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

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Система багатофакторної автентифікації користувачів за допомогою мобільного додатка на базі ESET Secure Authentication»

зі спеціальності *125 Кібербезпека*
(код, найменування спеціальності)

освітньо-професійної програми *Інформаційна та кібернетична безпека*
(назва програми)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Антон ЧУРІКОВ
(підпис)

Виконав: здобувач вищої освіти групи БСД-42
ЧУРІКОВ Антон
(прізвище, ім'я)

Керівник д.ф. СОБЧУК Андрій
(науковий ступінь, вчене звання, прізвище, ім'я)

Рецензент _____
(науковий ступінь, вчене звання, прізвище, ім'я)

Київ 2025

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ОС – операційна система

ПК – персональний комп’ютер

ЦОД – центр обробки даних

2FA – Two Factor Authentication

AD – Active Directory

API – Application Programming Interface

APT – Advanced Persistent Threat

DDoS – Distributed Denial of Service

DNS – Domain Name System

ECP – Exchange Control Panel

ESA – ESET Secure Authentication

FQDN – Fully Qualified Domain Name

GPO – Group Policy Object

IaaS – Infrastructure as a Service

IAM – Identity and Access Management

IdP – Identity Provider

MRK – Master Recovery Key

OS – Operating System.

OTP – One Time Password

OWA – Outlook Web Access

RDP – Remote Desktop Protocol

SOC – Security Operations Center

ВСТУП

Актуальність дослідження. Застосування системи багатофакторної автентифікації за допомогою мобільного додатку є важливим кроком для посилення безпеки облікових записів користувачів. Багатофакторна автентифікація додає додатковий рівень захисту, вимагаючи від користувача надати два або більше доказів ідентифікації. Це значно ускладнює несанкціонований доступ до облікового запису, навіть якщо зловмисник отримає пароль. Мобільний додаток забезпечує зручний та безпечний спосіб генерації одноразових кодів або отримання push-повідомлень для підтвердження особистості.

Багатофакторна автентифікація ефективно захищає від таких загроз, як фішинг, крадіжка паролів та атаки з використанням шкідливого програмного забезпечення. Навіть якщо зловмисник отримає пароль, він не зможе отримати доступ до облікового запису без додаткового фактора автентифікації, який надає мобільний додаток.

Застосування мобільних додатків для багатофакторної автентифікації користувачів є зручним у використанні та доступним на більшості сучасних смартфонів. Вони дозволяють швидко та легко підтверджувати особистість, не вимагаючи використання додаткових пристроїв або отримання SMS-повідомлень.

Використання багатофакторної автентифікації, особливо за допомогою мобільних додатків, є важливим кроком для забезпечення безпеки в сучасному цифровому світі. Вищесказане визначає актуальність теми даної кваліфікаційної роботи, основний зміст якої становлять дослідження методів та засобів багатофакторної автентифікації користувачів за допомогою мобільного додатка на базі ESET Secure Authentication.

Об'єкт дослідження – багатофакторна автентифікація користувачів інформаційними системами організацій.

Предмет дослідження – методи та засоби багатофакторної автентифікації

користувачів за допомогою мобільного додатка на базі ESET Secure Authentication.

Мета роботи – розробити рекомендації щодо застосування методів та засобів багатофакторної автентифікації користувачів за допомогою мобільного додатка на базі ESET Secure Authentication.

Наукові завдання:

дослідити сутність проблеми автентифікації користувачів інформаційними системами організацій;

проаналізувати підходи до автентифікації користувачів інформаційними системами організацій;

проаналізувати існуючі рішення для багатофакторної автентифікації користувачів;

проаналізувати методи та засоби багатофакторної автентифікації користувачів за допомогою мобільного додатка на базі ESET Secure Authentication;

розкрити порядок застосування методів та засобів багатофакторної автентифікації користувачів за допомогою мобільного додатка на базі ESET Secure Authentication.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння.

Практичне значення одержаних результатів: запропоновано порядок застосування методів та засобів багатофакторної автентифікації користувачів за допомогою мобільного додатка на базі ESET Secure Authentication, а також розроблено рекомендації фахівцям з кібербезпеки щодо її реалізації.

1 ДОСЛІДЖЕННЯ ПРОБЛЕМИ АВТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ ІНФОРМАЦІЙНИМИ СИСТЕМАМИ ОРГАНІЗАЦІЙ

1.1. Дослідження проблеми автентифікації користувачів інформаційними системами організацій

За даними Statista [3] у 2024 році кількість випадків витоку даних у Сполучених Штатах становила 3158. Тим часом понад 1,35 мільярда осіб постраждали того ж року від витоків даних, включаючи порушення безпеки даних, витік та розкриття інформації (рисунок 1.1). Хоча це три різні події, вони мають одну спільну рису. *В результаті всіх трьох інцидентів доступ до конфіденційних даних отримує неавторизований зловмисник*.

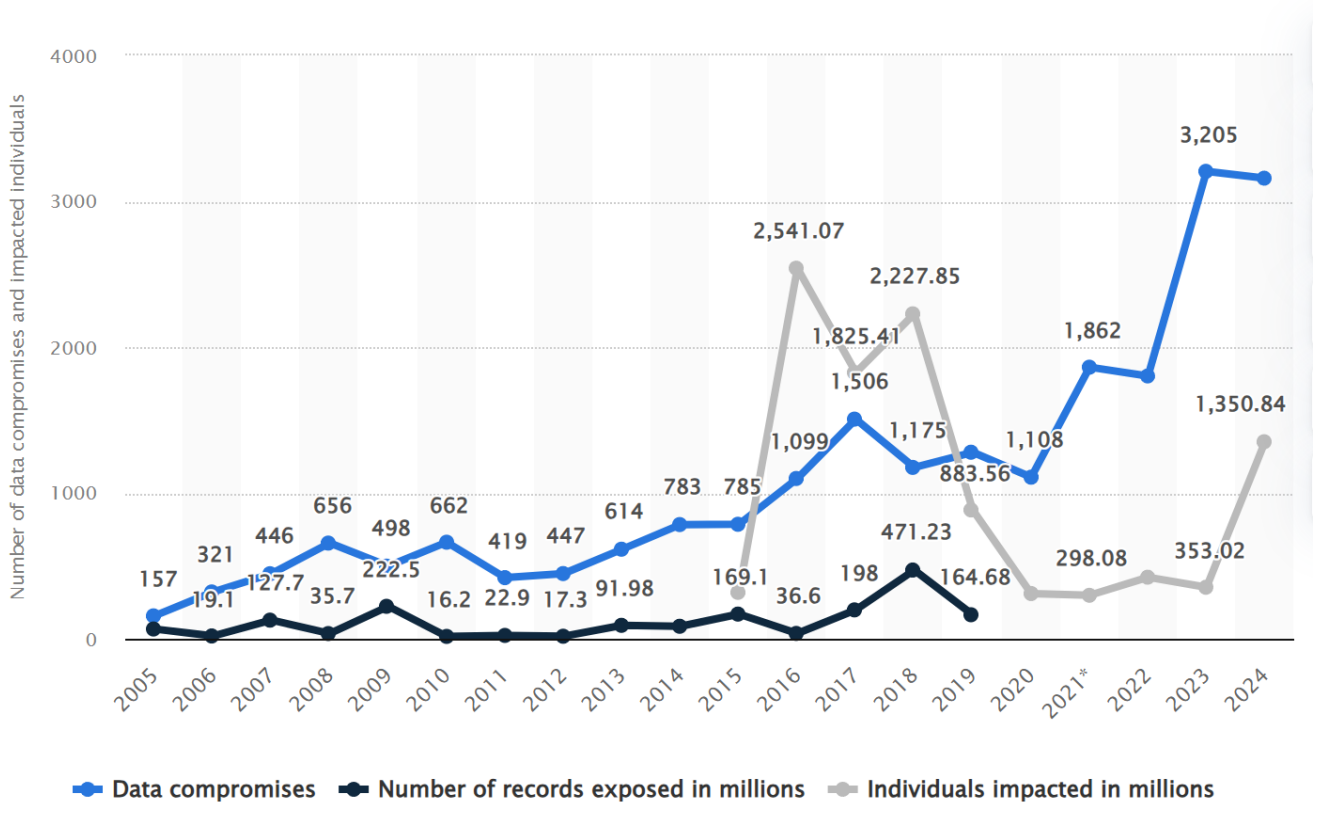

Рис. 1.1. Щорічна кількість витоків даних та кількість постраждалих осіб у Сполучених Штатах з 2005 по 2024 рік за даними Statista [2]

У деяких галузях промисловості зазвичай спостерігається більше значних

випадків порушення конфіденційності персональних даних, ніж в інших. Це визначається типом та обсягом персональної інформації, яку зберігають організації цих галузей. У 2024 році фінансові послуги, охорона здоров'я та професійні послуги були трьома галузями промисловості, в яких було зафіксовано найбільше порушень даних. Загалом, кількість порушень даних у сфері охорони здоров'я в деяких галузях промисловості Сполучених Штатів поступово зростала протягом останніх кількох років. Однак у деяких галузях спостерігалося зменшення [3].

У 2020 році веб-сайт потокового відео для дорослих CAM4 зазнав витоку майже 11 мільярдів записів. Це, безумовно, наймасштабніший зареєстрований витік даних. Однак цей випадок унікальний, оскільки дослідники з кібербезпеки виявили вразливість раніше за кіберзлочинців. Другим за величиною витоком даних є витік даних Yahoo, що датується 2013 роком. Спочатку компанія повідомила про один мільярд викритих записів, а пізніше, у 2017 році, опублікувала оновлену кількість витіків записів, яка склала три мільярди. У березні 2018 року стався третій за величиною витік даних, пов'язаний з національною ідентифікаційною базою даних Індії Aadhaar. В результаті цього інциденту було викрито понад 1,1 мільярда записів [3].

В [1] зазначається, що ще більше тривожить усвідомлення того, що понад 82% порушень були спричинені проблемами автентифікації – викраденими або ненадійними обліковими даними.

Вразливості автентифікації – це проблеми, які впливають на процеси автентифікації та роблять веб-сайти й додатки вразливими до атак безпеки, під час яких зловмисник може маскуватися під законного користувача.

Автентифікація є життєво важливою частиною будь-якого веб-сайту чи додатка, оскільки це просто процес розпізнавання ідентифікації користувачів [1].

Кілька поширених категорій проблем автентифікації можуть виникнути через вразливості в облікових даних для входу, захисті сайту або навіть базовому коді. Існує кілька способів виникнення вразливостей автентифікації, найпоширенішими з яких є нехтування областями ризику, помилки в коді або

логіці та неправильний вибір користувача, що може поєднуватися з двома попередніми. Якщо програма має поганий захист методом грубої сили, зловмисники можуть скористатися цим, щоб отримати доступ навіть до добре захищених облікових записів або дешевий масовий доступ до погано захищених. Так само, якщо є логічні помилки або помилки коду, зловмисники можуть обійти частину або весь процес автентифікації [1].

Вразливості автентифікації мають серйозні наслідки – чи то через слабкі паролі, чи то через поганий дизайн та реалізацію автентифікації. Зловмисники можуть використовувати ці вразливості, щоб отримати доступ до систем та облікових записів користувачів, щоб [1]:

здійснити крадіжку конфіденційної інформації;

маскуватися під законного користувача;

отримати контроль над додатком;

вивести з ладу систему повністю.

Якщо зловмисники можуть незаконно пройти процес автентифікації та отримати доступ до облікового запису користувача, вони можуть викрасти критично важливі дані, такі як імена, дані кредитних карток, номери соціального страхування (SSN), медичні записи та ідентифікаційні номери платників податків. Вони також можуть виконувати дії від імені користувача, такі як ініціювання фінансових транзакцій, видалення даних або передача права власності на ресурси.

Що ще гірше, зловмисники можуть повністю контролювати інформаційну систему або повністю її вимкнути, якщо знайдуть доступ до облікових записів верхнього рівня, таких як профілі адміністраторів. Після появи ці вразливості автентифікації можуть суттєво вплинути на життєздатність та довіру до компанії.

Крім того, організації можуть зіткнутися з юридичними наслідками відповідно до GDPR, CCPA, правил фінансових послуг або інших місцевих законів, залежно від того, який тип даних було вилучено [1].

Вразливості автентифікації, якщо їх належним чином не контролювати, можуть зашкодити не лише безпеці компанії, але й її репутації. Розглянемо найпоширеніші вразливості автентифікації.

Недосконалий захист від атак грубої сили. Атака методом перебору (атака за словником) є спробою отримати незаконний доступ до системи або облікового запису користувача шляхом введення великої кількості випадково згенерованих або попередньо згенерованих комбінацій імен користувачів та паролів, доки не буде знайдено ту, яка працює.

Якщо існує недосконала система захисту від методу грубої сили, тобто яка має недолік у логіці автентифікації, брандмауері або протоколі захищеної оболонки (SSH), зловмисники можуть викрасти облікові дані та процеси для входу, поставивши під загрозу безпеку облікових даних користувачів [1].

Слабкі дані для входу. Коли користувачі реєструють обліковий запис на сайті або в додатку, що використовує вхід на основі пароля, їм пропонується створити ім’я користувача та пароль. Однак, якщо пароль передбачуваний, це може призвести до вразливостей у процесі автентифікації. Передбачувані імена користувачів можуть полегшити зловмисникам атаку на певних користувачів.

Замість повноцінної атаки методом перебору, зловмисники шукатимуть облікові записи з паролями, які легко вгадати, але які використовуються занадто часто. Вони спробують використовувати поширені облікові дані, такі як «admin», «admin1» та «password1». Без обмежень щодо слабких паролів, навіть сайти, захищені від атак методом перебору, можуть бути скомпрометовані.

Перерахування імен користувачів. Перерахування імен користувачів не є саме вразливістю автентифікації. Однак воно може полегшити життя зловмиснику, знизивши вартість інших атак, таких як атаки методом повного перебору або слабкі перевірки облікових даних. Цей процес перерахування імен користувачів підтверджує, чи є ім’я користувача дійсним. [1].

Проблема з перерахуванням імен користувачів полягає в тому, що зловмисники можуть визначити, які імена користувачів є дійсними. Потім вони можуть спробувати зламати дійсні облікові записи користувачів за допомогою методів грубої сили, не витрачаючи свій час і гроші на перевірку безлічі недійсних імен облікових записів.

Базова автентифікація HTTP. Цей класичний протокол веб-автентифікації

легко реалізувати, проте він не позбавлений своїх ризиків.

Базова HTTP-автентифікація проста: з кожним запитом надсилаються ім'я користувача та пароль. Однак, якщо відповідні протоколи безпеки, такі як шифрування сеансу TLS, не використовуються для всього зв’язку, інформація про ім’я користувача та пароль може надсилатися у відкритому вигляді, що полегшує зловмисникам крадіжку облікових даних.

Оскільки включені облікові дані містять так мало контексту, їх можна легко використати в таких атаках, як підробка міжсайтових запитів (CSRF). Крім того, оскільки вони включені до кожного запиту, сучасні браузери зазвичай кешують цю інформацію необмежено довго, з мінімальною можливістю «вийти з системи» та запобігти повторному використанню облікових даних локальним зловмисником у майбутньому [1].

Погане управління сеансом. Вразливість в управлінні ідентифікаторами сеансів призводить до перехоплення дійсних автентифікованих сеансів. Це одна з поширених веб-вразливостей для обходу паролів.

Існує кілька вразливостей, пов’язаних з неправильним керуванням сеансами, таких як відсутність тайм-аутів сеансу, розкриття ідентифікаторів сеансу в URL-адресах, файли cookie сеансу без встановленого прапорця Http-Only та неналежнаануляція сеансу [1].

Якщо зловмисники можуть захопити контроль над існуючим сеансом, вони легко потрапляють у систему, припускаючи особу вже автентифікованого користувача, повністю минаючи процес автентифікації.

Залишатися в системі. Прапорець «Запам’ятати мене» або «Залишатися в системі» під формою входу дуже спрощує процес входу в систему після закриття сеансу. Він генерує файл cookie, який дозволяє пропустити процес входу.

Однак це може призвести до вразливості автентифікації на основі файлів cookie, якщо зловмисник може передбачити файл cookie або визначити шаблон його генерації. Вони можуть використовувати шкідливі методи, такі як атаки методом перебору, для прогнозування файлів cookie та міжсайтовий скриптинг (XSS) для злому облікових записів користувачів, дозволяючи шкідливому серверу

використовувати легітимний файл cookie [1].

Якщо файл cookie погано розроблений або захищений, зловмисники можуть отримати паролі або інші конфіденційні (та захищені законом) дані, такі як адреси користувачів або інформацію про обліковий запис, зі збереженого файлу cookie.

SQL-ін'єкція. SQL-ін'єкція – це вектор атаки, який використовує введення шкідливого SQL-коду неочікуваним чином для маніпулювання базою даних та доступу до неї.

SQL-ін'єкції можуть уможливлювати атаки на механізми автентифікації шляхом крадіжки відповідних даних (таких як погано захищені хеші паролів) із незахищеної бази даних. Вони також можуть обходити механізми автентифікації, якщо введений SQL-код виконується внутрішнім (і вже авторизованим) інструментом, який не зміг достатньо перевірити зовнішній вхід [1].

Незахищена зміна та відновлення пароля. Іноді користувачі забувають або просто хочуть змінити свої паролі та натискають посилання «Забули пароль» або «Втратили пароль».

Процес скидання пароля створює вразливість для автентифікації, якщо програма використовує слабкий механізм відновлення пароля, такий як прості контрольні питання, відсутність CAPTCHA або електронні листи для скидання пароля з надто довгим або відсутнім часом очікування.

Якщо функція відновлення пароля має недоліки, зловмисники можуть потенційно використовувати методи грубої сили або доступ до інших скомпрометованих облікових записів, щоб отримати доступ до облікових записів користувачів та облікових даних, які добре захищені за звичайних обставин.

Недосконала двофакторна автентифікація. Хоча двофакторна автентифікація (2FA) є ефективною для безпечної автентифікації, вона може спричинити критичні проблеми безпеки, якщо її не реалізувати належним чином.

Зловмисники можуть з'ясувати чотири- та шестизначні коди перевірки 2FA за допомогою атак заміни SIM-картки, якщо вони надсилаються через SMS. Деяка двофакторна автентифікація також не є справді двофакторною; якщо користувач намагається отримати доступ до конфіденційної інформації на викраденому

телефоні, використовуючи кешовані облікові дані, «другий фактор», який надсилає повідомлення на той самий телефон, не додає додаткової безпеки.

Вразливості двофакторної автентифікації також можуть виникати, якщо немає захисту методом перебору, який би блокував обліковий запис після певної кількості спроб входу.

Вразлива логіка автентифікації. Логічні вразливості є поширеними в програмних застосунках. Це трапляється в результаті поганого кодування або дизайну, що впливає на автентифікацію та авторизацію доступу, а також на функціональність застосунків.

Недосконала логіка застосунку може бути пов’язана зі зловживанням функціональністю, слабкими заходами безпеки або пропущеним кроком у процедурі перевірки. Наприклад, програма може запропонувати користувачеві відповісти на контрольне запитання, яке, за логікою, «може знати лише потрібна людина». Але такі запитання, як дата народження користувача чи дівоче прізвище матері, часто легко виявити. Ця вразливість дозволяє кіберзлочинцям легко обійти автентифікацію та отримати незаконний доступ до таких облікових записів [1].

Людська недбалість. Згідно зі звітом Shred-it за 2020 рік, до 31% керівників вищої ланки повідомили, що недбалість співробітників є другою основною причиною витоку їхніх даних [1].

Людська помилка може призвести до серйозних вразливостей автентифікації, якими набагато легше скористатися, ніж атаки методом перебору, SQL-ін’єкції та обхід автентифікації. Ця недбалість включає такі дії, як [1]:

залишення комп’ютера увімкненим та незамкненим у громадському місці;

втрата пристроїв через крадіжку;

витік конфіденційної інформації незнайомцям;

написання поганого коду.

Отже, вразливості автентифікації – незалежно від того, чи пов’язані вони з безпекою веб-сайтів чи додатків, чи доступом до інфраструктури – є критичними проблемами кібербезпеки, які потребують своєчасного виявлення та запобігання.

1.2. Аналіз підходів до автентифікації користувачів інформаційними системами організацій

Фахівці Palo Alto Networks [4] зазначають, що впровадження багатофакторної автентифікації (Multi-Factor Authentication, MFA) передбачає інтеграцію системи безпеки, яка вимагає від користувачів підтвердження своєї особи за допомогою двох або більше факторів автентифікації, таких як паролі, біометричні дані або одноразові коди. На відміну від однофакторної автентифікації, яка зазвичай спирається лише на пароль, MFA використовує щонайменше два незалежні облікові дані (рисунок 1.2):

щось, що знає користувач (наприклад, пароль);

щось, що є у користувача (наприклад, смартфон для одноразового пароля);

щось, чим є користувач (біометричні дані, такі як відбитки пальців або розпізнавання обличчя).

Це покращує контроль доступу та захищає конфіденційні дані, додаючи рівні безпеки, зменшуючи ризик несанкціонованого доступу та кібератак.

Рис. 1.2. Принцип багатофакторної автентифікації [4]

У сучасному цифровому середовищі кіберзагрози є більш складними та поширеними, ніж будь-коли, що робить критично важливим для організацій впровадження комплексних заходів безпеки. Багатофакторна автентифікація (MFA) є життєво важливою для зміцнення кібербезпеки, значно зменшуючи ймовірність несанкціонованого доступу [4].

Оскільки кіберзлочинці постійно вдосконалюють свою тактику, покладатися на один рівень безпеки, такий як пароль, більше недостатньо. Такий багаторівневий підхід підвищує безпеку, ускладнюючи зловмисникам доступ до системи. Він також забезпечує спокій компаніям та їхнім клієнтам, знаючи, що їхня інформація захищена нестандартними засобами.

Крім того, багатофакторна автентичність (MFA) має вирішальне значення для дотримання вимог та стандартів, встановлених різними регуляторними органами. Вона гарантує, що організації захищають свої дані та дотримуються найкращих практик у сфері інформаційної безпеки. Інтегруючи MFA, компанії значно підвищують свою стійкість до витоків даних та несанкціонованого доступу до облікових записів, захищаючи свою репутацію та фінансову стабільність.

Впровадження багатофакторної автентифікації (MFA) пропонує численні ключові переваги, які значно посилюють безпеку на різних цифрових платформах [4]:

ефективно зменшує ризик витоку даних та несанкціонованого доступу;

підтримує відповідність галузевим нормам і стандартам, таким як GDPR та PCI DSS;

має вирішальне значення для уникнення штрафів та пені, пов’язаних з недотриманням вимог;

підтримує довіру та авторитет з клієнтами та партнерами;

вимагає кількох методів перевірки, що надзвичайно ускладнює зловмисникам доступ до конфіденційної інформації;

діє як стримуючий фактор проти потенційних кібератак, оскільки складність відлякує зловмисників;

покращує загальний користувацький досвід;

забезпечує безперервність бізнесу та захищає цінні дані.

В [6] зазначається, що органи з кібербезпеки, такі як ANSSI (Національне агентство з безпеки інформаційних систем) або ENISA (Агентство Європейського Союзу з кібербезпеки), наголошують на важливості багатофакторної автентифікації як основного захисту від кіберзагроз, особливо для привілейованих облікових записів та чутливих систем.

Двофакторна автентифікація (2FA) – це найдавніша та найпоширеніша форма багаторівневої безпеки, яка вимагає від користувачів двічі підтверджувати свою особу. Хоча сучасні системи багатофакторної автентифікації є ефективними, вони виходять за рамки двох факторів, додаючи додаткові рівні перевірки для посилення захисту від загроз, що постійно змінюються.

Отже, коли варто використовувати MFA замість 2FA? Якщо ви входите у Facebook, 2FA, ймовірно, достатньо. Але якщо ми маємо справу з фінансовими даними, конфіденційними корпоративними обліковими записами або хмарною інфраструктурою, то варто перейти на новий рівень [6].

Таблиця 1.1

Порівняння 2FA та MFA [6]

Feature	2FA	MFA
Minimum Authentication Factors	2	2 or more
Security Level	Moderate	High
Resistance to Phishing	Medium to Low	High depending on the type of method
Common Methods	SMS OTP, Email OTP, App OTP	Hardware tokens, biometrics, risk-based authentication
Best Use Cases	Standard user authentication	High-security environments, compliance-driven industries

Існують різні методи MFA, кожен з яких пропонує різний рівень безпеки та зручності (рисунок 1.3).

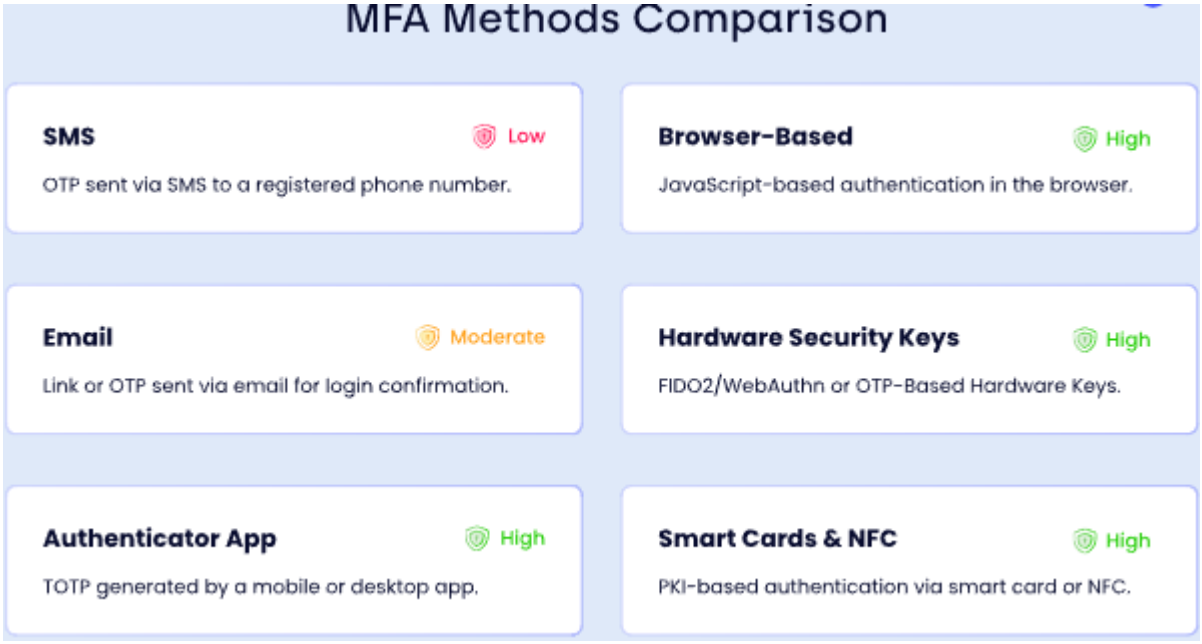

Рис. 1.3. Методи MFA [6]

Окрім вибору методу автентифікації, організації можуть оптимізувати своє впровадження за допомогою [6]:

адаптивна автентифікація: налаштовує вимоги безпеки на основі факторів ризику (наприклад, пристрій, місцезнаходження, поведінка під час входу), щоб збалансувати безпеку та взаємодію з користувачем;

безпарольна автентифікація: повністю виключає паролі, покладаючись на біометричні дані, ключі безпеки або токен браузера для багатофакторної автентифікації, стійкої до фішингу;

підвищена автентифікація: посилює безпеку доступу на основі політик, зазвичай для дій з високим ризиком або конфіденційністю (наприклад, великі фінансові транзакції, зміни в обліковому записі);

безперервна автентифікація: моніторить поведінку користувача протягом сеансу (наприклад, динаміку натискання клавіш, рухи миші) для виявлення аномалій та запобігання перехопленню сеансу;

автентифікація на основі ризику (Risk-Based Authentication, RBA):

використовує машинне навчання та історичні дані користувачів, щоб визначити, коли потрібні додаткові кроки перевірки.

Провідні дослідницькі фірми з кібербезпеки, такі як Gartner, та регуляторні органи, такі як ANSSI, наголошують на переході до безпарольної автентифікації як ключовому досягненні безпеки. Їхні рекомендації узгоджуються зі світовими тенденціями, що виступають за сильніші, стійкі до фішингу методи [6].

Хоча безпека є головним пріоритетом для підприємств, впровадження багатофакторної автентифікації іноді може впливати на робочі процеси співробітників. Щоб збалансувати безпеку та продуктивність, організації впроваджують рішення для автентифікації на основі ризиків, адаптивної автентифікації або навіть єдиного входу (SSO). Підходи, які гарантують, що безпека не перешкоджає операційній ефективності, зберігаючи при цьому надійний захист від несанкціонованого доступу [6].

Для компаній, що надають онлайн-послуги, багатофакторна автентифікація відіграє вирішальну роль у захисті облікових записів клієнтів та конфіденційних транзакцій. Однак впровадження таких рішень для клієнтів має здійснюватися з урахуванням зручності використання, щоб запобігти розчаруванню та відмовим. Прекрасним прикладом є компанії, які використовують безпарольну або посилену автентифікацію для підвищення безпеки, зберігаючи при цьому безперебійний досвід [6].

Організації, що співпрацюють зі сторонніми постачальниками, постачальниками або партнерами, повинні запроваджувати суворі політики багатофакторної автентифікації, щоб запобігти несанкціонованому доступу до внутрішніх систем. Ризиково-орієнтована багатофакторна автентифікація (MFA), федеративне управління ідентифікацією та єдиний вхід (SSO) є ключовими стратегіями для забезпечення доступу партнерів, одночасно забезпечуючи безперебійний процес входу. Як і співробітники, партнери потребують відповідного контролю доступу, але їхні потреби в перевірці особистості можуть відрізнятися, що робить детальне застосування автентифікації важливим, щоб гарантувати, що вони підтверджують свою особу лише тоді, коли це необхідно

для доступу до певних програм або даних [6].

В [5] зазначається, що багатофакторна автентифікація (MFA) може бути адаптивною, забезпечуючи гнучкість у безпеці. Наприклад, доступ до менш конфіденційних даних може вимагати менше факторів автентифікації, тоді як більш конфіденційна інформація може активувати додаткові методи автентифікації. Така адаптивність не лише підвищує безпеку, але й покращує взаємодію з користувачем, не створюючи зайвих бар'єрів для дій з меншим ризиком.

Найочевиднішим фактором багатофакторної автентифікації є пароль. Багато рішень MFA досі використовують паролі в поєднанні з іншими факторами, тоді як інші повністю безпарольні. Ось поширені фактори, що використовуються для доповнення або заміни традиційної автентифікації за паролем [5].

Коди електронної пошти. Поширеним методом багатофакторної автентифікації (MFA) є використання кодів електронної пошти. Під час спроби входу на вашу зареєстровану адресу електронної пошти надсилається унікальний код. Потім нам потрібно ввести цей код на сторінці входу, щоб підтвердити свою особу.

Перевага кодів електронної пошти полягає в тому, що вони прості та зручні для кінцевих користувачів. Однак безпека цього методу залежить від надійності захисту облікового запису електронної пошти. Якщо обліковий запис електронної пошти скомпрометовано, то й цей метод багатофакторної автентифікації також скомпрометовано. Тому вкрай важливо забезпечити користувачам надійні заходи безпеки.

Одноразові паролі (OTP) для текстових повідомлень та дзвінків. Ще одним поширеним методом багатофакторної автентифікації (MFA) є використання одноразових паролів (OTP), що надсилаються через текстове повідомлення або телефонний дзвінок. Коли ви намагаєтеся ввійти, OTP надсилається на ваш зареєстрований номер мобільного телефону. Потім ми повинні ввести цей OTP на сторінці входу, щоб підтвердити свою особу.

Хоча цей метод також простий у використанні, він вразливий до шахрайства

із заміною SIM-картки, коли шахрай переконує телефонну компанію призначити номер телефону новій SIM-картці. Після успіху шахрай може отримувати одноразові паролі, фактично обходячи цей рівень безпеки. Тому користувачам вкрай важливо захищати свої номери телефонів і знати про ознаки шахрайства із заміною SIM-картки.

Біометрична перевірка. Біометрична верифікація – це швидкозростаючий метод багатофакторної автентифікації (MFA). Вона передбачає використання унікальних фізичних або поведінкових характеристик для підтвердження особи користувача. Ці характеристики можуть включати відбитки пальців, розпізнавання обличчя, розпізнавання голосу та навіть сканування сітківки ока.

Перевага біометричної верифікації полягає в тому, що біометричні дані важко підробити або вкрасти, оскільки вони унікальні для кожної людини. Однак хакери вже знаходять способи маніпулювати біометричною верифікацією або обходити її. Це також викликає занепокоєння щодо конфіденційності, оскільки біометричні дані є дуже конфіденційними, їх необхідно зберігати безпечно та використовувати лише для цілей автентифікації.

Програми для автентифікації. Програми-автентифікатори – це відносно новий, але дедалі популярніший метод багатофакторної автентифікації (MFA). Ці програми генерують одноразові паролі (OTP), які потім вводяться на сторінці входу для підтвердження вашої особи. Перевага цього методу полягає в тому, що він не залежить від номера телефону чи облікового запису електронної пошти, які можуть бути скомпрометовані.

Однак, як і будь-який інший метод багатофакторної автентифікації (MFA), програми для автентифікації не є надійними. Вони залежать від безпеки мобільного пристрою та самої програми. Тому вкрай важливо оновлювати операційні системи пристроїв і програму та захищати їх за допомогою надійних заходів безпеки.

Магічні посилання. Магічні посилання – це зручний метод багатофакторної автентифікації (MFA), який передбачає надсилання унікального посилання з обмеженим часом дії на адресу електронної пошти користувача. Коли користувач

намагається увійти, він отримує це посилання, яке безпосередньо автентифікує його після натискання. Це обходить необхідність введення пароля чи коду.

Магічні посилання пропонують простоту та зручність, оскільки вони зменшують кількість кроків, необхідних для автентифікації. Однак їхня безпека залежить від безпеки облікового запису електронної пошти користувача. Якщо обліковий запис електронної пошти скомпрометовано, магічне посилання може бути перехоплене. Крім того, існує ризик фішингових атак, коли користувачів можуть обманом змусити перейти за шкідливими посиланнями.

Вхід через соціальні мережі. Вхід через соціальні мережі – це метод багатофакторної автентифікації (MFA), який дозволяє користувачам проходити автентифікацію за допомогою своїх існуючих облікових записів у соціальних мережах, таких як Facebook, Google або LinkedIn. Замість створення нового імені користувача та пароля користувачі можуть входити, використовуючи свої облікові дані в соціальних мережах. Цей метод зазвичай включає додаткові перевірки безпеки платформою соціальних мереж, такі як одноразові паролі або підтвердження електронною поштою.

Цей метод багатофакторної автентифікації популярний завдяки своїй зручності, оскільки більшість користувачів вже мають облікові записи в соціальних мережах і знайомі з їхніми інтерфейсами. Однак він залежить від безпеки платформи соціальних мереж та здатності користувача підтримувати надійний захист облікового запису. Крім того, існують проблеми конфіденційності, оскільки пов’язування автентифікації з обліковими записами в соціальних мережах може призвести до відстеження та профілювання даних користувачів третіми сторонами.

Комплекти розробки програмного забезпечення (SDK) для м’яких токенів. Комплекти розробки програмного забезпечення (SDK) для м’яких токенів є однією з найуніверсальніших форм багатофакторної автентифікації (MFA). Вони дозволяють компаніям вбудовувати функції безпеки безпосередньо у свої додатки, забезпечуючи додатковий рівень захисту для користувачів. Ці м’які токени зазвичай генеруються за допомогою застосунку для смартфонів і

регулярно змінюються, що ускладнює для зловмисників їх прогнозування або дублювання.

SDK також забезпечують гнучкість у налаштуванні, дозволяючи компаніям адаптувати процес автентифікації до своїх потреб. З точки зору зручності користувача, SDK з м'якими токенами часто є кращими, оскільки вони не потребують додаткового обладнання. Користувачі можуть використовувати свої існуючі пристрої, що робить процес автентифікації безперебійним та зручним.

Смарт-картки та криптографічні апаратні токени. Ще однією формою багатофакторної автентифікації (MFA) є використання смарт-карт та криптографічних апаратних токенів. Ці фізичні пристрої забезпечують додатковий рівень безпеки, гарантуючи, що доступ до захищеної системи зможуть отримати лише ті, хто володіє токеном.

Смарт-картки – це пристрої розміром з кредитну картку, оснащені вбудованим чіпом. Цей чіп може зберігати та обробляти дані, що робить його безпечним методом автентифікації. Криптографічні апаратні токени – це невеликі пристрої, які зазвичай поміщаються в кишеню та генерують унікальний код через певні проміжки часу. Цей код необхідно ввести для отримання доступу до системи.

Хоча ці методи забезпечують високий рівень безпеки, вони мають деякі потенційні недоліки. Наприклад, їх можна втратити або викрасти, що потенційно може надати неавторизованим особам доступ до вашої системи. Крім того, їх впровадження та обслуговування можуть бути дорогими, особливо для великих організацій.

Використання контрольних питань. Контрольні питання – це набагато простіша форма багатофакторної автентифікації, але вони все ще можуть бути ефективними за умови правильного використання. Це питання, на які відповідь повинен знати лише користувач, наприклад, ім'я домашнього улюбленця або перший роботодавець користувача.

Однак важливо зазначити, що контрольні питання ніколи не слід використовувати як єдиний спосіб автентифікації. Їх найкраще використовувати в

поєднанні з іншими методами, такими як пароль або сканування відбитків пальців. Це пояснюється тим, що відповіді на контрольні питання часто можна вгадати або отримати за допомогою методів соціальної інженерії.

Адаптивна автентифікація. Строго кажучи, адаптивна автентифікація не є ще одним методом автентифікації. Однак її можна використовувати для розумного використання перелічених вище методів. Адаптивна автентифікація налаштовує необхідний рівень автентифікації залежно від ризику, пов'язаного з певною дією.

Наприклад, користувач може мати доступ до програми з низьким рівнем ризику, використовуючи лише ім’я користувача та пароль. Однак, якщо він спробує отримати доступ до програми з високим рівнем ризику, йому потрібно буде надати додаткову автентифікацію, таку як відбиток пальця або одноразовий пароль. Аналогічно, користувачеві може знадобитися лише два фактори автентифікації для доступу до своєї банківської програми, але під час спроби здійснити фінансовий переказ його можуть попросити ввести третій фактор автентифікації.

Цей метод є корисним, оскільки покращує взаємодію з користувачем, не вимагаючи зайвої автентифікації. Однак, він також гарантує достатній захист дій з високим рівнем ризику.

Отже, 2FA – це базова форма MFA, але сучасні реалізації часто виходять за рамки двох факторів для посилення безпеки. Багатофакторна автентифікація має вирішальне значення для захисту від кіберзагроз, виконання нормативних вимог та покращення перевірки особи. Не всі методи багатофакторної автентифікації (MFA) пропонують однаковий рівень безпеки – автентифікація на основі SMS менш безпечна, ніж апаратні токени або біометричні дані.

Адаптивна та ризик-орієнтована автентифікація підвищує безпеку, динамічно оцінюючи контекст доступу. Безпека на основі штучного інтелекту та поведінкова біометрія формують майбутнє багатофакторної автентифікації (MFA), зменшуючи залежність від традиційних паролів. Впровадження MFA повинно балансувати між безпекою та зручністю використання , щоб уникнути

втоми користувачів та проблем із впровадженням.

1.3. Аналіз існуючих рішень для багатофакторної автентифікації користувачів інформаційними системами організацій

В [7] зазначається, що оскільки кіберзагрози продовжують виникати та розвиватися, компанії будь-якого розміру усвідомлюють критичну важливість впровадження надійних заходів безпеки. Один із найпростіших та найефективніших способів захисту цифрових активів будь-якої компанії – це впровадження багатофакторної автентифікації (MFA).

Ось деякі ключові характеристики, які слід враховувати під час оцінки потенційних постачальників багатофакторної автентифікації (MFA) [7]:

зручний інтерфейс. Рішення MFA зі зручним інтерфейсом може значно покращити впровадження та зменшити труднощі для співробітників. Шукайте постачальників, які пропонують інтуїтивно зрозумілі процеси реєстрації, чіткі підказки та прості у використанні методи автентифікації. Позитивний користувацький досвід може значною мірою сприяти тому, щоб MFA стала безперебійною частиною щоденного життя співробітників;

попередньо створені API та інтеграції. Рішення MFA, яке пропонує попередньо вбудовані API та інтеграції з програмами та сервісами, які організація вже використовує. Це значно спростить впровадження та забезпечить сумісність у технологічному стеку. Наприклад, якщо організація значною мірою залежить від Google Workspace, розумним вибором буде вибір постачальника MFA, такого як Google Authenticator, який безперешкодно інтегрується з екосистемою Google;

масштабованість та гнучкість. У міру зростання та розвитку організації рішення MFA повинно мати можливість масштабуватися та адаптуватися відповідно. Треба обирати постачальника, який пропонує гнучкість для врахування змін у робочому колективі, таких як додавання нових співробітників, зміна політик доступу або інтеграція з новими програмами. Масштабоване рішення MFA допоможе підтримувати надійний рівень безпеки, навіть коли

компанія зазнає значних змін;

хмарна багатофакторна автентифікація (MFA). Хмарні рішення MFA пропонують кілька переваг порівняно з локальними альтернативами, включаючи легшу масштабованість, автоматичні оновлення та менші вимоги до обслуговування. Вони також забезпечують більшу гнучкість, дозволяючи співробітникам безпечно отримувати доступ до ресурсів компанії з будь-якого місця, де є підключення до Інтернету;

кілька методів автентифікації. Не всі методи автентифікації однаково зручні та безпечні. Деякі користувачі можуть надавати перевагу простоті кодів на основі SMS, тоді як інші надають пріоритет додатковій безпеці апаратних токенів. Найкращі рішення MFA пропонують низку варіантів автентифікації для задоволення різних уподобань та потреб безпеки.

По суті, завдяки інструментам багатофакторної автентифікації (MFA) компанії мають додатковий рівень захисту своїх облікових записів. Це допомагає гарантувати, що кожен, хто отримує доступ до інформації компанії, справді є тим, за кого себе видає, що допомагає зменшити ризик компрометації облікового запису або втрати конфіденційних даних [8].

Програмне забезпечення MFA може перевірити кожного, хто намагається отримати доступ до інформації компанії, забезпечуючи надійну безпеку та зменшуючи ризик компрометації облікового запису. Користувачі зазвичай автентифікуються за допомогою застосунку, одноразового пароля (OTP), пристрою FIDO2 або біометричних даних, таких як розпізнавання обличчя або сканування відбитків пальців [8].

Багатофакторна автентифікація (MFA) розгортається як частина ширшого стеку ідентифікації робочої сили. Рішення для керування ідентифікацією та доступом (IAM) зазвичай включають єдиний вхід (SSO), автентифікацію без пароля, стійку до фішингу, та реєстрацію/відключення користувачів.

Розгортання MFA передбачає додаткову роботу для кінцевих користувачів, тому важливо шукати рішення з низьким тертям, а також безпечне [8].

ManageEngine ADSelfService Plus – це надійний менеджер паролів, рішення

для кінцевих точок MFA та SSO, яке захищає доступ до різних IT-ресурсів, включаючи комп'ютери, VPN, програми, кінцеві точки та Outlook Web Access. Він розроблений для захисту від атак на основі облікових даних шляхом застосування багатофакторної автентифікації (MFA) та ввімкнення єдиного входу (SSO) [8].

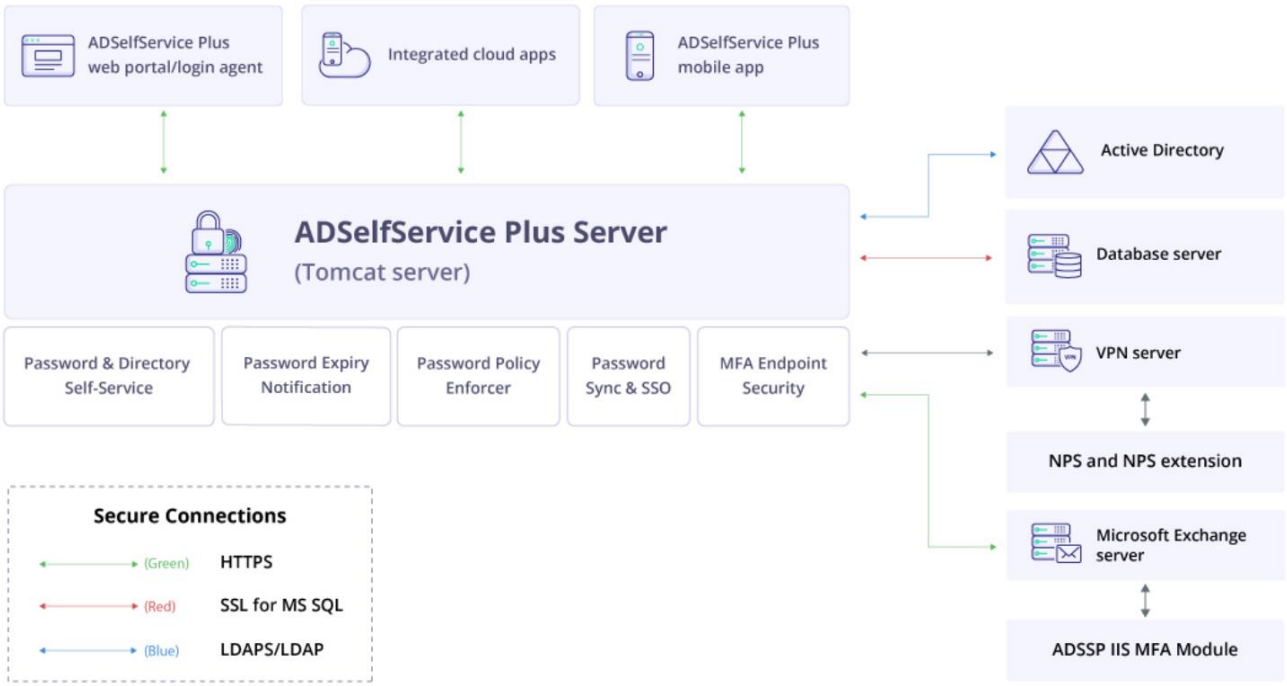

Рис. 1.4. Архітектура рішення ManageEngine ADSelfService Plus [9]

ManageEngine ADSelfService Plus є здатним захищати кілька точок доступу за допомогою безпечної багатофакторної автентифікації (MFA) та єдиного входу (SSO), а також інтеграцію з Active Directory для легшого розгортання та реєстрації користувачів.

Найкращі функції ManageEngine ADSelfService Plus включають гнучке самообслуговування для багатофакторної автентифікації (MFA) та керування паролями, надійні політики умовного доступу та підтримку різних факторів автентифікації, таких як контрольні питання, SMS, коди електронної пошти, програми-автентифікатори, апаратні токени безпеки, QR-коди, відбитки пальців та розпізнавання обличчя. Його можна розгортати на серверах або комп'ютерах, а також він легко інтегрується з Active Directory [8].

Перевагами рішення ManageEngine ADSelfService Plus є [8]:

захищає кілька точок доступу за допомогою MFA та SSO;

легке розгортання та адаптація через інтеграцію з Active Directory;

гнучкі варіанти самообслуговування для автентифікації;

підтримує широкий спектр факторів автентифікації;

забезпечує надійні політики умовного доступу.

Рішення ManageEngine ADSelfService Plus найкраще підходить для великих організацій, особливо у таких галузях, як фінанси, IT, охорона здоров'я та державне управління, яким потрібні комплексні рішення для захисту ідентифікаційних даних [8].

Cisco Duo Security – це платформа керування доступом, яка запобігає ризикам безпеки на основі облікових даних і допомагає дотримуватися нормативних вимог. Вона пропонує багатофакторну автентифікацію (MFA), єдиний вхід (SSO), видимість пристроїв і безпечний віддалений доступ [8].

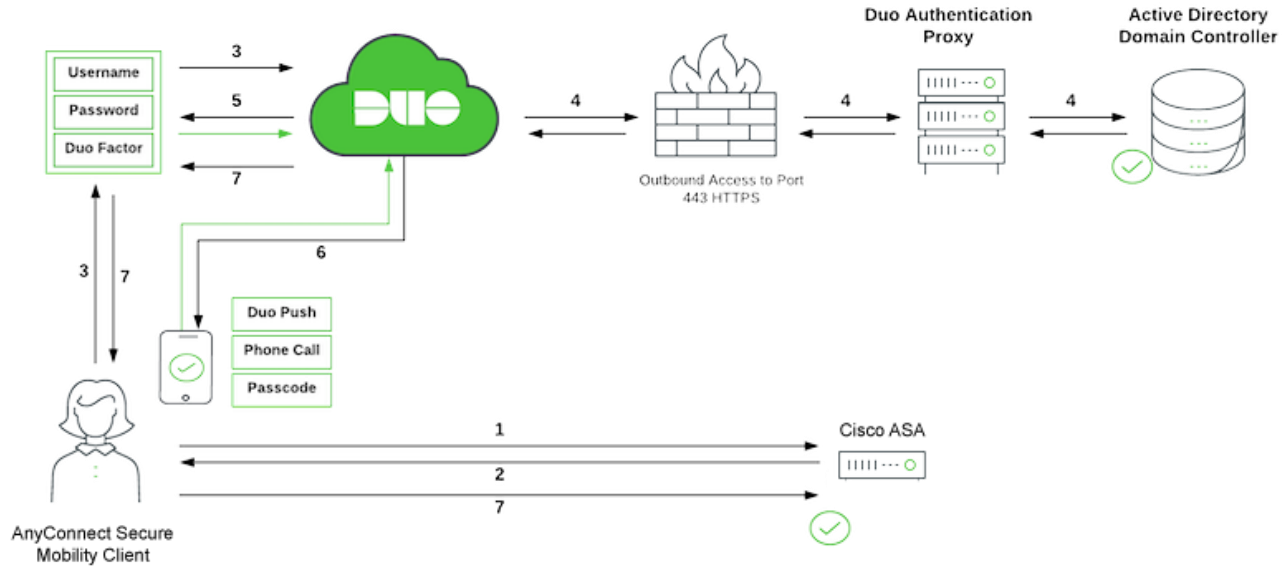

Рис. 1.5. Архітектура рішення Cisco Duo Security [10]

Перевагою рішення Cisco Duo Security є комплексні та детальні політики контролю доступу Duo. Його хмарна, масштабована природа та легке розгортання роблять його привабливим рішенням для компаній будь-якого розміру [8].

Найкращі функції Cisco Duo Security включають багатофакторну

автентифікацію (MFA) з підтримкою різних факторів, таких як мобільні додатки, універсальні токени автентифікації другого фактора, апаратні токени з підтримкою FIDO, коди доступу, USB-пристрої U2F та біометричні дані пристроїв, такі як FaceID. Це рішення також пропонує єдиний вхід (SSO), встановлення довіри до пристроїв, адаптивні політики автентифікації на основі місцезнаходження користувача та стану пристрою, а також підтримує хмарні, локальні або гібридні розгортання. Інтеграції включають сумісність з існуючими середовищами.

Перевагами рішення Cisco Duo Security також є [8]:

бездоганний та сучасний користувацький інтерфейс з інтуїтивно зрозумілим мобільним додатком;

масштабоване та просте в розгортанні хмарне рішення;

деталізовані політики контролю доступу для підвищення безпеки;

підтримує широкий спектр факторів багатосторонніх аварійних ситуацій (MFA).

Cisco Duo Security найкраще підходить для організацій будь-якого розміру, які прагнуть покращити свій рівень безпеки за допомогою надійного рішення для керування доступом. Це рішення особливо ефективний для компаній, що прагнуть впровадити стратегію нульової довіри [8].

Microsoft Entra ID (раніше Azure Active Directory) – це хмарна платформа керування ідентифікацією та доступом, яка забезпечує безпечний доступ до тисяч інтегрованих SaaS-додатків, а також до внутрішніх та користувацьких хмарних додатків. Вона використовує облікові дані Microsoft для забезпечення контролю доступу як до внутрішніх, так і до зовнішніх ресурсів [8].

Перевагою рішення Microsoft Entra ID є легкість розгортання для організацій, інтегрованих в екосистему Microsoft 365. Воно пропонує безперебійну автентифікацію користувачів та єдиний вхід для корпоративних додатків [8].

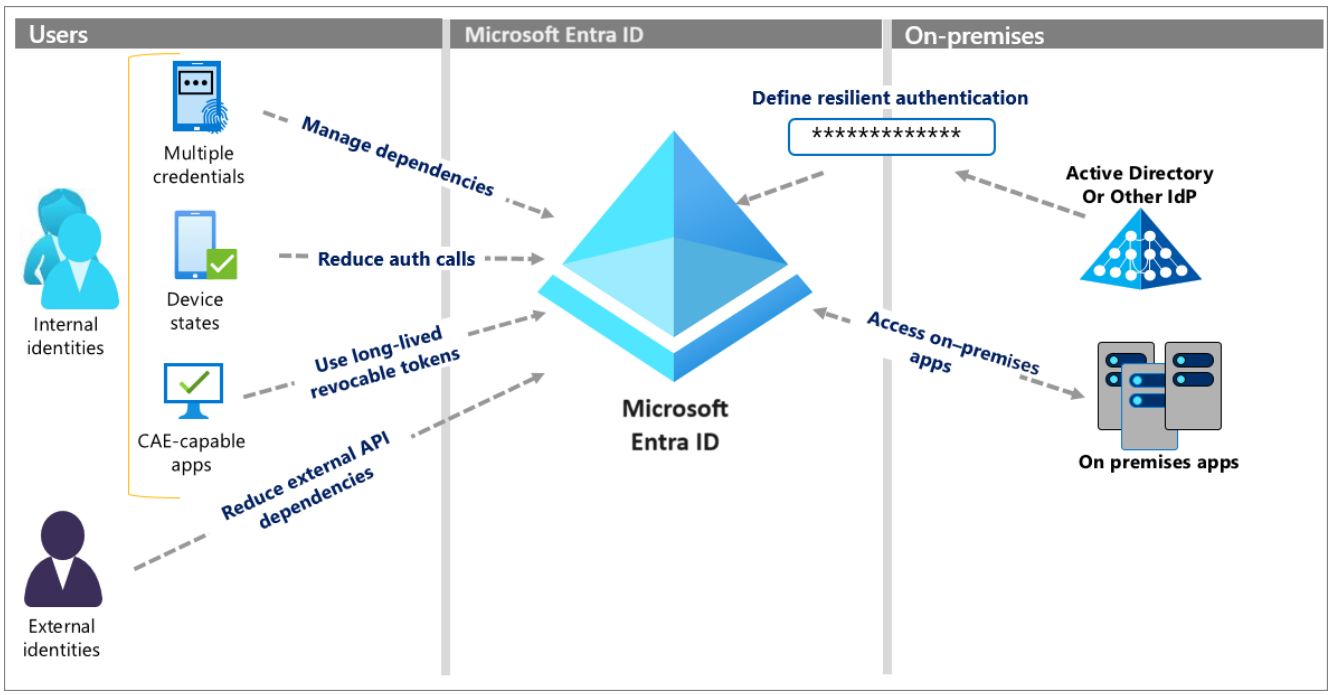

Рис. 1.6. Архітектура рішення Microsoft Entra ID [11]

Найкращі функції Microsoft Entra ID включають зручну багатофакторну автентифікацію, єдиний вхід для корпоративних програм, політики умовного доступу та безперешкодну інтеграцію з Microsoft 365. Підтримувані методи автентифікації включають програму Microsoft Authenticator, Windows Hello для бізнесу, ключі безпеки FIDO2, токени OATH, SMS-коди та голосові виклики [8].

Перевагами рішення Microsoft Entra ID також є [8]:

просте розгортання для користувачів Microsoft 365;

проста автентифікація користувачів та єдиний вхід;

гнучкі можливості багатофакторної автентифікації;

надійні політики умовного доступу.

Microsoft Entra ID найкраще підходить для організацій, які використовують або планують використовувати Microsoft 365 та прагнуть підвищити безпеку за допомогою автентифікації користувачів та єдиного входу для корпоративних застосунків [8].

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ БАГАТОФАКТОРНОЇ АВТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ ЗА ДОПОМОГОЮ МОБІЛЬНОГО ДОДАТКА НА БАЗІ ESET SECURE AUTHENTICATION

2.1. Призначення та основні функції рішення ESET Secure Authentication

Останнім часом стає актуальним забезпечення захищеного доступу до корпоративних ресурсів під час віддаленої роботи. Кількість випадків, коли потрібна праця у дистанційному режимі, зростає. Отже, виникає необхідність убезпечити доступ до інформаційних активів компанії ззовні. При цьому згадані випадки можуть бути різними, охоплюючи підключення і співробітників, які працюють поза офісом, і представників сторонніх організацій – підрядників, і фахівців аутсорсингових фірм, які займаються обслуговуванням інфраструктури.

Отже, процес підключення до корпоративних ресурсів має бути, з одного боку, досить простим, щоб не викликати труднощів у користувачів різного рівня комп'ютерної грамотності, а з іншого боку абсолютно безпечним. Ці критеріям відповідає, зокрема, механізм двофакторної автентифікації (Two-Factor Authentication, 2FA). Одним із способів реалізувати його у корпоративному середовищі є рішення ESET Secure Authentication.

Рішення ESET Secure Authentication (ESA) забезпечує безпечний доступ до корпоративних ресурсів за рахунок застосування різних методів двофакторної автентифікації (2FA) під час віддаленого підключення до них.

Рішення від ESET пропонує, крім класичної відправки одноразових паролів, застосування апаратних токенів, push-автентифікацію на мобільному пристрої, відправлення пароля електронною поштою або через інші додатки. Крім того, коли користувач отримує push-повідомлення на мобільний пристрій або смарт-годинник, у повідомленні вказується, з якої IP-адреси здійснюється підключення до ресурсів. Відповідно, співробітник може як схвалити автентифікацію, так і

відхилити її в тому випадку, якщо IP-адреса виявиться чужою або підозрілою.

Рішення ESET Secure Authentication (ESA) надає можливість забезпечити захищений доступ до корпоративних ресурсів з використанням двофакторної автентифікації локально або через інтеграцію з Microsoft Active Directory. На додаток до першого фактора – логіну та паролю – продукт пропонує на вибір кілька варіантів другого фактора: відправлення тимчасового пароля SMS на мобільний пристрій або смарт-годинник, використання апаратних токенів, відправлення пароля електронною поштою, push-автентифікацію. Також є можливість внести довірені робочі станції користувачів до списків винятків, дозволяючи їм підключатися до корпоративних ресурсів лише за логіном та паролем.

Це рішення може зацікавити замовників, у яких особливості інфраструктури або робочого процесу передбачають регулярні підключення ззовні офісу з боку співробітників, які перебувають у відрядженні або працюють з дому. Також це рішення можна розглянути, наприклад, у разі потреби організувати безпечний доступ співробітників підрядної організації до віддаленого робочого місця, через яке здійснюється обслуговування інфраструктури. Рішення ліцензується за кількістю користувачів.

Основними перевагами рішення ESET Secure Authentication є [13]:

push-автентифікація дозволяє автентифікуватися одним дотиком, без необхідності повторного введення одноразового пароля. Працює зі смартфонами iOS та Android.

захист хмарних додатків – додавання MFA посилює доступ до таких сервісів, як Google Apps, Dropbox та багато інших. ESET підтримує інтеграцію через протокол автентифікації SAML-2, який використовується основними постачальниками ідентифікаційних даних;

просте розгортання та налаштування – незалежно від того, чи має бізнес десятки чи тисячі користувачів, ESET Secure Authentication, завдяки своїй здатності надавати доступ кільком користувачам одночасно, мінімізує час налаштування;

кілька способів автентифікації – немає потреби в спеціальних токенах чи пристроях для співробітників. ESET Secure Authentication безперебійно працює на смартфонах, має власний PIN-код для додаткової безпеки та може інтегруватися з біометричними даними пристроїв (Touch ID, Face ID, відбиток пальця Android) для підвищення безпеки та кращого користувацького досвіду. За потреби рішення також підтримує апаратні токени або ключі безпеки FIDO.

не потрібно виділене обладнання – вимоги до ресурсів ESET Secure Authentication мінімальні, можна використовувати хмарну версію, тому не знадобиться виділений сервер. Водночас рішення також пропонує альтернативу локального розгортання;

безшовна інтеграція – рішення пропонує два режими інтеграції: інтеграцію з Active Directory для організацій, що використовують домен Windows, або автономний режим, який підходить для тих, у кого його немає. У будь-якому випадку налаштування та конфігурація швидкі та прості, і все це безперешкодно керується через хмарну консоль;

багатоклієнтська підтримка – хмарна версія ESET Secure Authentication розроблена з можливістю багатоклієнтського керування, щоб постачальники керованих послуг могли адмініструвати кілька компаній або сайтів, пропонуючи гнучкість визначення певних налаштувань для окремих груп користувачів;

підтримувані VDI та VPN – підтримуються VMware Horizon View, Citrix XenApp, Barracuda, Cisco ASA, Citrix Access Gateway, Citrix NetScaler, Check Point Software, Cyberoam, F5 FirePass, Fortinet, FortiGate, Juniper, Palo Alto та SonicWall. Також підтримується налаштування інтеграції з будь-якою VPN на базі RADIUS;

надання повного API ТА SDK – для організацій, які хочуть ще більше можливостей, додання повнофункціональних API та SDK, які клієнти можуть використовувати для розширення MFA на додатки або платформи, які вони використовують, навіть без спеціального плагіна.

2.2. Архітектура рішення ESET Secure Authentication

ESET Secure Authentication On-Prem (ESA) додає функцію двофакторної автентифікації (2FA) в домени Microsoft Active Directory або локальну мережу, що передбачає генерацію одноразового пароля (OTP) та його застосування додатково до облікових даних. Окрім того, двофакторна автентифікація може передбачати створення push-сповіщення, яке необхідно прийняти на мобільному телефоні користувача з ОС Android, iOS або Windows після успішної автентифікації користувача за допомогою облікових даних [12].

Архітектура ESET Secure Authentication складається з серверної та клієнтської частин. До першої відноситься сервер автентифікації, який можна встановити на базі Active Directory або в автономному режимі. Додатково доступні модуль звітності на базі Elasticsearch та інші компоненти, які будуть перераховані нижче. Клієнтська частина є мобільним програмним забезпеченням для операційних систем iOS, Android або Windows Phone. Мобільний додаток знадобиться для використання push-автентифікації та отримання одноразових паролів.

До складу рішення ESA входять такі компоненти [12]:

модуль ESA Web Application;

модуль ESA Remote Desktop;

модуль ESA Windows Login;

сервер ESA RADIUS Server;

служба ESA Authentication Service;

модуль ESA Management Tools.

При розгортанні останнього з перерахованих модулів можливі два сценарії.

У разі встановлення ESA у середовищі Active Directory знадобиться інсталяція наступних компонентів:

модуля керування користувачами ESA User Management,

консолі керування ESA Management Console,

консолі ESA Web Console.

У разі інсталяції ESA в режимі окремого сервера потрібна інсталяція лише компонента ESA Web Console.

Таблиця 2.1

Опис основних компонентів серверної частини ESA

Найменування компонента	Призначення компонента
ESA Web Application	Двофакторна автентифікація у різних веб-додатках Microsoft (Microsoft Web Applications).
ESA Remote Desktop	Двофакторна автентифікація для протоколу віддаленого робочого столу (Remote Desktop Protocol).
ESA Windows Login	Двофакторна автентифікація для комп'ютерів з Windows.
ESA RADIUS Server	Двофакторна автентифікація VPN з використанням RADIUS-сервера.
ESA Authentication Service	Основний модуль системи. Дозволяє додавати двофакторну автентифікацію до різних програм та сервісів.
ESA Management Tools	Керування користувачами, налаштування продукту та його компонентів.
ESA User Management для ADUC	Керування користувачами в Active Directory Users and Computers (ADUC).
ESA Management Console	Керування ESET Secure Authentication та його компонентами під час інтеграції сервера автентифікації у середовище Active Directory.
ESA Web Console	Налаштування ESET Secure Authentication та керування користувачами через веб-консоль.
Модуль звітності (Elasticsearch)	Перегляд звітів у веб-консолі ESET Secure Authentication.
Active Directory Federation Services (AD FS) Protection	Забезпечення двофакторної автентифікації під час інтеграції у середовище Active Directory.
Identity Providers Protection (SAML)	Забезпечення двофакторної автентифікації під час взаємодії з постачальниками посвідчень, які використовують стандарт SAML.

До ключових переваг рішення ESA можна віднести такі можливості, що відрізняють його від інших розробок подібного типу:

підтримка апаратних токенів, що працюють за стандартами OAuth (Open Authentication), HOTP (HMAC-based One-Time Password algorithm) та TOTP (Time-based One-Time);

можливість створити список винятків у вигляді IP-адрес або діапазонів, для яких тимчасовий пароль не запитуватиметься;

підтримка вбудованої біометрії iOS та Android для захисту мобільної програми;

наявність push-автентифікації через мобільний додаток для iOS або Android;

широкі можливості щодо інтеграції рішення з різними програмними та апаратними платформами;

рішення ESA є повністю програмним.

Рішення ESET Secure Authentication пропонує такі функціональні можливості:

безпечний та зручний доступ до VPN;

захищений віддалений доступ до корпоративних ресурсів;

додатковий захист під час входу до операційної системи Microsoft Windows;

двофакторна автентифікація між будь-якою хмарною службою (постачальником послуг) та постачальниками посвідчень, які використовують стандарт SAML;

двофакторна автентифікація для доступу до хмарних сервісів (Office 365, Google Apps, Dropbox та інші), веб-додатків Microsoft (Exchange, Outlook Web Access / Outlook Web App, Dynamics CRM, SharePoint / SharePoint Foundation, Remote Web Access / Remote Desktop Web Access, Terminal та мережного захисту (Barracuda, Cisco ASA, Citrix Access Gateway, Citrix NetScaler, Check Point Software, Cyberoam, F5 FirePass, Fortinet FortiGate, Juniper, Palo Alto, SonicWall) та застосування VDI-рішень VMware Horizon View та Citrix XenApp;

забезпечення захищеного доступу до ресурсів різних інформаційних систем;

застосування різних методів автентифікації: одноразовий пароль, що надсилається через мобільний додаток; push-автентифікація; одноразовий пароль, що надсилається через SMS; апаратні токени; інші канали передачі паролів (наприклад, електронна пошта).

Для першої інсталяції потрібні всі компоненти ESA, які показано на рисунку 2.1:

принаймні один екземпляр Authentication Server;

принаймні одна з кінцевих точок автентифікації (API, вхід у Windows, веб-додаток, AD FS, віддалений робочий стіл або RADIUS).

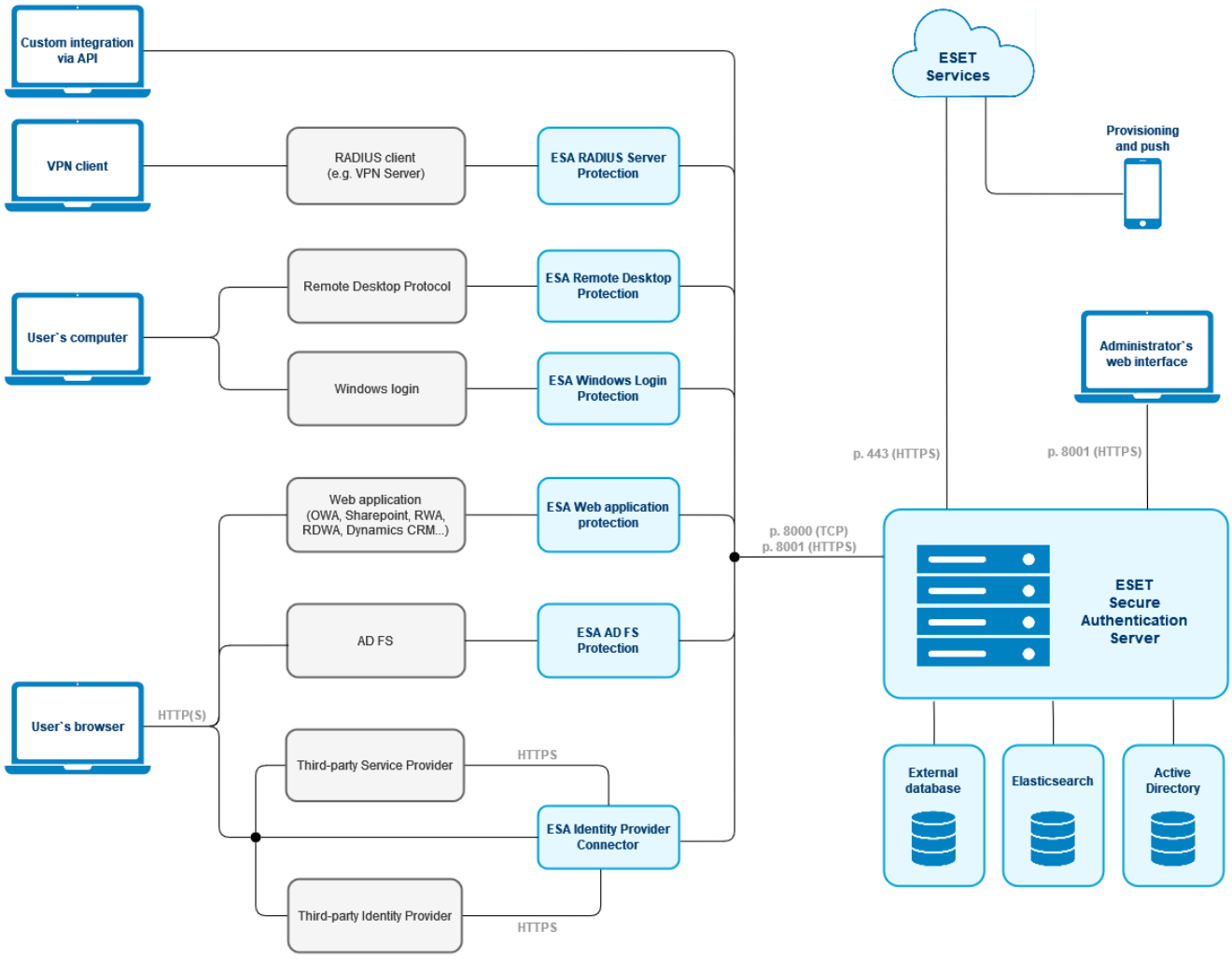

Рис. 2.2. Архітектура рішення ESET Secure Authentication [12]

Усі компоненти, окрім ESA Web Console, можна інсталювати на одному комп’ютері або на різних комп’ютерах у розподіленому середовищі. ESA Web Console є частиною сервера автентифікації. Для розподілених систем інсталяція може відбуватися за різними сценаріями.

У середовищі Active Directory не обов’язково інсталювати ESA Authentication Server саме на контролер домену. Це можна зробити й на будь-який інший комп’ютер, навіть у режимі Standalone.

На рисунку 2.2 показано сценарій загальної інсталяції в середовищі Active Directory. Цей приклад можна використати як базове керівництво для інших сценаріїв розгортання.

2.3. Основні можливості рішення ESET Secure Authentication

ESET Secure Authentication On-Prem (ESA) забезпечує кілька можливостей автентифікації користувачів для надання доступу до комп'ютерів або служб, захищених із використанням двофакторної автентифікації [12]:

одноразовий пароль (OTP), що надсилається в SMS-повідомленні. Для нього потрібні кредити на SMS або спеціальні варіанти, у яких використовується настроюваний шлюз SMS;

одноразовий пароль, згенерований у мобільному додатку ESA:

одноразовий пароль на основі події (HOTP): термін дії цього пароля завершується, коли його використано або створено новий одноразовий пароль;

одноразовий пароль на основі часу (TOTP): термін дії цього пароля завершується через кілька секунд (анімація про завершення терміну дії відображається в мобільному додатку), навіть якщо його не використано.

одноразовий пароль, надісланий електронною поштою;

автентифікація за допомогою push-сповіщення;

апаратні маркери;

одноразовий пароль, отриманий через спеціальний варіант доставки;

FIDO: для кожного користувача можна зареєструвати тільки один автентифікатор FIDO.

ESA пропонує широкий спектр способів 2FA, які задовольнять різні потреби клієнтів. Найбезпечніший і дуже зручний спосіб – push-сповіщення в мобільних додатках (push-автентифікація). Також дуже надійні, але не завжди зручні способи: одноразові паролі (OTP) у мобільних додатках, апаратні маркери, FIDO.

Також можна використовувати одноразові паролі в SMS-повідомленнях, але вони не дуже безпечні через недоліки захисту систем доставки SMS. OTP, які надсилаються електронною поштою, також не завжди безпечні, оскільки деякі схеми використання не дуже надійні.

З огляду на технічний аспект надсилання SMS-повідомлень, які зазвичай

обробляються місцевими операторами телекомунікаційних послуг, ESET не гарантує надійність доставки SMS-повідомлень на мобільний телефон кінцевого користувача.

Розглянемо способи автентифікації, доступні в автономному режимі. Перед автономним використанням [12]:

ESA потрібно активувати за допомогою ліцензійного ключа або облікових даних ESET Business Account;

щоб зареєструвати й додати користувачів, в ESA Core потрібен бути доступ до *esa.eset.com*.

Якщо Authentication Server не може підключитися до Інтернету, для автентифікації під час входу доступні наведені нижче способи:

апаратні маркери;

FIDO;

паролі OTP у SMS-повідомленнях, що доставляються спеціальним методом у внутрішній мережі, яка не підключена до Інтернету;

одноразовий пароль, згенерований у мобільному додатку ESA.

Захист входу в ОС Windows в автономному режимі.

Якщо використовується модуль захисту входу в ОС Windows в автономному режимі, доступні такі способи автентифікації під час входу [12]:

апаратні маркери (тільки одноразовий пароль на основі події);

одноразовий пароль, згенерований у мобільному додатку ESA (тільки одноразовий пароль на основі події);

FIDO.

Автономні одноразові паролі: в автономному режимі за замовчуванням кешуються лише 20 одноразових паролів. Оновлення кешу відбувається такими способами [12]:

автоматично після успішного входу в онлайн-режим;

через 10 хвилин після успішного входу в автономному режимі компонент ESA намагається завантажити нові одноразові паролі (подальші спроби відбуваються кожні 60 хвилин);

якщо підключається нова мережа (наприклад, перезавантажується мережевий адаптер), компонент ESA намагається негайно завантажити нові одноразові паролі.

Мобільний додаток ESET Secure Authentication On-Prem полегшує генерацію паролів OTP або схвалення запитів push-автентифікації для доступу до комп'ютерів і служб, захищених автентифікацією 2FA. Мобільний додаток версії 2.40+ підтримує автентифікацію кількох користувачів. Тому якщо ви використовуєте кілька облікових записів користувачів у домені або мережі, які захищено 2FA, маркери автентифікації всіх ваших облікових записів можуть зберігатися в одному мобільному додатку.

Версія мобільної програми 3.0 і новіші підтримують маркери Google Authenticator. Замість того щоб інсталювати додаток Google Authenticator, можна просто натиснути кнопку + у мобільному додатку ESET Secure Authentication On-Prem, щоб просканувати QR-код під час налаштування двоетапної перевірки за допомогою Google Authenticator. Тоді ви зможете створювати OTP в мобільному додатку ESA замість Google Authenticator, коли входитимете в служби Google, захищені двоетапною перевіркою.

Мобільний додаток можна захистити від несанкціонованого доступу, установивши PIN-код. Щоб швидше відкривати її, дозвольте використовувати сканер відбитків пальців Fingerprint scanner (Android, iOS) або розпізнавання облич Face recognition (iOS). Це можливо, якщо на мобільному пристрої налаштовано біометричну автентифікацію.

Якщо Mobile Application захищено PIN-кодом, на годиннику Android під час генерації push-сповіщення відображається повідомлення Approve on phone (Підтвердити на телефоні).

Якщо Mobile Application захищено PIN-кодом, користувач зможе входити за допомогою неправильного PIN-коду для захисту правильного PIN-коду від атак повним перебором. Наприклад, якщо зловмисник спробує ввійти в Mobile Application, указавши неправильний PIN-код, йому може бути надано доступ, проте OTP не працюватиме. Після кількох неправильних уведень коду OTP

автоматично блокуватиметься 2FA облікового запису користувача (до якого належить Mobile Application). Для звичайного користувача це не є значною проблемою. Якщо користувач увійде в Mobile Application, указавши неправильний PIN-код, а потім змінить PIN-код, усі маркери Mobile Application стануть непридатними для використання. Ці маркери не можна відновити. Єдине рішення – заново виділити маркери для Mobile Application. З огляду на вищенаведене рекомендується користувачам перевіряти функціональність кодів OTP, перш ніж змінювати PIN-код. Якщо коди OTP працюють, можна безпечно змінити PIN-код.

Паролі OTP відображаються в мобільному додатку з пробілом між третьою і четвертою цифрами (для кращого сприйняття). Для всіх способів автентифікації, за винятком MS-CHAPv2, зі вказаних облікових даних видаляються пробіли, тому користувач може застосовувати або видаляти пробіли, і це жодним чином не вплине на процес автентифікації.

Автентифікація за допомогою push-сповіщення

Автентифікація за допомогою push-сповіщень на мобільних пристроях уперше з'явилася в ESET Secure Authentication On-Prem (ESA) версії 2.5.X і була доступна лише для пристроїв з Android. В ESA версії 2.6.X цей спосіб автентифікації став доступний також для пристроїв iOS, а в ESA версії 2.7 – і для пристроїв Windows Phone.

У розділі ESA Web Console Users для одного користувача або кількох користувачів можна відразу ввімкнути обидва параметри автентифікації (OTP і Push).

Апаратні маркери

Апаратний маркер – це пристрій, що створює OTP та використовується в поєднанні з паролем як електронний ключ доступу. Апаратні маркери бувають різними: брелок для ключів, кредитна картка, яку можна носити в гаманці, тощо.

HOTP означає «HMAC-based One-time Password» (одноразовий пароль на базі механізму HMAC). Це OTP на основі події.

TOTP означає «Time-based One-time Password» (одноразовий пароль на основі часу).

HOTP і TOTP можна генерувати за допомогою як апаратних маркерів, так і додатків (наприклад, ESA Mobile App).

ESA підтримує всі апаратні маркери, сумісні з OATH, але компанія ESET їх не надає. Апаратні маркери HOTP можна використовувати так само, як паролі HOTP, створені мобільним додатком або отримані користувачем у повідомленні SMS. Це може стати в нагоді, наприклад, для підтримки перенесення успадкованих маркерів із метою забезпечення відповідності нормативним вимогам, або якщо це не заборонено політикою компанії.

Маркер даних можна імпортувати в ESET Secure Authentication On-Prem за допомогою файлу XML у форматі PSKC. Більшість постачальників апаратних маркерів надає файл у форматі PSKC під час покупки відповідних маркерів.

FIDO

ESET Secure Authentication On-Prem (ESA) версії 2.8 або більш пізньої підтримує двофакторну автентифікацію (2FA) на пристроях із підтримкою стандартів автентифікації FIDO2 (і FIDO U2F). Додаткову інформацію про FIDO див. за цим посиланням.

Вимоги [12]:

веб-браузер із підтримкою API веб-автентифікації: Mozilla Firefox, Google Chrome, Microsoft Edge;

безпечне підключення (HTTPS) (можна також використовувати сертифікати з власним підписом);

.NET Framework 4.7.2 інстальовано на машині з ESA Authentication Server.

Підтримуване середовище [12]:

середовище входу через Інтернет, захищене ESA:

ESA Web Console;

IIS;

AD FS;

Identity Provider Connector;

захист входу в ОС Windows.

Варіанти доставки

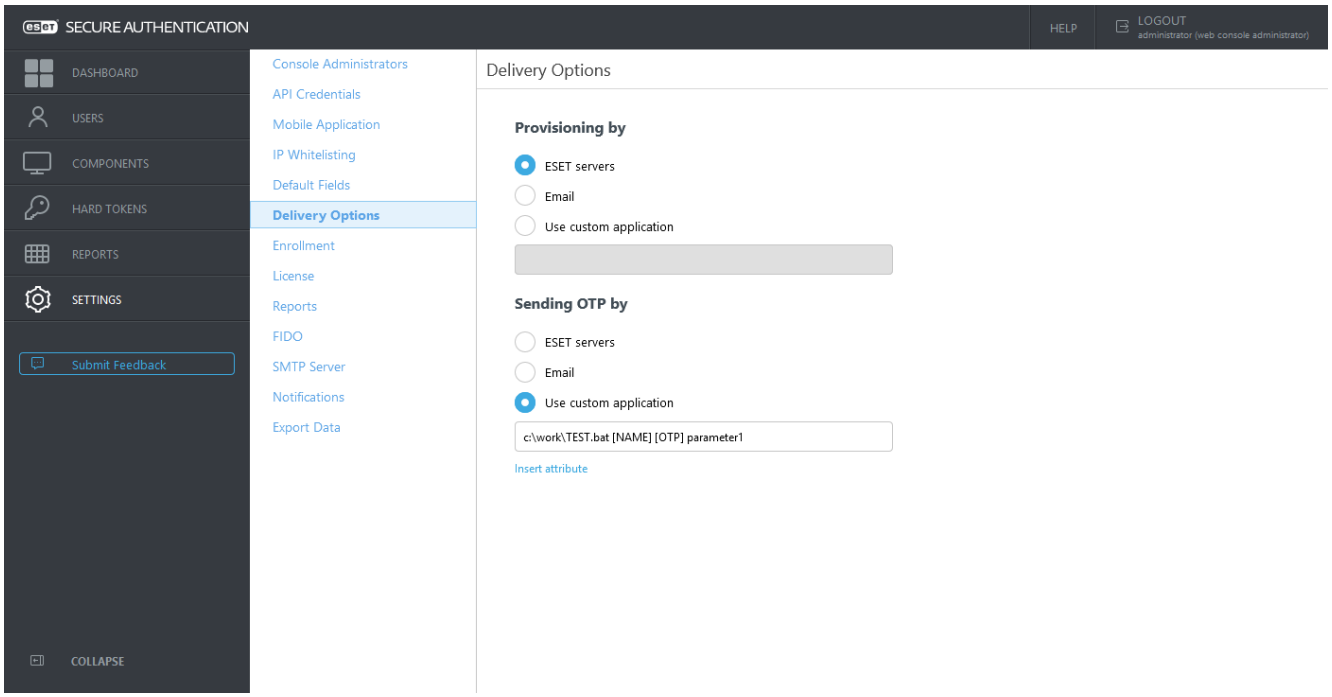

Рис. 2.3. Вибір варіанта доставки OTP

Варіанти доставки OTP за замовчуванням (у SMS-повідомленнях, у мобільному додтаку) відмінно підходять для більшості користувачів. Окрім цих способів, ESA дозволяє налаштувати й інші способи відповідно до потреб.

3 РЕКОМЕНДАЦІЇ ЩОДО ЗАСТОСУВАННЯ БАГАТОФАКТОРНОЇ АВТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ ЗА ДОПОМОГОЮ МОБІЛЬНОГО ДОДАТКА НА БАЗІ ESET SECURE AUTHENTICATION

3.1. Варіант системи багатофакторної автентифікації користувачів за допомогою мобільного додатку на базі ESET Secure Authentication

Система багатофакторної автентифікації (MFA) користувачів за допомогою мобільного додатку на базі ESET Secure Authentication створюється з метою підвищення рівня безпеки. Створюється додатковий рівень захисту для облікових записів користувачів. Навіть якщо зловмисник отримає пароль, йому буде потрібен додатковий фактор автентифікації (наприклад, підтвердження через мобільний додаток), щоб отримати доступ. Це значно ускладнює несанкціонований доступ до конфіденційних даних і зменшує ризик витоку інформації.

MFA ефективно протидіє таким загрозам, як фішинг, крадіжка паролів і атаки «людина посередині». Це допомагає захистити організації від фінансових втрат, пошкодження репутації та інших негативних наслідків кібератак. Багато галузей і стандартів безпеки вимагають використання MFA для захисту конфіденційних даних. Впровадження MFA допомагає організаціям відповідати цим вимогам і уникати штрафів. Також, використання MFA демонструє, що організація серйозно ставиться до безпеки даних своїх клієнтів. Це підвищує довіру клієнтів і зміцнює репутацію компанії.

Сучасні рішення MFA, такі як ESET Secure Authentication, пропонують зручні методи автентифікації, такі як push-сповіщення, які не вимагають введення складних кодів. Таким чином, система MFA є важливим інструментом для захисту даних і забезпечення безпеки в сучасному цифровому світі.

Мобільний додаток ESET Secure Authentication застосовується для захисту:

доступу до VPN організації;

протоколу віддаленого робочого столу;

додаткової автентифікації для входу в комп'ютер (вхід в операційну систему);

веб-/хмарних сервісів через Microsoft ADFS 3.0, наприклад Office 365;

Microsoft Web Apps, наприклад OWA;

панелі керування Exchange і Центру адміністрування Exchange;

VMware Horizon View;

сервісів на основі RADIUS.

Ми можемо здійснити інтеграцію з корпоративними сервісами на основі RADIUS або через API з існуючою автентифікацією на основі Active Directory. Клієнти, які не використовують Active Directory і мають спеціальні системи, можуть використовувати простий у розгортанні SDK.

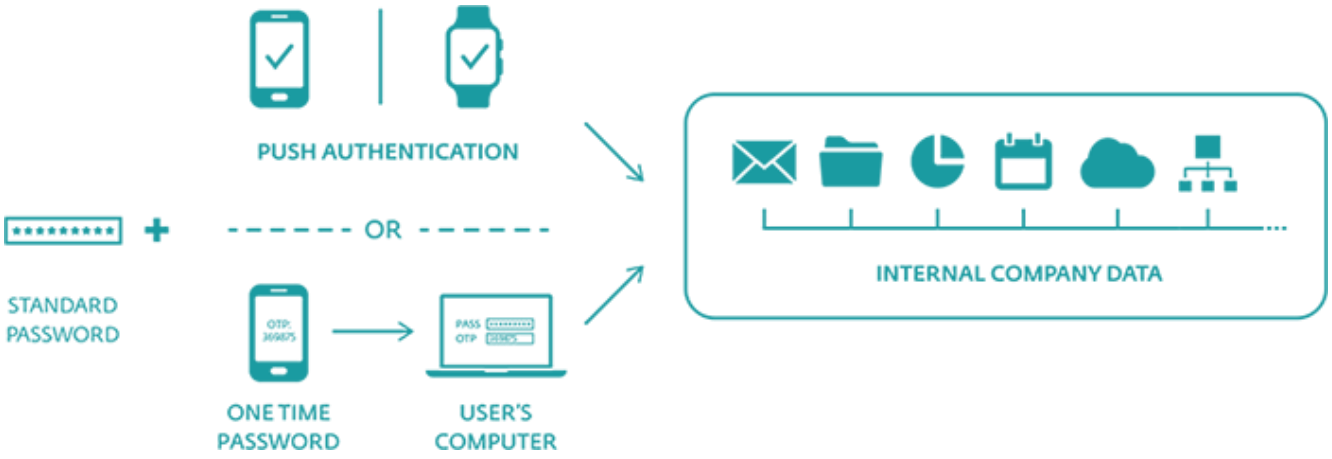

Рис. 3.1. Схема системи багатофакторної автентифікації користувачів за допомогою мобільного додатку на базі ESET Secure Authentication [13]

Основними компонентами системи багатофакторної автентифікації користувачів на базі мобільного додатку на базі ESET Secure Authentication є:

сервер ESET Secure Authentication (ESA). Це центральний компонент, який керує процесом MFA. Він інтегрується з існуючою корпоративною системою автентифікації (наприклад, Active Directory). Він генерує та перевіряє одноразові паролі (OTP) та push-сповіщення;

мобільний додаток ESET Secure Authentication. Встановлюється на

смартфони користувачів (iOS та Android). Генерує OTP або отримує push-сповіщення для підтвердження входу.

інтеграція з додатками та сервісами. ESA інтегрується з різними додатками та сервісами, які потребують MFA (наприклад, VPN, веб-додатки, віддалений доступ до робочого столу).

Процес автентифікації користувачів за допомогою мобільного додатку на базі ESET Secure Authentication складається з таких кроків:

введення облікових даних: користувач вводить своє ім’я користувача та пароль у додаток або сервіс, що потребує автентифікації;

запит на MFA: сервер ESA отримує запит на автентифікацію;

push-сповіщення або OTP: сервер ESA надсилає push-сповіщення на мобільний додаток користувача або генерує OTP. Користувач підтверджує вхід через push-сповіщення, або вводить OTP в додатку/сервісі.

перевірка: сервер ESA перевіряє push-підтвердження або OTP.

надання доступу: якщо перевірка успішна, користувач отримує доступ до програми або сервісу.

3.2. Порядок інсталяції та застосування мобільного додатка ESET Secure Authentication для Android

Для того, щоб ми змогли використовувати додаток ESET Secure Authentication на своєму мобільному пристрої, ми повинні встановити та налаштувати основну службу ESET Secure Authentication на своєму сервері, а потім надати пристрої, які ми хочемо використовувати, за допомогою мобільного додатка ESET Secure Authentication [14].

Нижче описано порядок конфігурації ESET Secure Authentication для використання з Microsoft Outlook Web Access.

Першим етапом є інсталяція мобільного додатка ESET Secure Authentication [14]:

1. Якщо нам буде запропоновано зареєструватися в мобільному додатку

ESET Secure Authentication (ESA), то необхідно натиснути «Set up», щоб почати процес реєстрації (рисунок 3.2).

2. Необхідно відсканувати QR-код, натиснути «Continue» → «Finish» та перейдіть до кроку 3 (рисунок 3.3).

3. Необхідно натиснути «Add Account». Якщо вже завантажено додаток, то необхідно перейти до кроку 6 (рисунок 3.4).

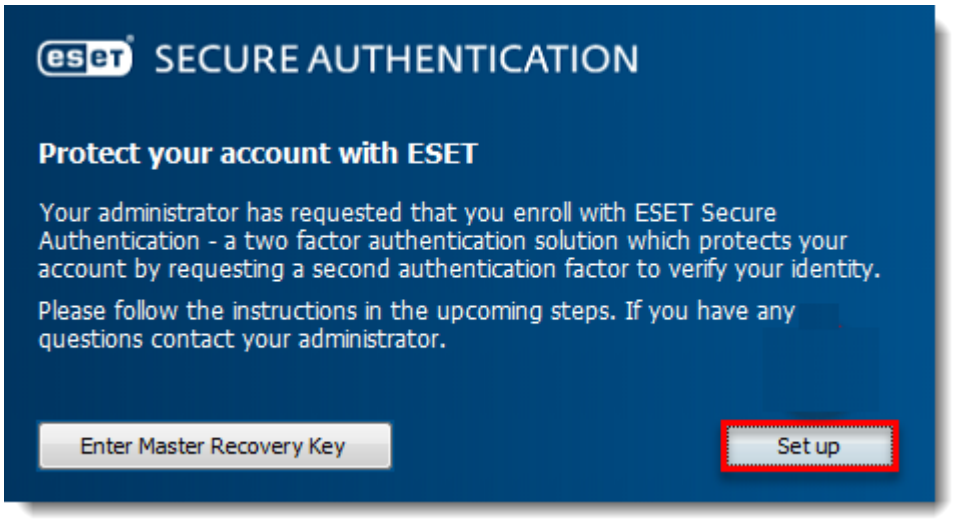

Рис. 3.2. Вікно реєстрації в мобільному додатку

Рис. 3.3. QR-код реєстрації в мобільному додатку

4. Необхідно натиснути «Install». Після завершення встановлення необхідно натиснути «Open» (рисунок 3.5).

5. Необхідно переглянути ліцензійну угоду та прийняти її (рисунок 3.6).

6. Рекомендується встановити PIN-код, щоб захистити ESA від несанкціонованого доступу (рисунок 3.7).

7. Необхідно ввести свій PIN-код у поля «Новий PIN-код» і «Підтвердьте PIN-код» і натисніть OK. Якщо після налаштування потрібно змінити PIN-код, торкніться меню додатка та виберіть «Змінити PIN» (рисунок 3.8). Після налаштування PIN-коду додаток ESET Secure Authentication готовий до використання.

Другим етапом є використання додатка ESET Secure Authentication для входу, наприклад, в Outlook Web Access.

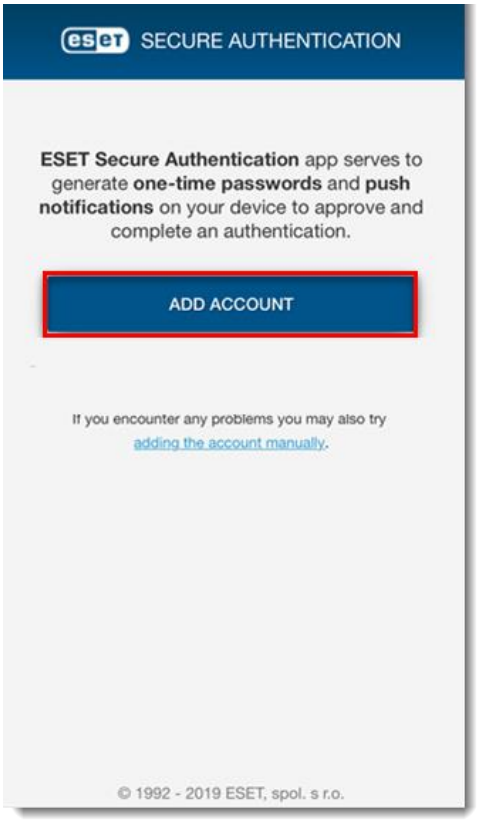

Рис. 3.4. Вікно «Add Account»

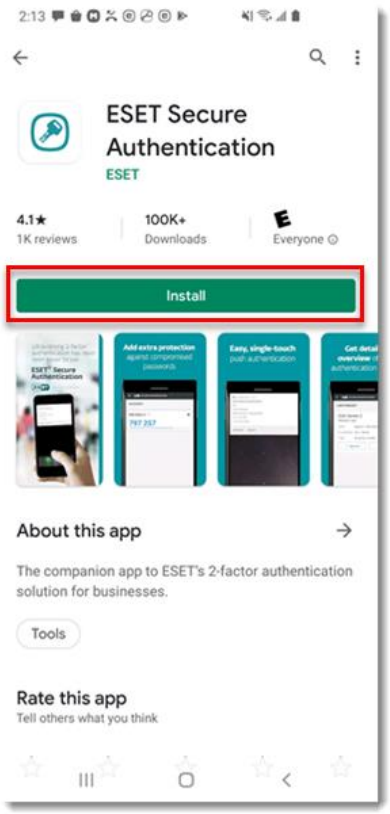

Рис. 3.5. Запуск «Install»

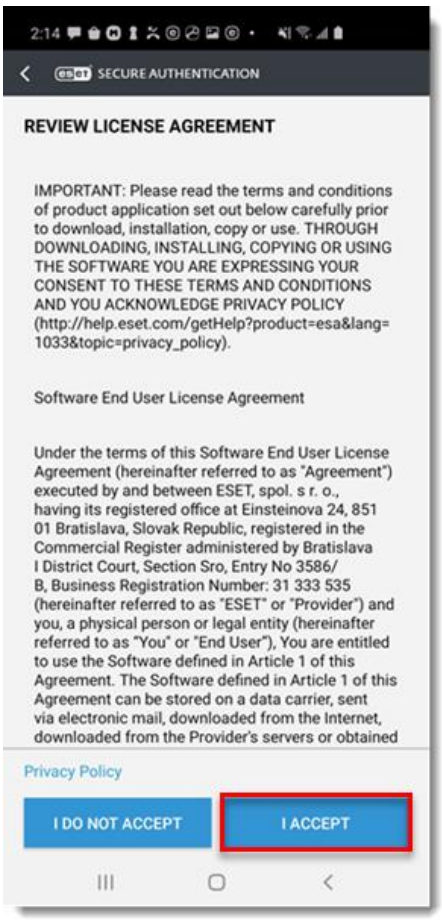

Рис. 3.6. Вікно ліцензійної угоди

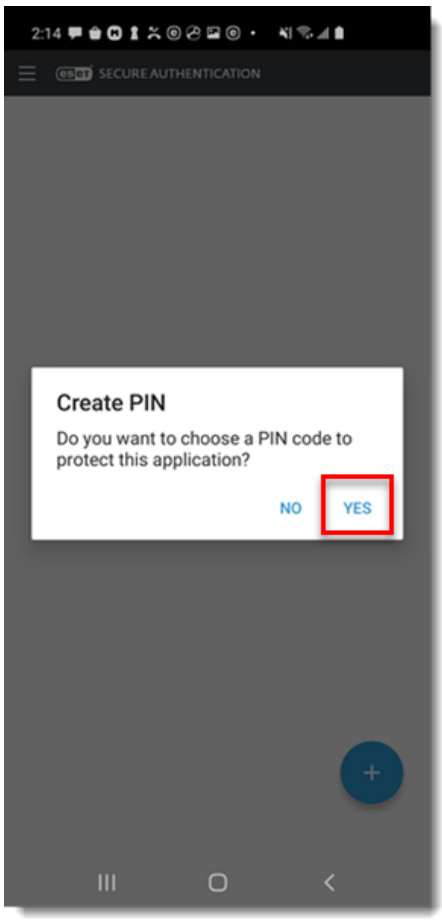

Рис. 3.7. Вікно створення PIN

1. На комп’ютері відкрийте Outlook Web Access (OWA) за вказівками адміністратора. Введіть своє ім’я користувача та пароль Microsoft Exchange на екрані входу в Outlook і натисніть «Sing in» (рисунок 3.9).

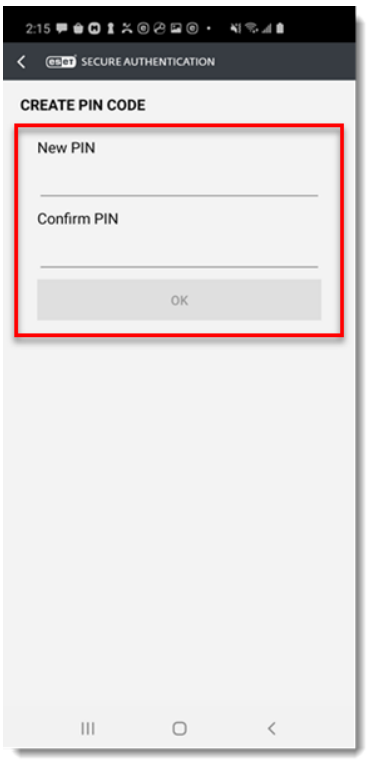

Рис. 3.8. Вікно створення нового PIN

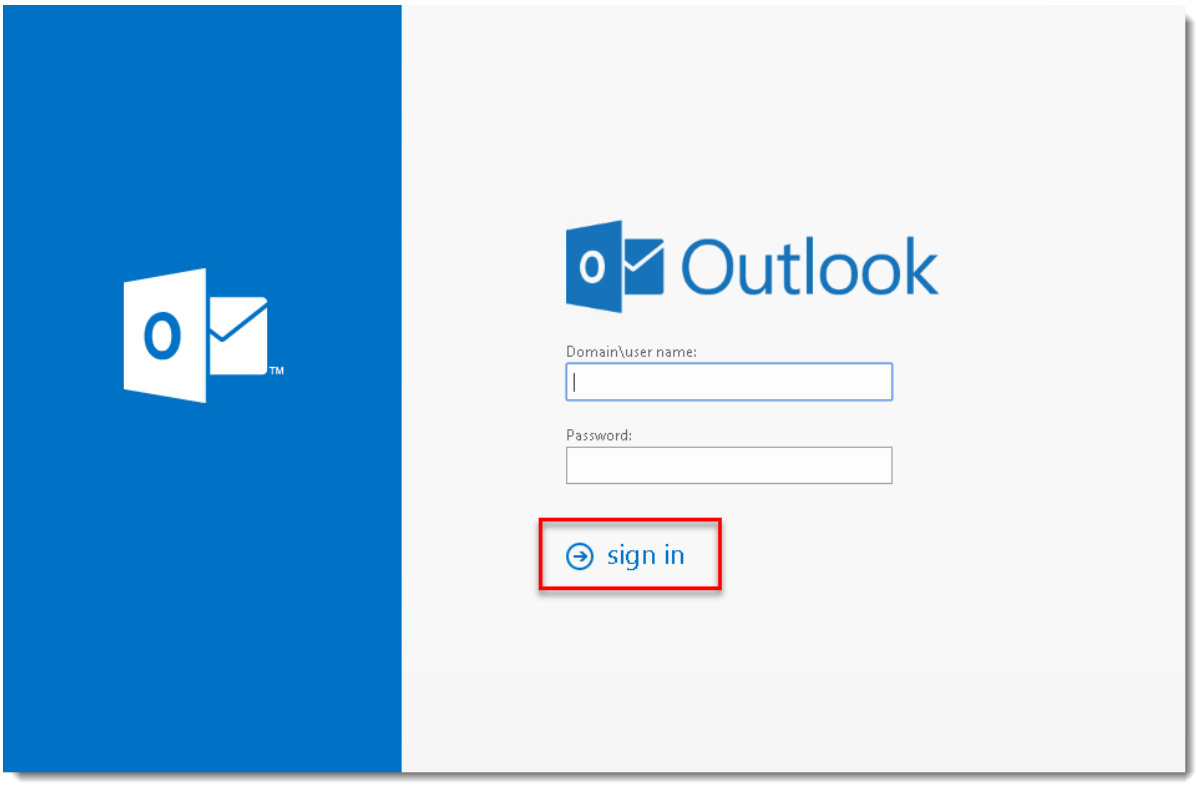

Рис. 3.9. Екрані входу в Outlook

2. Коли буде запропоновано, необхідно ввести одноразовий пароль (OTP) або схваліть push-автентифікацію за допомогою мобільного додатка ESET Secure Authentication.

3. На мобільному пристрої необхідно торкнутися піктограми ESET Authentication на головному екрані, щоб відкрити додаток ESA.

4. Залежно від адміністративних налаштувань:

а. *користувачі push-автентифікації*: необхідно торкнутися «Схвалити» (рисунок 3.10). Тепер є вхід у свій обліковий запис Outlook.

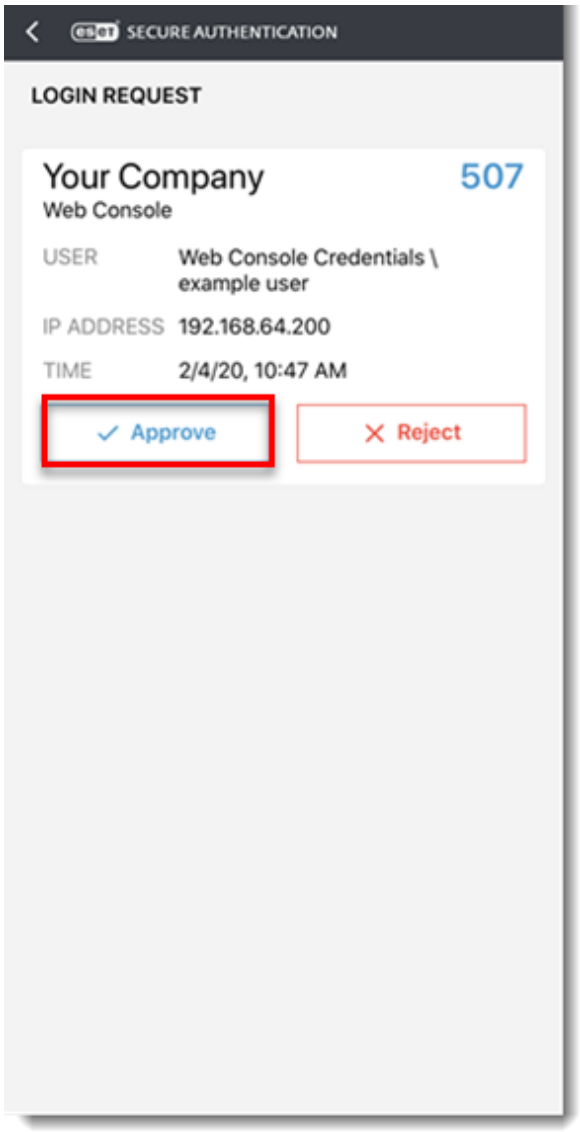

Рис. 3.10. Вікно мобільного додатка для користувачів push-автентифікації

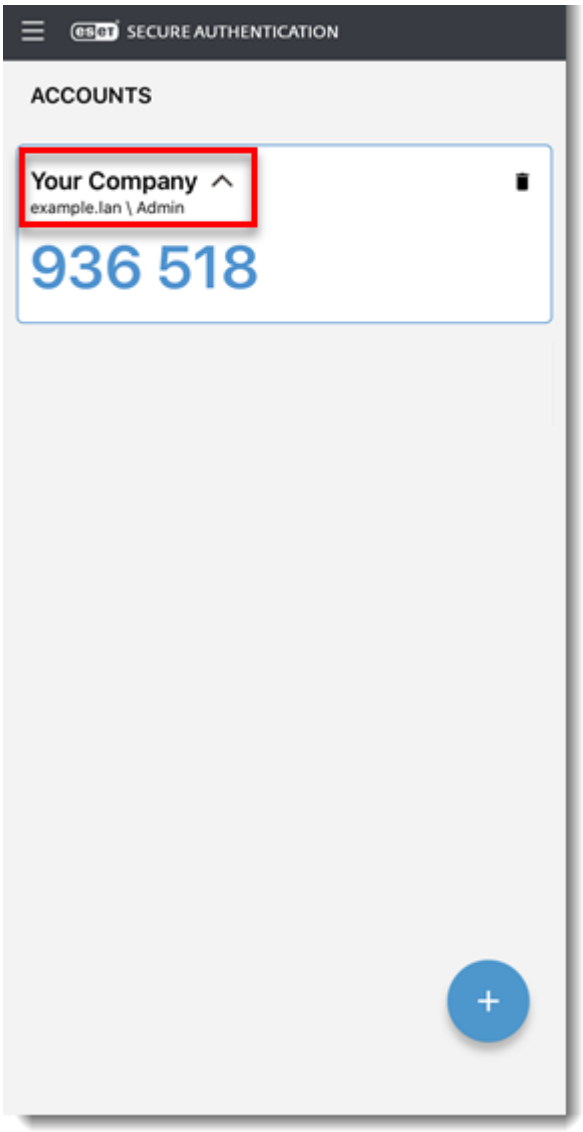

Рис. 3.11. Вікно мобільного додатка для користувачів одноразового пароля

б. *користувачі одноразового пароля*: необхідно натиснути «Ваша компанія» (цей текст може відрізнятися залежно від налаштувань адміністратора), щоб створити одноразовий пароль (рисунок 3.11).

5. На комп’ютері необхідно ввести 6-значний одноразовий пароль,

згенерований мобільним додатком ESA, у поле «Введіть одноразовий пароль» і натисніть «Автентифікувати» (рисунок 3.12), щоб отримати доступ до Microsoft OWA. Тепер є вхід у свій обліковий запис Outlook.

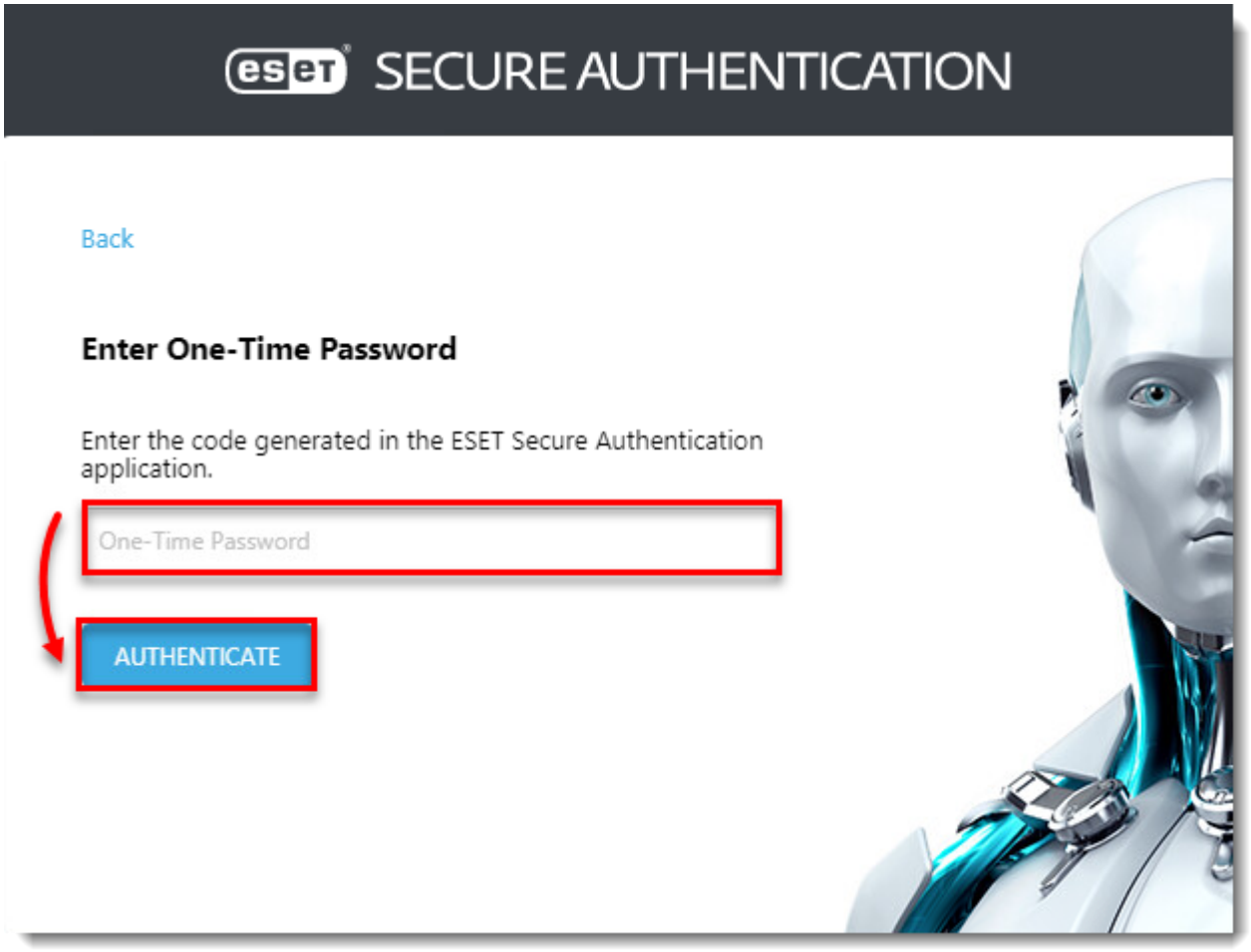

Рис. 3.12. Поле введення ідентифікатора користувача

3.3. Рекомендації щодо застосування багатофакторної автентифікації користувачів за допомогою мобільного додатка

Сьогодні кібератаки стають швидшими та складнішими, зростає кількість загроз, орієнтованих на ідентифікацію. Скомпрометовані облікові дані залишаються провідною причиною витоків даних та кіберінцидентів. MFA є високоефективним засобом, що блокує понад 99,9% автоматизованих атак та значно зменшує кількість захоплень облікових записів. Хоча існують методи обходу MFA, вони часто покладаються на використання слабших методів MFA

або людських вразливостей.

Для організацій пропонуються наступні практичні рекомендації:

необхідно впроваджувати рішення MFA, які менш вразливі до фішингу, такі як апаратні ключі FIDO2, біометрична автентифікація або програми-автентифікатори з підтвердженням номера. Уникайте покладання виключно на одноразові паролі (OTP) на основі SMS або електронної пошти;

необхідно забезпечити обов'язкове використання MFA для всіх облікових записів користувачів, особливо привілейованих: Вимагайте використання MFA для всіх співробітників, підрядників та сторонніх користувачів, що мають доступ до організаційних ресурсів. Приділіть особливу увагу захисту привілейованих облікових записів з адміністративним доступом, оскільки вони є цінними цілями для зловмисників;

необхідно впроваджувати програми навчання та підвищення обізнаності користувачів. Навчайте користувачів важливості MFA та поширеним тактикам його обходу, таким як вішинг, фішинг та MFA-втома. Проводьте регулярні тренінги та симуляції для закріплення безпечних практик автентифікації;

необхідно регулярно переглядати та оновлювати конфігурації MFA. Переконайтеся, що політики MFA правильно налаштовані та регулярно переглядаються для протидії новим загрозам та методам обходу. Впроваджуйте надійні політики паролів у поєднанні з MFA;

необхідно розглянути можливість використання контекстної та адаптивної MFA. Вивчайте рішення MFA, які враховують аналіз ризиків, такі як стан пристрою, поведінка користувача та місцезнаходження, щоб динамічно регулювати вимоги до автентифікації та забезпечувати додатковий рівень безпеки;

необхідно запровадити безпечні процеси відновлення облікових записів. Впровадьте безпечні та добре задокументовані процедури відновлення облікових записів на випадок втрати користувачами доступу до своїх пристроїв MFA, гарантуючи, що ці процеси не будуть легко використані зловмисниками.

За результатами цього дослідження ми можемо дати такі рекомендацій для

організацій щодо застосування багатофакторної автентифікації користувачів за допомогою мобільного додатка:

Необхідно ретельно спланувати впровадження багатофакторної автентифікації. Потрібно визначити, які інформаційні системи та дані потребують захисту за допомогою MFA. Необхідно оцінити ризики та обрати відповідні методи автентифікації через мобільний додаток (наприклад, push-сповіщення, біометрія, одноразові паролі).

Необхідно розробити чіткі політики MFA, які визначають, коли та як користувачі повинні використовувати MFA та втілити їх. Необхідно проводити роз'яснення та бесіди, щоб інформувати користувачів про майбутні зміни та переваги MFA.

Необхідно зробити процес автентифікації зрозумілим та зручним для користувачів. Необхідно обрати мобільний додаток MFA з інтуїтивно зрозумілим інтерфейсом. Необхідно надавати користувачам можливість вибору різних методів MFA, якщо це можливо.

Необхідно здійснити інтеграцію MFA з системами єдиного входу (SSO), щоб зменшити кількість необхідних автентифікацій. Треба розглянути можливість використання адаптивної MFA, яка вимагає додаткової автентифікації лише за певних обставин.

Необхідно забезпечити чіткі інструкції та підтримку для користувачів щодо встановлення та використання мобільного додатка MFA. Необхідно запровадити прості процедури відновлення доступу на випадок втрати пристрою або проблем з додатком.

Необхідно забезпечити високий рівень безпеки інформаційних ресурсів організації. Для цього необхідно відмовитися від менш безпечних методів MFA, таких як SMS-коди, на користь більш надійних варіантів, таких як push-сповіщення та біометрія.

Необхідно використовувати мобільні додатки, які підтримують стійкі до фішингу методи автентифікації. Необхідно регулярно оновлювати мобільний додаток MFA та операційні системи пристроїв користувачів для усунення

вразливостей.

Необхідно навчати користувачів розпізнавати та повідомляти про підозрілі запити на автентифікацію, щоб запобігти випадковому схваленню зловмисних спроб.

Необхідно розглянути можливість використання функції відповідності номерів у push-сповіщеннях для запобігання атак з використанням MFA.

Необхідно переконатися, що обраний метод MFA відповідає вимогам відповідних стандартів та регуляцій у сфері інформаційної безпеки, таких як GDPR, PCI DSS, HIPAA, NYDFS тощо. Необхідно звернути особливу увагу на вимоги щодо використання стійкої до фішингу MFA, якщо це необхідно.

Необхідно оцінювати вартість різних рішень MFA на базі мобільних додатків та враховувати потенційне зниження витрат на підтримку IT та запобігання порушенням безпеки.

Перед масштабним впровадженням необхідно проводити пілотне тестування MFA серед невеликої групи користувачів, щоб виявити та усунути можливі проблеми. Поступово розгортайте MFA для різних підрозділів або груп користувачів, забезпечуючи належну підтримку на кожному етапі.

Регулярно проводьте навчання для користувачів щодо важливості MFA та правильного використання мобільного додатка. Пояснюйте переваги MFA для захисту їхніх облікових записів та конфіденційної інформації організації.

Підсумовуючи, в умовах еволюції та зростання небезпеки кіберзагроз, багатофакторна автентифікація перестає бути необов'язковим заходом безпеки, а стає фундаментальною вимогою для захисту організаційних даних та систем в Україні. Впроваджуючи надійні рішення MFA та навчаючи своїх користувачів, українські організації можуть значно знизити ризик стати жертвою кібератак та забезпечити більш безпечне цифрове середовище.

Дотримуючись цих рекомендацій, організації можуть успішно впровадити багатофакторну автентифікацію за допомогою мобільних додатків, значно підвищивши свій рівень безпеки та захистивши свої цінні дані.

ВИСНОВКИ

В роботі досліджено проблему автентифікації користувачів інформаційними системами організацій. Встановлено, що застосування системи багатофакторної автентифікації за допомогою мобільного додатку є важливим кроком для посилення безпеки облікових записів користувачів. Багатофакторна автентифікація додає додатковий рівень захисту, вимагаючи від користувача надати два або більше доказів ідентифікації. Це значно ускладнює несанкціонований доступ до облікового запису, навіть якщо зловмисник отримає пароль. Мобільний додаток забезпечує зручний та безпечний спосіб генерації одноразових кодів або отримання push-повідомлень для підтвердження особистості.

Визначено існуючі підходи до автентифікації користувачів інформаційними системами організацій. Впровадження багатофакторної автентифікації передбачає інтеграцію системи безпеки, яка вимагає від користувачів підтвердження своєї особи за допомогою двох або більше факторів автентифікації, таких як паролі, біометричні дані або одноразові коди.

Проаналізовано існуючі рішення для багатофакторної автентифікації користувачів. Програмне забезпечення багатофакторної автентифікації може перевірити кожного, хто намагається отримати доступ до інформації компанії, забезпечуючи надійну безпеку та зменшуючи ризик компрометації облікового запису. Користувачі зазвичай автентифікуються за допомогою застосунку, одноразового пароля, пристрою FIDO2 або біометричних даних, таких як розпізнавання обличчя або сканування відбитків пальців тощо.

Проаналізовано методи та засоби багатофакторної автентифікації користувачів за допомогою мобільного додатка на базі ESET Secure Authentication. Рішення ESET Secure Authentication забезпечує безпечний доступ до корпоративних ресурсів за рахунок застосування різних методів двофакторної автентифікації під час віддаленого підключення до них.

В роботі розглянуто порядок застосування методів та засобів багатофакторної автентифікації користувачів за допомогою мобільного додатка на базі ESET Secure Authentication. Система багатофакторної автентифікації користувачів за допомогою мобільного додатку на базі ESET Secure Authentication створюється з метою підвищення рівня безпеки. Створюється додатковий рівень захисту для облікових записів користувачів.

Для того, щоб ми змогли використовувати додаток ESET Secure Authentication на своєму мобільному пристрої, ми повинні встановити та налаштувати основну службу ESET Secure Authentication на своєму сервері, а потім надати пристрої, які ми хочемо використовувати, за допомогою мобільного додатка ESET Secure Authentication.

Розроблено рекомендації фахівцям з кібербезпеки щодо багатофакторної автентифікації користувачів інформаційними системами організацій. Впроваджуючи надійні рішення багатофакторної автентифікації та навчаючи своїх користувачів, українські організації можуть значно знизити ризик стати жертвою кібератак та забезпечити більш безпечне цифрове середовище.

Таким чином, правильна реалізація багатофакторної автентифікації користувачів має забезпечити ефективний захист корпоративних даних та кібербезпеку інформаційної системи організації.

ПЕРЕЛІК ПОСИЛАНЬ

1. John Martinez, Justin McCarthy. 11 Common Authentication Vulnerabilities You Need to Know. Last updated on: February 24, 2025. URL: https://www.strongdm.com/blog/authentication-vulnerabilities

2. Annual number of data compromises and individuals impacted in the United States from 2005 to 2024. Statista. URL: https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/

3. Ani Petrosyan. Number of data compromises and impacted individuals in U.S. 2005-2024. Statista, Apr 2, 2025. URL: https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/

4. What is MFA (Multi-Factor Authentication) Implementation? Palo Alto Networks. URL: https://www.paloaltonetworks.com/cyberpedia/what-is-mfa-implementation

5. The Complete Multi-Factor Authentication (MFA) Cheat Sheet. TrustBuilder, February 6, 2025. URL: https://www.trustbuilder.com/en/multi-factor-authentication-mfa-cheat-sheet/

6. Sharon Solomon. 8 Multi Factor Authentication Types and How to Choose. February 07, 2024. URL: https://frontegg.com/blog/multi-factor-authentication-types

7. Marisa Krystian. Top 10 multi-factor authentication (MFA) providers and software. Published Sep 19, 2024. URL: https://www.rippling.com/blog/mfa-providers

8. Joel Witts, Craig MacAlpine. The Top 11 Multi-Factor Authentication (MFA) Solutions for Business. Expert Insights, Last updated on Apr 8, 2025. URL: https://expertinsights.com/user-auth/the-top-multi-factor-authentication-mfa-solutions-for-business

9. ADSelfService Plus Evaluator's guide. URL: https://download.manageengine.com/products/self-service-password/adselfservice-plus-evaluator-guide.pdf

10. Duo Solutions for Cisco AnyConnect or Cisco Secure Client VPN with ASA or Firepower. Last Updated: April 4th, 2024. URL: https://duo.com/docs/cisco

11. Microsoft Entra. Build resilience in your identity and access management infrastructure. Article, 03/27/2025. URL: https://learn.microsoft.com/en-us/entra/architecture/resilience-in-infrastructure

12. ESET Secure Authentication On-Prem. URL: https://help.eset.com/esa/30/en-US/

13. ESET Secure Authentication. Overview. URL: https://www.eset.com/fileadmin/ESET/IL/ESET_Secure_Authentication_Product_Overview.pdf

14. [KB3297] Install and use the ESET Secure Authentication mobile app for Android. URL: https://support.eset.com/en/kb3297-install-and-use-the-eset-secure-authentication-mobile-app-for-android

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

(Презентація)