МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ
КРИВОРІЗЬКИЙ ФАХОВИЙ КОЛЕДЖ
ДЕРЖАВНОГО НЕКОМЕРЦІЙНОГО ПІДПРИЄМСТВА
«ДЕРЖАВНИЙ УНІВЕРСИТЕТ «КИЇВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ»
Циклова комісія *комп'ютерних систем та мереж*
(повна назва циклової комісії)

Допустити до захисту
Голова випускової циклової комісії
комп'ютерних систем та мереж
(повна назва циклової комісії)
_____ *Ірина КРАВЧУК*
(підпис) (ім'я, ПРІЗВИЩЕ)
« *10* » *06* 2025 р.

КВАЛІФІКАЦІЙНА РОБОТА
(ПОЯСНЮВАЛЬНА ЗАПИСКА)

ВИПУСКНИКА ОСВІТНЬО-ПРОФЕСІЙНОГО СТУПЕНЯ
ФАХОВИЙ МОЛОДШИЙ БАКАЛАВР

Тема: *Дослідження механізмів безпеки та контролю доступу в SDA*

Група: *3-013* Спеціальність: *123 «Комп'ютерна інженерія»*

Здобувач освіти _____ *Олексій КОНОВАЛЬЧУК*
(підпис) (ім'я, ПРІЗВИЩЕ)

Керівник роботи _____ *Владислав СОБЧУК*
(підпис) (ім'я, ПРІЗВИЩЕ)

Консультант з оформлення
пояснювальної записки _____ *Оксана ОСАДЧА*
(підпис) (ім'я, ПРІЗВИЩЕ)

Кривий Ріг 2025 р.

КРИВОРІЗЬКИЙ ФАХОВИЙ КОЛЕДЖ
ДЕРЖАВНОГО НЕКОМЕРЦІЙНОГО ПІДПРИЄМСТВА
«ДЕРЖАВНИЙ УНІВЕРСИТЕТ «КИЇВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ»

Відділення *комп'ютерної та програмної інженерії*
Циклова комісія *комп'ютерних систем та мереж*
Освітньо-професійний ступінь *фаховий молодший бакалавр*
Спеціальність *123 «Комп'ютерна інженерія»*

ЗАТВЕРДЖУЮ
Голова випускової циклової комісії
комп'ютерних систем та мереж
(повна назва циклової комісії)
_____ *Ірина КРАВЧУК*
(підпис) (ім'я, ПРІЗВИЩЕ)
« *09* » *03* 2025 р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ ЗДОБУВАЧУ ОСВІТИ

КОНОВАЛЬЧУК Олексію Едуардовичу
(прізвище, ім'я, по батькові)

1.Тема роботи *Дослідження механізмів безпеки та контролю доступу в SDA*

Керівник роботи *СОБЧУК Владислав*
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по коледжу від « *04* » *04* 2025 року № *51-ст*

2. Строк подання здобувачем освіти роботи з _____ по _____

3. Вихідні дані до роботи *Дослідження механізмів безпеки в SDA*

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
Аналіз предметної області, інформаційна безпеки у корпоративному середовищі, основні загрози, традиційні методи контролю доступу, підходи до захисту корпоративних мереж (DLP, IAM, SIEM), концепція *SDN Software-Defined Networking, архітектуру SDA (Software-Defined Access), механізми контролю доступу в SDA: RBAC, ABAC, SGT, виконані порівняльні характеристики, впровадження Zero Trust,використання Cisco ISE, переваги SDA, інтеграції SDA*

з системами SIEM, EDR та IAM, модель CMM (Capability Maturity Model), проведено оцінку ефективності контролю доступу й рівня захисту, проаналізовано результати та надано пропозиції щодо їх вдосконалення.

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

6. Консультанти розділів роботи (проекту)

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

7. Дата видачі завдання _____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	*Узгодження технічного завдання*	*14.02.2025*	*Виконано*
2.	*Огляд літератури по темі роботи*	*10.03.2025*	*Виконано*
3.	*Аналіз предметної області*	*10.04.2025*	*Виконано*
4.	*Концепція SDN (Software-Defined Networking)*	*21.04.2025*	*Виконано*
5.	*Архітектура SDA (Software-Defined Access*	*05.05.2025*	*Виконано*
6.	*Механізми контролю (RBAC, ABAC, SGT)*	*15.05.2025*	*Виконано*
7.	*Оцінка ефективності контролю доступу*	*20.05.2024*	*Виконано*
8.	*Оцінка рівня захисту*	*25.05.2025*	*Виконано*
9.	*Оформлення пояснювальної записки*	*30.05.2025*	*Виконано*
10.	*Захист кваліфікаційної роботи*		

Здобувач освіти _____ *Олексій КОНОВАЛЬЧУК*
(підпис) (ім'я, ПРІЗВИЩЕ)

Керівник роботи _____ *Владислав СОБЧУК*
(підпис) (ім'я, ПРІЗВИЩЕ)

StrikePlagiarism.com

Дата звіту 6/10/2025

Дата редагування ---

Документ прийнятий

Звіт подібності

метадані

Назва організації

Ukrainian national aviation university

Заголовок

123_Коновальчук О._3-013_2025

Автор Науковий керівник / Експерт

Коновальчук О.Собчук В.

підрозділ

Криворізький Фаховий коледж

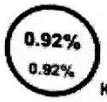
Обсяг знайдених подібностей

Коефіцієнт подібності визначає, який відсоток тексту по відношенню до загального обсягу тексту було знайдено в різних джерелах. Зверніть увагу, що високі значення коефіцієнта не автоматично означають плагіат. Звіт має аналізувати компетентна / уповноважена особа.

КП 1

25

Довжина фрази для коефіцієнта подібності 2



КЦ

9214

Кількість слів

71209

Кількість символів

РЕФЕРАТ

Пояснювальна записка до кваліфікаційної роботи «Дослідження механізмів безпеки та контролю доступу в *SDA*» викладена на 67 с., містить 35 рис., 8 табл., 12 використаних літературних джерел.

БЕЗПЕКА, МОДЕЛЬ, АВТОРИЗАЦІЯ, ДОСТУП, ЗАГРОЗА, ДАНІ, ЗАХИСТ, АДМІНІСТРУВАННЯ, МЕРЕЖА, СЕГМЕНТАЦІЯ, ІНТЕГРАЦІЇ **Мета:** дослідити механізми безпеки та контролю доступу в *SDA*. Впровадження *SDA* є актуальним і перспективним напрямом розвитку *IT* інфраструктури, забезпечуючи надійний захист корпоративних ресурсів і даних. В ході роботи проаналізовані основні загрози інформаційній безпеці в *IT* інфраструктурі, традиційні методи контролю доступу, підходи до захисту корпоративних мереж (*DLP, IAM, SIEM*), концепцію *SDN* (*Software-Defined Networking*), загальні характеристики архітектури *SDA* (*Software-Defined Access*), механізми контролю доступу в *SDA: RBAC, ABAC, SGT*, виконані порівняльні характеристики, політику безпеки у *SDA* та впровадження *Zero Trust*, використання *Cisco ISE* для ідентифікації та авторизації користувачів, сегментацію трафіку та динамічне управління доступом, переваги *SDA* у порівнянні з традиційними мережевими рішеннями.

Дослідження інтеграції *SDA* з системами *SIEM, EDR* та *IAM*, проведено оцінку ефективності контролю доступу й рівня захисту, модель *CMM* (*Capability Maturity Model*), проаналізовано результати та надано пропозиції щодо їх вдосконалення.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ ТА ТЕРМІНІВ

DAC (Discretionary Access Control) - дискреційний контроль доступу *IAM* (*Identity and Access Management*) - комплекс технологій, політик і процесів, які забезпечують ідентифікацію користувачів

SIEM (*Security Information and Event Management*) - система для централізованого збору, зберігання, аналізу та кореляції подій безпеки з різних джерел у мережі

SDN (Software-Defined Networking) - концепція побудови комп'ютерних мереж ЦОД - центр обробки даних

SDA (*Software-Defined Access*) - розширенням концепції *SDN*

DHCP (*Dynamic Host Configuration Protocol*) - мережевий протокол, який автоматично призначає *IP*-адреси

NTP (*Network Time Protocol*) - протокол мережевого часу

DNS (*Domain Name System*) - система доменних імен

ARP (*Address Resolution Protocol*) - протокол, який використовується для визначення *MAC*-адреси пристрою

SGT (*Security Group Tags*) - призначення тегів груп безпеки для користувачів/пристроїв

SGACL (*Security Group Access Control Lists*) - правила, які визначають дозволені або заборонені взаємодії між *SGT*

IDS (*Intrusion Detection System*) - система виявлення вторгнень

IPS (*Intrusion Prevention System*) - система запобігання атакам

CMM (*Capability Maturity Model*) - п’ятирівнева модель, яка дозволяє оцінити ступінь зрілості процесів в організації

ВСТУП

У сучасному світі інформаційні технології відіграють ключову роль у функціонуванні організацій різного масштабу - від невеликих компаній до міжнародних корпорацій.

Зі зростанням обсягів передавання даних, поширенням мобільних пристроїв та хмарних сервісів питання забезпечення безпеки мережі та контролю доступу до ресурсів набувають особливої актуальності.

У корпоративному середовищі впровадження системи інформаційної безпеки дозволяє запобігати витокам конфіденційних даних, виявляти та реагувати на кіберзагрози в реальному часі, дотримуватися законодавчих та галузевих норм, підвищити рівень довіри з боку клієнтів і партнерів, забезпечити стабільну роботу критично важливих бізнес-систем.

Ефективна система інформаційної безпеки вимагає комплексного підходу: технічних рішень (фаєрволи, антивіруси, *SIEM*-системи), політик доступу, навчання персоналу та регулярного аудиту ризиків. Особливої уваги набуває

побудова адаптивної моделі безпеки, яка враховує змінні загрози та дозволяє швидко реагувати на інциденти.

Традиційні моделі побудови мереж вже не здатні ефективно відповідати на виклики, що виникають у зв'язку з новими загрозами та ускладненням архітектури корпоративних інфраструктур.

У відповідь на ці виклики з'явилася концепція *Software-Defined Access* (*SDA*) - програмно-керованого доступу, яка передбачає централізоване управління мережею з акцентом на політики безпеки, сегментацію трафіку та гнучкий контроль доступу.

Software-Defined Access (*SDA*) дозволяє не лише оптимізувати адміністрування мережевих ресурсів, а й значно підвищити рівень їхньої захищеності завдяки використанню новітніх механізмів і протоколів.

РОЗДІЛ 1
АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Інформаційна безпека та її роль у корпоративному середовищі

Інформаційна безпека - це сукупність організаційно-технічних заходів, що забезпечують захист інформації від несанкціонованого доступу, модифікації, знищення або розповсюдження. ІБ охоплює як апаратні та програмні засоби, так і політики, процедури та методи управління інформаційними потоками. У сучасному корпоративному середовищі інформаційна безпека є критично важливою складовою стабільної роботи бізнесу, репутації організації та дотримання законодавчих вимог.

Основна мета інформаційної безпеки - забезпечення конфіденційності, цілісності та доступності інформаційних ресурсів, що часто позначаються абревіатурою *CIA* (*Confidentiality, Integrity, Availability*):

- конфіденційність (*Confidentiality*) - забезпечення доступу до інформації лише уповноваженим особам;
- цілісність (*Integrity*) - гарантія того, що дані не були змінені без дозволу; -

доступність (*Availability*) - забезпечення своєчасного і надійного доступу до інформації для авторизованих користувачів.

Рисунок 1.1 - *CIA* (*Confidentiality, Integrity, Availability*)

Корпоративне середовище - це сукупність усіх компонентів, що формують внутрішню інфраструктуру, культуру та організаційні процеси компанії або установи.

Корпоративне середовище охоплює:

- людей (керівництво, працівників, підрядників);
- процеси (управлінські, виробничі, фінансові);
- інформаційні системи (*IT*-інфраструктуру, сервіси, програмне забезпечення);
- правила та політики (внутрішні регламенти, стандарти безпеки, кодекси поведінки);
- цінності та культуру (корпоративна етика, стиль комунікації, принципи взаємодії).

У контексті інформаційної безпеки, корпоративне середовище - це також цифровий простір, у якому циркулює критично важлива інформація, що потребує захисту. До цього середовища входять локальні мережі, хмарні сервіси, мобільні пристрої, електронна пошта, бази даних.

Іншими словами, корпоративне середовище - це внутрішній світ організації, де взаємодіють люди, технології та бізнес-процеси з метою досягнення спільної мети. Його безпека - це запорука стабільної та ефективної роботи компанії.

У корпоративному середовищі інформація - це стратегічний ресурс, може охоплювати:

- персональні дані співробітників;

- комерційно важливу інформацію (фінансову звітність);
- конфіденційні дані клієнтів;
- дані про внутрішні процеси й системи управління.

Порушення інформаційної безпеки призводить до фінансових збитків, втрати довіри клієнтів, витоку персональних даних та, у деяких випадках, до юридичної відповідальності. Такі інциденти, як витік баз даних, фішингові атаки, шкідливе ПЗ або *DDoS*-атаки, стають дедалі поширенішими в умовах зростання кіберзагроз.

У зв'язку з цим в організаціях створюються підрозділи інформаційної безпеки, запроваджуються політики доступу, застосовуються технології автентифікації та шифрування, впроваджується моніторинг подій, а також інтегруються сучасні системи безпеки (*SIEM, DLP, IAM, EDR*).

Із розвитком гібридних і хмарних середовищ, зростає потреба в більш гнучких і масштабованих підходах до інформаційної безпеки.

Одним із таких підходів є *Software-Defined Access* (*SDA*), який дозволяє централізовано керувати доступом та сегментацією мережі, що є ефективним інструментом для протидії внутрішнім і зовнішнім загрозам.

Отже, інформаційна безпека є не лише технічною вимогою, а й стратегічним пріоритетом сучасних організацій, який безпосередньо впливає на конкурентоспроможність, правову відповідальність і цифрову стійкість бізнесу.

1.2 Основні загрози інформаційній безпеці в *IT*-інфраструктурі

У сучасному цифровому середовищі інформаційна безпека *IT* інфраструктури є критично важливою, оскільки загрози стають дедалі складнішими, цілеспрямованішими та динамічними.

IT-інфраструктура включає всі апаратні та програмні компоненти, які забезпечують зберігання, обробку та передавання даних в організації. Це сервери, мережеве обладнання, робочі станції, мобільні пристрої, сервіси хмарної інфраструктури, канали зв'язку та елементи керування доступом. Її уразливість напряму впливає на загальний рівень захищеності корпоративного середовища.

Серед основних загроз інформаційній безпеці в *IT*-інфраструктурі виділяють такі:

1. Зовнішні загрози (*External threats*)

- Шкідливе програмне забезпечення (*Malware*)

Це одна з найпоширеніших форм атак. До *malware* належать віруси, трояни, шпигунські програми, програми-вимагачі (*ransomware*) та руткіти. Їхня мета -

отримати несанкціонований доступ, пошкодити або викрасти дані, зашифрувати інформацію з вимогою викупу.

Рисунок 1.2 - Шкідливе програмне забезпечення

- Атаки типу «відмова в обслуговуванні» (*DoS/DDoS*)

Атаки типу «відмова в обслуговуванні» (*DoS*) - це різновид кібератак, під час яких зловмисник намагається вивести з ладу роботу комп'ютера, мережі або онлайн-сервісу, використовуючи ресурси одного пристрою.

Рисунок 1.3 - Атаки типу «відмова в обслуговуванні»

Існують два основні підходи до здійснення *DoS*-атак:

- атака затопленням - коли сервер перевантажується надмірною кількістю запитів, що заповнюють буфери й призводять до зупинки роботи; - атака через

злам (сбой) - використання вразливостей у системі жертви для її повного відключення або порушення стабільної роботи.

Розподілені атаки типу «відмова в обслуговуванні» (*DDoS*) - це форма *DoS* атаки, яка здійснюється одночасно з великої кількості пристроїв, що діють як єдиний координаційний механізм.

Головна відмінність полягає в тому, що *DDoS*-атака надходить з багатьох джерел одночасно, у той час як звичайна *DoS*-атака йде з одного пристрою. - Фішинг та соціальна інженерія

Соціальна інженерія - це метод управління діями людини без використання технічних засобів. Метод заснований на використанні слабкостей людського фактора і вважається дуже руйнівним. Найчастіше соціальну інженерію розглядають як незаконний метод отримання інформації.

Рисунок 1.4 - Соціальна інженерія

Претекстинг - це метод соціальної інженерії, що базується на попередньо підготовленому сценарії (так званому «претексті»), за яким зловмисник вводить жертву в оману, щоб отримати від неї конфіденційну інформацію або спонукати до певних дій.

Такий тип атаки найчастіше здійснюється телефоном, хоча може застосовуватись і через онлайн-месенджери. Успішний претекстинг зазвичай потребує ретельної підготовки - зловмисник збирає попередню інформацію про ціль (наприклад, дату народження, деталі останньої транзакції), щоб виглядати переконливо й викликати довіру.

Фішинг - техніка, спрямована на неправомірне отримання конфіденційної інформації. Зазвичай зловмисник посилає цілі електронної пошти, підроблений під

офіційний лист - від банку або платіжної системи - вимагає «перевірки» певної інформації або вчинення певних дій. Цей лист зазвичай містить посилання на фальшиву веб-сторінку, яка імітує офіційну, з корпоративним логотипом і

наповненням, і містить форму, що вимагає ввести конфіденційну інформацію - від домашньої адреси до пін-коду банківської картки.

Рисунок 1.5 - Фішинг

Кви про кво - зловмисник може зателефонувати за випадковим номером до компанії і представитися співробітником техпідтримки, опитували, чи є які небудь технічні проблеми. У випадку, якщо вони є, в процесі їх «рішення» ціль вводить команди, які дозволяють хакеру запустити шкідливе програмне забезпечення.

- Вразливості в ПЗ та мережевих службах

Хакери активно експлуатують уразливості в операційних системах, програмах або вебсервісах, які не були оновлені. Наприклад, вразливість *Log4Shell* у 2021 році призвела до масових зломів.

2. Внутрішні загрози (*Insider threats*)

- Недобросовісні працівники

Інсайдери, які мають доступ до конфіденційної інформації, можуть навмисно викрасти або знищити дані. Мотивація - помста, фінансова вигода або політичні переконання.

- Людський фактор і помилки користувачів

Навіть несвідомі дії, як-от відкриття фішингового листа, завантаження заражених файлів або неправильна конфігурація систем, можуть призвести до серйозних інцидентів безпеки.

- Надлишкові привілеї

Надання користувачам або адміністратору прав, які виходять за межі необхідного мінімуму, створює ризики зловживання або несанкціонованого доступу до критичних ресурсів.

3. Технічні загрози

- Вразливості у пристроях *IoT*

Інтернет речей (*IoT*) активно використовується в сучасних офісах і на виробництві, проте часто не має належного захисту, що робить його вразливим до атак.

- Недостатня ізоляція мереж

Відсутність сегментації мережі дозволяє зловмисникам після первинного проникнення в систему швидко переміщатися по ній (*lateral movement*), підвищуючи рівень загрози.

- Ненадійні канали зв’язку

Використання незашифрованих або погано захищених каналів (наприклад, публічного *Wi-Fi*) дає змогу перехоплювати або змінювати дані. 4. Організаційні загрози

- Відсутність політик інформаційної безпеки

Якщо компанія не має чітких правил щодо доступу, зберігання, резервування чи обробки даних - це відкриває шлях до багатьох ризиків.

- Низький рівень обізнаності персоналу

Без регулярного навчання працівники не знають, як розпізнавати фішинг, захищати паролі, працювати з конфіденційною інформацією, що також загрожує безпеці.

- Відсутність резервного копіювання (*backup*)

У разі атаки *ransomware* або технічного збою, відсутність резервних копій може спричинити втрату важливої інформації без можливості її відновлення.

1.3 Традиційні методи контролю доступу

Контроль доступу є одним із ключових елементів забезпечення

інформаційної безпеки в *IT*-інфраструктурі.

Основна мета - надати дозволи лише авторизованим користувачам та процесам на доступ до певних ресурсів, систем або даних, відповідно до визначених політик безпеки.

У традиційних мережах (до впровадження концепцій *Zero Trust, SDA*) використовувались переважно класичні моделі контролю доступу, які мали свої переваги та обмеження.

До традиційних методів контролю доступу відносяться:

1. Дискреційний контроль доступу *DAC (Discretionary Access Control*) Це одна з найстаріших і найпоширеніших моделей, яка надає право власнику ресурсу (наприклад, файлу, каталогу, пристрою) самостійно визначати, хто і на яких умовах має доступ до об'єкта.

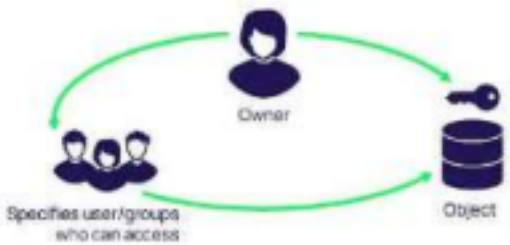


Рисунок 1.6 - *DAC (Discretionary Access Control)*

Характеристики *DAC*:

- кожен об'єкт має *ACL* (*Access Control List*) - список дозволів;
- користувач може передати доступ іншим (делегування);
- гнучка, але слабко контрольована адміністраторами;
- зустрічається у файлових системах *Windows, Unix/Linux* (через права на читання, запис, виконання).

Недоліки:

- високий ризик ненавмисного відкриття доступу;
- важко масштабувати у великих системах.

2. *MAC* контроль доступу (*MAC - Mandatory Access Control*)

У моделі *MAC* контроль доступу централізований і базується на рівнях

конфіденційності, наприклад: «Секретно», «Конфіденційно», «Для службового користування». Користувачі та ресурси мають відповідні мітки безпеки (*security labels*), і доступ можливий лише за відповідності рівнів.

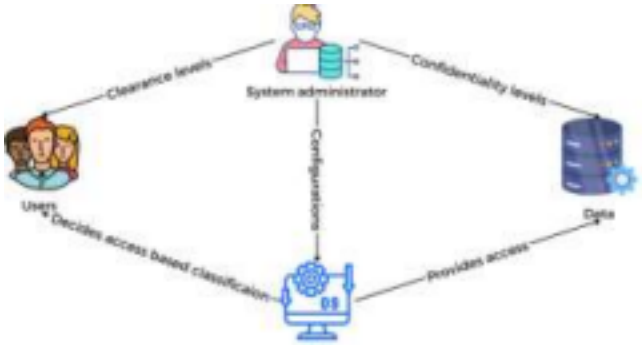


Рисунок 1.7 - *MAC (Mandatory Access Control)*

Характеристики *MAC*:

- неможливість змінити політики доступу без відповідного рівня привілеїв;
- використовується у військових системах, банках, державних структурах; - гарантує жорсткий контроль та регламентацію доступу.

Недоліки:

- низька гнучкість;
- висока вартість впровадження та адміністрування.

3. Контроль доступу *RBAC (Role-Based Access Control*)

У *RBAC* права доступу призначаються не окремим користувачам, а ролям наприклад - адміністратор, бухгалтер, менеджер. Кожен користувач отримує відповідну роль, яка визначає набір дозволених дій.

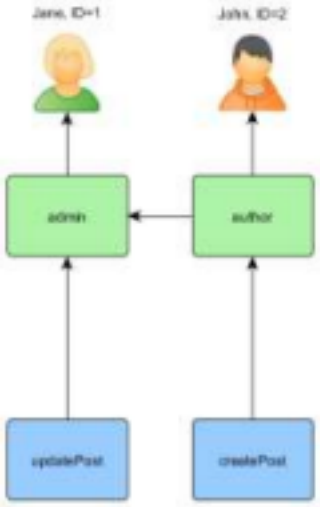


Рисунок 1.8 - *RBAC (Role-Based Access Control)*

Характеристики *RBAC*:

- централізоване управління політиками доступу;
- спрощення адміністрування;
- підвищення відповідності політикам безпеки (*compliance*);
- широко використовується в корпоративних системах (наприклад, *ERP, CRM, Active Directory*).

Недоліки:

- не враховує контекст доступу (наприклад, час доби, місце підключення);
- може бути неефективним у складних, динамічних середовищах. 4.

Контроль доступу *ACL (Access Control List*)

Цей метод доступу на основі списків широко використовується на мережевому рівні та в операційних системах. *ACL* визначає, які користувачі або групи мають які права доступу до об'єктів (читання, запис, виконання).

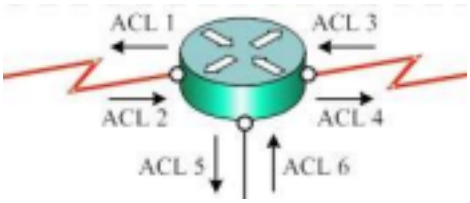


Рисунок 1.9 - *ACL* (*Access Control List*)

Переваги *ACL*:

- простота налаштування;

- гнучкість у малих середовищах.

Недоліки:

- складність керування великою кількістю об’єктів;
- відсутність централізованої політики контролю доступу.

5. Фізичний контроль доступу

Цей тип контролю забезпечує обмеження фізичного доступу до серверних кімнат, дата-центрів, терміналів. Він включає: ключ-карти, біометричну аутентифікацію, відеоспостереження, системи сигналізації.

Фізичний контроль є необхідною умовою для комплексного захисту *IT* інфраструктури, хоча сам по собі не є достатнім.

1.4 Підходи до захисту корпоративних мереж

З розвитком кіберзагроз класичні методи захисту - антивіруси, міжмережеві екрани (*firewalls*), ізольовані політики доступу - вже не здатні гарантувати належний рівень безпеки.

У відповідь на це в корпоративних мережах впроваджуються спеціалізовані системи безпеки, серед яких ключову роль відіграють *DLP, IAM* та *SIEM*-рішення.

1. *Data Loss Prevention* (*DLP*) - Захист від витоку даних

Системи *DLP* (*Data Loss Prevention*) призначені для виявлення, моніторингу та запобігання несанкціонованій передачі конфіденційної інформації за межі організації або до неналежних внутрішніх суб'єктів.

Ключові можливості *DLP*-систем:

- виявлення конфіденційних даних (файли, документи, ключові слова, шаблони номерів карток, ІПН);
- контроль каналів передачі (електронна пошта, зовнішні носії, веб, друк); - призупинення або блокування підозрілих дій користувача;
- ведення аудиту та звітності про інциденти безпеки.

Приклади *DLP*-систем: *Symantec DLP, McAfee Total Protection, InfoWatch Traffic Monitor, Zecurion DLP.*

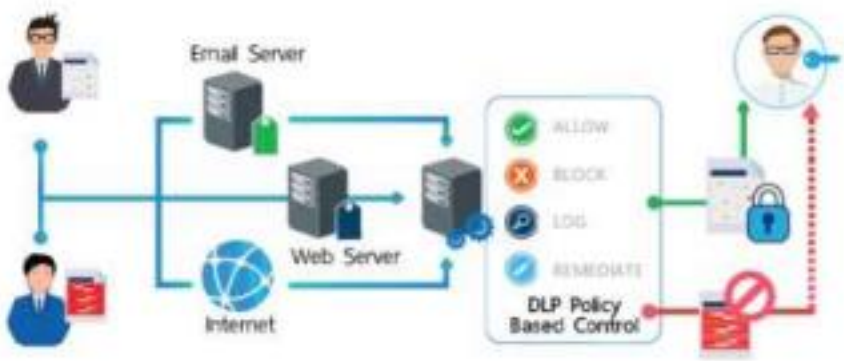


Рисунок 1.10 - *DLP* (*Data Loss Prevention*)

Значення для корпоративної мережі:

DLP дозволяє уникати витоків персональних даних, фінансової інформації, комерційної таємниці, зменшуючи ризики відповідальності та репутаційних втрат.

2. *Identity and Access Management* (*IAM*) - Управління ідентичністю та доступом

IAM (*Identity and Access Management*) - це комплекс технологій, політик і процесів, які забезпечують ідентифікацію користувачів, автентифікацію, авторизацію, аудит доступу та контроль за життєвим циклом облікових записів.

Рисунок 1.11 - *IAM* (*Identity and Access Management*)

Основні компоненти *IAM*:

- *Single Sign-On* (*SSO*) єдиний вхід до всіх систем;

- *Multi-Factor Authentication* (*MFA*) автентифікація за кількома факторами (пароль + *SMS*/аплікація);

- *RBAC/ABAC* контроль доступу на основі ролей або атрибутів; - *Provisioning/Deprovisioning* автоматичне надання/відкликання доступів при зміні статусу користувача;

- *Audit Trail* реєстрація всіх дій користувачів.

Приклади рішень *IAM*: *Microsoft Entra ID* (*ex Azure AD*), *Okta, Ping Identity, ForgeRock.*

Рисунок 1.12 - *IAM* (*Identity and Access Management*)

Значення для корпоративної мережі:

Завдяки *IAM* підприємства матимуть відповіді на такі питання: Хто? Система має багато ролей, значення кожної ролі. Що? Кожен обліковий запис використовується для якої програми, з якою метою. Коли? Час дії кожного облікового запису. Чому? Причина надання облікового запису, зміна статусу. Як? Як надавати рахунки, за допомогою яких процедур та погоджень. 3. *Security Information and Event Management* (*SIEM*) - Централізований моніторинг та реагування

Системи *SIEM* (*Security Information and Event Management*) призначені для збору, зберігання, кореляції та аналізу подій безпеки в масштабах усієї

організації. Це дає змогу виявляти інциденти, реагувати на них у режимі реального часу та розслідувати постфактум.

Рисунок 1.13 - *SIEM* (*Security Information and Event Management*)

Ключові функції *SIEM*:

- збір логів із серверів, мережевих пристроїв, прикладного ПЗ, безпекових рішень;

- кореляція подій та виявлення аномалій;

- сповіщення про підозрілі активності (наприклад, багаторазові спроби входу, атаки на сервіси);

- побудова дашбордів, генерація звітів, підтримка аналізу

відповідності; - інтеграція з інструментами реагування (*SOAR, EDR*).

Популярні S*IEM*-рішення: *Splunk, IBM QRadar, ArcSight, LogRhythm, Microsoft Sentinel.*

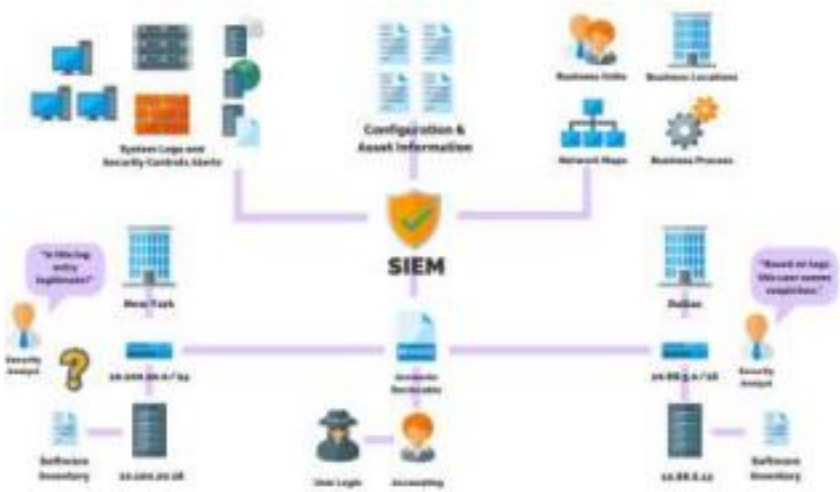


Рисунок 1.14 - *SIEM* (*Security Information and Event Management*)

Значення для корпоративної мережі:

SIEM-системи забезпечують проактивний моніторинг *IT*-інфраструктури, дають змогу швидко реагувати на загрози та будувати аналітику кіберризиків, зменшуючи час виявлення (*MTTD*) та реагування (*MTTR*) на інциденти. Кожен з підходів виконує свою роль:

- *DLP* - захищає дані від витоку**;**

- *IAM* - регулює, хто і до чого має доступ**;**

- *SIEM* - спостерігає за всією *IT*-інфраструктурою в реальному часі**.** Разом

вони створюють багаторівневу систему захисту, яка відповідає сучасним викликам цифрової безпеки та підтримує реалізацію концепцій *Zero Trust, SDA* та адаптивної кібербезпеки.

1.5 Висновки до розділу 1

У першому розділі проведено аналіз предметної області, а саме поняття інформаційної безпеки та її роль у корпоративному середовищі, основні загрози інформаційній безпеці в *IT*-інфраструктурі, традиційні методи контролю доступу, підходи до захисту корпоративних мереж (*DLP, IAM, SIEM*).

РОЗДІЛ 2
КОНЦЕПЦІЯ *SOFTWARE-DEFINED NETWORKING*

2.1 *SDN* (*Software-Defined Networking*)

Software-Defined Networking (*SDN*) - це підхід до проектування, реалізації та управління комп'ютерними мережами, який відокремлює (розділяє) контрольну площину від площини передачі даних, дозволяючи централізовано керувати мережею за допомогою програмного забезпечення.

У традиційних мережах функції маршрутизації, комутації та прийняття рішень про маршрути зосереджені на кожному окремому мережевому пристрої. Це ускладнює централізоване управління, зміну політик доступу, масштабування та швидке реагування на загрози.

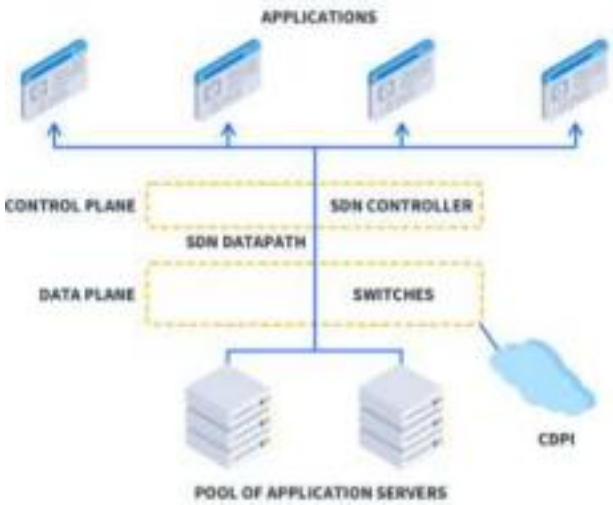


Рисунок 2.1 - *SDN* (*Software-Defined Networking*)

Програмно-визначену мережу (*SDN*) можно уявити як будівельний проект. Рівень додатків - це ваш план, який окреслює, чого має досягти мережа, включаючи безпеку, послуги та її загальне призначення.

Рівень керування - це ваш архітектор, який використовує *SDN*-контролер як свій мозок, щоб взяти ці креслення та перетворити їх на інструкції для працівників.

Рівень інфраструктури складається з ваших комутаторів, маршрутизаторів та інших пристроїв - це будівельна бригада та важка техніка, які фізично переміщують дані мережею, виконуючи вказівки контролера для побудови вашої мережевої структури.

SDN змінює цей підхід завдяки таким ключовим принципам:

- централізація управління мережею - усі рішення про маршрутизацію, політики доступу та пріоритезацію трафіку приймаються централізованим *SDN* контролером;

- програмна гнучкість - адміністратори можуть динамічно змінювати конфігурацію мережі через програмні інтерфейси (*API*), не втручаючись у фізичну інфраструктуру;

- відокремлення контрольної площини (*control plane*) від площини передачі (*data plane*) - комутатори та маршрутизатори виконують лише інструкції, надані контролером.

Архітектура *SDN* базується на трьох рівнях:

1. *Data Plane* - відповідає за пересилання пакетів, реалізується фізичними або віртуальними комутаторами (switches), які виконують інструкції від контролера. 2. *Control Plane* - містить *SDN*-контролер, який приймає рішення про маршрутизацію, політики доступу, сегментацію тощо.

3. *Application Plane* - включає програми безпеки, оптимізації, моніторингу та автоматизації, які взаємодіють з контролером через *Northbound API.* Комунікація між площинами здійснюється через стандартизовані інтерфейси: - *Southbound API* - для взаємодії між контролером та пристроями. - *Northbound API* - для інтеграції з зовнішніми програмами.

Переваги *SDN:*

- гнучкість - політики маршрутизації, фільтрації, *QoS* можна змінювати програмно без втручання в мережеві пристрої.

- централізоване управління - єдина точка контролю дозволяє управляти всією мережею з одного місця.

- швидке реагування на інциденти - завдяки централізованому логуванню та контролю.

- масштабованість - спрощення розширення мережі через віртуалізацію та централізовану логіку.

- автоматизація - політики та конфігурації можуть застосовуватись автоматично на основі подій.

Використання *SDN* у корпоративних мережах

SDN активно використовується в центрах обробки даних (ЦОД), хмарних платформах, телеком-операторах, а також у корпоративному середовищі.

Рисунок 2.2 - Модель архитектури ЦОД на базі *Cisco, NetApp* і *Veeam*

Особливо важливою є інтеграція *SDN* із технологіями безпеки: наприклад, динамічне блокування мережевого трафіку на основі виявлених загроз або порушень політики.

Зв’язок між *SDN* та *SDA*

SDA (*Software-Defined Access*) є розширенням концепції *SDN*, яке фокусується не лише на маршрутизації та управлінні трафіком, а на контролі доступу до мережі.

У *SDA* ідеї *SDN* поєднуються з концепціями автентифікації, сегментації, *Zero Trust* та автоматизованого управління політиками, що особливо актуально в умовах сучасних гібридних і динамічних корпоративних середовищ.

SDN відкрив нову епоху в управлінні мережами, зробивши їх гнучкішими, адаптивнішими та більш захищеними. Саме завдяки *SDN* стало можливим створення більш просунутих архітектур, таких як *SDA*, які інтегрують у мережу не лише маршрутизацію, а й інтелектуальний контроль доступу, автоматизацію та засоби безпеки.

2.2 Загальна характеристика архітектури *SDA* (*Software-Defined Access*)

Software-Defined Access (*SDA*) - це архітектура мережі нового покоління, яка розроблена компанією *Cisco* для забезпечення безпечного, гнучкого та централізованого керування доступом до мережевих ресурсів.

SDA є логічним розвитком концепції *Software-Defined Networking* (*SDN*) і ґрунтується на принципі автоматизованого контролю доступу з використанням політик безпеки, прив'язаних до ідентичностей користувачів та пристроїв.

Рисунок 2.3 - Програмно-визначений доступ *Cisco SDA* (*Software-Defined Access*)

SDA має на меті спростити керування корпоративною мережею, підвищити її захищеність та адаптивність шляхом централізованого управління доступом до ресурсів та автоматизації політик безпеки на основі ролей, атрибутів, місця розташування, типу пристрою.

Ключові компоненти архітектури *SDA*:

Архітектура *SDA* базується на чітко визначених складових, які тісно взаємодіють між собою:

1. *Cisco DNA Center* - централізована платформа керування мережею: - надає інтерфейс для налаштування політик, моніторингу трафіку, аналізу поведінки користувачів;

- забезпечує автоматизацію налаштувань мережі (provisioning) та інтеграцію з зовнішніми системами (наприклад, *SIEM*).

2. *Cisco ISE* (*Identity Services Engine*) - система керування ідентичностями: - виконує автентифікацію користувачів і пристроїв;

- присвоює *Security Group Tags* (*SGT*);

- керує політиками доступу (на основі ролей, атрибутів, поведінки).

3. *Fabric* - віртуалізований рівень передачі даних:

- формує логічну структуру мережі, ізольовану від фізичної інфраструктури; - використовує *VXLAN* (*Virtual Extensible LAN*) для інкапсуляції трафіку. 4. *Edge Nodes, Control Nodes, Border Nodes* - основні вузли *SDA*: - *Edge Node* - комутатори доступу, до яких підключаються кінцеві пристрої; - *Control Node* - взаємодіє з *Cisco ISE* та підтримує базу даних ідентичностей; - *Border Node* - шлюз між *SDA*-фабрикою та зовнішніми мережами.

Рисунок 2.4 - Фізичні топології *Cisco SDA (3-рівнева фізична топологія SDA)*

Для менших розгортань, тканину *SDA* можна реалізувати з використанням дворівневої конструкції. Слід застосовувати ті ж принципи проектування, але без необхідності агрегаційного рівня, реалізованого проміжними вузлами.

Рисунок 2.5 - Фізичні топології *Cisco SDA (2-рівнева фізична топологія SDA)*

SDA може складатися з кількох сайтів.

Кожен сайт може вимагати різних аспектів масштабування, стійкості та живучості. Загальна агрегація сайтів (тобто *Fabric*) також повинна мати можливість вмістити дуже велику кількість кінцевих точок, масштабуватися горизонтально шляхом агрегації сайтів та зберігати локальний стан у кожному сайті. Кілька сайтів *Fabric*, що відповідають одній *Fabric*, будуть з'єднані між собою областю транзитної мережі.

Область транзитної мережі можна визначити як частину *Fabric*, яка з'єднує межі окремих *Fabric* і має власні вузли площини керування, але не має крайових вузлів. Крім того, область транзитної мережі має спільний принаймні один крайовий вузол з кожним сайтом *Fabric*, який вона з'єднує.

Рисунок 2.6 - *SDA* з кількох сайтів

Принципи роботи *SDA*

1. Ідентифікація користувачів і пристроїв - приєднання до мережі супроводжується автентифікацією через *ISE.*

2. Присвоєння *SGT* - кожному суб’єкту (користувачу чи пристрою) присвоюється тег безпеки, що визначає його рівень доступу.

3. Приймання політик доступу - теги використовуються для визначення політик взаємодії з іншими суб’єктами або ресурсами мережі.

4. Автоматизоване застосування політик - політики безпеки застосовуються у

масштабі всієї мережі автоматично.

5. Моніторинг і аналітика - збирання телеметрії в реальному часі через *DNA Center* для виявлення аномалій.

Підключені клієнти почнуть надсилати *DHCP*-запити для отримання *IP* адреси. Потік *DHCP* у *Fabric* принципово відрізняється від традиційних мереж. Зв'язок між клієнтами (користувачами або пристроями) все ще працює на рівні 2, проте мережа в *Fabric* тепер працює на рівні 3 між *Fabric Edge* та вузлом *Border*, а протоколи між вузлом *Border* та сервером *DHCP* є специфічними для сервісу, наприклад, *NTP, DNS, DHCP.*

DHCP (*Dynamic Host Configuration Protocol*) - це мережевий протокол, який автоматично призначає *IP*-адреси та інші параметри мережі (наприклад, шлюз за замовчуванням, *DNS*-сервер) пристроям у комп'ютерній мережі.

DHCP дозволяє пристроям (наприклад, комп'ютерам, телефонам, принтерам), які підключаються до мережі, автоматично отримувати налаштування для доступу до мережі та Інтернету, без необхідності ручного введення *IP*-адреси.

NTP (*Network Time Protocol*) - протокол мережевого часу. Синхронізація годинника комп'ютера або пристрою з точним сервером часу в Інтернеті чи локальній мережі. Усі пристрої в мережі мають однаковий час. Важливо для безпеки (наприклад, правильна дата у сертифікатах), журналів подій, резервного копіювання.

DNS (*Domain Name System*) - система доменних імен. Перетворює зручні для людини адреси сайтів (наприклад, *www.google.com*) у *IP*-адреси (наприклад, 142.250.185.4), які розуміє комп'ютер. Без нього нам би довелося запам'ятовувати *IP*-адреси сайтів.

Рисунок 2.7 - *SDA* потік *DHCP* у *Fabric*

Коли клієнти починають підключатися до мережі, першим кроком є реєстрація хоста, тобто його реєстрація в площині керування (картографічний сервер).

ARP (*Address Resolution Protocol*) **-** це протокол, який використовується для визначення *MAC*-адреси пристрою за його *IP*-адресою в локальній мережі.

Рисунок 2.8 - *SDA* реєстрація хоста

Крім того, система також надсилає деякі макроси на порт комутатора для ідентифікації точок доступу під час їх підключення до мережі.

Рисунок 2.9 - *SDA* реєстрація хоста - точка доступу

Адміністратор налаштовує пул точок доступу у *Cisco DNA Center* в межах віртуальної мережі *INFRA_VN. Cisco DNA Center* автоматично генерує макрос конфігурації для всіх вузлів *Fabric Edge (FE).* Після підключення точка доступу вмикається. Комутатор *FE* виявляє її за допомогою *CDP* і застосовує відповідний

макрос, який налаштовує порт комутатора на потрібну *VLAN.* Цей макрос

надсилається до *FE* для забезпечення підключення точки доступу. У мережевому оверлеї точка доступу отримує *IP*-адресу через *DHCP. Fabric Edge* фіксує *IP*- та *MAC*-адресу точки доступу (ідентифікатори *EID*) і передає цю інформацію до площини керування (*Control Plane, CP*). Точка доступу отримує *IP*-адресу контролера бездротового доступу (*WLC*) і підключається до нього стандартними методами. У середовищі *Fabric* вона працює в локальному режимі.

WLC перевіряє сумісність точки доступу з *Fabric* (наприклад, моделі *Wave* 1 або *Wave* 2). Якщо точка доступу сумісна, *WLC* звертається до *CP* із запитом, чи вона підключена до *Fabric. CP* підтверджує це, надсилаючи *WLC* повідомлення з *RLOC*-адресою, що означає успішне підключення точки доступу до *Fabric*, і вона відображається як «*Fabric увімкнено*».

Далі *WLC* виконує реєстрацію точки доступу у площині керування через *L2 LISP* (так звана реєстрація «спеціального» безпечного клієнта). Це дозволяє передати ключові метадані від *WLC* до *FE.*

У відповідь *CP* інформує *FE* про цю точку доступу та передає отримані від *WLC* метадані - ознаку, що це точка доступу, та її *IP*-адресу.

FE обробляє ці дані, ідентифікує пристрій як точку доступу, після чого створює *VXLAN*-тунель до вказаної *IP*-адреси. Завдяки цьому комутатор готовий приймати клієнтів точки доступу.

Після того, як клієнти підключені до тканини та отримають *IP*-адресу, їхні записи будуть додані до вузлів *Fabric Edge* та площини керування.

Рисунок 2.10 - *SDA* роздільна здатність хоста

Мобільність хоста - використання хоста, що переміщується з одного краю мережі *Fabric* на інший. Прикладом можуть бути спеціальні пристрої в лікарнях або промислових компаніях, де неможливо змінити *IP*-адресу хостів, і ці хости

можуть переміщуватися з одного порту комутатора на інший.

Рисунок 2.11 - *SDA* мобільність хоста

Хост1 переходить з *FE*1 до *FE*2.

*FE*2 зберігає інформацію про хост у локальній базі даних. Надсилає повідомлення реєстрації до площини керування. Карт-сервер додає до бази даних запис для конкретного *EID*, пов'язаного з *RLOC*.

Картографічний сервер надсилає повідомлення *Map-Notify* останньому *FE*1, який зареєстрував префікс 10.2.1.99/32. *FE*1 отримує повідомлення *Map-Notify* від *CP* та додає маршрут, пов'язаний з *EID* 10.2.1.99, до таблиці віддалених маршрутів. Після того, як *FE*1 отримує *Map-Notify* від *CP, MAC*-адреса хоста (який тепер переміщений до *FE*2) поміщається в таблицю віддалених адрес і залишається там протягом 4 годин.

Переваги архітектури *SDA*:

- централізоване управління всією мережею з однієї платформи; - швидке виявлення та ізоляція загроз завдяки сегментації трафіку; - гнучкість у наданні доступу - дозволяє застосовувати політики на основі ідентичності, а не лише *IP*-адрес;

- зменшення ручної конфігурації - автоматизація процесів налаштування мережі;

- масштабованість - *SDA* підходить як для малих офісів, так і для великих розподілених організацій.

SDA як основа *Zero Trust* підходу

SDA підтримує концепцію *Zero Trust Network Access* (*ZTNA*) - «нікому не

довіряй, завжди перевіряй». У цій моделі довіра не базується на розташуванні в мережі, кожна сесія контролюється окремо, що дозволяє мінімізувати ризики внутрішніх атак.

Рисунок 2.12 - *Zero Trust Network Access* (*ZTNA*)

Архітектура *SDA* є ключовим етапом еволюції корпоративних мереж у напрямку глибшої автоматизації, масштабованості та безпеки. Її реалізація дозволяє організаціям перейти від ручного управління політиками до динамічної, адаптивної системи, що відповідає сучасним вимогам цифрової безпеки.

2.3 Механізми контролю доступу в *SDA*: *RBAC*

У контексті архітектури *Software-Defined Access* (*SDA*) контроль доступу відіграє ключову роль у забезпеченні безпеки корпоративної мережі. Одним із базових механізмів, який активно використовується в *SDA*, є *Role Based Access Control* (*RBAC*) - контроль доступу на основі ролей. Цей підхід дозволяє централізовано та гнучко визначати рівень доступу користувачів і пристроїв на основі їхньої ролі в організації.

RBAC ґрунтується на принципі:

«Користувач не отримує доступ до ресурсу напряму, а через свою роль, якій цей доступ дозволено». Іншими словами, доступ визначається не індивідуально для кожного користувача, а для ролей, до яких вони належать.

Наприклад, ролі можуть бути такими: «Системний адміністратор»,

«Бухгалтер», «Гість», «Працівник служби підтримки».

Кожна роль має чітко визначені права доступу до ресурсів, систем, сегментів мережі.

Компоненти *RBA*C у *SDA*

У реалізації *RBAC* у *SDA* беруть участь такі основні компоненти: - *Cisco ISE* (*Identity Services Engine*) -автентифікує користувача та присвоює йому роль на основі облікових даних, атрибутів пристрою, розташування тощо. - *Cisco DNA Center* - застосовує політики доступу на основі ролей до мережевої інфраструктури.

- *Security Group Tags* (*SGT*) - спеціальні теги безпеки, які відображають роль користувача та використовуються для прийняття рішень щодо доступу. Приклад реалізації *RBAC* у *SDA*

У корпоративній мережі є три основні ролі:

- адміністратори (*Admin*) - повний доступ до всіх сегментів мережі. - фінансовий відділ (*Finance*) - доступ лише до серверів бухгалтерії та офісного ПЗ.

- гості (*Guest*) - доступ лише до Інтернету.

Кроки реалізації в *SDA*:

1. Ідентифікація користувача через *Cisco ISE* - під час підключення користувач автентифікується (наприклад, через 802.1X).
2. Присвоєння *SGT* - *ISE* визначає, що користувач належить до ролі «*Finance*» і присвоює відповідний тег.
3. Застосування політики - трафік із тегом «*Finance*» допускається лише до дозволених ресурсів, а доступ до інших сегментів заборонений.

4. Моніторинг і контроль - *Cisco DNA Center* відслідковує застосування політик у режимі реального часу.

Переваги використання *RBAC* у *SDA*

- централізація управління доступом - адміністратор задає політики на рівні ролей, а не окремих *IP* чи *MAC*-адрес;

- масштабованість - нові користувачі легко інтегруються, просто отримавши відповідну роль;

- гнучкість і адаптивність - політики легко змінюються згідно зі змінами в організаційній структурі;

- зменшення людського фактора - виключення індивідуального конфігурування доступу зменшує ймовірність помилок.

Обмеження:

- недостатня гнучкість для складних сценаріїв, коли потрібно враховувати більше атрибутів, ніж просто роль;

- потреба в актуальній ролевій моделі - неправильне налаштування ролей може призвести до небажаного доступу.

У таких випадках доповнення механізму *RBAC* більш гнучкими моделями, наприклад *Attribute-Based Access Control* (*ABAC*), може забезпечити точніший контроль доступу.

RBAC у *SDA* забезпечує ефективний, простий у масштабуванні та безпечний підхід до контролю доступу в корпоративній мережі. *RBAC* дозволяє зменшити навантаження на адміністраторів, знизити ризики внутрішніх загроз і підтримувати політики *Zero Trust* на практиці. Водночас у поєднанні з іншими підходами, такими як *ABAC* або *Context-Aware Access*, можливе ще більш тонке налаштування рівнів безпеки в рамках сучасних гібридних мереж.

2.4 Механізми контролю доступу в *SDA*: *ABAC*

У контексті архітектури *Software-Defined Access* (*SDA*), одним із перспективних підходів до забезпечення гнучкого та контекстно-залежного

контролю доступу є *Attribute-Based Access Control* (*ABAC*) - контроль доступу на основі атрибутів. Ця модель дозволяє приймати рішення про надання доступу не лише на основі ролі користувача (як у *RBAC*), а за комплексом атрибутів, що описують суб’єкта, об’єкт доступу, дії та контекст.

ABAC реалізує доступ за принципом:

Доступ дозволено, якщо сукупність атрибутів суб’єкта, об’єкта та умов відповідає політиці безпеки.

Атрибути можуть включати:

- атрибути суб'єкта - ім'я, посада, відділ, рівень авторизації, сертифікати; - атрибути об'єкта - тип ресурсу, його чутливість, власник;

- контекстні атрибути - час доби, геолокація, тип пристрою, мережевий сегмент, рівень ризику.

В рамках *Cisco SDA*, механізм *ABAC* реалізується шляхом комбінування *Cisco ISE, Cisco DNA Center ma SGT*-політик (*Security Group Tags*), але з ширшим набором умов і атрибутів.

Користувач хоче отримати доступ до внутрішнього сервера.

ABAC-політика може містити такі умови:

- користувач працює у відділі фінансів;
- підключення відбувається в робочий час;
- використовується корпоративний ноутбук;
- користувач перебуває в корпоративній мережі (локально);
- рівень ризику пристрою - низький;

Якщо всі умови виконано - доступ надається. Якщо, наприклад, користувач підключається з публічної *Wi-Fi* мережі - система може відмовити в доступі або запропонувати лише обмежений доступ, наприклад, у режимі перегляду без редагування.

Ключові компоненти реалізації *ABAC* в *SDA*

- *Cisco ISE* - виконує автентифікацію, збір атрибутів та прийняття рішень за політикою;

- *Policy Sets* - механізм, у якому визначаються політики доступу за атрибутами;

- *TrustSec SGT* - використовується для маркування трафіку, що відповідає атрибутам;

- *Cisco DNA Center* - оркеструє застосування політик по всій мережевій інфраструктурі.

ABAC особливо ефективний у таких ситуаціях:

- хмарна інфраструктура - де користувачі працюють з різних місць і пристроїв;

- гібридні робочі моделі - коли треба враховувати тип підключення, пристрій, геолокацію;

- *Zero Trust Architecture* - коли кожен запит перевіряється за багатьма критеріями.

Виклики при впровадженні *ABAC*:

- складність конфігурації політик - потребує ретельного планування і тестування;

- необхідність якісного збору атрибутів - потрібно інтегрувати багато джерел інформації;

- продуктивність - складні політики можуть впливати на швидкість прийняття рішень.

ABAC є потужним інструментом забезпечення гнучкого, контекстно залежного контролю доступу у середовищі *SDA*. *ABAC* використання дозволяє значно підвищити рівень безпеки, особливо в умовах, де мережа не має чітких периметрів, а користувачі та пристрої змінюють свою поведінку та місцезнаходження.

2.5 Механізми контролю доступу в *SDA*: *SGT*

У контексті архітектури *Software-Defined Access* (*SDA*) компанії *Cisco*, ключову роль у реалізації політик доступу та сегментації мережі відіграє

технологія *Security Group Tags* (*SGT*) - теги груп безпеки. Цей механізм є центральним елементом концепції *Cisco TrustSec*, яка інтегрується в *SDA* для створення динамічних, масштабованих і безпечних мереж.

SGT - це цифрова мітка (тег), яка присвоюється користувачу або пристрою під час автентифікації, на основі його ролі, політики, або інших атрибутів. Ця мітка передається разом із трафіком у мережі *SDA*, дозволяючи застосовувати політики доступу незалежно від *IP*-адрес або фізичного розташування пристрою.

SGT = «цифровий ідентифікатор контексту доступу».

SGT реалізує доступ за принципом:

1. Користувач або пристрій автентифікується через *Cisco ISE* (*Identity Services Engine*).

2. На основі політики, *Cisco ISE* призначає пристрою або користувачу відповідний *SGT.*

3. Тег *SGT* інкапсулюється в трафік (за допомогою протоколу *Cisco TrustSec*).
4. Політики доступу (*SGACL - Security Group Access Control List*) застосовуються на основі *SGT*, наприклад: *SGT*= «Фінанси» має доступ до ресурсів з тегом «Сервери» тільки на портах 443 і 80.

Інтеграція з іншими компонентами *SDA*

- *Cisco ISE* - присвоює *SGT* на основі автентифікації та атрибутів; - *Cisco DNA Center* - централізовано керує політиками доступу та *SGT* мапінгами;

- *Network Devices* (комутатори, маршрутизатори) - зчитують, зберігають і застосовують політики на основі *SGT*;

- *SGACL* (*Security Group ACL*) - визначає дозволені або заборонені взаємодії між різними *SGT.*

Приклад застосування *SGT*

У компанії існують наступні теги: *SGT* 10: «Бухгалтерія», *SGT* 20: «Відділ продажу», *SGT* 30: «Сервери». Користувачі з тегом *SGT* 10 мають доступ до *SGT* 30 тільки на порту 443. *SGT* 20 не має жодного доступу до *SGT* 30. Завдяки *SG*T,

навіть якщо працівник бухгалтерії змінить офіс або *IP*-адресу - політика доступу залишиться незмінною.

Виклики при впровадженні *SGT*

- початкове налаштування вимагає узгодження ролей, тегів та політик;
- необхідна підтримка *TrustSec* на мережевому обладнанні;
- наявність *Cisco ISE* як обов'язкової складової архітектури.

SGT є фундаментальним елементом безпеки в *SDA*, що забезпечує динамічний, контекстно-залежний і масштабований контроль доступу. На відміну від традиційної моделі фільтрації за *IP*-адресами, цей підхід є значно гнучкішим і більш придатним до сучасних умов: віддаленої роботи, *BYOD, IoT* тощо. Завдяки інтеграції з *Cisco ISE* та *Cisco DNA Center*, механізм *SGT* створює новий рівень

адаптивної мережевої безпеки.

Таблиця 2.1 - Порівняння методів контролю доступу *RBAC*, *ABAC*

Критерій	***RBAC* (*Role-Based Access Control*)**	***ABAC* (*Attribute-Based Access Control*)**
Основний принцип	Доступ за роллю	Доступ за атрибутами
Формат політик	`Роль → дозволи`	`Атрибути + умови → дозволи`
Гнучкість	Обмежена	Висока
Контекстуальність	Відсутня	Є (атрибути можуть змінюватись динамічно)
Динамічність рішень	Статична	Динамічна
Масштабованість	Середня	Висока, але складна
Складність адміністрування	Просте	Складне
Типова сфера застосування	Традиційні системи з чіткими ролями	Динамічні, zero-trust архітектури
Підтримка в *SDA*	Часткова (через *Cisco ISE*)	Може бути реалізований через *ISE*

З таблиці 2.1 можно зробити висновок, що *ABAC* є значно гнучкішим і динамічнішим механізмом контролю доступу, ніж *RBAC*, але *RBAC* добре підходить для простих і стабільних середовищ з чіткими ролями, *ABAC* краще використовувати в умовах, де потрібен контекстуальний і атрибутивний контроль доступу**.**

Таблиця 2.2 - Порівняння методів контролю доступу *ABAC, SGT*

Критерій	***ABAC* (*Attribute-Based Access Control*)**	***SGT* (*Security Group Tag, Cisco TrustSec*)**
Основний принцип	`Атрибути → політика`	`Теги → матриця політик`
Формат політик	Атрибути + умови	*SGT-to-SGT* матриця доступу
Гнучкість	Висока	Середня
Контекстуальність	Висока	Відсутня
Динамічність рішень	Динамічна	Статична
Масштабованість	Висока (але складна)	Висока (просте масштабування

		тегів)
Складність адміністрування	Висока (керування атрибутами)	Середня (необхідне оновлення матриці *SGT*)
Типова сфера застосування	Складні середовища, що змінюються	Мережевий доступ у *SDA, TrustSec*
Підтримка в *SDA*	Частково (через *Cisco ISE*)	Основний механізм

З таблиці 2.2 можно зробити висновок, що *ABAC* забезпечує глибший рівень деталізації і враховує більше змінних, тоді як *SGT* забезпечує просте і масштабоване мережеве сегментування, особливо у рішеннях *Cisco SDA*. *SGT* простіший в управлінні, але менш гнучкий, ніж *ABAC.*

Таблиця 2.3 - Порівняння методів контролю доступу *RBAC, ABAC, SGT*

Критерій	***RBAC* (*Role-Based Access Control*)**	***ABAC* (*Attribute-Based Access Control*)**	***SGT* (*Security Group Tag, Cisco TrustSec*)**
Основний принцип	Доступ за роллю користувача	Доступ за атрибутами суб'єкта, об'єкта, середовища	Доступ за тегами безпеки, прив'язаними до пристроїв/користувачів
Формат політик	`Роль → дозволи`	`Атрибути + логічні умови → дозволи`	*SGT* → `політика доступу між тегами`
Гнучкість	Низька	Висока	Середня
Контекстуальність	Немає	Висока (атрибути можуть змінюватись динамічно)	Низька (*SGT* є статичним тегом)
Динамічність рішень	Статична	Динамічна (залежить від атрибутів у реальному часі)	Статична (*SGT* задається наперед)
Масштабованість	Добра при обмеженій кількості ролей	Висока, але складна в управлінні	Висока (централізоване тегування й матриця політик)
Складність адміністрування	Низька–середня	Висока (багато атрибутів і політик)	Середня (менше правил, але потрібна матриця *SGT-to-SGT*)
Типова сфера застосування	Системи з фіксованими ролями (корпоративні *IT*)	Динамічне середовище, хмарні сервіси, zero trust середовища	*SDA/TrustSec,* мережеве сегментування у *Cisco*

Підтримка в *SDA*	Обмежено (може бути частиною *Cisco ISE*)	Частково (через політики *Cisco ISE*)	Основний механізм контролю доступу в *SDA*

З таблиці 2.3 можно зробити висновок, що *ABAC* є найбільш гнучким і контекстуально чутливим підходом, *RBAC* - найпростіший у впровадженні, а *SGT* - найкраще підходить для масштабованого контролю доступу в *SDA*.

Вибір залежить від складності середовища та потреб у динамічному або статичному контролі доступу.

2.6 Політики безпеки у *SDA* та впровадження *Zero Trust*

У сучасних умовах цифрової трансформації, коли користувачі та пристрої працюють з будь-якого місця, традиційні підходи до безпеки, які базуються на периметрі, втрачають свою ефективність.

Архітектура *Software-Defined Access* (*SDA*) активно впроваджує концепцію *Zero Trust* (нульової довіри), що передбачає відсутність автоматичної довіри до будь-якого об'єкта - незалежно від його розташування або попередньої автентифікації.

Концепція *Zero Trust* у *SDA* реалізується за допомогою політик, які перевіряють, контролюють і обмежують доступ на основі контексту - хто, що, де, коли і як намагається отримати доступ. Основна ідея полягає в тому, що ніякий користувач або пристрій не повинен отримати доступ до ресурсу, поки не буде підтверджено його ідентичність і не буде дозволено політикою безпеки.

Ключові принципи *Zero Trust* у *SDA*:

1. *Verify Explicitly* (Явна перевірка)

- кожен запит на доступ перевіряється незалежно;
- використовується багатофакторна автентифікація (*MFA*), перевірка пристрою, розташування, типу з'єднання тощо.

2. *Least Privilege Access* (Мінімально необхідні права)

- користувачам і пристроям надається лише той доступ, який необхідний для

виконання завдань.

3. *Assume Breach* (Передбачення компрометації)

- безпека планується з урахуванням можливості проникнення в мережу;

- контроль за рухом трафіку всередині мережі (*lateral movement*) є критично важливим.

Політики безпеки в *SDA*

У *SDA* політики безпеки будуються на базі:

- *SGT* (*Security Group Tags*) - призначення тегів груп безпеки для користувачів/пристроїв;

- *SGACL* (*Security Group Access Control Lists*) - правила, які визначають дозволені або заборонені взаємодії між *SGT;*

- контекстної інформації - тип пристрою, операційна система, положення в мережі, тип підключення (провідне/безпровідне/*VPN*).

Приклад, користувач з тегом «*HR*» може мати доступ лише до ресурсів з тегом «*HR Files*», але не до «*Finance Systems*».

Cisco ISE - центральний елемент *Zero Trust* у *SDA*

Cisco Identity Services Engine (*ISE*) - платформа, що виконує:

- аутентифікацію та авторизацію користувачів;

- присвоєння *SGT*;

- впровадження політик доступу на базі ролей, атрибутів і контексту; - динамічну адаптацію політик на основі змін у поведінці або ризику. *ISE* також взаємодіє з *Cisco DNA Center*, що спрощує розгортання політик через єдиний інтерфейс керування.

Zero Trust Network Access (*ZTNA*) в *SDA*

Zero Trust у *SDA* є практичною реалізацією *ZTNA*, що забезпечує: - доступ лише після успішної автентифікації та перевірки пристрою; - мікросегментацію мережі - ізоляцію доступу між різними зонами; - постійний моніторинг активності користувача;

- інтеграцію з *SIEM, EDR, NDR* для виявлення та реагування на загрози.

Виклики впровадження:

- необхідність оновлення інфраструктури під *TrustSec* та *Cisco ISE*;
- потреба в точному визначенні ролей, *SGT* і політик;
- підвищена складність початкового налаштування.

Zero Trust у рамках *SDA* - це не просто концепція, а практична архітектура, яка дозволяє реалізувати безпечну, адаптивну і масштабовану *IT*-інфраструктуру. Завдяки використанню контекстуальних політик, мікросегментації, технологій *Cisco ISE* та *TrustSec, Zero Trust* у *SDA* забезпечує високий рівень безпеки, необхідний для сучасних динамічних середовищ із хмарними, гібридними або мобільними користувачами.

2.7 Використання *Cisco ISE* для ідентифікації та авторизації користувачів

У контексті архітектури *Software-Defined Access* (*SDA*), одним із ключових компонентів забезпечення контролю доступу та дотримання політик безпеки є *Cisco Identity Services Engine* (*ISE*).

ISE платформа забезпечує централізоване керування ідентифікацією, автентифікацією, авторизацією користувачів і пристроїв, а також дозволяє реалізувати динамічні політики доступу у відповідності до принципів *Zero Trust.*

Рисунок 2.13 - *Cisco ISE*

Cisco ISE виконує кілька критично важливих функцій у мережевій

безпеці: 1. Ідентифікація користувачів і пристроїв

- визначення, хто або що підключається до мережі (користувач, ПК, телефон, принтер);

- аналіз контексту - тип пристрою, операційна система, місце розташування, час доступу.

2. Автентифікація (*authentication*)

- підтвердження особи користувача або пристрою;

- підтримка методів автентифікації: 802.1*X*, *MAC Authentication Bypass* (*MAB*), *WebAuth*;

- можливість використання сертифікатів або логінів.

3. Авторизація (*authorization*)

- визначення, які ресурси доступні підключеному об'єкту;

- присвоєння *Security Group Tags* (*SGT*) - маркерів безпеки, які використовуються для подальшого застосування політик у мережі; - використання динамічних політик на основі ролей (*RBAC*), атрибутів (*ABAC*), типу підключення, положення в мережі.

4. Постійна оцінка стану пристрою (*posture assessment*)

- аналіз стану безпеки кінцевого пристрою (наявність антивірусу, оновлень, шифрування);

- у разі невідповідності політиці безпеки - доступ обмежується або спрямовується в карантинну зону.

5. Централізоване керування політиками доступу

- політики створюються в *ISE* і застосовуються до всіх компонентів *SDA* (*switch, WLC, router*);

- інтеграція з *Cisco DNA Center* для візуалізації та автоматизації.

ISE є реалізацією принципу «явної перевірки» у *Zero Trust*:

- не довіряє пристрою чи користувачу без детальної перевірки; - забезпечує гнучкий контроль доступу на основі детальної інформації; - автоматично адаптує політики при зміні контексту (наприклад, при зміні місця розташування або мережі).

Типовий сценарій роботи *Cisco ISE*

1. Підключення до мережі - користувач підключає ноутбук через *Ethernet* або *Wi-Fi.*

2. *ISE* здійснює автентифікацію - проводиться перевірка облікових даних (*Active Directory*, сертифікат).

3. Аналіз пристрою - визначається тип пристрою, його відповідність політикам (*posture check*).

4. Присвоєння *SGT* - наприклад, *HR*-співробітнику присвоюється тег *HR_SGT.*
5. Застосування політик - відповідно до тегу, застосовується набір *SGACL*, які визначають, до яких ресурсів мережі є доступ.

Інтеграція з іншими системами

Cisco ISE може взаємодіяти з:

- *SIEM* (*Splunk, QRadar*) - передача логів та подій;

- *EDR/NDR* - обмін контекстом про інциденти та ризики;

- *Firewall* - адаптація політик на основі поведінкової аналітики. *Cisco ISE* є критично важливим компонентом для реалізації ефективного контролю доступу у *SDA*, забезпечуючи гнучке, динамічне та масштабоване керування автентифікацією та авторизацією. Його інтеграція в *Zero Trust* архітектуру дозволяє мінімізувати ризики несанкціонованого доступу та забезпечити високу адаптивність до умов сучасного корпоративного середовища.

2.8 Сегментація трафіку та динамічне управління доступом

Сегментація трафіку - це процес поділу мережі на ізольовані логічні або фізичні частини (сегменти), між якими обмежено або контролюється обмін даними.

В традиційних мережах сегментація досягається шляхом створення *VLAN* (*Virtual LAN*) або використання міжмережевих екранів.

Рисунок 2.14 - *VLAN* мережа з трьома різними фізичними комутаторами

VLAN дозволяє взяти один фізичний комутатор і розбити його на менші міні комутатори.

Уявіть собі кожне коло на перемикачі нижче як окремий міні перемикач (або віртуальний *перемикач*). Кожен із цих міні-перемикачів являє собою набір портів перемикача, які працюють повністю незалежно від інших -так само, як і в випадку використання трьох *різних* фізичних перемикачів.

Рисунок 2.15 - *VLAN* розбиття одного фізичного комутатора
на кілька віртуальних комутаторів

Потік трафіку через єдиний комутатор цієї топології працює точно так само, як і в топології вище з трьома окремими фізичними комутаторами. Маршрутизатори налаштовані та працюють точно так само, як і вище.

Кожному порту комутатора може бути призначено певний віртуальний комутатор, або *VLAN*, що представлений числовим ідентифікатором. Наприклад, два порти на червоному міні-комутаторі можуть бути включені до *VLAN* 10, порти на помаранчевому - до *VLAN* 20, а порти на синьому - до *VLAN* 30. Якщо порт комутатора не має явно заданого номера *VLAN*, він автоматично потрапляє до *VLAN* за замовчуванням, яка у більшості виробників має номер 1 (*VLAN*1).

Трафік, що надходить на порт, прив’язаний до певної *VLAN*, може передаватися лише на інші порти в межах тієї ж *VLAN*. Комутатор ніколи не передає дані між різними *VLAN* - кожна *VLAN* функціонує як окремий, ізольований

комутатор у мережі.

Друга важлива функція *VLAN* полягає в тому, що вони дозволяють розширювати менші віртуальні комутатори на кілька фізичних комутаторів**.**

Рисунок 2.16 - *VLAN* розширення віртуальних комутаторів на кілька фізичних комутаторів

Зверніть увагу, що *VLAN* 10 і *VLAN* 30 були поширені на другий комутатор. Це дає змогу хостам *A* і *C* залишатися в межах однієї *VLAN*, навіть якщо вони підключені до різних фізичних комутаторів, які можуть бути розміщені в різних місцях. Головна перевага такого підходу полягає в тому, що логічна (рівень 2) структура мережі більше не залежить від фізичної. Це дозволяє одній *VLAN* охоплювати кілька приміщень, поверхів або навіть різні будівлі. У поданій топології кожен порт комутатора належить лише до однієї *VLAN*. Такий порт називається портом доступу - це порт, який асоційований з однією єдиною *VLAN*.

Натомість існує механізм, який дозволяє одному порту комутатора передавати трафік з кількох *VLAN.* Це називається транковим портом. Транковий порт - це порт комутатора, який передає трафік для кількох *VLA***.**

Мережевий екран (*Firewall*, або брандмауер) - це програмний або, як у нашому випадку, програмно-апаратний компонент комп’ютерної мережі, який здійснює контроль, а в деяких випадках і фільтрацію мережевого трафіку, що проходить через нього, відповідно до встановлених правил.

IDS (*Intrusion Detection System*) - система виявлення вторгнень.

IPS (*Intrusion Prevention System*) - система запобігання атакам.

Рисунок 2.17 - *FireWall*

IDS - це пасивний пристрій, який спостерігає за пакетами даних, що проходять по мережі, порівнюючи їх із шаблонами сигнатур та подає сигнал тривоги при виявленні підозрілої активності.

Рисунок 2.18 - *IDS* (*Intrusion Detection System*)

Навпаки, *IPS* - це активний пристрій, що працює у вбудованому режимі та запобігає атакам, блокуючи його. Основна відмінність полягає в тому, що брандмауер виконує такі дії, як блокування та фільтрація трафіку, в той час як *IPS/IDS* виявляє та попереджає системного адміністратора або запобігає атакі відповідно до конфігурації.

Рисунок 2.19 - *IPS* (*Intrusion Prevention System*)

У *SDA*-середовищі цей процес значно ускладнюється та вдосконалюється за рахунок *SGT* (*Security Group Tags*) та *TrustSec*.

Рисунок 2.20 - *SGT* (*Security Group Tags*)

У *SDA*, кожному користувачу або пристрою, після автентифікації, призначається *Security Group Tag* (*SGT*) - унікальний ідентифікатор, який вказує на роль або політику безпеки об’єкта. Далі, за допомогою *SGACL* (*Security Group Access Control Lists*), визначається, які типи трафіку дозволено між групами.

Наприклад, трафік між користувачами з тегом «*HR*» і сервером «*Finance*» може бути заблокований. Дозволено тільки *HTTPS* між *SGT* «*Support*» і «*Knowledge Base*».

TrustSec - це технологія *Cisco*, яка дозволяє забезпечити апаратну обробку тегів безпеки на комутаторах і маршрутизаторах, що підвищує продуктивність і

знижує навантаження на політики.

На відміну від статичних *ACL* (*Access Control Lists*), які важко масштабуються і підтримуються вручну, динамічне управління доступом в *SDA* передбачає:

- автоматичне призначення політик доступу залежно від: ролі користувача, типу пристрою, часу доби, фізичного розташування, відповідності політиці безпеки (*posture check*);

- централізоване адміністрування через *Cisco ISE* та *Cisco DNA Center*; - можливість миттєвої зміни політик без фізичних змін у конфігурації пристроїв.

Це забезпечує контекстну адаптацію коли змінюється контекст підключення, система автоматично застосовує відповідні політики безпеки.

Приклад, доступ користувача з підозрілим пристроєм

1. Користувач з ноутбуком проходить автентифікацію через *ISE*.

2. Система *posture* виявляє, що антивірус застарілий або відсутній. 3. *ISE* змінює *SGT* на «Q*uarantine*» (Карантин).

4. *SGACL* дозволяє лише доступ до внутрішньої сторінки з інструкціями щодо виправлення.

5. Після виправлення порушень *ISE* змінює тег і надає повний доступ.

Сегментація трафіку та динамічне управління дозволяють зменшити площу атаки, ізолювати інциденти безпеки та швидко адаптуватися до нових загроз, одночасно спрощуючи адміністрування та знижуючи витрати на обслуговування мережі.

2.9 Переваги *SDA* у порівнянні з традиційними мережевими рішеннями

Мережі з архітектурою *Software-Defined Access* (*SDA*) принципово відрізняються від традиційних мережевих рішень тим, що забезпечують централізоване управління, автоматизацію процесів та високий рівень безпеки, орієнтований на ідентичність користувача та контекст з’єднання. Це дозволяє усунути багато обмежень традиційних мереж та краще відповідати сучасним вимогам до безпеки, масштабованості й адаптивності.

1. Централізоване управління та автоматизація

У традиційних мережах конфігурація мережевих пристроїв здійснюється вручну - через *CLI* (*Command Line Interface*), що потребує значних ресурсів та є джерелом помилок. *SDA*, за підтримки *Cisco DNA Center*, забезпечує централізоване керування всіма політиками, пристроями та користувачами з єдиного графічного інтерфейсу.

2. Підвищена безпека за принципом *Zero Trust*

SDA підтримує підхід «нульової довіри» - жоден користувач або пристрій не довіряється за замовчуванням, навіть якщо він знаходиться всередині мережі. Для порівняння, у традиційних мережах часто існує довіра до всіх внутрішніх користувачів, що відкриває простір для *lateral movement* (горизонтального переміщення атак).

SDA забезпечує обов'язкову автентифікацію користувачів і пристроїв, постійний моніторинг та динамічне застосування політик, мікросегментацію трафіку на основі *SGT*.

3. Масштабованість та гнучкість

Традиційні мережі мають складнощі з масштабуванням через обмеження *VLAN, ACL*, статичних маршрутів. *SDA* використовує логічні сегменти, теги безпеки та централізовану політику, що дозволяє легко адаптувати мережу до змін в структурі організації.

Наприклад, додавання нового офісу або підрозділу не вимагає створення десятків *VLAN* і *ACL* - достатньо призначити відповідні теги та політики. 4. Контекстуальна політика доступу

У *SDA* політика доступу залежить не лише від *IP*-адреси або порту, як у традиційних мережах, а від: особи користувача, типу пристрою, рівня відповідності безпеці (*posture*), місцезнаходження, часу доступу.

Це дозволяє створювати гнучкі, адаптивні політики безпеки, які автоматично змінюються у відповідь на зміни контексту.

5. Інтеграція з сучасними системами безпеки

SDA легко інтегрується з рішеннями:

- *Cisco ISE* - для ідентифікації, автентифікації та авторизації;

- *SIEM* - для моніторингу та аналізу подій;

- *EDR/XDR* - для виявлення загроз на кінцевих точках;

- *IAM* - для централізованого управління ідентичностями.

Це створює єдину екосистему кібербезпеки, де всі елементи взаємодіють між собою та реагують на загрози у реальному часі.

6. Спрощення впровадження політик і аудиту

У традиційній мережі впровадження або зміна політик може займати дні, супроводжуватись простоєм або потребою в ручному тестуванні. *SDA* дозволяє миттєво застосовувати політики до будь-якого об'єкта, відстежувати та фіксувати зміни автоматично, вести аудит доступу й подій централізовано.

7. Покращена користувацька мобільність

У *SDA* користувач отримує доступ до своїх ресурсів незалежно від точки підключення (будь-який порт мережі, *Wi-Fi, VPN*), оскільки політика

«подорожує» разом з користувачем. У традиційній мережі доступ часто жорстко прив'язаний до конкретної *VLAN* або *IP*-сегменту.

Архітектура *SDA* має низку суттєвих переваг перед традиційними мережевими підходами. Забезпечує вищий рівень безпеки, зменшує складність управління, покращує досвід користувачів, а також забезпечує гнучкість та масштабованість, необхідні для сучасних цифрових підприємств.

Саме тому все більше організацій переходять до впровадження *SDA* як основної концепції побудови корпоративної мережі.

2.10 Висновки до розділу 2

У другому розділі проведено дослідження концепцію *SDN* (*Software-Defined Networking*), загальні характеристики архітектури *SDA* (*Software-Defined Access*), механізми контролю доступу в *SDA: RBAC, ABAC, SGT*, виконані порівняльні характеристики.

Політику безпеки у *SDA* та впровадження *Zero Trust*, використання *Cisco ISE*

для ідентифікації та авторизації користувачів, сегментацію трафіку та динамічне управління доступом, переваги *SDA* у порівнянні з традиційними мережевими рішеннями.

Таким чином, *SDA* не лише підвищує рівень інформаційної безпеки в корпоративному середовищі, а й спрощує адміністрування, пришвидшує впровадження змін та відповідає сучасним викликам цифрової трансформації.

РОЗДІЛ 3
ДОСЛІДЖЕННЯ ВПРОВАДЖЕННЯ МЕХАНІЗМІВ БЕЗПЕКИ В *SDA*-СЕРЕДОВИЩІ

3.1 Інтеграція з *SIEM, EDR, IAM*-системами

Інтеграція - це процес об'єднання окремих систем, компонентів або програмного забезпечення в єдину взаємодіючу систему, яка працює узгоджено. Простими словами, інтеграція означає, що різні програми або пристрої «вчаться спілкуватися» між собою і працювати разом для досягнення спільної мети.

Інтеграція з системами інформаційної безпеки є критично важливою складовою при розгортанні *SDA*-середовища, оскільки вона дозволяє забезпечити цілісне управління загрозами, централізоване логування, контроль доступу та моніторинг активності користувачів.

▪ Інтеграція з *SIEM*-системами

SIEM (*Security Information and Event Management*) - це система збору, кореляції та аналізу логів з різних мережевих та кінцевих пристроїв. У рамках дослідження було обрано систему *Splunk Enterprise Security* як *SIEM*-рішення. Основні етапи інтеграції:

- підключення мережевого обладнання (*SDA*-комутатори, контролери, *Cisco ISE*) до *SIEM* за допомогою *syslog* та *API*;
- налаштування дашбордів для візуалізації подій доступу, збоїв, спроб вторгнення;
- визначення кореляційних правил, що дозволяють автоматично виявляти

аномалії в поведінці користувачів, наприклад багаторазові спроби аутентифікації з різних локацій.

Завдяки цій інтеграції можно досягнути централізований контроль подій безпеки, що забезпечує оперативне виявлення інцидентів у мережі *SDA.*

▪ Інтеграція з *EDR*-системами

EDR (*Endpoint Detection and Response*) забезпечує моніторинг активності на кінцевих точках (робочих станціях, ноутбуках), виявлення підозрілих дій та реагування на інциденти.

У рамках дослідження було обрано рішення *Microsoft Defender for Endpoint*, яке інтегрується з контролером *Cisco DNA Center*.

Основні функції:

- збір телеметрії з хостів (активність процесів, підключення до мережі);
- виявлення шкідливого ПЗ або нетипової поведінки;
- можливість автоматизованого блокування доступу до *SDA*-мережі при виявленні загрози на пристрої.

Завдяки цій інтеграції можно забезпечити реакцію на загрози ще до їхнього проникнення в критичні сегменти мережі.

▪ Інтеграція з *IAM*-системами

IAM (*Identity and Access Management*) - це технологія управління ідентичністю користувачів, правами доступу та політиками авторизації. У рамках дослідження було обрано інтеграцію *SDA* з *Azure Active Directory* та *Okta*, які дозволяють:

- аутентифікувати користувачів на основі єдиного облікового запису (*SSO*); - застосовувати політики доступу до ресурсів на основі ролей (*RBAC*); - контролювати доступ до мережі через *Cisco ISE* на основі атрибутів з *IAM* (тип пристрою, місцезнаходження, рівень довіри).

Таблиця 3.1 - Порівняння *SIEM, EDR, IAM* за основними характеристиками

Критерій	***SIEM***	***EDR***	***IAM***
Основна функція	Збір, аналіз і кореляція подій	Моніторинг кінцевих точок	Ідентифікація та управління доступом

Реакція на загрози	Переважно пасивна (аналітика)	Активна (ізоляція, блокування)	Через політики доступу (умовна)
Інтеграція з *SDA*	Аналіз трафіку, логів, подій	Блокування небезпечних пристроїв	Управління рівнем доступу через політики *ISE*
Приклади рішень	*Splunk, IBM QRadar, ArcSight*	*CrowdStrike, SentinelOne, Defender*	*Okta, Azure AD, Ping Identity*

З таблиці 3.1 можно зробити висновок - *SIEM* фокусується на аналізі всієї мережевої активності та подій, *EDR* діє безпосередньо на кінцевих пристроях, зосереджуючись на запобіганні шкідливим діям, *IAM* регулює, хто і як отримує доступ до ресурсів, забезпечуючи базову логіку доступу в *SDA.*

Завдяки цій інтеграції можно досягнути гнучкості та точності в управлінні доступом до мережевих ресурсів у реальному часі.

Таблиця 3.2 - Порівняння *SIEM, EDR, IAM* за додатковими критеріями

Критерій	***SIEM***	***EDR***	***IAM***
Необхідність агентів	✗ (переважно ні, через *syslog/API*)	☑ (агенти на кожному пристрої)	✗ (через інтеграцію з *AD* або *API*)
Ресурсоємність	Висока (особливо при обробці великої кількості логів)	Середня	Низька
Гнучкість у налаштуваннях	Висока (можливість створення власних правил)	Середня (залежить від рішення)	Висока (*RBAC, MFA,* політики умов)
Сценарії використання в *SDA*	Аудит трафіку, виявлення інцидентів	Реагування на інфекцію на пристрої	Забезпечення доступу до ресурсів мережі

З таблиці 3.2 можно зробити висновок - *SIEM* не потребує агентів, проте споживає багато ресурсів і потребує окремих серверів для зберігання логів, *EDR* найвимогливіший до інфраструктури (агенти, оновлення), проте забезпечує гнучку реакцію на атаки, *IAM* найлегше масштабується і добре інтегрується з політиками

доступу в *SDA*, але сильно залежить від зовнішніх платформ (наприклад, *Azure AD*).

Таблиця 3.3 - Порівняння *SIEM, EDR, IAM*

Система	**Переваги**	**Недоліки**
SIEM	- Централізований моніторинг усіх подій - Аналітика загроз - Виявлення аномалій	- Висока складність налаштування - Дороге впровадження - Затримка в реагуванні
EDR	- Глибокий аналіз активності на хостах - Автоматичне реагування - Виявлення на ранніх етапах	- Потребує встановлення агентів - Може створювати помилкові спрацювання
IAM	- Єдиний вхід (*SSO*) - Контроль на основі ролей - Підтримка *MFA*	- Складність масштабування - Може стати «точкою відмови»

З таблиці 3.3 можно зробити висновок - *SIEM* є незамінною для глобального аналізу та виявлення загроз, але її складність і вартість можуть бути перешкодою для швидкої реалізації, *EDR* ефективно захищає кінцеві точки з активною реакцією на загрози, але потребує детального адміністрування й налаштування агентів, *IAM* дозволяє зменшити ризики за рахунок чіткої ідентифікації користувачів і управління доступом, але має залежність від стабільності зовнішніх служб.

Інтеграція *SDA*-середовища з *SIEM, EDR* та *IAM*-системами значно підвищує рівень захищеності інфраструктури. Забезпечується проактивне виявлення загроз, контроль поведінки користувачів і пристроїв, а також швидке реагування на інциденти. Такий підхід дозволяє не лише зменшити ризики, а й забезпечити відповідність сучасним стандартам безпеки.

3.2 Оцінка ефективності контролю доступу та рівня захисту

Оцінка ефективності контролю доступу та оцінка рівня захисту - це важливі етапи у процесі забезпечення інформаційної безпеки в будь-якій *IT*-системі, зокрема у системах з архітектурою *Software-Defined Access* (*SDA*).

Контроль доступу - це сукупність механізмів, які регулюють, хто і до яких

ресурсів має право доступу у системі.

Оцінка ефективності контролю доступу полягає у визначенні, наскільки ці механізми реально забезпечують належний рівень безпеки та відповідають встановленим політикам доступу.

Основні аспекти оцінки ефективності:

1. Політика контролю доступу:

- визначення, чи існує чітка політика доступу;
- наскільки вона відповідає вимогам безпеки організації.

2. Типи контролю доступу:

- *DAC (Discretionary Access Control)* - на розсуд власника ресурсу; - *MAC (Mandatory Access Control)* - базується на рівнях класифікації;

- *RBAC (Role-Based Access Control)* - доступ згідно з роллю користувача; - *ABAC (Attribute-Based Access Control)* - залежить від атрибутів користувача, ресурсу, контексту.

3. Реалізація контролю доступу:

- перевірка, чи правильно реалізовані механізми автентифікації та авторизації;
- аналіз журналів подій (логів) для виявлення аномалій доступу.

4. Тестування механізмів:

- проведення «*penetration testing* або *audit testing»* для виявлення слабких місць;
- аналіз на вразливості, наприклад, до атак типу «*privilege escalation*».

5. Наявність механізмів моніторингу та реагування:

- чи виявляється несанкціонований доступ;
- чи запускаються захисні дії у випадку порушень.

6. Відповідність стандартам:

- *ISO/IEC* 27001, *NIST SP* 800-53, *GDPR*.

Оцінка рівня захисту інформаційної системи - поняття, яке включає не лише ефективність контролю доступу, а й усі інші аспекти забезпечення безпеки. Основні елементи оцінки рівня захисту:

1. Ідентифікація активів і загроз:

- Які ресурси потребують захисту?

- Які загрози можуть завдати шкоди (віруси, атаки, витоки)?

2. Аналіз ризиків:

- оцінка ймовірності реалізації загроз та масштабів можливих наслідків.

3. Оцінка засобів захисту:

- фізичні (доступ до серверних приміщень);

- організаційні (політики, інструкції);

- технічні (брандмауери, шифрування, *IDS/IPS*).

4. Рівень відповідності моделі *CIA*:

- *Confidentiality* (конфіденційність) - чи не можуть треті сторони отримати несанкціонований доступ до інформації?

- *Integrity* (цілісність) - чи не було змін у даних без дозволу?

- *Availability* (доступність) - чи є доступ до ресурсів у потрібний момент? 5. Наявність інцидент-менеджменту:

- Як реагує система на події безпеки?

- Чи фіксуються та розслідуються інциденти?

6. Періодичність аудиту та перевірок:

- Регулярні перевірки дозволяють виявляти нові вразливості.

7. Зрілість системи захисту:

Наприклад, за моделлю *CMM* (*Capability Maturity Model*) - від 1 (хаотичний рівень) до 5 (оптимізований).

Модель *CMM* (*Capability Maturity Model*) - це п’ятирівнева модель, яка дозволяє оцінити ступінь зрілості процесів в організації. Кожен рівень демонструє, наскільки добре процеси задокументовані, реалізовані, керовані й оптимізовані.

Застосування цієї моделі в контексті інформаційної безпеки дозволяє оцінити, наскільки ефективно організація управляє ризиками, контролює доступ і забезпечує захист *IT*-інфраструктури.

Рисунок 3.1 - Модель *CMM* (*Capability Maturity Model*)

Рівні моделі *CMM*:

1. Рівень 1 - Ініціативний (хаотичний):

- процеси не визначені, виконуються спонтанно та залежно від ситуації; - відсутні формалізовані політики, процедури та стандарти безпеки; - у сфері ІБ часто діють реактивно: реагують на інциденти, не маючи стратегії;

- залежність від окремих співробітників, а не від системних підходів.

2. Рівень 2 - Повторюваний:

- основні процеси ідентифіковано та частково повторюються;

- існують окремі політики та процедури безпеки, але вони не охоплюють всю організацію;

- певна формалізація вже присутня, але впровадження ще не є стабільним; - упроваджується базовий контроль доступу, звітність, реагування на інциденти.

3. Рівень 3 - Визначений:

- процеси стандартизовані, задокументовані, адаптовані під потреби організації;

- ІБ інтегровано в загальні бізнес-процеси;

- ролі та відповідальність чітко визначені;

- забезпечується системний підхід до управління ризиками, аудиту та моніторингу.

4. Рівень 4 - Керований (вимірюваний):

- процеси безпеки активно контролюються за допомогою показників ефективності;

- впроваджені системи моніторингу, аналітики та автоматичного реагування;
- дані використовуються для прийняття рішень щодо вдосконалення ІБ. 5.

Рівень 5 - Оптимізований:

- безпека є стратегічною частиною управління організацією;
- постійне вдосконалення процесів за рахунок зворотного зв'язку, нових технологій і досвіду;

- високий рівень автоматизації, адаптації та гнучкості;
- підтримка інноваційних підходів, таких як *Zero Trust, AI/ML* у кіберзахисті.

Таблиця 3.4 - Критерії оцінки ефективності контролю доступу

Критерії	**Опис**
Надійність автентифікації	Наскільки точно система визначає користувача (наприклад, використання паролів, біометрії, багатоетапної автентифікації).
Точність авторизації	Чи відповідають надані права фактичній ролі/атрибутам користувача.
Мінімізація прав доступу (принцип найменших привілеїв)	Чи має користувач лише ті доступи, які необхідні для виконання його обов'язків.
Контроль дій користувачів	Чи фіксуються та аналізуються дії користувачів у системі (журнали подій, моніторинг).
Гнучкість налаштувань політик доступу	Наскільки просто змінювати політики при зміні умов або структури організації.
Масштабованість	Чи зберігається ефективність при збільшенні кількості користувачів, ресурсів та політик.
Контекстуальність	Чи враховує система змінні умови доступу (час, місце, пристрій, поведінкові фактори).
Стійкість до порушень	Наскільки важко обійти або зламати механізми контролю доступу.

Таблиця 3.5 - Критерії оцінки рівня захисту

Критерії	**Опис**
Ізоляція середовищ	Чи добре розділено різні рівні доступу або *VLAN*, щоб зменшити ризики поширення атак.
Виявлення та реагування на загрози	Чи здатна система виявити несанкціоновані спроби доступу і адекватно на них реагувати.

Цілісність і контроль змін	Чи є захист від несанкціонованого редагування критично важливих даних чи конфігурацій.
Безпечне зберігання облікових даних	Чи використовуються шифрування, хешування тощо для збереження паролів, сертифікатів.
Життєвий цикл облікових записів	Чи правильно створюються, оновлюються і видаляються облікові записи користувачів.
Аудит і звітність	Чи існує можливість перегляду історії дій для виявлення порушень або аналізу інцидентів.

З таблиць 3.4 - 3.5 можно зробити висновок - чим вища відповідність зазначеним критеріям, тим вищий загальний рівень безпеки в інформаційній системі. Оцінка ефективності контролю доступу фокусується на перевірці правильності реалізації й роботи механізмів доступу користувачів до ресурсів.

Оцінка рівня захисту охоплює весь спектр безпекових заходів, у тому числі контроль доступу, а також захист від зовнішніх і внутрішніх загроз.

3.3 Аналіз результатів та пропозиції щодо вдосконалення

На основі проведеного дослідження інтеграції архітектури *Software-Defined Access* (*SDA*) з системами *SIEM, EDR* та *IAM*, а також оцінки ефективності контролю доступу й рівня захисту за моделлю зрілості *CMM*, сформульовано такі пропозиції щодо вдосконалення інформаційної безпеки в корпоративному середовищі:

1. Підвищення рівня зрілості за моделлю *CMM*:

- рекомендується переходити від рівня 2-3 до рівня 4-5, зосередившись на вимірюванні ефективності безпекових процесів та впровадженні механізмів постійного вдосконалення;
- визначити ключові показники ефективності (*KPI*) для контролю доступу, моніторингу подій і реагування на інциденти.

2. Поглиблена інтеграція *SIEM, EDR* та *IAM* з *SDA*:

- забезпечити повну сумісність між *SDA* та обраними рішеннями *SIEM* і *EDR* для автоматичного обміну подіями безпеки, контекстною інформацією та ризик оцінками;
- використовувати *IAM*-системи як єдину точку контролю автентифікації,

авторизації та управління життєвим циклом облікових записів. 3. Автоматизація політик безпеки:

- впровадити автоматичну генерацію політик доступу на основі поведінкового аналізу користувачів (*UEBA*) та динамічного ризик-профілю; - використовувати тегування (*SGT*) у *SDA* для гнучкого управління доступом у режимі реального часу.

4. Розширення принципів *Zero Trust*:

- поглибити реалізацію концепції *Zero Trust*, запровадивши обов'язкову перевірку кожної взаємодії між вузлами мережі незалежно від їхнього розташування;

- використовувати багатофакторну автентифікацію (*MFA*) та контекстну авторизацію.

5. Підвищення кваліфікації персоналу:

- забезпечити регулярне навчання IT-фахівців з управління *SDA, SIEM, EDR, IAM* та політиками безпеки;

- розробити внутрішні методичні документи щодо дій у випадках інцидентів безпеки.

6. Проведення регулярного аудиту та тестування:

- виконувати регулярний аудит доступу, сегментації та налаштувань безпеки в *SDA*;

- залучати сторонніх експертів до періодичного аналізу вразливостей. Ці пропозиції спрямовані на побудову адаптивної, масштабованої та безпечної корпоративної мережі, здатної відповідати на сучасні виклики кібербезпеки.

3.4 Висновки до розділу 3

У третьому розділі проведено дослідження інтеграції *SDA* з системами *SIEM, EDR* та *IAM*, проведено оцінку ефективності контролю доступу й рівня захисту, модель *CMM* (*Capability Maturity Model*), проаналізовано результати та надано пропозиції щодо їх вдосконалення.

ВИСНОВКИ

У першому розділі проведено аналіз предметної області, а саме поняття інформаційної безпеки та її роль у корпоративному середовищі, основні загрози інформаційній безпеці в *IT*-інфраструктурі, традиційні методи контролю доступу, підходи до захисту корпоративних мереж (*DLP, IAM, SIEM*).

У другому розділі проведено дослідження концепцію *SDN* (*Software-Defined Networking*), загальні характеристики архітектури *SDA* (*Software-Defined Access*), механізми контролю доступу в *SDA: RBAC, ABAC, SGT*, виконані порівняльні характеристики. Політику безпеки у *SDA* та впровадження *Zero Trust*, використання *Cisco ISE* для ідентифікації та авторизації користувачів, сегментацію трафіку та динамічне управління доступом, переваги *SDA* у порівнянні з традиційними мережевими рішеннями.

SDA не лише підвищує рівень інформаційної безпеки в корпоративному середовищі, а й спрощує адміністрування, пришвидшує впровадження змін та відповідає сучасним викликам цифрової трансформації.

У третьому розділі проведено дослідження інтеграції *SDA* з системами *SIEM, EDR* та *IAM*, проведено оцінку ефективності контролю доступу й рівня захисту, модель *CMM* (*Capability Maturity Model*), проаналізовано результати та надано пропозиції щодо їх вдосконалення.

У результаті проведеного дослідження було всебічно розглянуто сучасні підходи до забезпечення інформаційної безпеки в корпоративних мережах із акцентом на використанні архітектури *Software-Defined Access* (*SDA*).

Аналіз предметної області дозволив окреслити основні виклики та загрози, притаманні *IT*-інфраструктурі підприємств, а також виявити обмеження традиційних засобів контролю доступу.

Детальне вивчення архітектури *SDA* продемонструвало її переваги в контексті забезпечення гнучкого, масштабованого та ефективного управління доступом до корпоративних ресурсів. Завдяки інтеграції з концепцією *Zero Trust*, використанню *Cisco ISE* та динамічному підходу до сегментації мережі, *SDA*

суттєво підвищує рівень безпеки, водночас оптимізуючи адміністрування *IT* середовища. Інтеграція *SDA* з такими системами, як *SIEM, EDR* та *IAM*, дозволяє створити цілісну й адаптивну екосистему захисту, що забезпечує високий рівень контролю, виявлення загроз та швидке реагування на інциденти. Підсумковий аналіз ефективності засвідчив доцільність використання *SDA* у корпоративному середовищі як одного з ключових компонентів сучасної інформаційної безпеки.

Впровадження *SDA* є актуальним і перспективним напрямом розвитку *IT* інфраструктури, забезпечуючи надійний захист корпоративних ресурсів і даних.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Арсенюк І.В., Яровий А.А. Компютерні мержі. Посібник. Частина 1. - Вінниця: ВНТУ, 2008. -117с.

2. Вараксін О.О., Василіу Є.В. Кібербезпека мереж наступних поколінь: навч. посібник. Одеса: ОНАЗ ім. О.С. Попова, 2012. - 240 с.

3. Євсеєв С. П., Дженюк Н. В. Комп'ютерні мережі: навчальний посібник / За редакцією Толкачов В.К. та ін. - Харків, - Львів:«Новий Світ - 2000», 2025. - 471 с.

4. Куланов Ю.О., Луцький Г.М. Компютерні мережі: Підручник./ За ред. Ю.С. Ковтанюка. - К.:Видавництво «Юніор», 2005.- 400с.

5. Лосев Ю. І. Комп'ютерні мережі: навчальний посібник / Ю. І. Лосев, К. М. Руккас, С. І. Шматков / За редакцією Ю. І. Лосева. - Х.: ХНУ імені В. Н. Каразіна, 2013. - 248 с.

6. Микитишин А.Г., Митник М.М. Комп'ютерні мережі: навч. посібник. Львів: «Магнолія 2006», 2013. - 256 с.

7. Мінухін С.В., Кавун С.В. Комп`ютерні мережі. Загальні принципи функціонування комп'ютерних мереж Харків: ХНЕУ, 2008. - 210 с. 8. Стрихалюк Б. М. Теорія побудови та протоколи інфокомунікаційних мереж: Конспект лекцій. Львів: Львівська політехніка, 2017. - 121 с.

9. Концепція *SDN* (*Software-Defined Networking*). *URL*: https://www.nomios.nl/ (дата звернення 03.05.2025).

10.Архітектура *SDA*. *URL*: https://www.sdaarchitecture.com/ (дата звернення

17.05.2025).

11. Сегментація мережі. *URL*: https://lanmarket.ua/ (дата звернення 25.05.2025).

12. *Zero Trust security. URL*: https://www.cloudflare.com (дата звернення 24.05.2025).

КРИВОРІЗЬКИЙ ФАХОВИЙ КОЛЕДЖ
ДЕРЖАВНОГО НЕКОМЕРЦІЙНОГО ПІДПРИЄМСТВА
«ДЕРЖАВНИЙ УНІВЕРСИТЕТ «КИЇВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ»

РЕЦЕНЗІЯ
керівника кваліфікаційної роботи

Випускника освітньо-професійного ступеня *фаховий молодший бакалавр*
спеціальність *123 «Комп'ютерна інженерія»*
Відділення *комп'ютерної та програмної інженерії*
Олексію КОНОВАЛЬЧУКУ
(ім'я, прізвище)

1. *Кваліфікаційна робота на тему «Дослідження механізмів безпеки та контролю доступу в SDA».*
2. *Кваліфікаційна робота відповідає темі, затвердженій начальником коледжу.*
3. *Завдання на виконання кваліфікаційної роботи виконано в повному обсязі.*
4. *У кваліфікаційній роботі проводиться дослідження основних загроз інформаційній безпеці в IT-інфраструктурі, традиційних методів контролю доступу, підходи до захисту корпоративних мереж (DLP, IAM, SIEM), концепцію SDN (Software-Defined Networking), загальні характеристики архітектури SDA (Software-Defined Access), механізми контролю доступу в SDA: RBAC, ABAC, SGT, виконані порівняльні характеристики, політику безпеки у SDA та впровадження Zero Trust, використання Cisco ISE для ідентифікації та авторизації користувачів, сегментацію трафіку та динамічне управління доступом, переваги SDA у порівнянні з традиційними мережевими рішеннями. Інтеграція SDA з системами SIEM, EDR та IAM, проведено оцінку ефективності контролю доступу й рівня захисту, рівні моделі CMM (Capability Maturity Model), проаналізовано результати та надано пропозиції щодо їх вдосконалення.*
5. *Якість виконання пояснювальної записки та ілюстративного (графічного) матеріалу відповідає вимогам Державних стандартів.*
6. *У кваліфікаційній роботі достатньо наукових обгрунтувань.*
7. *Кваліфікаційна робота заслуговує оцінку «добре».*