCP та Azure Security Center для Azure.

В якості прикладу розглянемо детальніше рішення від AWS, а саме AWS Security Hub. Security Hub – це сервіс, який надає можливість збирати, організовувати та керувати сповіщеннями та знахідками безпеки з різноманітних

сервісів безпеки AWS, або навіть сторонніх інструментів безпеки. Окрім цього, сервіс надає можливість проводити перевірки безпеки хмарного середовища відповідно до популярних стандартів та контролів інформаційної безпеки, включаючи вище згаданий стандарт NIST 800-53 та CIS контролі.

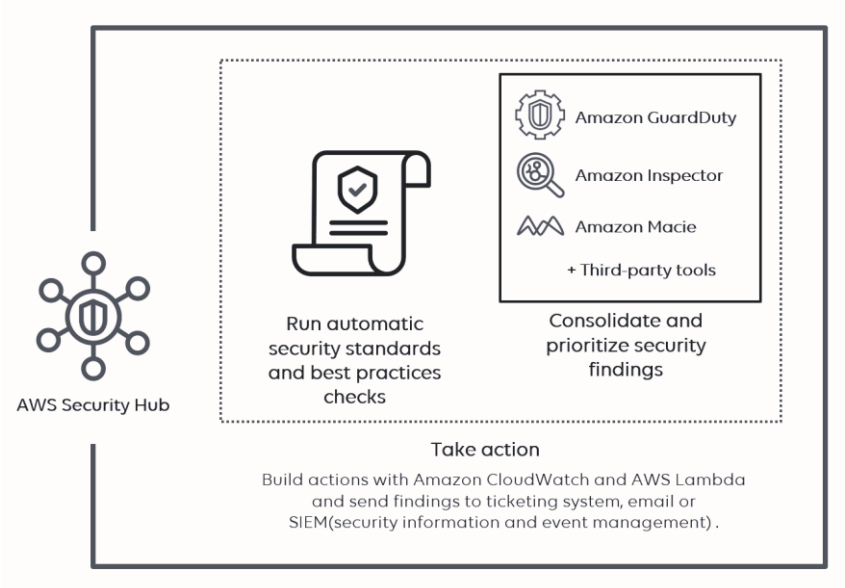

Рисунок 5.1

5.2 Практичне застосування

Для демонстрації практичного застосування контролів NIST 800-53 та CIS в хмарних сервісах, я використав Security Hub у власному обліковому записі AWS. Після проходження перевірки я отримав наступні результати:

- Загальна відповідність – 83 %
- Відповідність CIS контролям – 35%
- Відповідність NIST SP 800-53 – 88%

У випадку з CIS контролями, 24 з 39 контролів не пройшли перевірку. Далі розглянемо їх, та усунемо:

1. **Апаратний MFA має бути увімкнений для користувача root** – З огляду на те, перевірка відбувалась у персональному обліковому записі AWS, цей контроль можна вимкнути визначивши як «незастосовний для цього середовища»

2. **Віртуальний MFA має бути увімкнений для користувача root** – Ця невідповідність була усунута після налаштування віртуального MFA, у моєму випадку DUO MFA, для root користувача.
3. **CloudTrail має бути увімкнений та налаштований для логування подій запису та читання** – Цей контроль також не застосовний до персонального облікового запису, тому був відімкнутий.
4. **Групи безпеки VPC за замовчуванням повинні обмежувати весь вхідний та вихідний трафік –** Попередження було усунуте шляхом видалення вхідних та вихідних правил групи безпеки стандартного VPC, які дозволяли прохід всього вхідного та вихідного трафіку.
5. **AWS Config має бути увімкнутий для всіх регіонів –** Як правило я використовую AWS лише в одному регіоні, тому увімкнення AWS Config для всіх регіонів не є необхідним. Цей контроль також був відімкнутий.
6. **Мережеві списки контролю доступу не повинні дозволяти вхід із 0.0.0.0/0 на порт 22 або порт 3389 –** Цей контроль є надзвичайно важливим, так як він дозволяє переконатись, що SSH та RDP доступ до ресурсів є обмеженим, проте не у випадку з особистим хмарним середовищем.
7. **Логування потоку VPC має буте увімкненим для всіх VPC –** Як і попередній контроль, функція логування потоку VPC є важливою, але не у випадку з особистим аккаунтом, так як збереження логів призведе до зайвих витрат. Контроль був відімкнутий.
8. **Шифрування EBS має бути увімкнуте за замовчуванням –** Попередження безпеки було усунуте шляхом увімкнення шифрування EBS за замовчуванням.
9. **Політика паролів IAM повинна вимагати мінімальної довжини пароля в 14 символів, або більше –** Невідповідність була усунута шляхом зміни мінімальної довжини пароля у політиці паролів IAM з 8 до 14 символів.
10. **Налаштування блокування публічного доступу S3 має бути ввімкнене –** Блокування публічного доступу до S3 було увімкнене.

11. **Політика паролів IAM має запобігати повторному використанню пароля –** Невідповідність була усунута шляхом увімкнення функції запобігання повторному використанню паролів.
12. **Роль підтримки для керування інцидентами має бути визначена –** Створення подібних ролей не є необхідним для персонального облікового запису AWS. Контроль був відімкнутий.

Наступні 12 невідповідностей відносяться до логування CloudWatch і не необхідними для персонального облікового запису. Усі вони були відімкнуті.

Далі розглянемо та попрацюємо з результатами перевірок відповідно до стандарту NIST 800-53. 24 з 220 контролів не пройшли перевірку:

1. **Групи безпеки не повинні дозволяти необмежений доступ до портів з високим ризиком –** Контроль перевіряє чи групи безпеки дозволяють необмежений вхідний трафік до портів з високим ризиком (22, 3389, 23 і т. д.). Для усунення невідповідності 2 непотрібні групи безпеки які дозволяли вхідний трафік на порт 22 були видалені.
2. **Апаратний MFA має бути увімкнений для користувача root –** Як і у випадку з аналогічною перевіркою відповідності CIS контролям, апаратний MFA не є застосовним у випадку з особистим обліковим записом AWS. Контроль був відімкнутий.
3. **Віртуальний MFA має бути увімкнений для користувача root –** Ця невідповідність була усунута в межах роботи з перевірками CIS.
4. **Групи безпеки повинні дозволяти необмежений вхідний трафік лише для авторизованих портів –** За замовчуванням лише порти 80 та 443 є авторизованими для необмеженого вхідного трафіку. Перелік авторизованих портів може бути розширеним, проте у нашому випадку це не є необхідним, так як усі групи безпеки, окрім стандартної, були видалені.
5. **Групи безпеки не повинні дозволяти вхідний трафік на порт 22 з будь-якого джерела (0.0.0.0/0) –** Невідповідність була усунута в межах попередніх контролів.

6. **Обліковий запис AWS має бути частиною AWS організації –** З огляду на те, що приватний обліковий запис AWS як правило використовується лише в одному регіоні, впровадження AWS організації не є необхідним. Контроль був відімкнутий.
7. **CloudTrail має бути увімкнений та налаштований для логування подій запису та читання –** Аналогічний контроль був відімкнутий в рамках перевірки відповідності CIS контролям. Тому відповідно перевірка була відімкнута і у випадку з NIST 800-53.
8. **Групи безпеки VPC за замовчуванням повинні обмежувати весь вхідний та вихідний трафік** – Невідповідність була усунута в межах перевірки відповідності CIS контролям.
9. **Екземпляри EC2 мають використовувати службу метаданих версії 2 (IMDSv2) –** Цей контроль не пройшов перевірку тому, що на момент аналізу екземпляр EC2 був запущений без увімкненого IMDSv2. З огляду на те, що екземпляр був зупинений та видалений, невідповідність була усунута.
10. **Сканування зображень має бути увімкненим для приватних репозиторіїв ECR –** Невідповідність була усунута шляхом увімкнення сканування зображень при завантаженні для приватного репозиторію ECR.
11. **GuardDuty має бути увімкненим –** Сервіс GuardDuty – це сервіс виявлення загроз. З урахуванням того, що в приватному обліковому записі AWS немає постійно розгорнутих сервісів, які потенційно можуть містити загрози безпеки та вразливості, це контроль не є застосовним тут і був відімкнутий.
12. **Підмережі EC2 не повинні автоматично призначати публічні IP-адреси –** Запропоновані контролем зміни не є зручними для приватного облікового запису AWS. Контроль був відімкнутий.
13. **Контакти служби безпеки мають бути визначені для облікового запису AWS –** Контроль не є застосовним для приватного облікового запису, тому був відімкнутий.

14. **AWS Config сервіс має бути увімкнений –** Беручи до уваги те, що сервіс AWS Config покликаний аналізувати конфігурацію ресурсів AWS, а у випадку з особистим обліковим записом життєвий цикл ресурсів є доволі коротким, немає необхідності в моніторингу їх конфігурації. Контроль був відімкнутий.
15. **Amazon EC2 має бути налаштований на використання кінцевих точок VPC, створених для EC2 –** Кінцеві точки VPC допомагають покращити безпеку віртуальних хмар, шляхом уникання публічних IP-адрес, тобто трафік між сервісами та віртуальними хмарами не буде покидати мережу AWS. Проте цей функціонал не є необхідним для особистого облікового запису AWS. Контроль був відімкнутий.
16. **Мережеві списки контролю доступу не повинні дозволяти вхід із 0.0.0.0/0 на порт 22 або порт 3389 –** Як і у випадку з аналогічним контролем для CIS, контроль був відімкнутий.
17. **Групи безпеки EC2, які не використовуються мають бути видалені –** Для усунення невідповідності, 3 групи безпеки, які не використовуються були видалені.
18. **Прикріплені EBS диски мають бути зашифровані –** Шифрування EBS було увімкнене у рамках усунення невідповідностей CIS контролям, а існуючий диска EBS був видалений разом із екземпляром EC2. Надалі усі EBS диски будуть створюватись шифруванням за замовчуванням
19. **Логування потоку VPC має буте увімкненим для всіх –** Цей контроль був відімкнутий тут так само як і у межах перевірки відповідності CIS контролям.
20. **Шифрування EBS має бути увімкнуте за замовчуванням –** Невідповідність була виправлена у межах перегляду відповідності CIS контролям.
21. **У приватних репозиторіях ECR має бути налаштована незмінність тегів** – Контроль не є застосовним тому, що специфіка тегування зображень приватного репозиторію ECR вимагає змін тегів.

22. **ECR репозиторії повинні мати хоча б одну налаштовану політику життєвого циклу** – Для усунення невідповідності була створена політика життєвого циклу для видалення зображень без тегів через 7 днів після завантаження.
23. **Політики паролів IAM користувачів повинні мати надійну конфігурацію** – Для усунення невідповідності у політику паролів було додано вимоги щодо створення паролів. Паролі повинні містити великі та малі літери, спец символи та цифри.
24. **Диски EBS повинні бути включені в план резервного копіювання** – З огляду на те, що персональний обліковий запис AWS не містить постійних екземплярів EC2, які вимагають резервного копіювання, цей контроль був відімкнутий.

В результаті роботи з виявленими в результаті перевірок AWS Security Hub недоліками, вдалось усунути деякі з них, тим самим покращивши стан безпеки власного облікового запису AWS. Інші невідповідності були відімкнуті, так як вони не є застосовними у даному випадку.

У підсумку можна сказати, що AWS Security Hub – надзвичайно корисний та зручний сервіс, який може допомогти в організації інформаційної безпеки як організаціям, так і рядовим користувачам AWS сервісів.

ВИСНОВКИ

В ході дослідження була розглянута тема стандартів та контролів інформаційної безпеки для хмарних сервісів та проведений аналіз відповідності контролів NIST 800-53 та CIS в хмарному сервісі AWS за допомогою AWS Security Hub.

Інформаційна безпека є критично важливим аспектом використання хмарних сервісів, оскільки на їх основі організації будують ту чи іншу інфраструктуру, в якій, як правило, зберігається та обробляється конфіденційна інформація. В свою чергу використання стандартів та контролів інформаційної безпеки є необхідним для забезпечення інформаційної безпеки в хмарних сервісах.

Стандарт NIST 800-53 є одним з основних стандартів інформаційної безпеки. Він надає широкий спектр контролів та заходів безпеки, які можуть бути застосовані для хмарних сервісів.

CIS контролі так само надають рекомендації, щодо інформаційної безпеки, зокрема безпеки хмарних сервісів.

Під час роботи було проведено аналіз відповідності контролям NIST 800-53 та CIS в хмарному сервісі AWS. Це було досягнуто за рахунок використання вбудованого в AWS сервісу AWS Security Hub, який надає можливість контролю відповідності популярним стандартам та контролям інформаційної безпеки, в тому числі NIST 800-53 та CIS контролів.

В результаті перевірки відповідності, було виявлено значну кількість недоліків у налаштуваннях сервісів AWS, які на пряму впливали на стан інформаційної безпеки облікового запису AWS. Більшість невідповідностей були усунуті шляхом налаштувань ресурсів AWS. Також деякі з контролів були відімкнуті через свою незастосовність в межах особистого облікового запису AWS. Як результат було досягнуто відповідності стандарту NIST 800-53 та CIS контролям.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. https://www.ifsecglobal.com/cyber-security/a-history-of-information-security/
2. https://uk.wikipedia.org/wiki/%D0%A5%D1%80%D0%BE%D0%B1%D0%B0%D0%BA_%D0%9C%D0%BE%D1%80%D1%96%D1%81%D0%B0
3. https://www.dataversity.net/brief-history-cloud-computing/
4. https://advisera.com/27001academy/what-is-iso-27001/
5. https://secureframe.com/hub/iso-27001/history
6. https://en.wikipedia.org/wiki/ISO/IEC_27001
7. https://resources.infosecinstitute.com/topic/iso-27001-framework-what-it-is-and-how-to-comply/
8. https://www.standardfusion.com/blog/iso-27001-mandatory-clauses/
9. https://preteshbiswas.com/2023/01/01/iso-270012022-a-5-23-information-security-for-use-of-cloud-services/
10. https://resources.infosecinstitute.com/topic/key-elements-information-security-policy/
11. https://nira.com/nist-sp-800-53-control-families-explained/
12. https://www.researchgate.net/publication/326414873_Analysis_of_NIST_SP_800-53_Rev3_Controls_Effectiveness_for_Cloud_Computing
13. https://sprinto.com/blog/soc-2-controls/
14. https://www.upguard.com/blog/cis-controls
15. https://docs.aws.amazon.com/securityhub/latest/userguide/what-is-securityhub.html