ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

Кафедра Систем та технологій кібербезпеки
Ступінь вищої освіти Бакалавр
Спеціальність 125 Кібербезпека та захист інформації
Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри СТКБ
_____ Галина ГАЙДУР
“___” _____ 2025 року

З А В Д А Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Федосєєва Максима Андрійовича
(прізвище, ім’я)

1. Тема кваліфікаційної роботи: «Система захисту облікових записів користувачів у корпоративних інформаційних системах з використанням двофакторної аутентифікації»

керівник кваліфікаційної роботи Бондаренко Зоя,
(прізвище, ім’я, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «24» лютого 2025 року № 56.

2. Строк подання здобувачем вищої освіти кваліфікаційної роботи 30.05.2025

3. Вихідні дані до кваліфікаційної роботи
інформаційні ресурси організації;
рішення та рекомендації для двофакторної аутентифікації
наукова та технічна література, експлуатаційна документація, нормативні документи, міжнародні стандарти.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Аналіз проблематики ідентифікації та аутентифікації
2. Аналіз наявних методів двофакторної аутентифікації
3. Розроблення рекомендацій щодо захисту облікових записів користувачів у корпоративних інформаційних системах з використанням двофакторної аутентифікації

5. Перелік графічного матеріалу
Презентація PowerPoint.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Визначення актуальності проблеми	27.02.2025 р.	
2.	Аналіз наукової та технічної літератури з питань теми кваліфікаційної роботи.	17.03.2025 р.	
3.	Аналіз проблематики ідентифікації та аутентифікації	25.03.2025 р.	
4.	Аналіз наявних методів двофакторної аутентифікації	11.04.2025 р.	
5.	Розроблення рекомендацій щодо захисту облікових записів користувачів у корпоративних інформаційних системах з використанням двофакторної аутентифікації	16.05.2025 р.	
6.	Оформлення результатів дослідження.	23.05.2025 р.	
7.	Підготовка презентації до захисту.	30.05.2024 р.	

Здобувач вищої освіти _____ Максим ФЕДОСЄЄВ
(підпис) *(ім'я, прізвище)*

Керівник кваліфікаційної роботи _____ Зоя БОНДАРЕНКО
(підпис) *(ім'я, прізвище)*

6. Дата видачі завдання 15.02.2025 р.

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня бакалавра: 67 стор., 7 табл., 4 рис., 40 джерел.

Мета роботи – розробити рекомендації щодо використання методів та засобів двофакторної аутентифікації у корпоративних інформаційних системах для підвищення рівня безпеки облікових записів користувачів.

Об’єкт дослідження – процес аутентифікації користувачів у корпоративних інформаційних системах.

Предмет дослідження – методи та засоби двофакторної аутентифікації, що використовуються для підтвердження особистості користувача.

Короткий зміст роботи:

У роботі здійснено огляд сучасних методів захисту облікових записів у корпоративних інформаційних системах. Особливу увагу приділено двофакторній аутентифікації (2FA) як засобу підвищення безпеки. Проаналізовано технології, які лежать в основі 2FA, а також інструменти її реалізації на прикладі рішень Cisco ISE та Cisco Duo.

Розглянуто принципи роботи RADIUS-інтеграції між Cisco ISE та Duo Authentication Proxy, а також механізми доставки push-повідомлень через Duo Cloud. Вивчено конфігурацію Duo Authentication Proxy, а також журнали подій Cisco ISE як інструмент контролю доступу.

Надано практичні рекомендації щодо впровадження двофакторної аутентифікації у корпоративне середовище для забезпечення надійного управління доступом до ресурсів.

КЛЮЧОВІ СЛОВА: ДВОФАКТОРНА АУТЕНТИФІКАЦІЯ, КОРПОРАТИВНА ІНФОРМАЦІЙНА СИСТЕМА, CISCO ISE, CISCO DUO, БЕЗПЕКА ОБЛІКОВИХ ЗАПИСІВ, УПРАВЛІННЯ ДОСТУПОМ.

ЗМІСТ

ВСТУП 6
1 АНАЛІЗ ПРОБЛЕМАТИКИ ІДЕНТИФІКАЦІЇ ТА АУТЕНТИФІКАЦІЇ В КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ …… 9
1.1 Основні поняття ідентифікації та аутентифікації …….....9
1.2 Проблеми традиційних методів аутентифікації ……..10
1.3 Специфіка корпоративних інформаційних систем……. 12
1.4 Роль двофакторної аутентифікації в захисті облікових записів…… 14
2 АНАЛІЗ НАЯВНИХ МЕТОДІВ ДВОФАКТОРНОЇ АУТЕНТИФІКАЦІЇ.. 17
2.1 Класифікація методів 2FA……..17
2.2 Переваги та недоліки 2FA ……18
2.3 Тенденції розвитку 2FA ……19
2.4 Дослідження Cisco Duo як засобу двофакторної аутентифікації…….30
2.5 Порівняння Cisco Duo з іншими рішеннями……..35
3 РОЗРОБЛЕННЯ РЕКОМЕНДАЦІЙ ЩОДО ЗАХИСТУ ОБЛІКОВИХ ЗАПИСІВ КОРИСТУВАЧІВ У КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ З ВИКОРИСТАННЯМ ДВОФАКТОРНОЇ АУТЕНТИФІКАЦІЇ……..……..21
3.1 Фундаментальні принципи ефективного впровадження двофакторної аутентифікації ……..…..21
3.2 Аналіз Cisco Identity Services Engine (ISE) як корпоративної системи управлінням доступом…….…… 23
3.3 Рекомендовані методи верифікації в інтегрованій системі Cisco ISE та Duo ……32
3.4 Практичні кроки ефективного впровадження Cisco Duo та Cisco ISE.....35
3.5. Комплексне управління ризиками, пов'язаними з 2FA……40
3.6 Очікувані результати від впровадження комплексного рішення Cisco Duo та ISE…….....46

3.7 Сценарії використання Cisco Duo та ISE ……..48
ВИСНОВКИ..... 55
ПЕРЕЛІК ПОСИЛАНЬ..... 57
ДОДАТОК А. ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація) 61

ВСТУП

У сучасному цифровому світі корпоративні інформаційні системи (КІС) є основою для управління бізнес-процесами, зберігання даних та забезпечення взаємодії між співробітниками, клієнтами та партнерами. Зі зростанням кіберзагроз захист облікових записів користувачів стає одним із найважливіших завдань для забезпечення безпеки організацій. Традиційні методи аутентифікації, такі як паролі, більше не відповідають сучасним вимогам безпеки через їхню вразливість до атак, таких як фішинг, крадіжка даних чи перехоплення.

Двофакторна аутентифікація (2FA) є ефективним рішенням для підвищення рівня безпеки, оскільки вона вимагає двох незалежних факторів для підтвердження особи користувача: знання (наприклад, пароль), володіння (наприклад, смартфон або токен) або ідентичність (наприклад, біометричні дані). Впровадження 2FA в КІС дозволяє значно знизити ризик несанкціонованого доступу, захистити конфіденційні дані та забезпечити відповідність міжнародним стандартам безпеки.

Об’єкт дослідження: процес аутентифікації користувачів у корпоративних інформаційних системах.

Предмет дослідження: методи та засоби двофакторної аутентифікації, що використовуються для підтвердження особистості.

Мета роботи: розробити рекомендації щодо використання методів та засобів двофакторної аутентифікації в корпоративних інформаційних системах для забезпечення захисту облікових записів користувачів.

Завдання роботи:

1. Провести аналіз проблематики ідентифікації та аутентифікації в КІС.
2. Дослідити наявні методи та засоби двофакторної аутентифікації, оцінити їхні переваги та недоліки.
3. Розробити практичні рекомендації щодо впровадження 2FA в КІС, враховуючи специфіку корпоративного середовища.

Методи дослідження: аналіз літературних джерел, порівняльний аналіз методів 2FA, синтез рекомендацій на основі отриманих даних, моделювання сценаріїв використання 2FA.

Новизна роботи: розробка комплексного підходу до впровадження 2FA в КІС, який враховує сучасні кіберзагрози, специфіку корпоративного середовища та баланс між безпекою і зручністю для користувачів.

Практична цінність: запропоновані рекомендації можуть бути використані організаціями для підвищення безпеки їхніх інформаційних систем, зменшення ризиків компрометації облікових записів та забезпечення відповідності стандартам безпеки, таким як ISO 27001 і GDPR.

Структура роботи: робота складається зі вступу, трьох основних розділів, висновків, списку використаних джерел та додатків. Перший розділ присвячений аналізу проблематики ідентифікації та аутентифікації. Другий розділ досліджує методи та засоби 2FA. Третій розділ містить рекомендації щодо впровадження 2FA в КІС.

1 АНАЛІЗ ПРОБЛЕМАТИКИ ІДЕНТИФІКАЦІЇ ТА АУТЕНТИФІКАЦІЇ В КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ

1.1 Основні поняття ідентифікації та аутентифікації

Корпоративні інформаційні системи (КІС) є основою функціонування будь-якого сучасного бізнесу, забезпечуючи критично важливі процеси від управління персоналом до фінансових операцій. У той же час, вони стають основною мішенню для кіберзлочинців. У цьому контексті ідентифікація та аутентифікація відіграють ключову роль, виступаючи першим і найважливішим рубежем захисту. Проте їх ефективність знаходиться під постійною загрозою, вимагаючи глибокого розуміння існуючих проблем та пошуку нових рішень.

Щоб повноцінно розібратися в проблематиці, необхідно чітко розмежувати базові терміни.

Ідентифікація – це первинний етап, на якому суб'єкт або користувач заявляє про свою приналежність до певної особистості в системі. Це досягається шляхом надання унікального ідентифікатора. Такими ідентифікаторами можуть бути логін, ім'я користувача, адреса електронної пошти або навіть унікальний ідентифікатор пристрою. По суті, ідентифікація відповідає на питання: "Хто ти заявляєш, що ти є?". Це декларативний процес, що не передбачає перевірки достовірності заявлених даних. Наприклад, коли ви вводите свій логін на сайті, ви ідентифікуєте себе як певного користувача.

Після успішної ідентифікації настає етап аутентифікації. Це критичний процес, який полягає в перевірці достовірності заявленої ідентичності. Аутентифікація підтверджує, що суб'єкт є тим, за кого він себе видає. Цей процес ґрунтується на підтвердженні наданих даних, які можуть включати:

Знання: те, що користувач знає (наприклад, пароль, PIN-код, відповідь на секретне питання).

Володіння: те, що користувач має (наприклад, токен, смартфон з мобільним застосунком, смарт-карта, фізичний ключ).

Приналежність: те, ким є користувач (наприклад, біометричні характеристики – відбиток пальця, сканування обличчя, райдужної оболонки ока, голос).

У корпоративних інформаційних системах, де доступ до чутливих даних та стратегічно важливих ресурсів є повсякденною потребою, ідентифікація та аутентифікація є не просто функцією, а першим і найважливішим бар'єром захисту. Вони забезпечують контроль доступу до широкого спектру ресурсів: від внутрішніх баз даних клієнтів та фінансових реєстрів до систем планування ресурсів підприємства (ERP), внутрішніх порталів співробітників, систем управління взаємовідносинами з клієнтами (CRM) та високозахищених фінансових платформ. Однак, незважаючи на їхню фундаментальну важливість, традиційні методи аутентифікації, що історично базувалися переважно на паролях, виявилися недостатніми та вразливими в умовах еволюції кіберзагроз.

1.2 Проблеми традиційних методів аутентифікації

Історично склалося так, що паролі були основним і часто єдиним методом аутентифікації. Їхня простота в реалізації та використанні зробила їх повсюдними. Проте, з розвитком кіберзлочинності, стало очевидним, що ця простота обертається величезними ризиками. Традиційні методи аутентифікації мають низку фундаментальних недоліків, які роблять їх вкрай неефективними у боротьбі з сучасними кіберзагрозами.

Фішинг-атаки: Це одна з найпоширеніших і найпідступніших загроз. Зловмисники використовують підроблені вебсайти, електронні листи чи повідомлення, що імітують довірені джерела (наприклад, банк, державну установу, внутрішній ІТ-відділ компанії), щоб обманним шляхом змусити користувачів ввести свої облікові дані. Після введення цих даних, вони потрапляють безпосередньо до рук зловмисників. Згідно з авторитетним Verizon Data Breach

Investigations Report 2024, вражаючі 36% усіх кібератак у звітному періоді були пов'язані саме з фішингом, підкреслюючи його домінуючу роль у компрометації облікових записів.

Слабкі паролі та повторне використання: Ця проблема є наслідком людського фактора та прагнення до зручності. Користувачі часто обирають прості, легко вгадувані комбінації (наприклад, "123456", "password", "qwerty", власні імена, дати народження). Більше того, поширена практика повторного використання одного й того ж пароля для різних сервісів. Якщо один із цих сервісів буде скомпрометований, зловмисники отримають доступ до всіх облікових записів користувача, де використовується цей пароль. За даними численних досліджень, мільйони облікових записів щорічно компрометуються саме через слабкі або повторно використовувані паролі.

Крадіжка баз даних (Data Breaches): Це одна з наймасштабніших загроз. Зловмисники цілеспрямовано атакують сервери компаній з метою викрадення баз даних, що містять облікові дані користувачів, включаючи зашифровані (хешовані) паролі. Незважаючи на хешування, багато слабких або поширених паролів можуть бути дешифровані або зламані за допомогою Rainbow Tables або методів Brute-Force та Dictionary Attacks. Ці витоки стають джерелом мільйонів скомпрометованих облікових записів, які потім продаються на чорному ринку або використовуються для подальших атак.

Перехоплення даних (Man-in-the-Middle, Keyloggers, Malware): Це більш технічно складні, але не менш руйнівні методи.

Кейлогери – це шкідливе програмне забезпечення, яке таємно записує кожне натискання клавіші на зараженому пристрої, включаючи логіни та паролі.

Шкідливе програмне забезпечення може бути розроблене для викрадення облікових даних безпосередньо з пам'яті комп'ютера або перехоплення мережевого трафіку.

Атаки Man-in-the-Middle (MITM) – це ситуації, коли зловмисник перехоплює комунікацію між користувачем та сервером, читаючи та потенційно модифікуючи дані, що передаються. Це дозволяє йому "підслухати" передачу облікових даних.

Наслідки цих проблем є катастрофічними для бізнесу. Вони призводять до:

- Витоку конфіденційної інформації: компрометація персональних даних клієнтів, комерційної таємниці, інтелектуальної власності.

- Фінансових втрат: прямі збитки від шахрайства, штрафи за порушення регуляторних норм, витрати на відновлення після інцидентів.

- Порушення бізнес-процесів: простої в роботі систем, втрата довіри клієнтів, репутаційні збитки.

Масштаб цих втрат ілюструють дані IBM Security Cost of a Data Breach Report 2024, згідно з яким середня вартість витоку даних у 2023 році склала staggering 4,45 мільйона доларів США. Це підкреслює, що інвестиції в надійні методи аутентифікації є не просто питанням безпеки, а й ключовим фактором фінансової стабільності та операційної безперервності.

1.3 Специфіка корпоративних інформаційних систем

Корпоративні інформаційні системи (КІС) не є статичними середовищами; вони динамічні, складні та постійно розвиваються, що створює додаткові виклики для забезпечення безпеки облікових записів. Їхня унікальна специфіка вимагає більш глибокого та комплексного підходу до аутентифікації, ніж той, що застосовується в індивідуальних користувацьких сценаріях.

Масштабність: Великі організації – це не одиничні користувачі, а сотні, тисячі, а іноді й десятки тисяч співробітників. Кожен із цих користувачів потребує індивідуального облікового запису та різного рівня доступу до широкого спектру ресурсів. Управління такою кількістю облікових записів, забезпечення їх унікальності, відстеження активності та підтримка належного рівня безпеки стає надзвичайно складним завданням. Простий вихід з ладу навіть кількох облікових записів може призвести до системних збоїв та значних збитків.

Різноманітність пристроїв: Сучасні КІС функціонують у середовищі, де співробітники використовують не лише корпоративні, а й особисті пристрої (BYOD – Bring Your Own Device). Це включає ноутбуки, стаціонарні комп'ютери,

смартфони, планшети та інші мобільні пристрої. Кожен із цих пристроїв може мати різний рівень захисту, операційні системи та програмне забезпечення, що значно підвищує ризики компрометації. Зловмисник може отримати доступ до корпоративних даних через незахищений особистий пристрій співробітника, навіть якщо корпоративна інфраструктура добре захищена.

Віддалений доступ та гібридні моделі роботи: Зростання популярності віддаленої роботи та поширення гібридних моделей зробили доступ до корпоративних ресурсів з-за меж офісу нормою, а не винятком. Це вимагає забезпечення безпечного доступу через такі канали, як віртуальні приватні мережі (VPN), хмарні сервіси (наприклад, Microsoft 365, Google Workspace) чи віддалені робочі столи. Кожен із цих методів доступу створює нові потенційні точки входу для зловмисників, що потребує посилених механізмів аутентифікації для захисту від несанкціонованого доступу.

Інтеграція з зовнішніми системами та хмарними платформами: Сучасні підприємства активно використовують хмарні платформи (AWS, Google Cloud, Azure) та інтегруються з безліччю сторонніх сервісів. Це означає, що КІС не існують ізольовано; вони є частиною великої екосистеми. Така інтеграція вимагає сумісності з різними протоколами аутентифікації (наприклад, OAuth, SAML, OpenID Connect) та створення єдиної системи управління ідентичністю та доступом (IAM), що здатна забезпечити безпечний та безперешкодний доступ до всіх необхідних ресурсів.

Регуляторні вимоги та відповідність стандартам: Багато галузей та країн мають суворі регуляторні вимоги щодо захисту даних та інформаційної безпеки. Організації повинні дотримуватися міжнародних та національних стандартів безпеки, таких як GDPR (Загальний регламент про захист даних), ISO 27001 (Стандарт управління інформаційною безпекою), PCI DSS (Стандарт безпеки даних індустрії платіжних карток) та HIPAA (Закон про переносність та підзвітність медичного страхування). Ці вимоги часто прямо передбачають використання надійних методів аутентифікації, включаючи багатофакторну, як обов'язкову умову для уникнення значних штрафів та збереження репутації.

Всі ці фактори, взяті разом, рішуче вказують на те, що використання лише паролів є недостатнім і надзвичайно ризикованим. Вони підкреслюють критичну необхідність впровадження двофакторної аутентифікації (2FA) як базового рівня захисту. 2FA здатна не лише забезпечити значно надійніший захист облікових записів, а й надати адаптивність, необхідну для функціонування в складному та мінливому корпоративному середовищі.

1.4 Роль двофакторної аутентифікації

У відповідь на зростаючу кількість загроз і недоліки традиційних методів, двофакторна аутентифікація (2FA) виникла як стандарт де-факто для посилення безпеки облікових записів. Її основна перевага полягає в тому, що вона значно ускладнює компрометацію облікового запису, оскільки для успішного входу зловмисникам необхідно отримати доступ до двох різних, незалежних факторів аутентифікації. Цей підхід ґрунтується на комбінації щонайменше двох факторів із трьох основних категорій:

Фактор знання (те, що користувач знає): Це класичний елемент аутентифікації. Він включає інформацію, яка є конфіденційною і відома лише авторизованому користувачу.

Найпоширенішими прикладами є:

- Пароль: комбінація символів, яку користувач вводить для доступу.

-PIN-код: короткий числовий код, часто використовуваний для мобільних пристроїв або банківських карток.

Відповідь на секретне питання: заздалегідь визначена відповідь на особисте питання.

- Фактор володіння (те, що користувач має): Цей фактор ґрунтується на фізичному предметі або пристрої, який належить користувачеві. Це додає суттєвий рівень безпеки, оскільки зловмисник, навіть знаючи пароль, не зможе увійти без фізичного доступу до цього предмета.

Приклади включають:

- Смартфон: найбільш поширений варіант, який використовується для отримання SMS-кодів, push-повідомлень або генерації одноразових паролів (TOTP) через спеціальні застосунки-автентифікатори (наприклад, Google Authenticator, Microsoft Authenticator).

- Апаратний токен: спеціальний фізичний пристрій (наприклад, USB-ключ FIDO U2F, брелок), який генерує одноразові коди або використовується для криптографічного підтвердження.

- Смарт-карта: картка з вбудованим чіпом, що містить облікові дані, яка вимагає зчитувача.

- SIM-картка: використовується для надсилання SMS-повідомлень з кодами.

- Фактор приналежності/ідентичності (те, ким є користувач): Цей фактор базується на унікальних біологічних характеристиках користувача, які практично неможливо імітувати або викрасти.

- Відбиток пальця: сканування унікального візерунка пальця.

Сканування обличчя: розпізнавання унікальних рис обличчя (наприклад, Face ID).

- Сканування райдужної оболонки ока: високоточне біометричне розпізнавання.

- Голос: аналіз унікальних голосових характеристик.

Ключова перевага 2FA полягає в її здатності істотно ускладнити завдання зловмисникам. Наприклад, навіть якщо зловмисник зумів викрасти пароль користувача через фішинг, він не зможе увійти до системи, оскільки йому буде потрібен другий фактор аутентифікації. Якщо цим другим фактором є, наприклад, push-повідомлення на смартфон користувача або одноразовий код, згенерований на цьому смартфоні, зловмисник, що знаходиться десь далеко, не матиме доступу до цього пристрою. Таким чином, компрометація одного фактора (наприклад, пароля) не призводить до негайної компрометації всього облікового запису.

Впровадження 2FA для корпоративних інформаційних систем не є просто додатковою функцією, а необхідною умовою для побудови надійної архітектури безпеки. Це дозволяє компаніям ефективно протистояти більшості сучасних

кіберзагроз, знизити ризики витоку даних та забезпечити відповідність регуляторним вимогам.

2 АНАЛІЗ НАЯВНИХ МЕТОДІВ ДВОФАКТОРНОЇ АУТЕНТИФІКАЦІЇ

2.1 Класифікація методів 2FA

Система двофакторної аутентифікації (2FA) базується на використанні двох незалежних чинників підтвердження особи, що дозволяє значно зменшити ризик несанкціонованого доступу до систем. Усі наявні методи 2FA можна класифікувати за типом другого фактора, який доповнює основний пароль користувача.

Найпоширенішими видами є:

- Фізичні токени. Це окремі апаратні пристрої, зокрема токени або USB-ключі, які генерують одноразові паролі або використовуються для підпису транзакцій. Вони не залежать від операційної системи та можуть забезпечити високий рівень безпеки.

- Мобільні додатки. Програми на смартфоні, які генерують одноразові коди або використовують push-нотифікації для підтвердження входу. Найпоширенішими прикладами є Google Authenticator, Microsoft Authenticator та Duo Mobile.

- SMS-коди. Одноразові коди, які надсилаються на мобільний номер телефону користувача. Цей метод має широку доступність, але поступово втрачає популярність через низьку стійкість до атак.

- Біометричні методи. Способи, які базуються на фізичних або поведінкових характеристиках користувача: сканування відбитків пальців, розпізнавання обличчя, сітківки ока, голосу тощо.

- Електронна пошта. Один з найбільш простих методів, коли код підтвердження надсилається на електронну скриньку користувача.

- Смарт-карти. Пластикові картки з вбудованим мікрочипом, які вставляються у спеціальний зчитувач. Часто використовуються в урядових або корпоративних системах.

2.2 Переваги та недоліки методів 2FA

Фізичні токени забезпечують високий рівень безпеки завдяки тому, що працюють автономно та не залежать від мережевих підключень. Вони унеможливлюють віддалене перехоплення коду. Водночас недоліком є висока вартість впровадження та обслуговування, а також незручність для користувачів, які змушені постійно носити окремий пристрій.

Мобільні додатки:

Ці засоби є одними з найзручніших для сучасного користувача, адже не потребують додаткового обладнання — лише смартфона. Завдяки push-нотифікаціям процес підтвердження входу здійснюється швидко й інтуїтивно. Однак існують ризики, пов'язані з безпекою самого мобільного пристрою, особливо якщо він не захищений або заражений шкідливим ПЗ. Також зловмисники можуть скористатися методами на кшталт SIM-swapping.

SMS-коди:

Найпростішим і найдоступнішим методом є надсилання кодів через SMS. Перевагою є його доступність майже для кожного користувача мобільного зв’язку. Разом із тим, саме цей метод є найбільш вразливим до атак, включно з перехопленням повідомлень, атаками на телекомунікаційні мережі та підміну SIM-карт.

Біометричні методи:

Методи, що ґрунтуються на унікальних особливостях користувача, дозволяють досягти високого рівня безпеки та зручності. Їх важко підробити або передати іншій особі. Проте реалізація таких рішень вимагає спеціального обладнання та супроводжується складнощами щодо конфіденційності та захисту біометричних даних.

Електронна пошта:

Цей варіант 2FA є простим для реалізації і не потребує додаткового програмного чи апаратного забезпечення. Він широко використовується в онлайн-сервісах.

Проблемою є можливість компрометації поштової скриньки та нестабільність доставки кодів через затримки в мережі.

Смарт-карти:

Смарт-карти часто використовуються у державних установах або компаніях із суворими вимогами до безпеки. Вони надають високий рівень захисту та можуть служити багатофункціональним засобом ідентифікації. Водночас їхнє використання вимагає спеціального зчитувача, а також має певні ризики, пов’язані з втратою або крадіжкою картки.

Таблиця 2.1 Порівняльний аналіз методів

Метод	Безпека	Зручність	Вартість	Стійкість до атак
Фізичні токени	Висока	Низька	Висока	Висока
Мобільні додатки	Середня	Висока	Низька	Середня
SMS-коди	Низька	Висока	Низька	Низька
Біометричні методи	Висока	Висока	Висока	Середня
Електронна пошта	Низька	Середня	Низька	Низька
Смарт-карти	Висока	Середня	Висока	Висока

2.3 Тенденції розвитку 2FA

Ринок засобів двофакторної аутентифікації постійно розвивається, орієнтуючись на поєднання високої безпеки та зручності користувача.

Серед основних тенденцій слід відзначити:

- Поширення стандартів FIDO2 та WebAuthn. Це відкриті стандарти, що дозволяють реалізовувати безпарольну аутентифікацію на основі криптографічних ключів, які зберігаються на локальному пристрої користувача.

- Адаптивна аутентифікація. Ця технологія дозволяє системі оцінювати ризики входу на основі контексту — IP-адреси, геолокації, часу доби, пристрою тощо — і вирішувати, чи потрібно застосовувати додатковий фактор перевірки.

- Глибша інтеграція з хмарними сервісами. Провідні провайдери (Microsoft, Google, Amazon) вбудовують підтримку 2FA як обов’язкову складову авторизації для корпоративних акаунтів.

- Використання апаратних ключів нового покоління. Сучасні рішення підтримують декілька протоколів одночасно (USB, Bluetooth, NFC), що дозволяє використовувати один ключ для доступу до різних платформ.

Таким чином, розвиток технологій аутентифікації відображає загальну тенденцію до зниження залежності від паролів і підвищення ролі багатофакторної, контекстно-чутливої безпеки.

3 РОЗРОБЛЕННЯ РЕКОМЕНДАЦІЙ ЩОДО ЗАХИСТУ ОБЛІКОВИХ ЗАПИСІВ КОРИСТУВАЧІВ У КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ З ВИКОРИСТАННЯМ ДВОФАКТОРНОЇ АУТЕНТИФІКАЦІЇ

У сучасних умовах, коли кіберзагрози набувають все більшої витонченості та масштабу, забезпечення надійного захисту облікових записів користувачів стає критично важливим аспектом кібербезпеки будь-якої корпоративної інформаційної системи (КІС).

Традиційні методи аутентифікації, що базуються виключно на паролях, вже не є достатніми для протидії більшості сучасних кібератак. Цей розділ присвячений розробленню детальних, науково обґрунтованих рекомендацій щодо ефективного впровадження двофакторної аутентифікації (2FA), з особливим акцентом на комплексному рішенні, що поєднує можливості Cisco Identity Services Engine (ISE) та Cisco Duo.

3.1 Фундаментальні принципи ефективного впровадження двофакторної аутентифікації

Успішне розгортання 2FA в КІС вимагає не лише глибоких технічних знань, а й стратегічного підходу, що враховує організаційні, людські та економічні фактори. Дотримання викладених нижче принципів є наріжним каменем для побудови стійкої, масштабованої та зручної у використанні системи безпеки:

Оптимальний баланс між посиленою безпекою та бездоганною зручністю використання: Це, мабуть, один із найбільш критичних аспектів. Надмірно складні, обтяжливі або неінтуїтивні методи 2FA можуть не лише викликати суттєвий опір з боку кінцевих користувачів, а й, що значно гірше, спровокувати пошук "обхідних шляхів" або навіть призвести до прихованого саботажу ініціативи з безпеки.

Мета полягає в тому, щоб зробити процес аутентифікації максимально надійним, але водночас швидким, інтуїтивно зрозумілим і, по можливості, непомітним. Наприклад, сучасні push-повідомлення через мобільні додатки чудово ілюструють цей баланс, пропонуючи миттєве підтвердження одним дотиком при збереженні високого рівня безпеки. Ретельний вибір методів, що мінімізують "тертя" для користувачів, є запорукою високого рівня прийняття та неухильного дотримання всіх встановлених політик безпеки.

Адаптація рішення до унікального корпоративного середовища та бізнес-процесів: Універсального рішення "один розмір для всіх" у сфері кібербезпеки не існує. Вибір конкретних методів 2FA, а також загальної архітектури впровадження, повинен бути глибоко занурений у специфічні характеристики та реалії конкретної організації.

Це включає цілий спектр факторів:

- Масштаб та складна структура компанії: Для малих та середніх підприємств можуть бути цілком достатні простіші, більш прямолінійні рішення, тоді як великим корпораціям з тисячами співробітників необхідні масштабовані, централізовано керовані системи з розширеними функціональними можливостями.

- Наявний бюджет та ресурсні обмеження: Деякі передові методи, такі як масове придбання апаратних токенів або впровадження корпоративних біометричних систем, можуть вимагати значних капіталовкладень. Важливо знайти рішення, що відповідає фінансовим можливостям.

- Поточна технічна інфраструктура та її зрілість: Критично важливо забезпечити сумісність з існуючими застарілими системами (legacy systems) та безшовну інтеграцію з усіма мережевими пристроями (VPN-шлюзи, Wi-Fi-контролери, мережеве обладнання).

- Специфіка бізнес-процесів та робочих місць: Наприклад, для працівників виробничих цехів, які не мають доступу до смартфонів, або для персоналу, що працює в умовах відсутності інтернет-з'єднання, може знадобитися застосування альтернативних, офлайн-орієнтованих підходів.

Глибока та безшовна інтеграція з існуючими системами управління ідентифікацією та доступом (IAM): 2FA не повинна розглядатися як ізольований, відокремлений компонент, а як невід'ємна, органічна частина загальної стратегії управління ідентифікацією та доступом в організації. Це передбачає гармонійну інтеграцію з такими ключовими елементами, як Active Directory, Okta, Azure AD та інші служби каталогів.

Безшовна інтеграція забезпечує централізоване управління, спрощує адміністрування, усуває фрагментацію безпеки та забезпечує послідовну, зрозумілу політику доступу до всіх корпоративних ресурсів.

Комплексне навчання користувачів та налагоджена постійна підтримка: Навіть найбільш інтуїтивно зрозуміла та зручна технологія потребує належного навчання. Важливо не просто надати інструмент, а навчити ним користуватися та розуміти його цінність. Це включає систематичні тренінги, що пояснюють сутність 2FA, її критичну важливість для безпеки компанії та особистої безпеки користувача, демонстрацію правильного використання та, що не менш важливо, методи розпізнавання спроб фішингу та соціальної інженерії. Надання чітких інструкцій, створення посібників та оперативної підтримки допомагає подолати потенційні труднощі та формує міцну культуру кібергігієни в організації.

3.2 Аналіз Cisco Identity Services Engine (ISE) як корпоративної системи управління доступом

Cisco Identity Services Engine (ISE) є передовою, універсальною платформою для управління доступом і забезпечення безпеки в корпоративних інформаційних системах. Вона надає організаціям можливість централізовано контролювати ідентифікацію, аутентифікацію та авторизацію (AAA) користувачів і пристроїв, які підключаються до мережі, незалежно від способу підключення (дротовий, бездротовий, VPN). ISE відіграє ключову роль у реалізації сучасних стратегій безпеки, зокрема архітектури "нульової довіри" (Zero Trust), інтегруючись з різними елементами інфраструктури та, зокрема, з Cisco Duo для реалізації

посиленої двофакторної аутентифікації, забезпечуючи тим самим комплексний і багаторівневий захист облікових записів.

Cisco ISE пропонує широкий спектр передових функціональних можливостей, спрямованих на посилення контролю доступу та загальної безпеки мережі:

- Централізоване управління політиками доступу: ISE дозволяє створювати та застосовувати надзвичайно гнучкі та динамічні правила доступу, що базуються на глибокій ідентифікації користувача (його ролі, групі належності), типу пристрою (ноутбук, смартфон, IoT-пристрій), його стані безпеки (наявність актуального антивірусу, шифрування диска, встановлені оновлення ОС) та контексті підключення (геолокація, час доби, метод підключення). Це дозволяє забезпечити доступ лише тим користувачам і пристроям, які відповідають встановленим політикам безпеки.

- Розширена аутентифікація, авторизація та облік (AAA): Платформа підтримує широкий спектр стандартних та промислових протоколів, таких як RADIUS (Remote Authentication Dial-In User Service) для мережевого доступу, TACACS+ (Terminal Access Controller Access-Control System Plus) для адміністративного доступу до мережевих пристроїв, а також SAML (Security Assertion Markup Language) для інтеграції з хмарними додатками та системами єдиного входу (SSO). Це забезпечує високу сумісність з більшістю мережевих пристроїв, серверів та додатків.

- Детальне профілювання та ідентифікація пристроїв: ISE автоматично виявляє, класифікує та профілює всі пристрої, що підключаються до мережі. Це включає ідентифікацію типу пристрою (наприклад, корпоративний ноутбук, особистий смартфон, IP-камера, принтер, пристрої Інтернету речей IoT), операційної системи та інших характеристик. Ця можливість дозволяє застосовувати гранульовані та контекстно-залежні політики доступу для різних категорій пристроїв.

- Безперервний моніторинг і детальний аудит безпеки: Система здійснює постійне та детальне журналювання всіх подій аутентифікації, авторизації, обліку

та змін політик. Це надає вичерпні дані для оперативного аналізу безпеки, виявлення аномалій, підозрілої активності, розслідування інцидентів та забезпечення відповідності внутрішнім та зовнішнім регуляторним вимогам.

- Потужна інтеграція з 2FA-рішеннями: Однією з найважливіших функцій є можливість глибокої інтеграції з передовими системами двофакторної аутентифікації, такими як Cisco Duo, що забезпечує додатковий, критично важливий рівень захисту облікових записів.

Інтеграція Cisco ISE з Cisco Duo є потужним поєднанням, що дозволяє реалізувати надійну, багаторівневу двофакторну аутентифікацію для доступу до різноманітних корпоративних ресурсів, включаючи VPN-мережі, бездротові мережі, хмарні сервіси та локальні додатки.

Цей процес інтеграції включає кілька ключових етапів:

- Налаштування Duo Authentication Proxy: Цей компонент є критично важливим. Duo Authentication Proxy – це локальний програмний компонент, який встановлюється у корпоративній мережі. Він виступає в ролі посередника, забезпечуючи безпечний зв'язок між Cisco ISE (що працює в локальній мережі) та хмарним сервісом Duo. Проксі виконує роль RADIUS-сервера для ISE, отримуючи запити на аутентифікацію, та одночасно взаємодіє з Duo Cloud Service через захищений канал TLS 1.3 для перевірки другого фактора.

- Конфігурація RADIUS у Cisco ISE: Необхідно налаштувати Cisco ISE для використання Duo Authentication Proxy як зовнішнього сервера аутентифікації за протоколом RADIUS. Це дозволяє ISE перенаправляти запити на перевірку другого фактора до Duo через проксі. Зазвичай, ISE надсилає запит до Duo Authentication Proxy на стандартний RADIUS-порт (наприклад, 1812 або 1645).

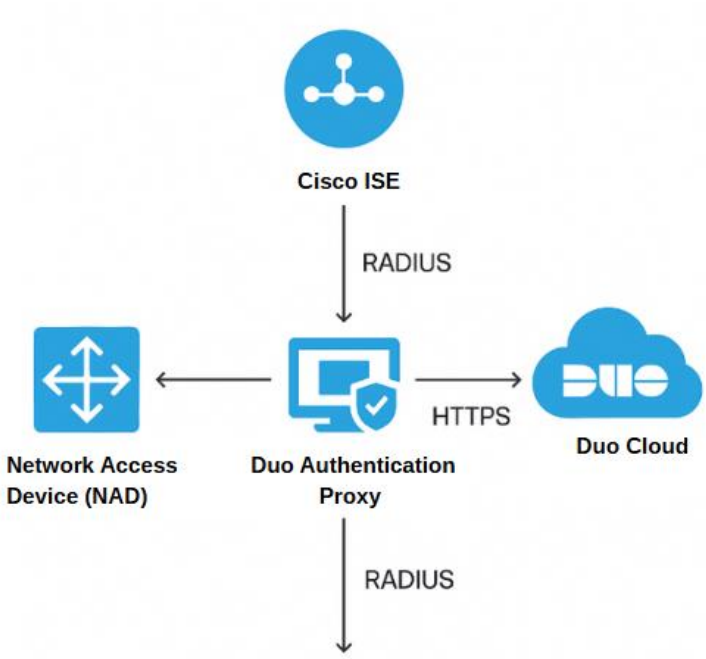
- Створення та застосування політик аутентифікації в ISE: В ISE створюються деталізовані політики, що визначають, коли та для яких користувачів, груп (наприклад, адміністратори, звичайні користувачі), ролей або типів пристроїв (наприклад, корпоративні ноутбуки, особисті смартфони) вимагається проходження двофакторної аутентифікації через Duo. Ці політики можуть бути

дуже гранульованими, дозволяючи адаптувати вимоги 2FA до конкретного контексту доступу.

- Ретельне тестування інтеграції та сценаріїв доступу: Після завершення всіх налаштувань критично важливо провести комплексне тестування, щоб переконатися, що 2FA працює коректно для всіх передбачених сценаріїв доступу через ISE та Duo. Це включає тестування успішних входів, невдалих спроб, а також перевірку реакції системи на різні умови (наприклад, вхід з невідомого пристрою)

.

Рисунок 3.1 - Схема налаштування RADIUS-інтеграції між Cisco ISE та Duo Authentication Proxy



Надана схема чітко ілюструє потік даних та взаємодію між компонентами: Cisco ISE надсилає RADIUS-запит (зазвичай на порт 1812) до Duo Authentication Proxy. Проксі, своєю чергою, встановлює безпечне з'єднання з Duo Cloud Service, використовуючи протокол TLS 1.3 та унікальні API-ключі. Duo Cloud обробляє запит, ініціює перевірку другого фактора (наприклад, надсилає push-повідомлення на мобільний пристрій користувача), і після отримання підтвердження від

користувача, повертає відповідь (успіх/невдача) до Duo Authentication Proxy, а той – до Cisco ISE. Саме ця відповідь визначає, чи буде надано доступ користувачеві.

Розглянемо типовий, деталізований процес аутентифікації користувача, який проходить через інтегровану систему Cisco ISE та Cisco Duo:

- Ініціація запиту на доступ: Користувач намагається отримати доступ до захищеного корпоративного ресурсу. Це може бути підключення до корпоративного VPN-клієнта, авторизація у бездротовій Wi-Fi мережі, спроба входу до внутрішнього веб-додатку або хмарного сервісу. Користувач вводить свої первинні облікові дані – логін і пароль.

- Первинна аутентифікація та делегування ISE: Cisco ISE перехоплює запит на аутентифікацію. Вона спочатку перевіряє первинний фактор (логін і пароль), як правило, делегуючи цю перевірку до основної корпоративної служби каталогів, такої як Active Directory або LDAP.

- Запит на другий фактор до Duo: Після успішної перевірки первинних облікових даних, згідно з налаштованими в ISE політиками, Cisco ISE визначає, що для даного користувача/ресурсу/контексту необхідна двофакторна аутентифікація. ISE надсилає запит на перевірку другого фактора до Duo Authentication Proxy за протоколом RADIUS.

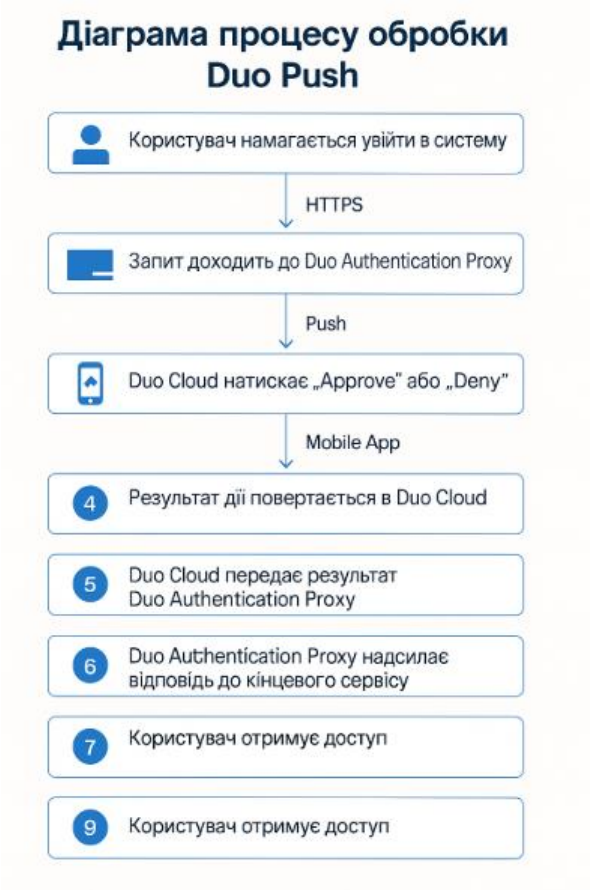
- Взаємодія Duo Proxy та Duo Cloud: Duo Authentication Proxy отримує RADIUS-запит від ISE та перенаправляє його до хмарного сервісу Duo (Duo Cloud Service) через захищене TLS-з'єднання.

- Ініціація 2FA та підтвердження користувачем: Duo Cloud обробляє запит і, залежно від налаштованого методу, ініціює процес другого фактора. Найчастіше це надсилання push-повідомлення на мобільний пристрій користувача, де встановлений додаток Duo Mobile. Користувач отримує сповіщення на своєму смартфоні і підтверджує вхід, натискаючи кнопку "Approve". Альтернативно, користувач може ввести згенерований в Duo Mobile одноразовий пароль (TOTP).

- Повернення результату до ISE та авторизація: Після успішного підтвердження другого фактора користувачем, Duo Cloud повертає результат успішної верифікації до Duo Authentication Proxy, який, своєю чергою, передає його

назад до Cisco ISE. Cisco ISE, отримавши підтвердження обох факторів, аналізує додаткові контекстні дані (такі як тип пристрою, його стан безпеки, геолокація користувача, час доби). На основі всіх цих даних та відповідності налаштованим політикам доступу, ISE приймає рішення: надає або відмовляє в доступі до запитуваного ресурсу, а також застосовує відповідні політики доступу (наприклад, розміщення в певному сегменті мережі).

Рисунок 3.2 - Діаграма процесу обробки push-повідомлення в Cisco Duo



Представлена діаграма детально показує життєвий цикл запиту на аутентифікацію з використанням Duo Push: від початкового запиту на вхід, його передачі до Duo Cloud, надсилання push-сповіщення до додатка Duo Mobile на пристрої користувача, підтвердження дії користувачем, і, нарешті, повернення результату успішної аутентифікації назад до Cisco ISE.

Поєднання функціональних можливостей Cisco ISE та Cisco Duo надає низку значних переваг для безпеки, управління доступом та операційної ефективності організації:

- Надзвичайно централізоване управління політиками доступу: Cisco ISE виступає як єдина, уніфікована платформа для створення, застосування та контролю гранульованих політик доступу до всіх корпоративних ресурсів. Це значно спрощує адміністрування безпеки, зменшує ймовірність помилок конфігурації та забезпечує послідовність застосування правил доступу.

- Потужна адаптивна безпека та контекстно-залежний доступ: Інтеграція передових функцій Risk-Based Authentication (RBA) від Cisco Duo (які аналізують поведінку користувача, географічне розташування, тип пристрою тощо) з можливостями профілювання пристроїв та оцінки стану безпеки в ISE дозволяє системі динамічно оцінювати ризики кожної спроби доступу.

У разі виявлення підозрілої активності або відхилення від норми, система може автоматично вимагати додаткову верифікацію або навіть тимчасово блокувати доступ, забезпечуючи багаторівневий захист.

- Широка сумісність та гнучкість розгортання: Інтегроване рішення підтримує безшовну інтеграцію як з локальними (on-premises) системами, так і з різноманітними хмарними сервісами та додатками. Це забезпечує універсальний захист незалежно від архітектури IT-інфраструктури організації.

- Забезпечення відповідності міжнародним стандартам та регуляторним вимогам: Впровадження надійного двофакторного контролю доступу через ISE та Duo є критично важливим для відповідності вимогам багатьох міжнародних стандартів безпеки (таких як ISO 27001, NIST Cybersecurity Framework) та регуляторних актів (як-от GDPR для захисту персональних даних, PCI DSS для обробки платіжних даних, HIPAA для медичної інформації). Це не лише допомагає уникнути штрафів, а й підвищує довіру партнерів та клієнтів.

Незважаючи на значні переваги, варто усвідомлювати та враховувати деякі потенційні обмеження, які можуть виникнути при впровадженні цієї потужної інтеграції:

- Складність початкового налаштування та подальшого адміністрування ISE: Впровадження та підтримка Cisco ISE вимагає значних знань і досвіду в адмініструванні складних мережевих інфраструктур, систем безпеки та протоколів

аутентифікації. Це може вимагати інвестицій у навчання персоналу або залучення зовнішніх експертів.

- Потенційно висока вартість ліцензій та обладнання: Ліцензії на Cisco ISE та Cisco Duo можуть бути досить дорогими, особливо для малих та середніх організацій. Крім того, може знадобитися оновлення або придбання нового мережевого обладнання Cisco для повної реалізації всіх функцій ISE. Це вимагає ретельного планування бюджету та аналізу ROI.

- Залежність від якості мережевої інфраструктури: Ефективність та стабільність роботи всієї системи значною мірою залежить від надійності та якості базової мережевої інфраструктури. Будь-які збої або проблеми з продуктивністю мережі можуть безпосередньо вплинути на процес аутентифікації та доступність ресурсів.

Для повноти картини та обґрунтованості вибору Cisco ISE, доцільно провести порівняльний аналіз з іншими провідними системами управління ідентифікацією та доступом (IAM), що використовуються на ринку(Таблиця 3.1 – Порівняльний аналіз Cisco ISE з іншими системами AM):

Таблиця 3.1 – Порівняльний аналіз Cisco ISE з іншими системами AM

Система	Інтеграція з 2FA	Адаптивність (Risk-Based Auth)	Профілювання пристроїв	Вартість (Оцінка)
Cisco ISE	Висока (глибока інтеграція з Duo, Okta)	Висока (через Duo RBA)	Висока	Висока
Okta Identity Cloud	Висока (власний Okta Verify,	Висока	Середня	Висока

	FIDO2, TOTP)			
Microsoft Azure AD	Висока (Microsoft Authenticator, FIDO2)	Висока	Низька	Середня

Висновок з порівняння: Як видно з таблиці, Cisco ISE вирізняється серед конкурентів завдяки своїй винятковій можливості глибокого профілювання пристроїв та їхнього стану безпеки, що дозволяє застосовувати надзвичайно гранульовані політики доступу. Крім того, її гнучкість інтеграції з передовими 2FA-рішеннями, особливо з Cisco Duo, робить її потужним інструментом для побудови адаптивної та контекстно-залежної системи безпеки, що може бути критично важливою для великих та складних корпоративних мереж. Хоча вартість може бути вищою, комплексність та функціональність, які надає ISE, часто виправдовують ці інвестиції.

3.3 Рекомендовані методи верифікації в інтегрованій системі Cisco ISE та Duo

На основі детального аналізу функціоналу Cisco ISE та Cisco Duo, а також з урахуванням фундаментальних принципів балансу безпеки та зручності, пропонується наступний пріоритетний підхід до вибору та застосування методів двофакторної аутентифікації:

Основний та найбільш рекомендований метод: Duo Push через Duo Mobile.

Обґрунтування: Цей метод є лідером за швидкістю, зручністю та високим рівнем безпеки. Push-повідомлення дозволяють користувачеві підтвердити вхід одним дотиком на своєму мобільному пристрої, що значно спрощує та прискорює процес аутентифікації. Крім того, Duo Push забезпечує ефективний захист від таких атак, як "Man-in-the-Middle" (MITM), оскільки верифікація відбувається без обміну чутливими обліковими даними через потенційно скомпрометовані канали.

Впровадження Verified Duo Push додатково посилює захист: він вимагає від користувача введення унікального числового коду, що з'являється на екрані входу, безпосередньо у додаток Duo Mobile, тим самим мінімізуючи ризики "MFA fatigue" (коли користувачі несвідомо підтверджують безліч запитів, що можуть бути шкідливими).

Надійний резервний метод: TOTP (Time-based One-Time Password) через Duo Mobile або апаратні токени (наприклад, YubiKey).

Обґрунтування: TOTP є чудовим резервним варіантом, який функціонує автономно, без необхідності активного підключення до мережі інтернет у момент генерації коду. Це робить його ідеальним для користувачів, які працюють офлайн, або в середовищах з нестабільним/відсутнім інтернет-з'єднанням. Використання апаратних токенів, таких як YubiKey, значно підвищує безпеку, оскільки вони є фізичними пристроями, які надзвичайно складно скомпрометувати дистанційно, на відміну від програмних рішень. Вони ідеально підходять для критичних сценаріїв доступу або для захисту облікових записів з підвищеними привілеями, де потрібен максимальний рівень захисту.

Додатковий метод для високочутливих систем та безпарольного доступу: Біометрична аутентифікація.

Обґрунтування: Якщо корпоративний бюджет та технічна інфраструктура дозволяють, інтеграція біометричних даних (наприклад, відбиток пальця, розпізнавання обличчя) через відкриті стандарти WebAuthn/FIDO2 забезпечує найвищий рівень безпеки та неперевершену зручність для користувачів. Біометричні дані є унікальними для кожної людини, а процес аутентифікації відбувається майже миттєво та без зусиль. Важливо зазначити, що завдяки архітектурі WebAuthn/FIDO2, біометричні дані користувача ніколи не передаються на сервер і не зберігаються централізовано. Вони використовуються лише локально, на пристрої користувача, для підтвердження володіння криптографічним ключем, що забезпечує максимальну конфіденційність та захист від витоків біометричних даних.

Категорично не рекомендовані як основні методи для корпоративного середовища: SMS-коди та телефонні дзвінки.

Обґрунтування: Хоча ці методи були досить поширеними раніше, вони є надзвичайно вразливими до низки сучасних кібератак, зокрема SIM-swapping (коли зловмисник перехоплює контроль над номером телефону жертви) та різноманітних фішингових атак. Тому їх використання в корпоративному середовищі як основних або регулярних резервних методів є вкрай небажаним і може наражати організацію на значні ризики компрометації. Їх можна розглядати лише як екстрений, аварійний, тимчасовий варіант з жорсткими політиками та постійним моніторингом.

Для кращого розуміння переваг та недоліків кожного рекомендованого методу 2FA в контексті Duo, наведемо їх порівняльний аналіз(Таблиця 3.2 – Порівняльний аналіз переваг та недоліків кожного рекомендованого методу 2FA в контексті Duo):

Таблиця 3.2 – Порівняльний аналіз переваг та недоліків кожного рекомендованого методу 2FA в контексті Duo

Метод	Безпека	Зручність	Залежність від мережі	Потенційні ризики
Duo Push	Висока	Висока	Так	Компрометація мобільного пристрою
TOTP	Висока	Середня	Ні	Помилка введення коду
Біометрія	Дуже висока	Дуже висока	Ні (локально)	Конфіденційність біометричних даних (у разі неправильної реалізації)
SMS	Низька	Висока	Так	SIM-swapping, перехоплення SMS

3.4 Практичні кроки ефективного впровадження Cisco Duo та Cisco ISE

Успішне та безболісне впровадження двофакторної аутентифікації за допомогою інтегрованого рішення Cisco Duo та Cisco ISE вимагає чіткої послідовності дій та системного підходу:

Комплексний аудит системи та детальне планування:

- Ідентифікація та категоризація всіх точок доступу: Провести повну інвентаризацію всіх корпоративних ресурсів, які потребуватимуть захисту за допомогою 2FA. Це включає VPN-шлюзи, бездротові мережі (Wi-Fi), внутрішні веб-додатки (наприклад, CRM, ERP), хмарні сервіси (Microsoft 365, Salesforce), сервери, мережеве обладнання. Кожну точку слід оцінити за рівнем її критичності та чутливості інформації, що до неї надається.

- Оцінка поточної IAM-інфраструктури: Проаналізувати існуючі системи управління ідентифікацією та доступом (IAM), визначити, які з них потребують інтеграції з Cisco ISE та Duo, та оцінити їхню готовність до такого впровадження.

Базова конфігурація Cisco ISE:

- Встановити та налаштувати екземпляри Cisco ISE: Розгорнути необхідну кількість вузлів ISE відповідно до архітектури (розподілена або компактна) та вимог до масштабованості й відмовостійкості.

- Підключити ISE до Active Directory або іншої корпоративної служби каталогів: Налаштувати інтеграцію для забезпечення первинної аутентифікації користувачів.

- Налаштувати профілювання пристроїв та базові політики доступу: Визначити правила для автоматичної ідентифікації пристроїв, що підключаються до мережі, та надання початкового рівня доступу на основі їхнього типу та стану.

- Створити деталізовані політики аутентифікації: Визначити умови, за яких вимагатиметься двофакторна аутентифікація, та методи 2FA, які будуть застосовані для різних груп користувачів, ролей або типів доступу.(Таблиця 3.1 - Параметри політики аутентифікації в Cisco ISE)

Таблиця 3.1 - Параметри політики аутентифікації в Cisco ISE

№	Параметр	Значення / Опис

1	Назва політики	Default Network Access
2	Тип доступу	Wired / Wireless
3	Джерело ідентифікації	Internal Users / Active Directory
4	Метод аутентифікації	PEAP (EAP-MSCHAPv2) / EAP-TLS
5	Умови запуску політики	IF Device Type = "Corporate" AND Location = "HQ"
6	Дії при успішній аутентифікації	Permit Access / Apply Authorization Profile
7	Дії при невдалій аутентифікації	Reject Access / Redirect to Web Portal
8	Використання зовнішнього сервера	Duo Authentication Proxy (через RADIUS)
9	Додаткові параметри	Enable Logging, Track Failed Attempts

Надана таблиця є прикладом структури політики аутентифікації в Cisco ISE. Вона включає такі ключові параметри, як Назва політики (наприклад, "VPN Access Policy"), Умова (група користувачів, які підпадають під цю політику, наприклад, "HR Department"), Метод аутентифікації (наприклад, "RADIUS-Duo", що вказує на використання Duo як другого фактора) та Дії (дозволити/відхилити доступ).

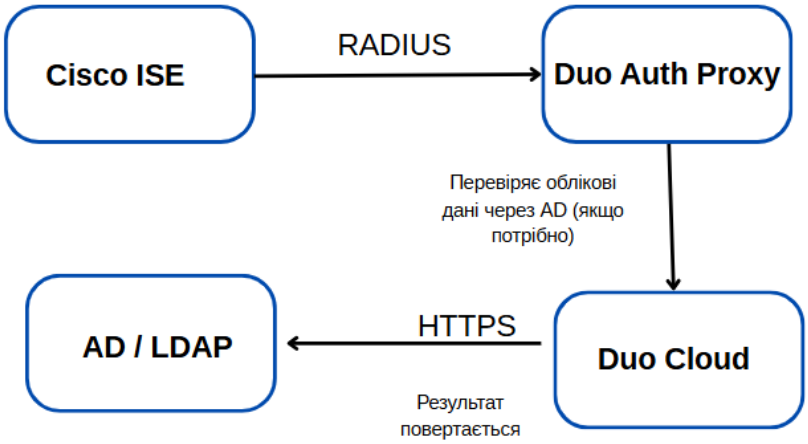
Безшовна інтеграція з Cisco Duo:

- Встановити та налаштувати Duo Authentication Proxy: Розгорнути один або кілька екземплярів Duo Authentication Proxy у корпоративній мережі та налаштувати їх для зв'язку з хмарним сервісом Duo.

- Налаштувати RADIUS-сервери в ISE для зв'язку з Duo: Створити зовнішні RADIUS-сервери в Cisco ISE, що вказують на IP-адреси та порти Duo Authentication Proxy.

- Активувати розширені функції Duo: Ввімкнути такі критично важливі функції, як Verified Duo Push для додаткового захисту від "MFA fatigue" та Risk-Based Authentication для адаптивного аналізу ризиків на основі контексту.

Рисунок 3.3 - Схема конфігурації Duo Authentication Proxy



Наведена схема ілюструє ключові компоненти конфігурації Duo Authentication Proxy: взаємодія між Cisco ISE та Duo Proxy, а потім між Duo Proxy та Duo Cloud, із зазначенням використаних ключів API (ikey, skey), портів (наприклад, 1812) та протоколів (TLS 1.3).

Нижче наведено типовий приклад конфігурації файлу authproxy.cfg для Duo Authentication Proxy, що ілюструє налаштування для зв'язку з Cisco ISE через RADIUS(Рисунок 3.4 Налаштування Cisco ISE через RADIUS):

Рисунок 3.4 Налаштування Cisco ISE через RADIUS

Ini, TOML

```
[radius_server_auto]
ikey=DIXXXXXXXXXXXXXXXXX # Інтеграційний ключ Duo для програми
skey=XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX # Секретний
ключ Duo для програми
api_host=api-xxxxxxxx.duosecurity.com # Хост API Duo Cloud
radius_ip_1=192.168.1.100 # IP-адреса Cisco ISE (або іншого RADIUS-
клієнта)
radius_secret_1=secretkey123 # Загальний секретний ключ між ISE та Duo
Proxy
port=1812 # Порт, на якому Duo Proxy прослуховує RADIUS-запити від ISE
failmode=safe # Режим відмовостійкості: "safe" дозволяє вхід без 2FA, якщо
Duo недоступний (потребує уваги)
client=ad_client # Вказує на секцію клієнта для AD-аутентифікації
```

Пояснення: Цей приклад ілюструє базові параметри, необхідні для налаштування Duo Authentication Proxy як RADIUS-сервера для Cisco ISE. Він включає унікальні ідентифікатори Duo (ikey, skey, api_host) для зв'язку з Duo Cloud, а також параметри для взаємодії з Cisco ISE (IP-адреса ISE, спільний секрет, порт прослуховування). Параметр failmode є важливим для стратегії відмовостійкості, але потребує ретельного обмірковування.

Контрольоване пілотне тестування:

- Впровадити 2FA для невеликої, але репрезентативної групи користувачів: Зазвичай це IT-відділ, відділ безпеки або група добровольців.

- Зібрати детальний зворотний зв'язок: Активно взаємодіяти з учасниками пілотного проєкту, щоб оцінити зручність використання, виявити технічні проблеми, помилки в документації або процесах. Використати цей фідбек для внесення необхідних коригувань перед повномасштабним розгортанням.

Поетапне масштабування на всю організацію:

- Розробити та реалізувати план поетапного розгортання 2FA для всіх користувачів: Це може включати розгортання за відділами, за рівнями критичності доступу або за географічним розташуванням.

- Забезпечити централізовану та доступну підтримку через IT-відділ: Надати користувачам чіткі інструкції, посібники та визначені канали для звернення за допомогою у разі виникнення проблем (наприклад, втрата пристрою 2FA, проблеми з активацією).

Постійний моніторинг, аналіз та підтримка:

- Налаштувати детальне журналювання подій: Забезпечити збір та агрегацію всіх журналів аутентифікації та авторизації як у Cisco ISE, так і в адміністративній панелі Duo.

- Регулярний аналіз подій: Проводити періодичний аналіз журналів для відстеження активності користувачів, виявлення аномалій, підозрілих спроб входу та потенційних інцидентів безпеки. Рекомендується інтегрувати ці журнали з системами SIEM (Security Information and Event Management) для централізованого збору, кореляції та аналізу.

Таблиця 3.4 - Структура журналу подій у Cisco

№	Поле журналу	Опис
1	Timestamp	Дата і час події
2	Username	Ім’я користувача, який ініціював доступ
3	Source IP	IP-адреса джерела запиту
4	NAS IP Address	IP-адреса мережевого пристрою (NAD)
5	Authentication Protocol	Протокол автентифікації (наприклад, PEAP, EAP-TLS)
6	Authentication Status	Статус автентифікації (успіх / помилка)
7	Failure Reason	Причина помилки (у разі відмови)
8	Device Type	Тип пристрою користувача (наприклад, мобільний, ноутбук)

9	Policy Set Name	Назва застосованого набору політик
10	Identity Source	Джерело ідентифікації (наприклад, Active Directory, Internal Users)
11	Authorization Result	Результат авторизації (профіль або дія, що застосована)
12	Session ID	Унікальний ідентифікатор сесії

Представлена таблиця ілюструє типову структуру записів журналу подій аутентифікації в Cisco ISE. Вона включає такі важливі поля, як Час події, Користувач (ідентифікатор користувача, який намагався увійти), Метод аутентифікації (наприклад, "Duo Push", "TOTP"), Статус (успіх/невдача), Використаний пристрій (тип пристрою користувача), Геолокація (IP-адреса або географічне розташування спроби входу).

3.5. Комплексне управління ризиками, пов'язаними з 2FA

Навіть найдосконаліша система двофакторної аутентифікації (2FA) не може бути абсолютно невразливою до всіх типів атак та непередбачених ситуацій. Тому, для забезпечення максимальної стійкості та безперервності доступу до корпоративних інформаційних систем, вкрай важливо розробити та впровадити ефективні стратегії управління ризиками, що дозволяють мінімізувати потенційні загрози та оперативно реагувати на виниклі інциденти.

Нижче представлена розширена таблиця ключових ризиків, пов'язаних з 2FA, їхній опис та рекомендовані рішення.(Таблиця 3.3 – Розгорнутий аналіз ризиків, пов'язаних з 2FA, їхній опис та рекомендовані рішення.)

Таблиця 3.3 – Розгорнутий аналіз ризиків, пов'язаних з 2FA, їхній опис та рекомендовані рішення.

Ризик	Опис	Рекомендоване рішення
MFA Fatigue	Зловмисник бомбардує ціль запитами 2FA, сподіваючись на помилкове схвалення.	Verified Duo Push: Вимагає введення коду для підтвердження. Адаптивні політики: Обмежують кількість запитів за певний час. Навчання: Пояснювати користувачам небезпеку підтвердження неініційованих запитів. Alerting: Налаштувати сповіщення для адміністраторів про надмірну кількість 2FA-запитів до одного користувача.
Компрометація пристрою (смартфона)	Встановлення шкідливого ПЗ на смартфон користувача, що може перехоплювати push-повідомлення або коди.	Duo Device Health: Перевіряє стан безпеки мобільного пристрою (наявність руту/jailbreak, актуальність ОС, наявність антивірусного ПЗ). Політики доступу: Обмежувати доступ з пристроїв, що не відповідають корпоративним стандартам безпеки. Системи MDM/UEM: Використання Mobile Device Management або Unified Endpoint Management для централізованого контролю

		та застосування політик безпеки на мобільних пристроях.
Фішинг та соціальна інженерія	Зловмисник створює фальшиву сторінку входу для викрадення облікових даних та 2FA-кодів.	Навчання та підвищення обізнаності користувачів: Регулярні тренінги з розпізнавання фішингових атак, акцентування на необхідності перевіряти URL-адреси. Використання FIDO2/WebAuthn: Ці стандарти забезпечують криптографічну прив'язку до сайту, роблячи фішинг значно складнішим. Conditional Access: Використання ISE для аналізу контексту (IP-адреса, геолокація) та блокування доступу з підозрілих джерел.
Втрата пристрою 2FA	Користувач втрачає смартфон з Duo Mobile або апаратний токен.	Налаштування резервних методів: Забезпечити альтернативні методи (TOTP на іншому пристрої, апаратний токен). Контрольована процедура скидання: Розробити та впровадити сувору процедуру скидання 2FA через службу підтримки, що вимагає багаторівневої перевірки особистості користувача

		(наприклад, перевірка особистості, секретні питання). Самостійне управління 2FA (Self-Service Portal): Надати користувачам можливість самостійно реєструвати нові пристрої або управляти існуючими через захищений портал.
Доступ з невідомої локації / аномальна поведінка	Спроба входу з незвичної географічної локації, нового пристрою або у незвичайний час.	Risk-Based Authentication (RBA): Використання функціоналу Duo для аналізу контексту входу (геолокація, IP-адреса, тип пристрою, історія входів) та автоматичного вимагання додаткових перевірок або блокування доступу у разі виявлення аномалій. Адаптивні політики в ISE: Налаштування ISE для динамічної зміни вимог доступу на основі оцінки ризиків. Інтеграція з SIEM: Передача даних про аутентифікацію до SIEM-системи для комплексного аналізу та виявлення аномалій, що можуть вказувати на компрометацію.

Людський фактор / помилки конфігурації	Неправильне налаштування систем 2FA або IAM, що створює вразливості.	Регулярний аудит конфігурацій: Проведення періодичних аудитів налаштувань ISE, Duo та інтеграцій для виявлення та усунення помилок. Автоматизоване тестування безпеки: Використання інструментів для автоматизованого тестування конфігурацій на відповідність кращим практикам. Обмеження привілеїв: Застосування принципу мінімальних привілеїв для адміністраторів, які налаштовують системи безпеки.
Проблеми з доступністю сервісів 2FA	Збій у роботі Duo Cloud Service або Duo Authentication Proxy, що унеможливлює аутентифікацію.	Розгортання надлишкових Duo Authentication Proxy: Використання декількох екземплярів Duo Proxy для забезпечення відмовостійкості. Failmode на Duo Proxy: Ретельне налаштування параметра failmode (наприклад, failmode=safe дозволяє вхід без 2FA, якщо Duo недоступний; failmode=secure блокує вхід, якщо Duo недоступний). Вибір залежить від політик безпеки та

		критичності системи. Резервні методи аутентифікації: Наявність альтернативних, офлайн-орієнтованих методів (наприклад, апаратні токени або аварійні коди).
Використання скомпрометованих пристроїв для другого фактора	Якщо пристрій, що використовується для 2FA, вже скомпрометований (наприклад, інфікований шкідливим ПЗ).	Політики оцінки стану пристроїв: ISE може перевіряти відповідність пристрою політиці безпеки перед наданням доступу (наприклад, наявність антивірусу, актуальність патчів). Duo Device Trust: Функція, яка дозволяє перевіряти, чи є пристрій керованим організацією, і чи відповідає він вимогам безпеки. Обмеження використання особистих пристроїв (BYOD): Впровадження чітких політик для BYOD та, за можливості, використання лише корпоративних пристроїв для доступу до чутливих ресурсів.
Недостатня обізнаність користувачів	Користувачі не розуміють важливості 2FA, її переваг та правил	Постійні програми навчання та підвищення обізнаності: Проведення регулярних вебінарів, розсилок, інформаційних кампаній з

	безпечного використання.	акцентом на реальні кейси загроз. Гейміфікація та заохочення: Мотивація користувачів до дотримання політик безпеки. Зручний інтерфейс та простота використання: Чим простіше і зручніше 2FA, тим охочіше користувачі її прийматимуть.

3.6 Очікувані результати від впровадження комплексного рішення Cisco Duo та ISE

Впровадження інтегрованого рішення Cisco Duo та Cisco Identity Services Engine (ISE) — це не просто модернізація системи безпеки; це стратегічна інвестиція, яка принесе організації низку значних та вимірюваних переваг.

Ці переваги охоплюють ключові аспекти кібербезпеки, операційної ефективності та відповідності регуляторним вимогам:

- Значне зниження ризику компрометації облікових записів: Це, мабуть, найважливіший очікуваний результат. Завдяки додаванню другого фактора аутентифікації (2FA), система стає набагато стійкішою до поширених векторів атак, таких як фішинг, використання вкрадених або слабких паролів, атаки грубої сили та повторне використання облікових даних. За даними провідних аналітичних агентств та внутрішніх досліджень Cisco, впровадження 2FA може призвести до зниження ймовірності успішної компрометації облікових записів на вражаючі 80–90%. Це означає, що переважна більшість спроб несанкціонованого доступу буде ефективно заблокована ще на ранніх етапах, що значно підвищує загальний рівень захищеності корпоративних даних та систем.

- Забезпечення відповідності ключовим міжнародним стандартам безпеки та регуляторним вимогам: У сучасному світі, де регуляторне навантаження постійно

зростає, відповідність стандартам є не просто бажаною, а часто обов'язковою умовою для ведення бізнесу.

Впровадження надійної 2FA через Cisco ISE та Duo є критично важливим кроком до досягнення та підтримки відповідності таким важливим нормативним актам та стандартам, як:

ISO 27001: Міжнародний стандарт для систем управління інформаційною безпекою (СУІБ). 2FA є фундаментальним контролем у рамках цього стандарту.

GDPR (General Data Protection Regulation): Регламент ЄС щодо захисту персональних даних. Посилена аутентифікація допомагає забезпечити належний рівень захисту конфіденційної інформації.

PCI DSS (Payment Card Industry Data Security Standard): Стандарт безпеки даних індустрії платіжних карток. Вимагає сильної аутентифікації для доступу до середовищ, що обробляють дані платіжних карток.

NIST Cybersecurity Framework: Рамки кібербезпеки, розроблені Національним інститутом стандартів і технологій США, які активно пропагують використання багатофакторної аутентифікації як ключового засобу захисту. Відповідність цим стандартам не лише допомагає уникнути значних штрафів, а й підвищує довіру з боку партнерів, клієнтів та інвесторів.

- Відчутне підвищення зручності та загального користувацького досвіду: Хоча на перший погляд 2FA може здатися додатковим кроком, правильно реалізована система, така як Duo Push, насправді підвищує зручність. Користувачам більше не потрібно запам'ятовувати складні та довгі паролі або постійно їх змінювати. Достатньо одного натискання на смартфоні, щоб підтвердити вхід. Це зменшує "парольну втому", підвищує продуктивність, оскільки користувачі витрачають менше часу на процеси аутентифікації, і покращує їхнє загальне сприйняття корпоративної безпеки.

Істотне спрощення адміністрування та управління безпекою через централізовану платформу: Cisco ISE слугує єдиним центром управління політиками доступу та моніторингу аутентифікації для всієї корпоративної мережі.

Це дозволяє IT-відділу та команді безпеки:

- Централізовано застосовувати політики: Не потрібно конфігурувати 2FA окремо для кожного ресурсу; всі правила керуються з одного місця.

- Швидко реагувати на інциденти: Централізовані журнали та звіти в ISE та Duo дозволяють оперативно виявляти аномалії та реагувати на загрози.

- Оптимізувати процеси: Автоматизація профілювання пристроїв, інтеграція з AD та Duo значно скорочують ручні операції та адміністративні витрати.

- Забезпечити послідовність: Усі користувачі та пристрої підпадають під єдину, чітко визначену політику безпеки.

3.7 Практичні сценарії використання двофакторної аутентифікації з Cisco ISE та Duo

Комплексне рішення Cisco ISE та Cisco Duo демонструє свою високу ефективність та гнучкість у захисті доступу до різноманітних корпоративних ресурсів, покриваючи широкий спектр сценаріїв використання. Ось кілька ключових прикладів, які ілюструють, як інтеграція працює на практиці:

Доступ до корпоративної VPN-мережі

Сценарій: Співробітник підключається до корпоративної мережі з віддаленого місця через VPN-клієнт.

Детальний процес:

1. Користувач запускає VPN-клієнт на своєму ноутбуці або мобільному пристрої та вводить свої традиційні облікові дані: логін і пароль.
2. VPN-шлюз перенаправляє запит на аутентифікацію до Cisco ISE.
3. Cisco ISE спочатку перевіряє первинний фактор (логін і пароль) шляхом інтеграції з корпоративною службою каталогів, такою як Active Directory.
4. Після успішної перевірки пароля, ISE, згідно з налаштованими політиками, визначає, що для VPN-доступу вимагається другий фактор. Вона надсилає запит на аутентифікацію до Duo Authentication Proxy за протоколом RADIUS.

5. Cisco Duo надсилає push-повідомлення до додатка Duo Mobile на зареєстрованому смартфоні користувача.

6. Користувач отримує сповіщення та одним натисканням кнопки "Approve" підтверджує спробу входу.

7. Duo повертає позитивний результат аутентифікації до ISE.

8. Cisco ISE додатково аналізує контекст підключення: це може бути профілювання пристрою (чи це корпоративний ноутбук, чи відповідає він вимогам безпеки), перевірка геолокації (чи вхід здійснюється з дозволеного регіону) та інші політики.

9. Лише після успішної перевірки всіх факторів (пароль, 2FA, відповідність пристрою та контексту) ISE надає користувачеві доступ до корпоративної VPN-мережі, застосовуючи відповідні політики авторизації (наприклад, дозволяючи доступ до певних сегментів мережі).

Захищений доступ до хмарних сервісів

Сценарій: Співробітник намагається отримати доступ до корпоративного хмарного сервісу, такого як Microsoft 365 (Outlook, Teams, OneDrive) або Salesforce.

Детальний процес:

1. Користувач відкриває веб-браузер і переходить на сторінку входу до хмарного сервісу.

2. Завдяки інтеграції хмарного сервісу з Cisco ISE як провайдером ідентифікації (Identity Provider, IdP) через протокол SAML (Security Assertion Markup Language), запит на аутентифікацію перенаправляється до ISE.

3. Користувач вводить свій корпоративний логін і пароль.

4. ISE перевіряє ці облікові дані та, відповідно до політики, вимагає другий фактор.

5. У цьому сценарії Duo може бути налаштований на використання TOTP (Time-based One-Time Password). Користувач відкриває додаток Duo Mobile на своєму смартфоні або використовує апаратний токен (наприклад, YubiKey) для генерації одноразового коду.

6. Користувач вводить згенерований OTP-код у відповідне поле на сторінці аутентифікації.

7. ISE надсилає OTP-код до Duo для перевірки.

8. Після успішної перевірки обох факторів, ISE генерує SAML-відповідь, яка містить інформацію про успішну аутентифікацію та авторизацію користувача.

9. Ця SAML-відповідь повертається до хмарного сервісу, який, довіряючи ISE як IdP, надає користувачеві доступ.

Контрольований доступ до корпоративної Wi-Fi мережі

Сценарій: Співробітник або гостьовий користувач намагається підключитися до корпоративної бездротової мережі.

Детальний процес:

1. Пристрій користувача (ноутбук, смартфон) ініціює підключення до корпоративної Wi-Fi мережі.

2. Запит на підключення перехоплюється точкою доступу Wi-Fi, яка інтегрована з Cisco ISE.

3. Cisco ISE в режимі реального часу починає профілювання пристрою: вона ідентифікує тип пристрою (наприклад, корпоративний ноутбук, особистий смартфон, планшет), операційну систему, MAC-адресу, чи встановлене відповідне програмне забезпечення безпеки тощо.

4. На основі профілювання пристрою та ролі користувача, ISE застосовує відповідну політику аутентифікації. Для критичних користувачів (наприклад, адміністраторів) або для доступу до найбільш чутливих сегментів мережі може бути встановлена вимога до 2FA.

5. У такому випадку, Cisco Duo може бути налаштований на застосування біометричної аутентифікації (через Duo Mobile або WebAuthn/FIDO2) для підтвердження особистості користувача. Наприклад, користувач може бути попрошений підтвердити вхід за допомогою відбитка пальця або розпізнавання обличчя на своєму пристрої.

6. Після успішної біометричної верифікації та перевірки стану пристрою, ISE надає доступ до Wi-Fi мережі, застосовуючи відповідні мережеві політики

(наприклад, розміщення користувача в певному VLAN, застосування обмежень пропускної здатності або доступу до ресурсів). Для гостьових користувачів можуть бути визначені окремі, більш обмежені політики доступу без 2FA.

Таблиця 3.4 - Аналіз сценаріїв використання

Сценарій	Метод 2FA, що використовується	Рівень безпеки (Оцінка)	Складність впровадження	Переваги для користувача
VPN-доступ	Duo Push	Високий	Середня	Швидке та зручне підтвердження, захист від фішингу
Хмарні сервіси	TOTP (через Duo Mobile)	Високий	Низька	Працює офлайн, незалежність від push-сповіщень
Wi-Fi доступ	Біометрія	Дуже високий	Висока	Максимальна зручність та надійність, безпарольний доступ

Ефективне впровадження 2FA — це не одноразова акція, а безперервний процес, який вимагає стратегій для масштабування та оптимізації з плином часу.

Для мінімізації ризиків та забезпечення плавного переходу, рекомендується застосовувати поетапний підхід до масштабування 2FA:

- Почати з критичних систем та груп: Спершу впровадити 2FA для доступу до найбільш критичних систем (наприклад, VPN-шлюзи, сервери доменних контролерів, CRM-системи, фінансові додатки) та для груп користувачів з підвищеними привілеями (IT-адміністратори, керівництво, фінансовий відділ). Це дозволить захистити найцінніші активи першими.

- Розширити на всі ресурси та користувачів: Після успішного пілотного впровадження та збору зворотного зв'язку, поступово масштабувати застосування

2FA на всіх користувачів та всі корпоративні ресурси, що вимагають захисту. Це може бути здійснено за відділами або за пріоритетністю ресурсів.

Для забезпечення ефективності та зниження адміністративного навантаження критично важливо автоматизувати процеси управління 2FA:

- Використання Duo Self-Service Portal: Активувати та навчити користувачів використовувати портал самообслуговування Duo. Це дозволить їм самостійно реєструвати нові пристрої, керувати існуючими методами аутентифікації або скидати свій другий фактор (за встановленими політиками), що значно зменшить навантаження на службу підтримки.

- Інтеграція з SIEM-системами: Налаштувати передачу всіх журналів подій аутентифікації з Cisco ISE та Cisco Duo до централізованої системи управління інформаційною безпекою та подіями (SIEM). Це дозволить:

Централізований моніторинг: Збирати, агрегувати та корелювати події безпеки з різних джерел.

Виявлення аномалій: Використовувати аналітичні можливості SIEM для автоматичного виявлення підозрілої активності (наприклад, багаторазові невдалі спроби входу, вхід з аномальних локацій, несанкціоновані зміни в конфігурації).

Автоматизовані сповіщення: Налаштувати оповіщення для команди безпеки у разі виявлення потенційних загроз.

Звітність: Формувати звіти для аудиту та відповідності регуляторним вимогам.

- Автоматизація provisioning/deprovisioning: Інтегрувати Duo та ISE з існуючими HR-системами або системами управління ідентифікацією для автоматичного додавання або видалення користувачів та їхніх 2FA-пристроїв при наймі або звільненні співробітників, що зменшить ручну роботу та ризик помилок.

‘ Для забезпечення стабільної роботи та масштабованості системи, необхідно оптимізувати використання ресурсів:

- Розгляд використання хмарного ISE для малих та середніх організацій: Для менших компаній, які не мають ресурсів для підтримки складної локальної

інфраструктури ISE, хмарні або віртуалізовані рішення ISE можуть бути більш економічно вигідним та простим в управлінні варіантом.

- Балансування навантаження на Duo Authentication Proxy: Для великих організацій з великою кількістю одночасних запитів аутентифікації, рекомендується розгорнути кілька екземплярів Duo Authentication Proxy та використовувати балансувальник навантаження. Це забезпечить високу доступність та продуктивність сервісу 2FA, навіть за значного навантаження.

- Регулярне оновлення та обслуговування: Своєчасне застосування оновлень та патчів для Cisco ISE, Cisco Duo та Duo Authentication Proxy є критично важливим для підтримки високого рівня безпеки та виправлення виявлених вразливостей. Регулярні перевірки продуктивності та оптимізація конфігурацій також сприятимуть стабільній роботі системи.

Впровадження цих стратегій забезпечить, що рішення 2FA буде не тільки ефективним на момент розгортання, але й буде масштабованим, стійким та адаптованим до майбутніх викликів безпеки, забезпечуючи надійний захист корпоративних облікових записів.

ВИСНОВКИ

У процесі виконання дипломної роботи було проведено комплексне дослідження проблематики ідентифікації та аутентифікації в корпоративних інформаційних системах (КІС), проаналізовано сучасні методи двофакторної аутентифікації (2FA), а також розроблено рекомендації щодо захисту облікових записів користувачів із використанням Cisco Duo та Cisco Identity Services Engine (ISE). Робота дозволила досягти поставленої мети та вирішити визначені завдання, забезпечивши ґрунтовний аналіз і практичні рекомендації для підвищення безпеки КІС.

Аналіз проблематики ідентифікації та аутентифікації показав, що традиційні методи, засновані на паролях, є вразливими до сучасних кіберзагроз, таких як фішинг, крадіжка даних і атаки типу "man-in-the-middle". Згідно з даними Verizon Data Breach Investigations Report 2024, 36% кібератак пов’язані з фішингом, а середня вартість витоку даних становить 4,45 млн доларів США (IBM Security, 2024). Специфіка КІС, зокрема масштабність, різноманітність пристроїв, віддалений доступ і регуляторні вимоги (ISO 27001, GDPR), підкреслює необхідність впровадження надійних методів аутентифікації, таких як 2FA.

Дослідження методів двофакторної аутентифікації виявило, що найефективнішими для КІС є методи, що використовують мобільні додатки (зокрема Cisco Duo Mobile), завдяки балансу безпеки, зручності та низької вартості. Фізичні токени та біометричні методи підходять для високочутливих систем, тоді як SMS-коди та електронна пошта мають низьку безпеку через вразливість до атак. Cisco Duo вирізняється підтримкою широкого спектра методів верифікації (push-повідомлення, OTP, біометрія, апаратні токени), адаптивною аутентифікацією та інтеграцією з різними системами через протоколи SAML, OAuth і RADIUS.

Інтеграція Cisco Duo з Cisco ISE є оптимальним рішенням для захисту облікових записів у КІС. Cisco ISE забезпечує централізоване управління доступом, профілювання пристроїв і налагодження політик, тоді як Cisco Duo додає надійний другий фактор аутентифікації. Процес верифікації, що включає первинну перевірку

через ISE, запит другого фактора через Duo (наприклад, push-повідомлення) і аналіз контексту входу, дозволяє ефективно протидіяти кіберзагрозам. Адаптивна аутентифікація (Risk-Based Authentication) і перевірка стану пристроїв (Duo Device Health) підвищують безпеку, а функція самообслуговування (Duo Self-Service Portal) спрощує управління для користувачів.

Рекомендації щодо впровадження включають використання Duo Push як основного методу верифікації через його швидкість, зручність і захист від атак, таких як "MFA fatigue", завдяки функції Verified Duo Push. TOTP і біометрія рекомендуються як резервні методи для критичних сценаріїв, тоді як SMS і телефонні дзвінки слід виключити через вразливість до SIM-swapping. Поетапне впровадження Cisco Duo та ISE передбачає аудит системи, налаштування інтеграції через RADIUS, пілотне тестування, масштабування та постійний моніторинг. Використання Cisco ISE дозволяє централізовано керувати політиками доступу, що відповідає вимогам великих організацій.

Новизна роботи полягає в детальному дослідженні інтеграції Cisco Duo з Cisco ISE, з акцентом на адаптивність до сучасних кіберзагроз, сумісність із різноманітними КІС і забезпечення відповідності стандартам безпеки.

Практична цінність полягає в розробці рекомендацій, які можуть бути застосовані для підвищення безпеки облікових записів, зниження ризиків компрометації на 80–90% (згідно з даними Cisco) і спрощення адміністрування через централізоване управління.

Перспективи подальших досліджень включають аналіз безпарольної аутентифікації (FIDO2/WebAuthn) у поєднанні з Cisco ISE та Duo, а також оцінку впливу автоматизації та штучного інтелекту на адаптивну аутентифікацію. Запропонований підхід із використанням Cisco Duo та Cisco ISE забезпечує надійний захист КІС, відповідає сучасним викликам кібербезпеки та сприяє безпечному функціонуванню корпоративних інформаційних систем.

ПЕРЕЛІК ПОСИЛАНЬ

1. Cisco. (2023). Cisco Duo: Multi-Factor Authentication (MFA). Retrieved from https://duo.com
2. Cisco. (2023). Cisco Identity Services Engine (ISE) Documentation. Retrieved from https://www.cisco.com/c/en/us/products/security/identity-services-engine/index.html
3. FIDO Alliance. (2023). FIDO2: Web Authentication Specification. Retrieved from https://fidoalliance.org/specs/fido-v2.0-ps-20190130/fido-client-to-authenticator-protocol-v2.0-ps-20190130.html
4. IBM Security. (2024). Cost of a Data Breach Report 2024. Retrieved from https://www.ibm.com/reports/data-breach
5. International Organization for Standardization. (2022). ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements. Geneva: ISO.
6. National Institute of Standards and Technology. (2022). Digital Identity Guidelines: Authentication and Lifecycle Management (NIST SP 800-63B). Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf
7. Verizon. (2024). Data Breach Investigations Report 2024. Retrieved from https://www.verizon.com/business/resources/reports/dbir/
8. Duo Security. (2023). Duo Authentication Proxy Reference Guide. Retrieved from https://duo.com/docs/authproxy-reference
9. OWASP. (2023). Authentication Cheat Sheet. Retrieved from https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html
10. Microsoft. (2023). Microsoft Authenticator Documentation. Retrieved from https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-authenticator-app
11. Okta. (2023). Okta Verify: Multi-Factor Authentication. Retrieved from https://www.okta.com/products/okta-verify/

12. Yubico. (2023). YubiKey FIDO2 and U2F Security Key. Retrieved from https://www.yubico.com/products/yubikey-fido-u2f/

13. Aloul, F., Zahidi, S., & El-Hajj, W. (2009). Two factor authentication using mobile phones. IEEE International Conference on Computer Systems and Applications, 641–644. https://doi.org/10.1109/AICCSA.2009.5069329

14. Bhadauria, R., & Sanyal, S. (2012). Survey on security issues in cloud computing and associated mitigation techniques. International Journal of Computer Applications, 47(18), 47–66. https://doi.org/10.5120/7292-0578

15. Bhargav-Spantzel, A., Squicciarini, A. C., & Bertino, E. (2007). Trust negotiation in identity management. IEEE Security & Privacy, 5(2), 55–63. https://doi.org/10.1109/MSP.2007.46

16. Burr, W. E., Dodson, D. F., & Polk, W. T. (2006). Electronic authentication guideline (NIST SP 800-63). National Institute of Standards and Technology. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63v1.0.2.pdf

17. Dasgupta, D., Roy, A., & Nag, A. (2017). Advances in user authentication. Springer. https://doi.org/10.1007/978-3-319-58808-7

18. De Cristofaro, E., Du, H., Freudiger, J., & Norcie, G. (2013). A comparative usability evaluation of two-factor authentication. Proceedings of the 2013 NDSS Symposium. Retrieved from https://www.ndss-symposium.org/ndss2013/

19. Dhamija, R., & Perrig, A. (2000). Déjà vu: A user study using images for authentication. Proceedings of the 9th USENIX Security Symposium, 45–58. Retrievedfrom https://www.usenix.org/legacy/publications/library/proceedings/sec2000/dhamija.html

20. European Union. (2016). General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679). Retrieved from https://eur-lex.europa.eu/eli/reg/2016/679/oj

21. Grassi, P. A., Garcia, M. E., & Fenton, J. L. (2017). Digital identity guidelines: Authentication and lifecycle management (NIST SP 800-63-3). National Institute of Standards and Technology. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf

22. Gunson, N., Marshall, D., Morton, H., & Jack, M. (2011). User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking. Computers & Security, 30(4), 208–220. https://doi.org/10.1016/j.cose.2010.12.001

23. Huang, X., Xiang, Y., Chonka, A., Zhou, J., & Deng, R. H. (2011). A generic framework for three-factor authentication: Preserving security and privacy in distributed systems. IEEE Transactions on Parallel and Distributed Systems, 22(12), 1859–1871. https://doi.org/10.1109/TPDS.2010.206

24. Jain, A. K., Ross, A., & Pankanti, S. (2006). Biometrics: A tool for information security. IEEE Transactions on Information Forensics and Security, 1(2), 125–143. https://doi.org/10.1109/TIFS.2006.873653

25. Kim, J. J., & Hong, S. P. (2011). A method of risk assessment for multi-factor authentication. Journal of Information Processing Systems, 7(1), 187–198. https://doi.org/10.3745/JIPS.2011.7.1.187

26. Kizza, J. M. (2017). Guide to computer network security (4th ed.). Springer. https://doi.org/10.1007/978-3-319-55606-2

27. Krol, K., Philippou, E., De Cristofaro, E., & Sasse, M. A. (2015). “They brought in the horrible key ring thing!” Analysing the usability of two-factor authentication in UK online banking. Proceedings of USEC’15. https://doi.org/10.14722/usec.2015.23004

28. Lee, D., Kim, Y., & Lee, S. (2018). A study on the usability and security of two-factor authentication. Journal of Internet Services and Information Security, 8(2), 1–14. https://doi.org/10.22667/JISIS.2018.05.31.001

29. Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T., & Koucheryavy, Y. (2018). Multi-factor authentication: A survey. Cryptography, 2(1), 1. https://doi.org/10.3390/cryptography2010001

30. Ponemon Institute. (2023). 2023 State of Cybersecurity Report. Retrieved from https://www.ponemon.org/research/ponemon-library/security/2023-state-of-cybersecurity-report.html

31. RSA Security. (2023). RSA SecurID Access. Retrieved from https://www.rsa.com/products/securid-access/

32. Schneier, B. (2011). Secrets and lies: Digital security in a networked world. Wiley. https://doi.org/10.1002/9781119183631

33. Silver, D., Jana, S., Boneh, D., Chen, E., & Jackson, C. (2014). Password managers: Attacks and defenses. Proceedings of the 23rd USENIX Security Symposium,449–464. Retrieved from https://www.usenix.org/conference/usenixsecurity14/technical-sessions/presentation/silver

34. Sun, H., Zhang, Y., & Wang, J. (2019). A survey of two-factor authentication techniques in mobile computing. Journal of Network and Computer Applications, 145, 102430. https://doi.org/10.1016/j.jnca.2019.102430

35. Symantec. (2023). Internet Security Threat Report 2023. Retrieved from https://www.broadcom.com/products/cyber-security/threat-intelligence/internet-security-threat-report

36. Ulven, J. B., & Wangen, G. (2021). A systematic review of cybersecurity risks in higher education. Future Internet, 13(2), 39. https://doi.org/10.3390/fi13020039

37. Wang, D., & Wang, P. (2014). On the usability of two-factor authentication. International Conference on Security and Privacy in Communication Networks, 141–150. https://doi.org/10.1007/978-3-319-23829-6_10

38. Weir, C. S., Douglas, G., Carruthers, M., & Jack, M. (2009). User perceptions of security, convenience and usability for e-banking authentication tokens. Computers & Security, 28(1–2), 47–62. https://doi.org/10.1016/j.cose.2008.09.008

39. Wu, M., Miller, R. C., & Garfinkel, S. L. (2006). Do security toolbars actually prevent phishing attacks? Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 601–610. https://doi.org/10.1145/1124772.1124863

40. Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. Future Generation Computer Systems, 28(3), 583–592. https://doi.org/10.1016/j.future.2010.12.006

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ
Кафедра Систем та технологій кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА
на тему: "Система захисту облікових записів користувачів у корпоративних інформаційних системах з використанням двофакторної аутентифікації"

Виконав: Федосєєв Максим Андрійович
Керівник:Зоя БОНДАРЕНКО

Актуальність теми:

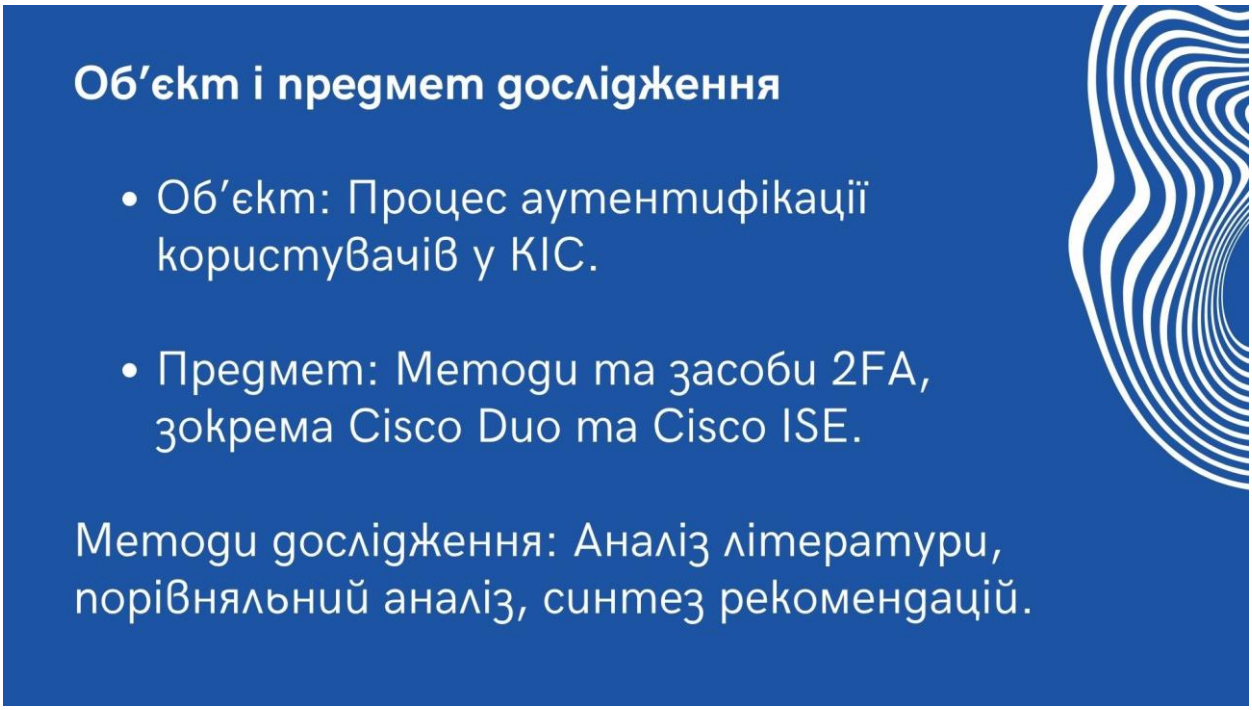
Зростання кіберзагроз: фішинг, крадіжка даних, атаки MITM.

Слабкість паролів: 36% атак пов'язані з фішингом (Verizon, 2024).

Вимоги стандартів: ISO 27001, GDPR.

Рішення: двофакторна аутентифікація (2FA) із Cisco Duo та Cisco ISE.


Мета: Розробити рекомендації щодо захисту облікових записів у КІС з використанням 2FA на основі Cisco Duo та Cisco ISE.
Завдання:
- Проаналізувати проблематику ідентифікації та аутентифікації.
- Дослідити методи 2FA.
- Розробити рекомендації з інтеграцією Cisco Duo та ISE.


Об'єкт і предмет дослідження
- Об'єкт: Процес аутентифікації користувачів у КІС.
- Предмет: Методи та засоби 2FA, зокрема Cisco Duo та Cisco ISE.
Методи дослідження: Аналіз літератури, порівняльний аналіз, синтез рекомендацій.

Проблематика ідентифікації та аутентифікації

- Вразливості паролів:
  - Фішинг, слабкі паролі, крадіжка даних.
  - Середня вартість витоку: $4,45 млн (IBM, 2024).
- Особливості КІС:
  - Масштабність, різноманітність пристроїв, віддалений доступ.
  - Регуляторні вимоги (GDPR, ISO 27001).
- Рішення: Впровадження 2FA.

Методи двофакторної аутентифікації

- Класифікація:
  - Фізичні токени (YubiKey).
  - Мобільні додатки (Cisco Duo Mobile).
  - SMS-коди, біометрія, електронна пошта, смарт-карти.
- Переваги та недоліки:
  - Мобільні додатки: висока зручність, низька вартість.
  - SMS: вразливість до SIM-swapping.

Cisco Duo

- Функціонал:
  - Методи: push-повідомлення, OTP, біометрія, токени.
  - Інтеграція: SAML, OAuth, RADIUS.
  - Адаптивна аутентифікація (Risk-Based Authentication).
- Процес верифікації:
  a. Введення пароля.
  b. Запит другого фактора (наприклад, Duo Push).
  c. Аналіз контексту (геолокація, пристрій).

Порівняння Cisco Duo з іншими рішеннями

- Рішення:
  - Microsoft Authenticator: міцна інтеграція з Microsoft.
  - Google Authenticator: лише TOTP, низька адаптивність.
  - Okta Verify: висока вартість.
- Переваги Cisco Duo:
  - Універсальність, підтримка FIDO2.
  - Адаптивна аутентифікація.
  - Легкість інтеграції.

Cisco Identity Services Engine (ISE)

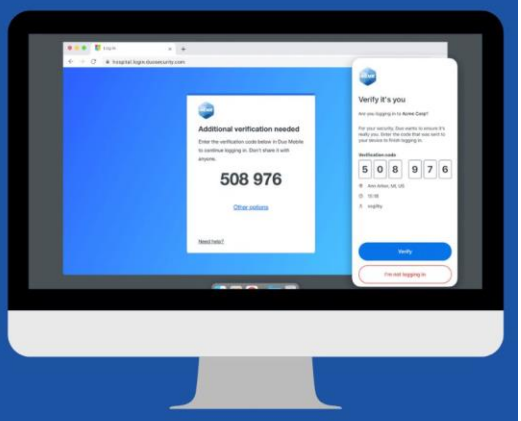
- Функції ISE:
  - Управління доступом, профілювання пристроїв.
  - Підтримка RADIUS, SAML.

- Інтеграція з Duo:
  - ISE перевіряє пароль через Active Directory.
  - Duo надсилає push-повідомлення.
  - Аналіз контексту для надання доступу.

Процес аутентифікації через ISE та Duo

Етапи:

1. Користувач вводить логін і пароль.
2. ISE перевіряє первинну аутентифікацію.
3. Duo надсилає другий фактор (push, OTP).
4. ISE аналізує пристрій і контекст.



Рекомендації щодо впровадження

- Методи верифікації:
  - Основний: Duo Push (Verified Duo Push).
  - Резервний: TOTP, біометрія.
  - Виключити: SMS, телефонні дзвінки.
- Кроки впровадження:
  a. Аудит системи.
  b. Налаштування ISE та Duo.
  c. Пілотне тестування.
  d. Масштабування.

Управління ризиками та результат

Ризики:

Втрата пристрою: резервні методи.
MFA fatigue: Verified Duo Push.
Підозрілі спроби: адаптивна аутентифікація.

Очікувані результати:

Зниження ризиків на 80-90% (Cisco).
Відповідність ISO 27001, GDPR.
Спрощення адміністрування.

Висновки

- Традиційні методи аутентифікації вразливі до кіберзагроз.
- Cisco Duo забезпечує надійну 2FA з адаптивною аутентифікацією.
- Інтеграція з Cisco ISE дозволяє централізовано керувати доступом.
- Рекомендації включають Duo Push, TOTP і поетапне впровадження.
- Новизна: детальний аналіз інтеграції Duo та ISE.