Міністерство освіти і науки України
Харківський національний університет імені В.Н. Каразіна
Навчально-науковий інститут комп'ютерних наук та штучного інтелекту
Спеціальність 125 «Кібербезпека»
Освітня програма «Кібербезпека»

«Допущено до захисту»
Зав. кафедрою КБІСМіТ
Марина ЄСІНА _____
« » червня 2025 р.

Пояснювальна записка
до кваліфікаційної роботи бакалавра
на тему: «Аналіз сучасних методів автентифікації та дослідження відомих реалізацій RSA і YubiKey»

Оцінка « »

Голова ЕК

Мичуда Л. З.

_____

Керівник: к.т.н Малахов С. В.

Рецензент: PhD, Родінко М. Ю.

Виконавець студент групи КБ41

Чудновський В. Є.

Харків – 2025

РЕФЕРАТ

Пояснювальна записка містить 58 сторінок, 11 рисунки, 9 таблиць, 1 додаток, 53 джерела.

Метою дипломної роботи є дослідження відомих методів автентифікації персоналу сучасних інформаційних систем та оцінка потенціалу використання апаратних токенів YubiKey, як перспективного засобу підтвердження повноважень легітимних користувачів.

Об’єкт дослідження – процеси автентифікації користувачів в інформаційних системах.

Предмет дослідження – апаратні засоби автентифікації користувачів, їх взаємодія з криптографічною інфраструктурою та стійкість до потенційних атак.

Методами дослідження є аналіз і узагальнення джерел інформації, та комп’ютерне моделювання, обраних для тестування, способів автентифікації в умовах впливу характерних загроз безпеки (атак).

У роботі виконано огляд класифікації методів автентифікації, зокрема: паролі, програмні токени, використання «біометрії» та апаратні пристрої. Детально проаналізовано переваги й недоліки кожного підходу. Особливу увагу приділено апаратним токенам, які забезпечують збереження приватних ключів у незавантажуваному середовищі, що значно знижує ризики компрометації.

У практичній частині досліджено роботу пристрою YubiKey, його підтримку протоколів FIDO2, WebAuthn, OTP, PIV, а також взаємодію з інструментами GPG та PKI-інфраструктурою. Розглянуто питання генерації ключів, зберігання, підпису даних, автентифікації до систем та інтеграції з Linux-середовищем. Проаналізовано реальні (найбільш ймовірні) загрози безпеки, зокрема можливість атаки через побічні канали та механізми захисту від подібних векторів.

Результати дослідження можуть бути використані у сфері кібербезпеки для підвищення поточного рівня захисту процедури автентифікації користувачів, в державних та корпоративних системах. Крім того, робота буде корисна, як

довідковий матеріал для профільних фахівців, при виборі та впровадженні політик зберігання та використання криптографічних ключів в корпоративне середовище.

Ключові слова: АВТЕНТИФІКАЦІЯ, RSA, YubiKey, SSH, АПАРАТНИЙ ТОКЕН, КРИПТОГРАФІЯ, FIDO2, WebAuthn, PKI, MFA, GPG, АТАКИ ЧЕРЕЗ ПОБІЧНІ КАНАЛИ, ІНФОРМАЦІЙНА БЕЗПЕКА, ФІШИНГ, СОЦІАЛЬНІЙ ІНЖЕНЕРИНГ.

ABSTRACT

The explanatory note contains 58 pages, 11 figures, 9 tables, 1 appendix, and 53 sources.

The aim of this thesis is to explore well-known user authentication methods in modern information systems and to assess the potential of using YubiKey hardware tokens as a promising means of verifying legitimate user credentials.

The object of the research is the user authentication processes in information systems.

The subject of the research is hardware-based user authentication tools, their interaction with cryptographic infrastructure, and their resilience to potential attacks.

The methods employed in this research include analysis and generalization of information sources, as well as computer-based modeling of selected authentication mechanisms under the influence of common security threats (attacks).

The thesis provides an overview of various authentication method classifications, including passwords, software tokens, biometric techniques, and hardware devices. The advantages and disadvantages of each approach are thoroughly analyzed. Particular attention is given to hardware tokens, which ensure the storage of private keys in non-extractable environments, significantly reducing the risk of compromise.

The practical part of the work investigates the functionality of the YubiKey device, its support for protocols such as FIDO2, WebAuthn, OTP, and PIV, and its integration with GPG tools and PKI infrastructure. Key aspects examined include key generation, storage, data signing, system authentication, and integration within a Linux environment. Realistic and likely security threats are analyzed, with a focus on side-channel attacks and the mechanisms used to defend against such vectors.

The results of this research can be applied in the field of cybersecurity to enhance the current level of user authentication protection in governmental and corporate systems. Furthermore, this work may serve as a reference for cybersecurity

professionals when selecting and implementing cryptographic key storage and usage policies in enterprise environments.

Keywords: AUTHENTICATION, RSA, YubiKey, SSH, HARDWARE TOKEN, CRYPTOGRAPHY, FIDO2, WebAuthn, PKI, MFA, GPG, SIDE-CHANNEL ATTACKS, INFORMATION SECURITY, PHISHING, SOCIAL ENGNEERING.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ ТА СИМВОЛІВ

ІБ	–	Інформаційна безпека
ІКС	–	Інформаційно-комунікаційна система
ІС	–	Інформаційна система
ОС	–	Операційна Система
ПЗ	–	Програмне забезпечення
ПК	–	Приватний (секретний) криптографічний ключ
СПЗ	–	Спеціалізоване програмне забезпечення
2FA	–	Two-Factor Authentication
AES	–	Advanced Encryption Standard
CIA	–	Три принципи ІБ: - Confidentiality, Integrity, Availability
CTAP	–	Client To Authenticator Protocol
ECDSA	–	Elliptic Curve Digital Signature Algorithm
EdDSA	–	Edwards-curve Digital Signature Algorithm
FIDO2	–	Fast Identity Online 2
GPG	–	GNU Privacy Guard
MFA	–	Multi-Factor Authentication
MitM	–	Man in the Middle
OTP	–	One-Time Password
PDF	–	Portable Document Format
PEM	–	Privacy Enhanced Mail
PGP	–	Pretty Good Privacy
PIV	–	Personal Identity Verification
PKI	–	Public Key Infrastructure
RSA	–	Rivest-Shamir-Adleman
S/MIME	–	Secure/Multipurpose Internet Mail Extensions

SE	–	Social Engineering Attack
SSH	–	Secure Shell
TLS	–	Transport Layer Security
U2F	–	Universal 2nd Factor
UX	–	User experience
VPN	–	Virtual Private Network
WSL2	–	Windows Subsystem for Linux

ВСТУП

У сучасному світі інформаційна безпека (ІБ) відіграє ключову роль у забезпеченні стабільного функціонування цифрових систем, сервісів та інфраструктур. З огляду на стрімкий розвиток технологій, питання автентифікації користувачів інформаційних систем (ІС), захисту конфіденційних даних та запобігання несанкціонованому доступу до інформаційних й апаратних ресурсів ІС, набули особливої актуальності. Одним із базових елементів систем ІБ є надійна і зручна автентифікація користувачів, що повинна забезпечувати баланс між високим рівнем захисту та юзабіліті (від англ. *usability*) застосованого рішення для окремої групи користувачів (*наприклад, процедура інтегрованої автентифікації мобільних користувачів за рахунок суміщення даних геолокаційної метки та вводу даних біометричного паролю*).

Традиційні методи автентифікації, такі як логін і пароль або зберігання приватних ключів на локальних пристроях (в т.ч. мобільних гаджетах), поступово втрачають ефективність через зростання кількості таргетованих атак та відповідних вразливостей. У відповідь на ці виклики з’являються нові технології, зокрема апаратні засоби автентифікації, які забезпечують вищу стійкість до типових загроз. Одним із найбільш відомих представників таких засобів є YubiKey – апаратний токен, що забезпечує двофакторну автентифікацію, криптографічну операційність та захист ключів на фізичному рівні.

Актуальність теми: Розвиток нових процедур і технологій автентифікації користувачів, що здатні ефективно протидіяти впливу, як вже відомих так й потенційних загроз безпеки, є важливою складовою у загальній системі заходів з кібербезпеки та суттєво поліпшує поточний рівень ІБ сучасних інформаційно-комунікаційних систем (ІКС).

Мета роботи: Порівняльне дослідження технологій RSA і YubiKey з точки зору їх безпеки, стійкості до атак й зручності використання та формування концептуальних пропозицій з покращення окремих параметрів захисту сучасних

ІКС за рахунок впровадження YubiKey, на основі узагальнення результатів аналізу специфіки обох технологій, та моделювання типових загроз.

Результати дослідження можуть бути корисними для фахівців у галузі кібербезпеки, розробників спеціалізованого програмного забезпечення (СПЗ), а також організацій і установ, які планують покращити поточний рівень захисту інформаційних ресурсів власних ІС за рахунок інтеграції рішень рівня YubiKey, не жертвуючи при цьому зручністю роботи персоналу та/чи користувачів послуг й сервісів відповідних систем.

1. ОГЛЯД СУЧАСНОГО СТАНУ МЕТОДІВ АВТЕНТИФІКАЦІЇ, ЇХ ОСНОВНІ ПЕРЕВАГИ ТА ВІДМІННОСТІ

1.1. Поняття автентифікації та її роль у проблематиці захисту інформації

Автентифікація – це процес підтвердження особи користувача або пристрою, який намагається отримати доступ до певних функцій та/чи ресурсів умовної ІКС. За своєю сутністю, ця процедура відповідає на запитання *«Хто ти є?»* та є відправною точкою в організації базових засад інформаційної безпеки, дозволяючи контролювати доступ до апаратури, даних і сервісів. При цьому, надійна автентифікація одночасно забезпечує конфіденційність, цілісність і доступність інформації – ключові аспекти моделі CIA. Крім того, без надійного способу встановлення/підтвердження особи, неможливо ефективно впровадити механізми авторизації, журналювання чи виявлення загроз.

За даними звіту Verizon DBIR 2023, близько 74% кіберінцидентів [1] від самого початку були пов’язані з втратою та/чи компрометацією облікових даних, що ґрунтовно свідчить про необхідність переходу від традиційних паролів до більш надійних рішень – наприклад, багатофакторної автентифікації, біометрії чи апаратних ключів (див. рис.1.1).

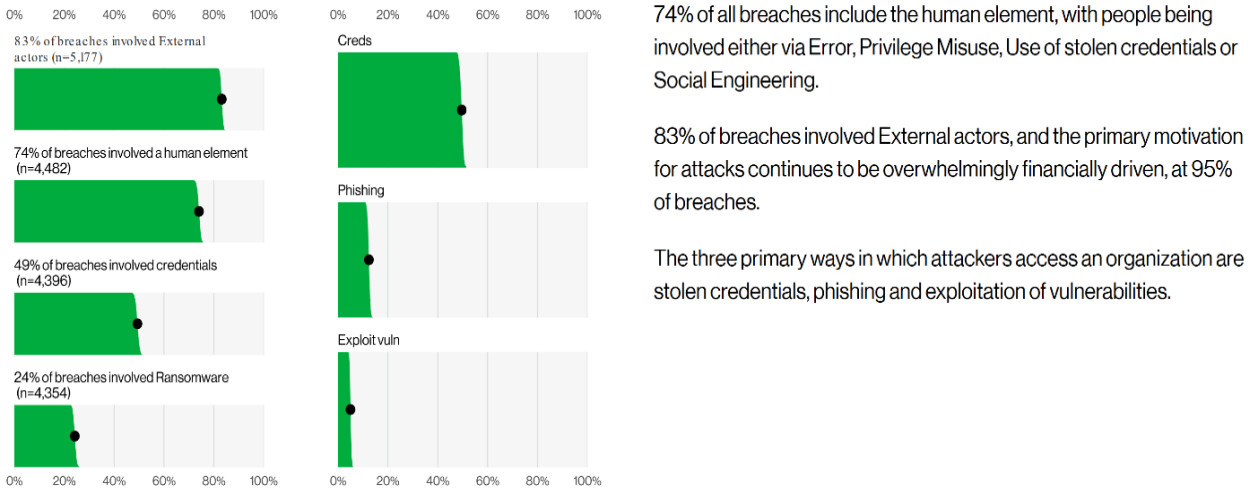

Рисунок 1.1 – Відомості про інциденти, котрі пов’язані з втратою та/чи компрометацією облікових даних *(за даними [1])*

Популярні хмарні та корпоративні сервіси, зокрема Google, Microsoft, GitHub – дедалі частіше підтримують автентифікацію на основі відкритого стандарту FIDO2 (*Fast Identity Online 2*), що забезпечує високий рівень захисту та зручність для користувачів. Стандарт FIDO2, розроблений *«FIDO Alliance»* у співпраці з *«World Wide Web Consortium»* (міжнародна організація зі стандартизації веб-технологій), передбачає використання криптографічних ключів, які зберігаються на фізичному пристрої, наприклад Yubikey, і ніколи не покидають його меж.

1.2. Основні категорії методів автентифікації

Методи автентифікації зазвичай класифікують відповідно до типу даних, які використовуються для підтвердження особи користувача. Найпоширенішими є три категорії:

- Щось, що ви знаєте (*knowledge-based*) – наприклад, пароль, *PIN*-код, відповідь на секретне запитання. Це найстаріший і найменш захищений тип автентифікації. Основна проблема – легкість підбору (*brute force attack*) або атака типу - соціальна інженерія (SE) [2 - 4].
- Щось те, що ви маєте (*possession-based*) – фізичний об’єкт, наприклад такий як смартфон з OTP-додатком *(One-Time Password)* або апаратний токен (наприклад, *YubiKey*).
- Щось, що ви є (*inherence-based*) – біометричні дані: відбитки пальців [5], розпізнавання обличчя або голосу.

Всі ці категорії часто комбінуються в рамках процедур багатофакторної автентифікації (MFA), що суттєво підвищує рівень захисту ІС від спроб несанкціонованого доступу (НСД) [6] та протидії доксінгу персональних даних [7]. Наприклад, при вході в систему банкінгу користувач вводить пароль (*щось, що знає*), підтверджує доступ через додаток на смартфоні (*щось, що має*) і додатково проходить біометричну перевірку (*щось, що є*).

На сьогодні впровадження MFA стало вимогою багатьох міжнародних стандартів, таких як NIST SP 800-63B [8], які рекомендують використання факторів, що є незалежними один від одного та не можуть бути одночасно скомпрометовані одним і тим самим інцидентом.

Згідно з даними звіту Exploding Topics за 2024 рік [9], найпоширенішими методами багатофакторної автентифікації (MFA) є одноразові паролі, що надсилаються через SMS (55,96%) та електронну пошту (51,38%). Також значна частка користувачів застосовує *push*-сповіщення на мобільні пристрої (36,7%) та апаратні токени, такі як YubiKey (20,18%). Біометричні методи, включаючи відбитки пальців та розпізнавання обличчя, використовуються приблизно 26% організацій, що свідчить про зростаючу довіру до інгерентних факторів автентифікації (див. рис.1.2):

Multi-Factor Authentication (MFA) Method	Share of Respondents
SMS TOTPs	55.96%
Email TOTPs	51.38%
Mobile device push notifications	36.7%
Email OTPs (not time-based)	30.28%
SMS OTPs (not time-based)	30.28%
Email web links	26.61%
QR code scanned by mobile device	26.61%
SMS web links	25.69%
PC push notifications	21.1%
Hardware token	20.18%
Fast Identity Online (FIDO) security keys	16.51%
FIDO mobile authenticator	13.76%

Рисунок 1.2 – Розподіл найпопулярніших форм MFA (*за даними* [9])

1.3. Традиційні методи автентифікації

Традиційні методи автентифікації використовують принципи перевірки даних, що належать користувачу, частіше за все на основі знань або володіння. Найбільш поширеними серед них є [10]:

- Паролі та PIN-коди. Це найбільш широко використовуваний метод, що базується на знанні користувачем секретної інформації, яку він вводить для доступу до системи. Однак, цей метод є вразливим до атак методом підбору чи через використання слабких паролів. Статистика показує, що 81% порушень ІБ сталися саме через «слабкі» чи викрадені паролі [1].
- Токени. Вони використовуються для надання доступу на основі фізичного пристрою, що містить унікальний код. До прикладу, старі методи автентифікації включають апаратні токени, які генерують одноразові паролі (OTP). Хоча цей метод безпечніший за паролі, він може бути вразливим до викрадення пристроїв або витоку даних.
- Картки доступу *(наприклад, смарт-картки).* Вони використовують вбудовану електронну мікросхему, яка зберігає криптографічний ключ. Цей метод застосовується для автентифікації в корпоративних системах і фінансових установах [11]. Незважаючи на підвищену безпеку, картки можуть бути втрачені або вкрадені.

Традиційні методи, хоч і широко використовуються, однак при цьому часто не забезпечують достатньо високого рівня захисту, що спонукає до розробки більш надійних, багатофакторних рішень, таких як MFA (*багатофакторна автентифікація*), які поєднують відразу кілька з методів автентифікації [10]. Більшість організацій зараз активно інтегрують MFA, щоб зменшити ймовірність компрометації [9].

1.4. Сучасні методи автентифікації

Сучасні методи автентифікації спрямовані на подолання вразливостей, які характерні для традиційних підходів і використовують новітні технології для

підвищення поточного рівня безпеки. Сучасні методи автентифікації поєднують наступні основні складові:

- Біометрична автентифікація. Цей метод використовує фізичні характеристики людини, такі як відбитки пальців [5], розпізнавання обличчя, райдужки ока або голосові зразки для підтвердження особи. Біометричні системи надають високий рівень безпеки, оскільки важко підробити або викрасти біометричні дані користувача. Сьогодні ці технології інтегруються в смартфони, ноутбуки та навіть системи банківської безпеки. Згідно з даними [12], 56% усіх нових мобільних пристроїв надають можливість біометричної автентифікації.
- Багатофакторна автентифікація (MFA). MFA є стандартом у більшості сучасних інформаційних систем і передбачає використання кількох незалежних факторів для підтвердження особи. Це може бути комбінація пароля, біометричних даних, фізичних токенів або OTP. Наприклад, популярні сервіси, такі як Google, Microsoft та Apple, використовують MFA для захисту акаунтів користувачів [13]. Таке рішення істотно знижує ймовірність несанкціонованого доступу, навіть якщо один із факторів вже скомпрометовано.
- Апаратні токени. Технології, як YubiKey, використовують апаратні пристрої для забезпечення високої безпеки при автентифікації. YubiKey підтримує FIDO2, U2F (Universal 2nd Factor), та інші протоколи для автентифікації без використання паролів, що робить ці пристрої ефективними для захисту акаунтів і корпоративних ІС. У порівнянні з традиційними методами, наприклад такими як паролі, апаратні токени зменшують вразливість до фішингових атак, оскільки зловмисник не може отримати фізичний доступ до токена через мережу [14].
- FIDO2. Це відкритий стандарт автентифікації, який забезпечує автентифікацію без паролів, використовуючи криптографію з відкритим ключем для підтвердження особи. *FIDO2* включає два основних компоненти: *WebAuthn*, що є інтерфейсом для веб-додатків, та *CTAP*

(Client To Authenticator Protocol), який дозволяє використовувати апаратні пристрої для автентифікації. Цей стандарт широко підтримується провідними технологічними компаніями, такими як *Google, Microsoft* та *Facebook*. *FIDO2* стає стандартом для автентифікації в багатьох онлайн-сервісах, завдяки своїй високій безпеці та зручності для користувачів.

В цілому, сучасні методи автентифікації не тільки підвищують безпеку, але й значно полегшують доступ користувачів до їхніх облікових записів, знижуючи ризики викрадення паролів і захищаючи дані від фішингових атак та інших видів їх злому. Водночас, ці технології вимагають постійного оновлення та інтеграції з іншими системами для досягнення оптимального рівня захисту [10].

1.5. Порівняння методів за ключовими характеристиками

Для визначення оптимального, для умов конкретної ІКС, методу автентифікації, важливо враховувати низку ключових характеристик, таких як рівень безпеки, зручність для користувачів, вартість впровадження, масштабованість та стійкість до атак. У таблиці 1.1 наведено порівняння основних методів:

Таблиця 1.1 – Порівняння методів автентифікації

Метод автентифікації	**Рівень безпеки**	**Зручність**	**Вартість**	**Захист від фішингу**	**Потреба у додатковому обладнанні**
Пароль	Низький	Висока	Низька	Низький	Ні
SMS/Email OTP	Середній	Середня	Низька	Низький	Ні
Біометрія	Високий	Висока	Середня	Високий	Так
Апаратні токени	Дуже високий	Висока	Висока	Дуже високий	Так
FIDO2/WebAuthn	Дуже високий	Висока	Середня	Дуже високий	Можливо
MFA	Високий	Середня	Середня	Високий	Можливо

Деякі пояснення до відомостей таблиці 1.1:

- Рівень безпеки: Біометричні та апаратні методи забезпечують найвищий рівень захисту, особливо у поєднанні з багатофакторною автентифікацією.
- Зручність: Паролі залишаються найпростішими у використанні, однак новітні методи, як-от *Face ID* або *FIDO2*, демонструють зростання популярності завдяки зручному UX.
- Захист від фішингу: Традиційні методи, що базуються на паролях або SMS, вразливі до фішингових атак, тоді як криптографічні підходи (*наприклад, FIDO2*) виключають можливість передачі секретної інформації через інтернет [15].

Більшість сучасних організацій переходять на багатофакторну автентифікацію або стандарти, як-от FIDO2, для зменшення ризиків. Наприклад, у звіті [1] вказано, що 74% витоків даних у 2023 році були пов’язані із компрометацією облікових даних, що вкотре підтверджує необхідність переходу до безпарольних та більш надійних рішень.

1.6. Труднощі та виклики сучасної автентифікації

Попри значний розвиток технологій автентифікації, існує низка викликів (загроз), які суттєво впливають на безпеку й зручність використання відповідних процедур. Однією з головних проблем є загроза викрадення облікових даних, що досі залишається основним вектором атак [2-4]. Паролі можуть бути слабкими, багаторазово використовуваними чи викраденими через фішинг і SE.

Іншою серйозною загрозою є недостатній захист одноразових кодів, зокрема тих, що надсилаються через SMS повідомлення, оскільки такі повідомлення можуть бути перехоплені або «зламані» через атаки на мобільні мережі (наприклад, *SIM-swap [16]*). Також слід відзначити низький рівень впровадження багатофакторної автентифікації (MFA) в малих організаціях чи серед звичайних користувачів, що часто обумовлено складністю налаштування або браком знань та необхідного досвіду.

Також, варто зазначити що і сучасні методи автентифікації, попри вищу безпеку (*наприклад, FIDO2, апаратні токени*), мають певні труднощі у

впровадженні: - високу вартість, необхідність сумісності з існуючими системами, а також супротив персоналу до відповідних процедурних змін. Це, в свою чергу, створює потребу у балансі між зручністю, вартістю [17] та рівнем безпеки.

Висновки за Розділом:

1) Автентифікація – критично важливий етап у захисті інформаційних систем, оскільки саме вона визначає, хто отримує доступ до ресурсів, і є основою для авторизації, журналювання та виявлення загроз.

2) Традиційні методи (паролі, PIN-коди, токени) мають серйозні вразливості – зокрема, до соціальної інженерії, підбору або втрати пристроїв. Близько 74% кіберінцидентів пов’язані з компрометацією облікових даних.

3) Сучасні методи автентифікації (біометрія, багатофакторна автентифікація, FIDO2) значно підвищують рівень безпеки, поєднуючи кілька факторів, які складно скомпрометувати одночасно.

4) MFA стало стандартом безпеки: його впровадження вимагається багатьма міжнародними нормами (наприклад, NIST SP 800-63B), а підтримка FIDO2 поширюється в найбільших цифрових екосистемах (*Google, Microsoft, GitHub*), зокрема із застосуванням апаратних ключів як YubiKey.

2. УЗАГАЛЬНЕННЯ ПРИНЦИПІВ РОБОТИ І ДОСВІДУ ВПРОВАДЖЕННЯ ТЕХНОЛОГІЙ RSA ТА YUBIKEY В СУЧАСНИХ ІС

2.1 Особливості криптографії з відкритим ключем

Криптографія з відкритим ключем (асиметрична криптографія) є основою багатьох сучасних механізмів автентифікації та цифрової безпеки. Її принципова особливість, це використання пов’язаної пари криптографічних ключів: – публічного (*відкритого*) та приватного (*закритого*). Принцип дії полягає в тому, що дані, котрі зашифровані одним ключем, можуть бути розшифровані лише іншим з цієї пари, і навпаки.

У контексті реалізації механізмів автентифікації, асиметрична криптографія дозволяє створювати цифрові підписи та забезпечувати цілісність даних. Користувач «підписує» повідомлення своїм приватним ключем, а сервер або система перевіряє підпис, використовуючи відповідний публічний ключ. Таким чином, підтверджується автентичність відправника без передачі конфіденційної інформації по каналах зв’язку незахищених мереж.

Асиметричні алгоритми, зокрема RSA, ECDSA (*Elliptic Curve Digital Signature Algorithm*), EdDSA (*Edwards-curve Digital Signature Algorithm*), широко використовуються в таких сферах як:

- Протоколи безпечного з'єднання: Transport Layer Security (TLS), Secure Schell (SSH);
- Електронний документообіг і цифрові підписи: Secure/Multipurpose Internet Mail Extensions (S/MIME), Portable Document Format (PDF), Pretty Good Privacy (OpenPGP);
- Автентифікація користувачів через криптографічні токени (YubiKey, smart cards).

Однак важливо розуміти, що криптографія з відкритим ключем має високу обчислювальну складність [18], тому у багатьох системах вона використовується лише на етапі встановлення сесії або підтвердження особи, а вже далі інформація

передається по «симетричному каналу» (наприклад, з використанням алгоритму *Advanced Encryption Standard* (AES) [19]). Так, згідно з даними аналітичного звіту [20], понад 94% веб-сайтів у світі використовують HTTPS-з'єднання на основі TLS, що майже завжди базується на криптографії з відкритим ключем. При цьому найбільш поширеними алгоритмами залишаються RSA (2048 біт) та ECDSA (P-256), де ECDSA поступово набирає популярності завдяки своїй ефективності (див. табл.2.1).

Таблиця 2.1 – Відомості щодо специфіки з'єднань на основі TLS [20]

Алгоритм	***Частка серед TLS-сертифікатів (за 2024 р)***
RSA (2048)	61%
ECDSA (P-256)	35%
Інші (EdDSA, DSA)	4%

Таким чином, криптографічні протоколи/стандарти з відкритим ключем – це фундамент для безпечної цифрової взаємодії, яка забезпечує процедури автентифікації і шифрування, що лежать в основі технологій на кшталт YubiKey.

2.2 Алгоритм RSA: архітектура та особливості

RSA (*від прізвищ розробників Rivest, Shamir та Adleman*) – один із найстаріших та найбільш вживаних алгоритмів асиметричного шифрування, названий на честь своїх авторів: Рон Рівест, Аді Шамір і Леонард Адлеман. Він був вперше розглянутий у 1977 році та досі залишається стандартом для забезпечення задач конфіденційності, цифрового підпису та автентифікації користувачів [21]. Алгоритм RSA є асиметричним алгоритмом шифрування та базується на математичній складності факторизації великих цілих чисел. Схема генерації ключів включає:

- Вибір двох великих простих чисел p та q;
- Обчислення модуля $n = p * q$, який входить до складу як відкритого, так і закритого ключа;
- Вибір експоненти e для відкритого ключа та розрахунок відповідного d для приватного ключа.

Відкритий ключ: (n, e).

Приватний ключ: (n, d).

Шифрування та підпис даних відбувається за формулами:

- Шифрування: $c = m^e \ mod \ n$;
- Розшифрування: $m = c^d \ mod \ n$.

Аналогічно для цифрового підпису – навпаки: спочатку дані підписуються закритим ключем, потім перевіряються відкритим.

Попри ефективність і перевірену безпеку, RSA має кілька особливостей:

- Потребує більших розмірів ключа для гарантування стійкості (мінімум 2048 біт);
- Порівняно повільний в обчисленнях (особливо для мобільних та вбудованих пристроїв);
- Широко використовується для встановлення ключів (наприклад, у TLS), але не для симетричного шифрування сесій.

YubiKey, популярний апаратний токен, підтримує генерацію і зберігання RSA-ключів у захищеній пам’яті. Пристрій реалізує інтерфейс PIV (*Personal Identity Verification*), згідно з вимогами NIST SP 800-73, що дозволяє підписувати документи та провести автентифікацію користувача за допомогою RSA [22].

RSA, також, широко підтримується в таких середовищах:

- OpenSSH (SSH автентифікація) [23];
- Microsoft Active Directory (*зокрема через смарт-карти*) [24];
- Java Cryptography Architecture (JCA) і PKCS#11 [25].

2.3 Сутність апаратної автентифікації: загальна концепція і розвиток

В загальному уявленні апаратна автентифікація – це метод підтвердження особи користувача за допомогою апаратної фізичного пристрою, який зберігає секретні криптографічні ключі та здійснює операції автентифікації локально, не розкриваючи сам ключ. Основною перевагою такого підходу є високий рівень безпеки (див. табл.2.2), оскільки приватний ключ (PK) ніколи не залишає цього пристрою. Такі пристрої зазвичай використовують [26]:

- Асиметричну криптографію (RSA, ECC);
- Протоколи OTP, FIDO2/WebAuthn, PIV;
- Двофакторну автентифікацію (2FA).

Таблиця 2.2 – Переваги апаратної автентифікації над її програмними релізами

Характеристика	Програмна автентифікація	Апаратна автентифікація
Захист від викрадення ключа	Низький	Високий
Стійкість до фішингу	Середня	Висока
Необхідність додаткового ПЗ	Так	Ні *(в більшості випадків)*
Переносимість	Висока	Залежить від формфактора

Особливо важливою є стійкість до фішингу: - згідно з [1], більшість компрометацій відбуваються саме через крадіжку облікових даних, що знижує ефективність паролів або SMS-кодів.

Приклади пристроїв апаратної автентифікації:

1) YubiKey (Yubico) – підтримує FIDO2, OTP, PIV, OpenPGP, U2F;
2) Feitian ePass, SoloKeys, Nitrokey – open-source варіанти;
3) Google Titan Key – створений спеціально для захисту Google-акаунтів співробітників [27];
4) Thales eToken – активно використовується в банківському секторі.

Розвиток стандартів. В останні роки впровадження апаратної автентифікації на основі стандартів FIDO2 та WebAuthn суттєво прискорилося в усьому світі. Ці технології дозволяють користувачам входити до облікових записів без паролів, використовуючи апаратні токени або біометричні дані, що значно підвищує рівень безпеки та зручності.

На основі доступних джерел, зокрема FIDO Alliance, Identity Week та інших публічних аналітичних звітів [28-29], можна отримати орієнтовну оцінку темпів впровадження *passkeys* у різних країнах з 2018 по 2024 рр. Наведені дані можуть варіюватися залежно від методології збору інформації та специфіки обчислення

показників. Гістограма на рис.2.1 ілюструє цю динаміку для п’яти країн, що демонструють найбільші темпи зростання відповідного процесу.

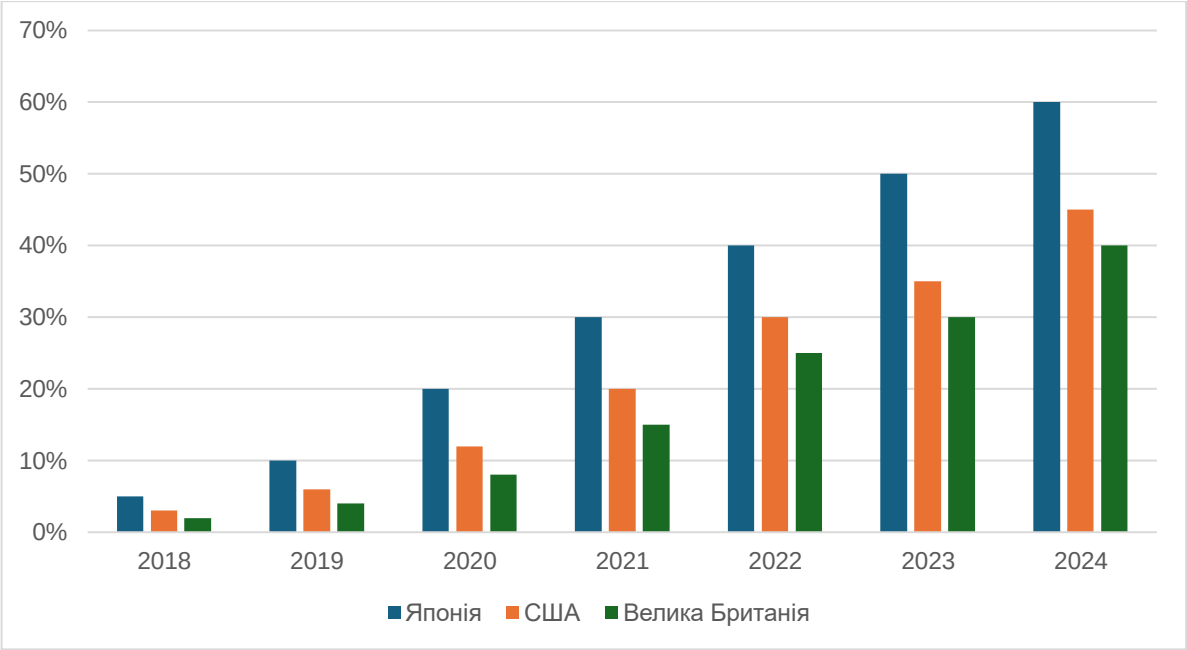

Рисунок 2.1 – Динаміка впровадження *passkeys* в різних країнах *(за даними [28 - 29])*

Деякі уточнення сутності динаміки процесів на рис.2.1:

- Японія: Лідер у впровадженні passkeys завдяки активній підтримці приватного сектору та академічних установ. Згідно з FIDO Alliance (2024) [28], компанії Nikkei, Nulab та Tokyu Corporation масово переходять на passwordless-автентифікацію. Наприклад, 45% користувачів TOKYU ID вже використовують passkeys, а Nikkei планує повномасштабний перехід до лютого 2025 року. Це підтверджує високі темпи адоптації — 50% у 2023 році та прогнозовані 60% у 2024;
- США: Згідно з звітом Identity Week (2024) [29], 87% американських компаній вже впроваджують passkeys, з 47% використовуючи гібридний підхід (апаратні токени та синхронізовані passkeys). Це забезпечило адоптацію на рівні 35% у 2023 році з прогнозом до 45% у 2024;
- Велика Британія: Європейський ринок розвивається дещо повільніше через жорсткі регуляторні вимоги (наприклад, GDPR). Однак деякі банки (наприклад, *HSBC* і *Barclays*) та фінтех-компанії почали масово

впроваджувати passkeys, що дозволило досягти 30% адоптації у 2023 році [29].

2.4 YubiKey: структура та функціональні можливості

YubiKey – це компактний апаратний токен, розроблений компанією Yubico [14] для забезпечення високого рівня автентифікації та захисту доступу до ІС. Пристрій виготовлений у вигляді USB-ключа або NFC-токена і підтримує широкий спектр стандартів безпеки [30].

Фізично YubiKey (див. рис.2.2) має захищений мікроконтролер, вбудовану пам'ять для зберігання криптографічних ключів та інтерфейси для підключення (*USB-A, USB-C, NFC*). Пристрій не має батареї або вбудованого дисплея, що підвищує його надійність та знижує ризик апаратних атак.

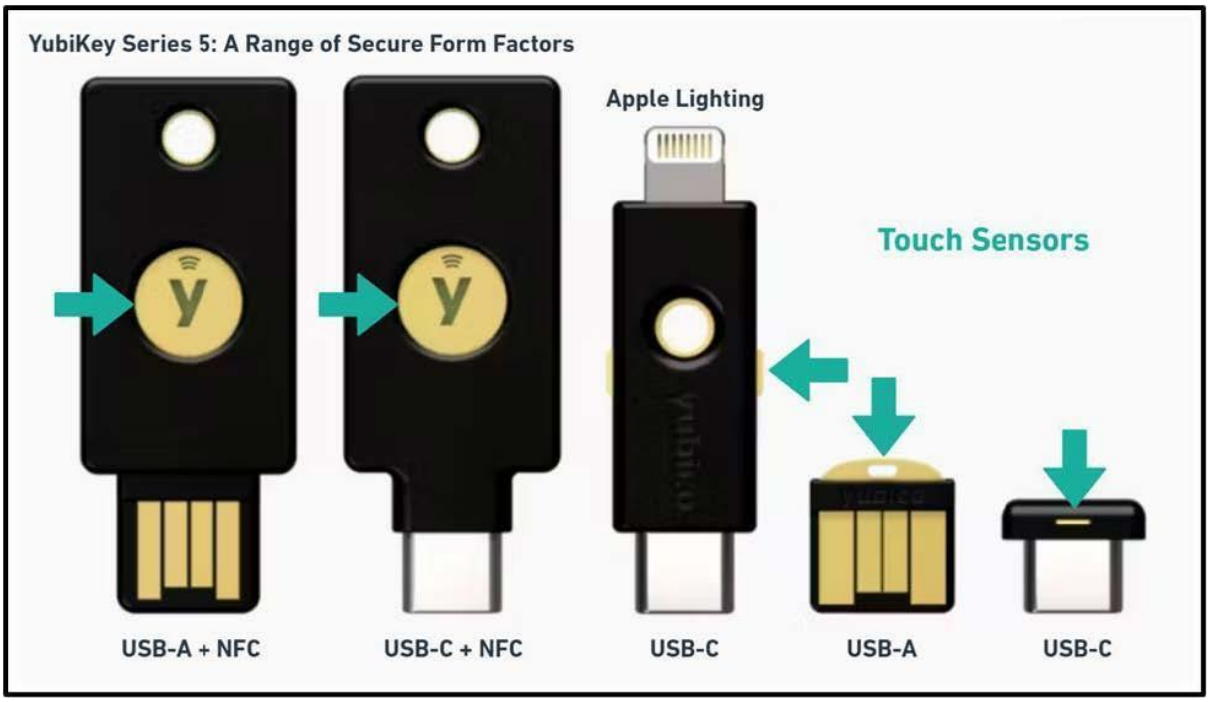

Рисунок 2.2 – Варіанти виконання апаратних токенів YubiKey [31]

Основні функції складових елементів апаратних токенів:

- Захищений елемент (Secure Element) для зберігання приватних ключів;
- Механізми генерації одноразових паролів (OTP);
- Підтримка криптографічних операцій на пристрої без витоку приватного ключа за межі конструктиву токена;

- Функціональність управління (натискання або дотику) для ініціації процедури автентифікації.

Відомі реалізації YubiKey одночасно підтримують декілька методів автентифікації (див. табл.2.3), що дозволяє використовувати YubiKey для різних задач одночасно: - від входу в облікові записи до підписання електронних документів.

Таблиця 2.3 – Основні протоколи та функції апаратних токенів YubiKey

Протокол	**Опис** ***(функції та завдання)***
OTP	Генерація одноразових кодів автентифікації
FIDO U2F / FIDO2	Безпарольна автентифікація на базі відкритих стандартів
PIV ***(Personal Identity Verification)***	Управління RSA та ECC сертифікатами для цифрового підпису та автентифікації
OpenPGP	Зберігання ключів для шифрування, підпису та автентифікації у системах, що підтримують OpenPGP
Smart Card (CCID)	Робота як смарт-карта для цілей корпоративної автентифікації

2.5 Аналіз прикладів впровадження RSA та YubiKey

Апаратні рішення для автентифікації, такі як RSA SecurID та YubiKey, вже тривалий час застосовуються в різних сферах діяльності. Наприклад, у 2003 році RSA SecurID займав понад 70% ринку двофакторної автентифікації [32], а до того часу було виготовлено понад 25 мільйонів пристроїв. Ці токени широко використовувалися у банківській сфері для захищеного доступу до внутрішніх систем через Virtual Private Network (VPN), а також у корпоративних мережах для автентифікації співробітників за межами офісу. Урядові установи також активно застосовували RSA SecurID для захисту конфіденційної інформації, прив'язуючи апаратні токени до облікових записів конкретних співробітників.

Рішення YubiKey, у свою чергу, забезпечує підтримку сучасних стандартів автентифікації, включно з FIDO2, U2F, PIV та OpenPGP. Так наприклад, компанія Google впровадила обов'язкове використання YubiKey для всіх співробітників, що дало змогу повністю ліквідувати «успішні» атаки фішингу [3].

У фінансовому секторі YubiKey активно використовується для підпису електронних документів і автентифікації в корпоративних системах. Зокрема, одна з глобальних фінансових компаній впровадила понад 10 000 YubiKey Nano для підтвердження транзакцій у роздрібних відділеннях, що дозволило зменшити витрати на понад 12 мільйонів доларів США та значно підвищити безпеку операцій [33].

Освітні заклади також інтегрують апаратну автентифікацію для захисту доступу студентів та викладачів до навчальних порталів. Наприклад, Collège de Paris впровадив YubiKey для безпарольного входу, автентифікації в хмарних сервісах та фізичного доступу до приміщень, що дозволило спростити процеси автентифікації та підвищити рівень безпеки [34].

Крім того, YubiKey застосовується в інфраструктурах відкритих ключів (PKI), де він виконує функції безпечного зберігання сертифікатів для цифрового підпису та шифрування даних. Наприклад, місто Southgate у США впровадило YubiKey разом із сертифікатною автентифікацією Microsoft Entra для захисту муніципальної інфраструктури, що дозволило досягти високого рівня відповідності вимогам безпеки [35]. Ці приклади демонструють широке впровадження YubiKey у різних сферах, що підтверджує ефективність апаратної автентифікації в забезпеченні високого рівня ІБ та зручності для користувачів.

Окремі порівняльні характеристики процесу впровадження RSA SecurID та YubiKey наведено в табл. 2.4. Як видно, сучасні вимоги до інформаційної безпеки, зокрема захист від атак типу MitM (*Man-in-the-Middle*) та фішингу [3,36], зумовлюють підвищений інтерес до використання багатофункціональних апаратних токенів нового покоління, наприклад таких, як YubiKey.

2.6 Технічні аспекти інтеграції YubiKey до складу комплексних систем безпеки сучасних ІС

Процес інтеграції YubiKey в реальні системи автентифікації передбачає декілька ключових етапів, які мають бути дотримані для забезпечення максимальної ефективності та безпеки використання пристрою. Перед початком

налаштування важливо мати фізичний доступ до YubiKey і переконатися у його зовнішньої цілісності і справності (заявленої функціональності). Так наприклад, для користувачів пристроїв серії «YubiKey Bio» необхідно заздалегідь зареєструвати відбиток пальця, оскільки це є передумовою роботи біометричної автентифікації з цим токеном [37].

Таблиця 2.4 – Порівняння впровадження RSA SecurID та YubiKey

Критерій	RSA Secur ID	YubiKey
Підтримка стандартів	Власний протокол OTP	FIDO2, OTP, PIV, OpenPGP
Адміністрування	Потребує синхронізації та заміни токенів	Мінімальне налаштування, автопідтримка
Гнучкість використання	Лише автентифікація OTP	Автентифікація, підпис, шифрування
Захист від фішингу	Частково	Повний захист (FIDO2/WebAuthn)

Типові кроки налаштування YubiKey виглядають наступним чином:

1) Вибір сумісного сервісу.

До найпоширеніших належать *Google, Microsoft, Dropbox* та інші. При цьому необхідно враховувати, що кожен сервіс має власний механізм реалізації підтримки апаратних ключів, тому специфіка налаштування може дещо відрізнятися. Для отримання актуальної інформації, щодо сумісних сервісів, слід використовувати каталог «Works With YubiKey» (див. рис.2.3, [38]).

2) Перевірка параметрів безпеки акаунту.

Наступним етапом є перевірка доступних опцій безпеки в обраному сервісі. Після входу в обліковий запис необхідно перейти до налаштувань безпеки та знайти такі опції, як:

- Двофакторна автентифікація (2FA);
- Багатофакторна автентифікація (MFA);
- Налаштування «Security Key» або «Authentication App».

У залежності від доступних варіантів, YubiKey може бути інтегрований через один із підтримуваних механізмів: – додавання апаратного ключа безпеки,

використання автентифікатора або створення секретного криптографічного ключа (Passkey).

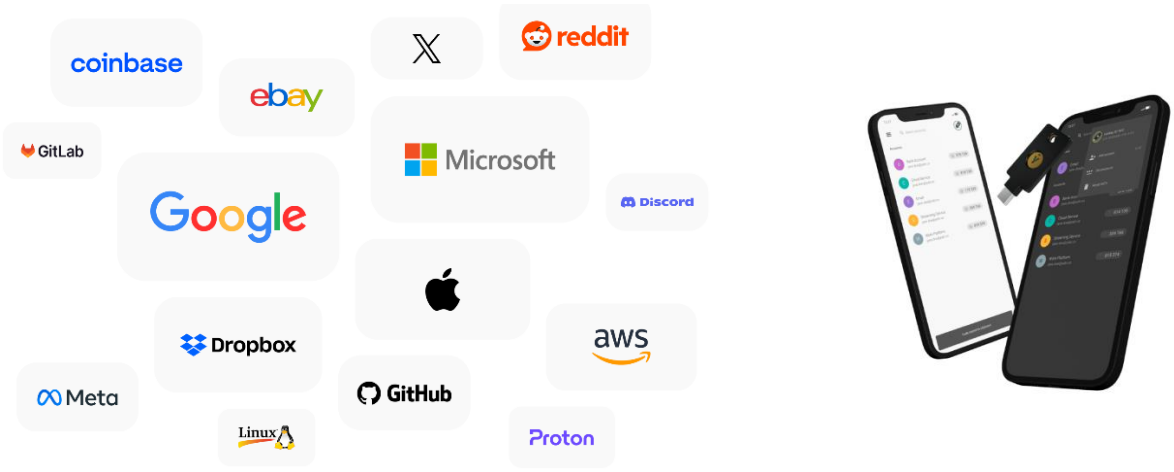

Рисунок 2.3 – Сервіси підтримки апаратних токенів

3) Додавання YubiKey.

Підключення криптотокену YubiKey виконується шляхом його фізичного під'єднання до USB-порту або використання NFC для мобільних пристроїв. Важливо пам'ятати, що при першому використанні NFC-інтерфейсу, необхідно спочатку активувати пристрій через підключення до USB-джерела живлення. Далі користувачу необхідно слідувати інструкціям обраного сервісу (див. рис.2.3), які зазвичай ініціюються натисканням відповідної кнопки на YubiKey (див. рис.2.2) або підтвердженням через браузер для завершення процедури прив’язки ключа.

На сьогодні практично використовуються три основні способи інтеграції токенів YubiKey, котрі залежать від підтримуваного протоколу:

- Використання «Security Key MFA», що є найбільш поширеним варіантом, передбачає додавання апаратного ключа безпосередньо до облікового запису користувача (див. рис.2.4);
- Використання Yubico Authenticator для генерації одноразових кодів (*у разі, якщо сервіс підтримує автентифікацію через додаток*);
- Налаштування Passkey — сучасного стандарту автентифікації, що дозволяє створювати криптографічно захищені облікові дані для доступу до цифрових сервісів без використання традиційних паролів.

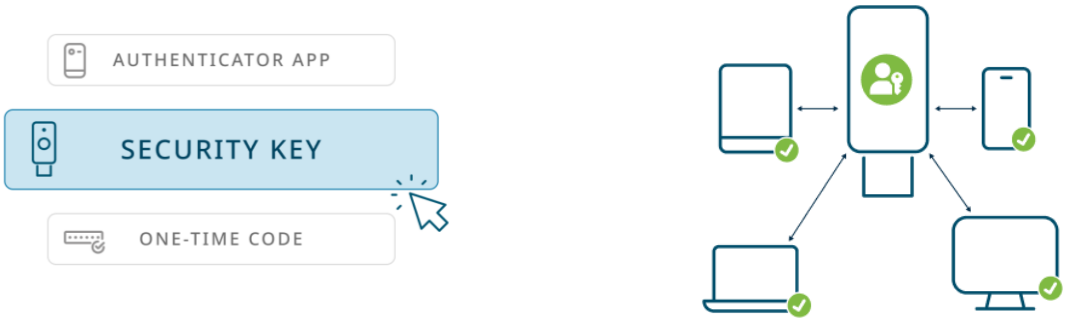

Рисунок 2.4 – Користувальницький інтерфейс і платформи Security Key MFA

В основі *Passkey* лежить криптографія з відкритим ключем, де приватний ключ (ПК) зберігається на пристрої користувача (наприклад, у YubiKey, смартфоні або комп'ютері), а публічний ключ передається до сервера для автентифікації.

Механізм роботи Passkey:

- Реєстрація: Користувач створює облікові дані (Passkey) шляхом генерації пари ключів. ПК зберігається локально, а публічний ключ – на сервері;
- Авторизація: Під час входу користувач підтверджує свою особу за допомогою біометричних даних або PIN-коду, а пристрій використовує приватний ключ для підпису автентифікаційного запиту;
- Перевірка: Сервер перевіряє підпис, використовуючи публічний ключ, та надає доступ до ресурсу у разі успішної верифікації.

Таким чином, Passkey усуває ризики, пов’язані з крадіжкою паролів, фішингом та атаками типу MitM, оскільки приватний ключ ніколи не передається до сервера і не підлягає компрометації.

4) Наявність резервного ключа.

При використанні апаратних ключів YubiKey додатково рекомендується завжди мати дублюючий токен, налаштований «паралельно» з основним. Це дозволяє забезпечити безперервний доступ до облікових записів у разі втрати або пошкодження основного пристрою. Налаштування резервного ключа здійснюється за тією ж процедурою, що і для основного (розглянуто вище).

5) Перевірка роботи.

Після завершення налаштування важливо провести тестування: спробувати увійти до облікового запису із використанням нового *YubiKey*. Якщо пристрій не

запитується, необхідно перевірити налаштування безпеки або можливу активацію функцій «*Trusted Devices*», які можуть обмежувати використання додаткових факторів автентифікації.

YubiKey зазвичай готовий до використання без необхідності попереднього налаштування, однак для певних специфічних сценаріїв може знадобитися використання додаткового ПЗ, такого як *Yubico Authenticator* або *YubiKey Manager*. У більшості випадків рекомендується змінювати конфігурацію пристрою лише за вказівкою відповідного сервісу або адміністратора системи.

Таким чином, правильна інтеграція *YubiKey* значно підвищує загальний рівень безпеки облікових записів і забезпечує надійний захист даних навіть у випадках втрати або компрометації традиційних методів автентифікації.

Висновки за Розділом:

1) Асиметрична криптографія є базовим компонентом сучасної цифрової безпеки, забезпечуючи автентифікацію, цілісність даних і шифрування на основі пари відкритого та закритого ключів.

2) Алгоритм RSA – один із найпоширеніших асиметричних алгоритмів, що використовується для захисту даних, цифрових підписів і встановлення ключів у безпечних протоколах, таких як TLS / SSH.

3) YubiKey та інші апаратні токени реалізують підтримку RSA і інших криптографічних алгоритмів, зберігаючи ключі у фізично захищеному середовищі, що суттєво підвищує загальний рівень безпеки.

4) Сучасні стандарти автентифікації (зокрема FIDO2 і WebAuthn), що підтримуються апаратними токенами, активно впроваджуються у світі, обумовлюючи відмову від використання традиційних паролів при одночасному підвищенні зручності доступу і покращенні рівня ІБ.

3. ПОРІВНЯЛЬНИЙ АНАЛІЗ СТАНУ БЕЗПЕКИ СИСТЕМ З RSA І YUBIKEY ТА ДОСЛІДЖЕННЯ ПИТАНЬ ЗРУЧНОСТІ ВИКОРИСТАННЯ YUBIKEY

3.1 Специфіка проведення порівняльного аналізу RSA та YubiKey

З огляду на зростаючу потребу у надійних механізмах автентифікації, порівняння традиційних криптографічних рішень, в даному випадку RSA, з відомими реалізаціями апаратних токенів, такими, як YubiKey, є важливою складовою процесу оцінки, фактичного рівня ІБ сучасних організацій. Оскільки ці технології мають принципово різну архітектуру, то для їх об’єктивного аналізу необхідно спиратись на чітко визначені критерії. Відповідно, у цьому дослідженні використано системний підхід, згідно з яким безпекові і експлуатаційні характеристики кожної з технологій оцінювалися за наступними аспектами (критеріями):

- Принципи генерації та зберігання ключів (зокрема — де саме і як формується приватний ключ);
- Стійкість до типових атак (фішинг, перехоплення, клонування, MitM);
- Вимоги до програмного забезпечення та складність інтеграції;
- Зручність користування з погляду кінцевого користувача і адміністратора;
- Можливості масштабування в корпоративному середовищі.

Кожен із цих аспектів докладно розглядається у наступних підрозділах (3.2–3.3), а зведена характеристика наведена у таблиці 3.1, п. 3.4. Такий хід логіки розгляду, дозволяє сформувати не лише загальне уявлення про ці технології, а й забезпечує практичну цінність і наочність результатів аналізу для прийняття рішень, щодо впровадження тієї чи іншої автентифікаційної інфраструктури.

Таким чином, мета цього розділу – не лише порівняти два окремі підходи, а й обґрунтувати вибір більш надійного та зручного механізму автентифікації користувачів для в умовах впливу сучасних загроз ІБ [2-4].

3.2 Особливості забезпечення безпеки систем з використанням RSA

Системи автентифікації, побудовані на основі RSA, ґрунтуються на принципах асиметричної криптографії, де пара ключів (відкритий і закритий) забезпечує ідентифікацію та захист доступу. Однак, попри математичну надійність алгоритму, на практиці захищеність таких систем значною мірою залежить від умов зберігання та використання приватного ключа [1] .

Так наприклад, у типовій реалізації приватний ключ зберігається у файловій системі пристрою користувача, зазвичай у форматі *Privacy Enhanced Mail* (PEM) або P12, захищеному паролем. Проте така система має наступні недоліки:

- у випадку доступу до файлової системи зловмисник може скопіювати файл і здійснити офлайн-атаку на пароль;
- користувач може несвідомо зберігати ключі у відкритому вигляді або синхронізувати їх через хмарні сервіси;
- зловмисне ПЗ (*keyloggers, sniffing malware*) може перехопити ключі в момент їх використання.

Також RSA-системи особливо вразливі до SE- атак [2, 4]. В цьому разі, якщо користувач вводить пароль або використовує ключ на фальшивому сайті, зловмисник може отримати доступ до ресурсів без жодного криптоаналізу. Крім того, в умовах ненадійного мережевого середовища можливі атаки типу MitM, якщо автентифікація не супроводжується перевіркою цілісності домену або TLS-сертифікатів. Більш того, у реальних корпоративних сценаріях проблеми тільки посилюються:

- складно забезпечити контроль над приватними ключами для великої кількості користувачів;
- адміністратори змушені реалізовувати власні політики безпеки (*наприклад, ротація ключів, логування доступу, шифрування носіїв*);
- інтеграція з іншими системами вимагає поширення відкритих ключів, що також створює ризики при неправильному конфігуруванні [39].

Крім того слід враховувати наступні особливості:

- приватний ключ потенційно підлягає клонуванню у разі компрометації клієнтського пристрою;
- при використанні SSH ключів, сам процес автентифікації часто не передбачає жодного додаткового підтвердження особи;
- відсутній зв'язок між ключем та фізичною присутністю користувача;
- програмні агенти на кшталт *ssh-agent* або *Pageant,* можуть зберігати ключ у відкритому вигляді у пам’яті апаратної платформи.

У підсумку, реалізація автентифікації на основі RSA вимагає ретельного контролю з боку IT-спеціаліста за середовищем, у якому виконується зберігання та обробка ключів. Як свідчить практичний досвід [46], без апаратного захисту та/чи багатоетапної верифікації користувача, такий механізм (або процедура) автентифікації не здатний протистояти сучасним атакам, навіть попри математичну надійність самого алгоритму RSA.

3.3 Аналіз стану безпеки систем, що використовують YubiKey

Як було зазначено вище, *YubiKey* – це апаратний токен, розроблений компанією Yubico®, який забезпечує захищене зберігання криптографічних ключів і автентифікацію користувача без потреби у зберіганні секретних даних на диску (*пам’яті пристрою, гаджету тощо*). Цей апаратний токен підтримує сучасні протоколи автентифікації, включно з FIDO2, U2F, PIV (*Personal Identity Verification*), *OpenPGP* та *OTP*, що робить його універсальним рішенням для корпоративного використання [40].

YubiKey відрізняється тим, що приватний ключ ніколи не покидає пристрій-носій. Усі криптографічні операції (*підпис, розшифрування тощо*) виконуються всередині цього пристрою. Це знижує ризики витоку, навіть якщо ОС скомпрометовано.

Переваги використання YubiKey:

- Обов'язкова фізична присутність: пристрій повинен бути вставлений і активований (дотик кнопки, рис. 2.2), що виключає приховані атаки;

- Немає експорту ключа: приватний ключ недоступний ні користувачу, ні зловмиснику, навіть із *root*- доступом;
- Захист від фішингу: при автентифікації через *FIDO2*, враховується домен сайту, тому підроблений сайт не отримає дійсний підпис [41];
- Сумісність з PKI: YubiKey підтримує стандарт PIV, тому може бути використаний як смарт-карта для цифрових підписів [42];
- Уніфікація автентифікації — один пристрій можна використовувати одночасно для *SSH, GNU Privacy Guard (GPG), VPN,* браузера тощо.

Можливі ризики та обмеження YubiKey:

- Втрата або поломка пристрою: у разі втрати YubiKey, доступ до системи може бути ускладнений. Тому рекомендується мати резервний ключ та/чи передбачити альтернативний механізм автентифікації [37];
- Фізичні атаки: хоча «витягти» ключ з YubiKey надзвичайно складно, пристрій все ж може бути ціллю для апаратного аналізу при умові тривалого (*тобто. неконтрольованого зберігання - недбалості власника*) доступу до нього;
- Неправильна конфігурація: у разі хибного налаштування (*наприклад, збереження PIN або адміністраторського коду в небезпечному місці*) пристрій може втратити свій початковий захисний ефект.

Таким чином, YubiKey поєднує високий рівень захисту з простотою використання, що робить його вкрай зручним варіантом для корпоративного середовища з підвищеними вимогами до безпеки, але при цьому, потребує більш ретельної підготовки з боку профільних фахівців з ІБ та певні фінансові витрати.

3.4 Порівняння безпеки систем авторизації з RSA та YubiKey

Як свідчить досвід [45] системи авторизації, що базуються на RSA-ключах, можуть бути реалізовані, як з використанням локального зберігання приватного ключа, так і за допомогою апаратних токенів, таких як YubiKey. Вочевидь що, з точки зору безпеки між цими підходами існують суттєві відмінності.

У таблиці 3.1 наведено результати порівняння безпекових характеристик в умовах використання класичної схеми з RSA- ключами (*тобто, файл приватного ключа зберігається безпосередньо на комп'ютері (гаджеті)*) та YubiKey, який реалізує апаратне зберігання ключа та апаратне підписування.

Таблиця 3.1 – Порівняння автентифікаційних систем за найбільш важливими критеріями

Критерій порівняння	**RSA (файл приватного ключа)**	**YubiKey (апаратний токен)**
Генерація ключа	Зазвичай локально на ПК користувача або централізовано	Генерація безпосередньо на пристрої
Зберігання приватного ключа	У файловій системі, можливо з шифруванням	У захищеній пам'яті токена, неможливо експортувати
Механізм підпису	Програмний (через OpenSSH, GPG тощо)	Апаратний (вбудований у токен)
Стійкість до фішингу	Низька: – можливе перехоплення через підроблені сайти	Висока: підтримка FIDO2/WebAuthn, зв'язок з доменом
Можливість викрадення ключа	Висока при компрометації системи	Мінімальна: – ключ не покидає пристрій
Атаки MitM	Можливі без додаткового захисту (TLS, VPN)	Неможливі через криптографічну перевірку домену
Клонування ключа	Можливе у разі крадіжки або витоку з диску	Неможливе: – секрет зберігається в пристрої, не експортується
Необхідність встановлення ПЗ	Так, потрібні SSH-клієнти, агент ключів тощо	Мінімальна: працює з браузером, ОС має рідну підтримку
Захист від шкідливого ПЗ	Слабкий (ключ може бути зчитаний)	Сильний: – ключ недоступний ПЗ
Автентифікація токена	Не застосовується	Підтвердження дотиком або PIN-кодом
Досвід користувача	Складний: – вручну запуск, введення паролів	Простий: – фізичне натискання кнопки на пристрої

Як слід з таблиці, YubiKey забезпечує значно вищий рівень безпеки завдяки апаратному ізолюванню приватного ключа та неможливості його копіювання і захисту від програмних атак. У той час як класичний підхід з RSA-файлом

схильний до ризиків, пов'язаних з компрометацією ОС та/або неналежним захистом файлової системи апаратної платформи (комп’ютери, гаджети тощо).

3.5 Дослідження питань зручності практичного використання YubiKey

Результати дослідження *«A Tale of Two Studies: The Best and Worst of YubiKey Usability»* [43] демонструють значні відмінності у сприйнятті зручності використання YubiKey на різних етапах взаємодії користувача з пристроєм. Стисло розглянемо основні з них.

Проблеми при налаштуванні:

- У лабораторному дослідженні, де учасники самостійно намагалися налаштувати YubiKey для облікових записів *Windows, Google* та *Facebook*, були зафіксовані такі труднощі:
  - учасники блокували доступ до своїх операційних систем;
  - помилково вважали, що успішно активували двофакторну автентифікацію;
  - зіштовхнулися з незрозумілими інструкціями та заплутаними робочими процесами.

Ці результати свідчать про те, що початкове налаштування YubiKey може бути складним для користувачів без технічного досвіду.

Зручність у повсякденному використанні:

- У дослідженні, де учасники використовували YubiKey у своїх повсякденних облікових записах, було встановлено, що:
  - учасники високо оцінили зручність використання та поводження з апаратними токенами;
  - процес автентифікації зводився до простого вставлення пристрою в USB-порт і натискання відповідної кнопки ініціації процедури (*див. рис.2.2*);
  - користувачі відзначили перевагу YubiKey над іншими методами двофакторної автентифікації, наприклад такими, як SMS-коди.

Ці дані підкреслюють тезу, що після коректного налаштування, YubiKey забезпечує високий рівень зручності у повсякденному використанні.

Рекомендації для покращення зручності:

- Стандартизувати процес налаштування YubiKey для різних платформ;
- Забезпечити чіткі та зрозумілі інструкції для користувачів;
- Інтегрувати мультимедійні (візуальні або звукові) підказки для підтвердження успішної автентифікації (*в тому числі для користувачів з різними фізичними вадами*);
- Розробити прости й надійні механізми запобігання блокуванню облікових записів під час налаштування відповідної системи.

Таким чином, хоча YubiKey забезпечує високу зручність у повсякденному використанні, однак етап початкового налаштування може стати певним викликом для деяких користувачів, але в більшої мірі для фахівців, які відповідають за налагодження всього процесу. Впровадження вищезазначених рекомендацій може значно покращити загальний досвід користувачів.

3.6 Інтегровані висновки, щодо особливостей авторизації з RSA та YubiKey

Спираючись на результати проведеного порівняльного аналізу можна зробити висновок, що апаратний токен YubiKey, в цілому, демонструє суттєво більш високий рівень захисту у порівнянні з класичною реалізацією автентифікації на основі RSA-ключів, котрі зберігаються у файловій системі пристрою/гаджету користувача. При цьому, серед основних чинників, які визначають перевагу саме YubiKey, слід відзначити наступні:

- Неможливість експорту приватного ключа: виключає сценарії його крадіжки або клонування (*принаймні без факту фізичного руйнування апаратного токену*);
- Інтеграція із сучасними протоколами WebAuthn/FIDO2: забезпечує захист від фішингових атак та враховують контекст, зокрема перевіряє домен вебсайту, на якому відбувається вхід, і блокує спроби використання ключа на підроблених сайтах;

- Прив’язка до фізичної присутності користувача: ускладнює несанкціонований доступ до ресурсів в умовах відсутності користувача;
- Уніфікація автентифікації: забезпечує єдину апаратну платформу для роботи з *SSH, GPG, VPN*, браузером, що покращує такі властивості й процеси системи, як керованість, масштабованість та узгодженість політик безпеки.

Однак процес впровадження апаратної автентифікації, також має і свої незручності, наприклад такі як:

- необхідність закупівлі нових пристроїв (токенів);
- налаштування системи та створення реєстру основних й дублюючих токенів, що працюють в цієї системі;
- налаштування варіантів резервних сценаріїв, на випадок втрати токенів персоналом та порядку відміни повноважень втрачених токенів;
- попереднє навчання та інструктаж персоналу.

У той же час, традиційні RSA-схеми залишаються актуальними у випадках, коли:

- необхідна швидка та недорога реалізація без додаткового обладнання;
- користувачі працюють в ізольованих середовищах із суворим контролем доступу до системних файлів;
- існує вже налагоджена інфраструктура розповсюдження відкритих ключів.

Кумулятивні рекомендації, стосовно впровадження рішень RSA та YubiKey:

- Для середовищ з підвищеними вимогами до безпеки (*державні установи, корпоративні VPN, критично важливі системи*) доцільно перейти на апаратні токени з підтримкою FIDO2/PIV (*зокрема YubiKey*);
- Для перехідного етапу варто передбачити гібридну модель/механізм, де частина користувачів використовує RSA-файли, а частина – токени;
- Необхідно забезпечити користувачів резервними/дублюючими способами доступу (*наприклад, запасний токен або автентифікацію через адміна*) у разі втрати пристрою або пін коду апаратного ключа.

Таким чином, вибір технології автентифікації, що притаманна саме для даних умов функціонування конкретної ІС, повинен базуватись не лише на її загальних технічних характеристиках, а й на практичних аспектах її експлуатації, моделі загроз та готовності організації до впровадження нових рішень безпеки.

3.7 Захист від клонування апаратних токенів YubiKey та ідентифікація легітимних пристроїв

Захист від клонуванняя: YubiKey побудований на принципі апаратної ізоляції приватного ключа, тобто він генерується і зберігається всередині чіпа пристрою (*токену*) і жодна операція не дозволяє його експорту. Таким чином, традиційне клонування криптографічного матеріалу, як це наприклад, можливо з файлами або менш захищеними токенами – такими як USB-накопичувачі з незашифрованими ключами або програмні токени, що зберігають приватні ключі у вигляді звичайних файлів на диску – є технічно неможливим [8].

Проте у вересні 2024 року дослідники виявили критичну уразливість у пристроях типу YubiKey [44]. Ця вразливість дозволяла зловмиснику, що мав доступ до пристрою під час виконання криптографічних операцій, провести атаку через побічні канали (*Side-Channel Attack*) і частково відновити приватний ключ. Це могло призвести до фактичного клонування YubiKey, що раніше вважалося неможливим. Цю проблему було усунуто в прошивці ver. 5.7, у якій змінили механізм виконання операцій, підвищивши стійкість токенів до побічного аналізу.

В цьому контексті важливо зазначити наступне:

- Ключі з прошивкою раніше ver. 5.7, залишаються вразливими назавжди, оскільки YubiKey не підтримує оновлення вихідної прошивки, з міркувань безпеки всієї процедури;
- Користувачам рекомендується відмовитися від вразливих/старих моделей токенів у критичних сценаріях або замінити їх на оновлені пристрої.

Ідентифікація легітимних пристроїв: Сучасні протоколи автентифікації дозволяють точно розпізнавати конкретний апаратний токен. Ідентифікація здійснюється за допомогою наступних механізмів/можливостей:

- Серійного номера пристрою, який є унікальним для кожного YubiKey (*особливо в протоколах OTP, FIDO2*);
- Credential ID — унікального ідентифікатора ключа, що формується при реєстрації (*WebAuthn/FIDO2*);
- Публічного ключа, пов'язаного з конкретним токеном (у *GPG, PIV, SSH*).

Таким чином, навіть за наявності кількох зареєстрованих YubiKey, система безпеки може перевірити, чи це саме той пристрій, який було раніше прив'язано до конкретного облікового запису. Це є основою виявлення підробок та/або несанкціонованих замін пристрою. В комплексі, всі ці заходи і можливості дозволяють:

- Відмовити у доступі при спробі автентифікації з невідомого токена;
- Реалізувати механізми довіреного «білого» списку, що містить відомості (реєстр) дозволених пристроїв/токенів;
- Контролювати, який саме пристрій використовується для конкретної дії.

Висновки за Розділом:

1) Захищеність RSA-систем критично залежить від умов зберігання ПК, що робить їх вразливими до фішингу, MitM-атак, клонування та компрометації, у разі доступу до файлової системи або пам'яті пристрою.

2) YubiKey забезпечує принципово вищий рівень безпеки: – приватний ключ ніколи не «покидає» пристрій, всі операції виконуються всередині нього, що унеможливлює його витік, навіть при атаці ОС або *root*- доступі.

3) Фізична присутність користувача є обов'язковою для автентифікації через YubiKey. Це ефективно захищає від фішингу та несанкціонованого доступу – зловмисник не зможе пройти автентифікацію без фізичного токена.

4) YubiKey значно зручніший у корпоративному використанні, оскільки підтримує кілька протоколів (*FIDO2, PIV, GPG, SSH*), легко масштабується, уніфікує автентифікацію і мінімізує вплив людського фактору.

4. МОДЕЛЮВАННЯ ПОТЕНЦІЙНИХ АТАК НА СИСТЕМИ З RSA ТА YUBIKEY І РОЗРОБКА РЕКОМЕНДАЦІЙ, ЩОДО ВПРОВАДЖЕННЯ YUBIKEY В ІСНУЮЧІ СИСТЕМИ АВТЕНТИФІКАЦІЇ

4. 1 Умови моделювання та обґрунтування вибору типів атак

У рамках моделювання були створені умови, що дозволили практично оцінити рівень захищеності систем автентифікації, побудованих на традиційному підході до зберігання ПК, в даному випадку – у файлі *«id_RSA»* на диску, та систем із застосуванням апаратних токенів YubiKey (див. рис.4.1). При цьому, основна увага, насамперед, була зосереджена на атаках, котрі загрожують:

– конфіденційності приватного ключа;
– цілісності процесу автентифікації;
– цілісності ідентифікації користувача.

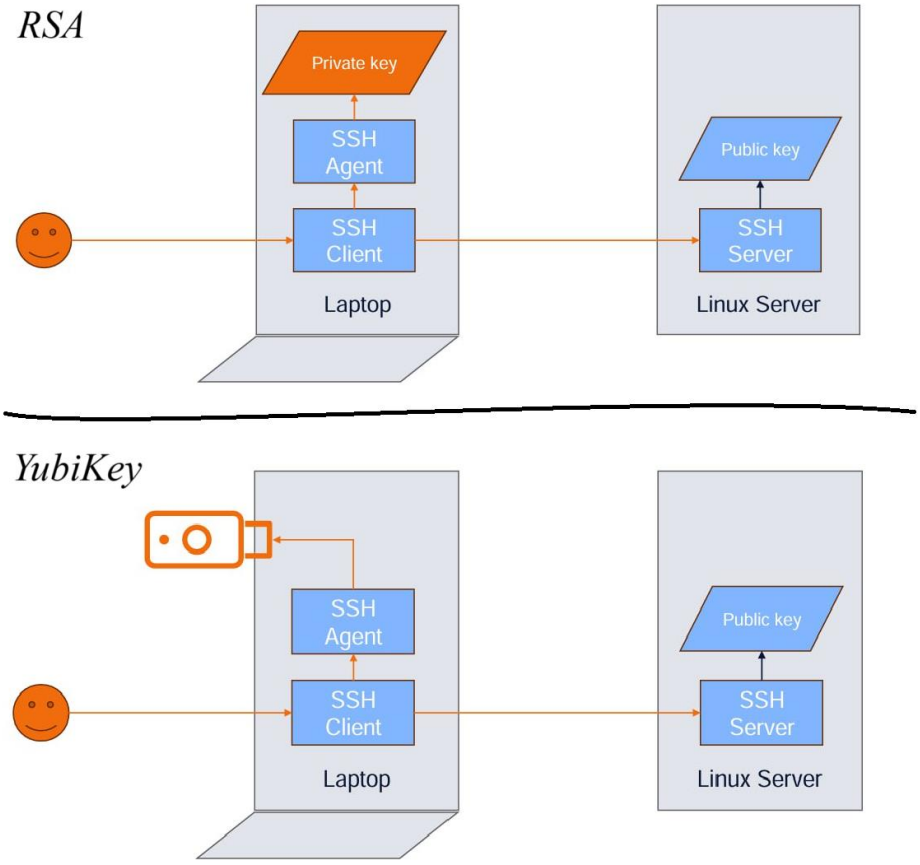

Рисунок 4.1 – Умови моделювання автентифікації: *файл «id_RSA» та YubiKey*

Моделювання проводилося в умовах, максимально наближених до реальних, із використанням наступних середовищ (умов):

- Локальна машина під управлінням ОС Linux (*Ubuntu 22.04 LTS*);
- Сервер з доступом по SSH;
- YubiKey 5C NFC, як апаратний токен, що тестується;
- GPG-інтеграція через *open-source менеджер сертифікатів* – Kleopatra;
- Створене внутрішнє середовище організації з прикладами видачі токенів користувачам.

У рамках імітаційного моделювання було синтезовано внутрішнє середовище умовної організації, яке включало: – окремий сервер для зберігання публічних ключів співробітників, налаштування доступу до систем через SSH з обов'язковою автентифікацією за допомогою токенів, та політику управління ключами. Це середовище дозволило реалізувати сценарії роботи корпоративної мережі з апаратною автентифікацією, включаючи взаємодію між співробітниками, IT-спеціалістами та службою безпеки.

Створене тестове середовище, підтримувало базовий механізм видачі токенів, якій містив наступні кроки: – IT-спеціаліст генерував ключову пару безпосередньо на пристрої YubiKey через інтерфейс GPG, зберігав публічний ключ у внутрішньому реєстрі (сервері), після чого фізично передавав токен користувачеві разом з інструкцією та PIN-кодом. Таким чином, процес імітував типовий сценарій корпоративного розгортання без необхідності складної інфраструктури PKI.

Типи атак, які були обрані для проведення моделювання, базуються на результатах аналізу відомостей, стосовно загальновідомих сценаріїв реалізації характерних загроз [2-4, 36, 39], а також на виявлених уразливостях у реальних пристроях [44]. За результатами узагальнення інформації про відомі інциденти безпеки, використана класифікація, що притаманна саме до умов й властивостей процесу автентифікації (далі - *процесу*) користувачів:

- Фізичне викрадення приватного ключа – актуальне для традиційної моделі процесу, коли ключ зберігається у відкритому вигляді на диску;

- Side-channel атаки на апаратні токени, загроза що дозволяє потенційно зчитати частини приватного ключа, як це було доведено у дослідженні 2024 року (*див. роботу* [44]);
- Фішингові атаки з підміною домену – загроза, котра дозволяє обходити класичні системи автентифікації, але блокуються протоколами WebAuthn/FIDO2 [15];
- Використання скомпрометованого клієнтського ПЗ – загроза, експлуатація якої передбачає можливість викрадення не лише ключа, а й пароля та OTP [48].

Як показали експерименти, кожна з розглянутих моделей автентифікації має різну вразливість до зазначених загроз. В табл. 4.1 в загальному вигляді, наведено відповідності між обраними типами загроз та рівнем захисту, який забезпечують різні підходи.

Таблиця 4.1 – Стійкість традиційної і апаратної автентифікації до атак

Тип атаки	**RSA** ***(файл)***	**YubiKey** ***(до v5.7)***	**YubiKey** ***(від v5.7)***
Викрадення приватного ключа з ПК	Вразливий	Не вразливий	Не вразливий
Side-channel атаки (наприклад, Tempest)	Невідносна	Вразливий	Не вразливий
Фішинг / підміна домену	Вразливий	Не вразливий	Не вразливий
***Викрадення* пароля до ключа**	Вразливий	Частково вразливий	Частково вразливий
Утилізація ключа після компрометації ПК	Неможлива	Автоматична	Автоматична

Як свідчать результати моделювання, апаратні токени YubiKey забезпечують:

- Ізоляцію приватного ключа від операційної системи;
- Підтвердження фізичної присутності користувача;
- Підтримку сучасних криптографічних протоколів (FIDO2, PIV, OpenPGP);
- Неможливість експорту/вилучення ключа з пристрою (*immutable keys*) [45].

Проте, як показало дослідження, що було опубліковане на *Ars Technica* у вересні 2024 року [44], існує вразливість в YubiKey, котра дозволяла вилучати частини приватного ключа, шляхом аналізу часу обробки запитів, використовуючи для цього «Side-Channel» методи. Ця вразливість стосувалася всіх пристроїв із програмною прошивкою до версії 5.7 [2]. У новіших версіях *Yubico* усунула цю уразливість, реалізувавши нові механізми рандомізації криптографічних операцій. Як наслідок, токени, які вже було видано до цієї дати, залишаються вразливими назавжди, оскільки прошивка YubiKey не може оновлюватися користувачем, а відбувається виключно розробником токенів.

Таким чином, у процесі впровадження YubiKey до систем автентифікації слід враховувати наступні особливості:

- Забезпечити використання пристроїв виключно з версією прошивки 5.7 або новішою;
- Враховувати специфіку атак, спрямованих не на витік ключа, а перш за все, на соціо-технічні різновиди атак [2-4, 36, 47];
- Розробити політику періодичного аудиту стану апаратних токенів;
- Проводити навчання і періодичний інструктаж користувачів, щодо правил поводження з токеном та підозрілих дій під час автентифікації.

Розглянуті умови моделювання, типи атак та результати порівняння різних механізмів автентифікації були використані для побудови сценаріїв впровадження YubiKey у практичному середовищі – з реальними прикладами генерації ключів, інтеграції в системи SSH та організації процесу їх видачі користувачам.

4. 2 Аналіз типових атак на традиційні системи з RSA

Традиційні системи автентифікації, які використовують зберігання приватного ключа RSA у відкритому вигляді на диску (наприклад, у файлі *~/.ssh/id_rsa*), залишаються одними з найпоширеніших на практиці. Водночас вони демонструють низький рівень стійкості до широкого спектра атак. Тому коротко розглянемо найбільш типові сценарії атак на відповідні системи та деякі особливості, що характерні до умов проведеного імітаційного моделювання:

- Крадіжка приватного ключа (key exfiltration). Це найбільш поширений вектор атаки на традиційні системи з RSA. Зловмисник, отримавши фізичний або логічний доступ до клієнтського пристрою, може скопіювати файл *«id_rsa»* або отримати його через вразливість у ПЗ. У випадку, коли ключ не захищено фразою-паролем *(Passphrase)*, зловмисник отримує повний контроль над обліковим записом користувача [39, 49]. Навіть при наявності фрази-паролю, можливе проведення офлайн-атаки з перебором *(Bruteforce)*;
- *Brute-force* та *Dictionary-* атаки на фразу-пароль. Якщо приватний ключ захищено використовуючи механізм *Passphrase*, то зловмисник може спробувати підібрати її офлайн за допомогою словникових або перебірних атак. Це можливо через те, що сам ключ вже знаходиться у зловмисника, і для атаки не потрібен доступ до віддаленого сервера [8];
- Фішингові атаки. Традиційні RSA-системи не мають вбудованих механізмів захисту від цих атак. При цьому, користувач може несвідомо ввести свої облікові дані (або *Passphrase* до ключа) на підробленому SSH-сервері або небезпечному термінальному емуляторі [50];
- Атаки «людина посередині» (MitM). Попри те, що SSH-протокол включає механізми перевірки хост-ключів, на практиці користувачі часто ігнорують попередження про зміну ключа сервера (наприклад, при появі повідомлення - `WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!`). Це дозволяє реалізовувати MitM-атаки та перехоплювати авторизацію через підставний сервер [51];
- Використання скомпрометованого клієнтського ПЗ. Якщо зловмисник отримує контроль над середовищем користувача (через *Malware*, *Rootkit* чи вразливість у ОС), він може не лише викрасти ключі, але й перехоплювати OTP-коди, паролі або навіть інтерактивну сесію після автентифікації [52]. У таких випадках навіть «сильна» криптографія не рятує від компрометації ключової інформації, оскільки атака здійснюється на рівні ОС користувача - жертви;

- Відсутність ізоляції ключа (*тобто ключової інформації*). Оскільки приватний ключ у традиційних RSA-системах зберігається у звичайному файлі, то він повністю підконтрольний користувачеві та, потенційно, всім процесам, які виконуються в його середовищі. Це робить такі системи надзвичайно вразливими до шкідливого ПЗ (скриптів, бекдорів та ін.), що може зчитати файл із ключем без будь-яких обмежень [49].

У якості проміжного висновку можна стверджувати, що традиційна автентифікація з RSA-ключами демонструє низький рівень стійкості до атак у реальних умовах, особливо в середовищі користувачів з низьким рівнем базових цифрових компетенцій. В даному разі основною проблемою є повна відсутність ізоляції ключа (даних) та залежність від поведінки користувача (*фраза-пароль, підтвердження хостів тощо*). Це створює передумови для впровадження більш безпечних методів автентифікації, зокрема – апаратних токенів.

4. 3 Дослідження стійкості та атаки на YubiKey

Попри високу репутацію апаратних токенів, як надійного засобу автентифікації, важливо розглянути можливі вектори атак на них. Апаратні ключі, зокрема YubiKey, пройшли численні незалежні оцінки безпеки та випробування на вразливості, що дозволяє надати об'єктивну оцінку, щодо їх стійкості.

- Фішинг атаки. Однією з ключових переваг YubiKey, що працює за протоколом FIDO2/WebAuthn, є *повний захист* від фішингу. На відміну від традиційної автентифікації за паролем або OTP, які користувач вводить вручну і які можуть бути викрадені через фішингові сайти, FIDO2 реалізує прив’язку автентифікації до конкретного домену (*див. рис. 4.2*). Практично це означає, що ключ не підпише (підтвердить) автентифікаційний запит для підробленого сайту [53];
- Side-Channel атаки. У 2024 році дослідники виявили, що пристрої YubiKey з прошивкою до версії 5.7 були вразливими до Side-Channel атак (див. п.п. 3.7). Такі атаки дозволяли зловмиснику, що мав безпосередній фізичний доступ до пристрою під час виконання криптографічних

операцій, частково відновити приватний ключ і потенційно клонувати токен – всупереч загальноприйнятій думці про його абсолютну стійкість. Цю вразливість вже було усунено через зміну внутрішнього механізму обчислень. Важливою обставиною є те, що старі моделі токенів не підтримують оновлення їх прошивки, тож користувачам потрібно замінити їх у безпечних середовищах;

- Fallback-атаки *(соціальна інженерія)*. YubiKey не забезпечує гарантований захист у разі повної компрометації середовища користувача та/чи здійснення доступу до ключа через експлуатацію людського фактору (наприклад, неявний примус користувача власноруч натиснути «потрібну» кнопку на підробленому сайті). Проте завдяки вбудованій перевірці контексту (*Origin/Domain*), така атака на YubiKey, є достатньо складною для реалізації [2-4].

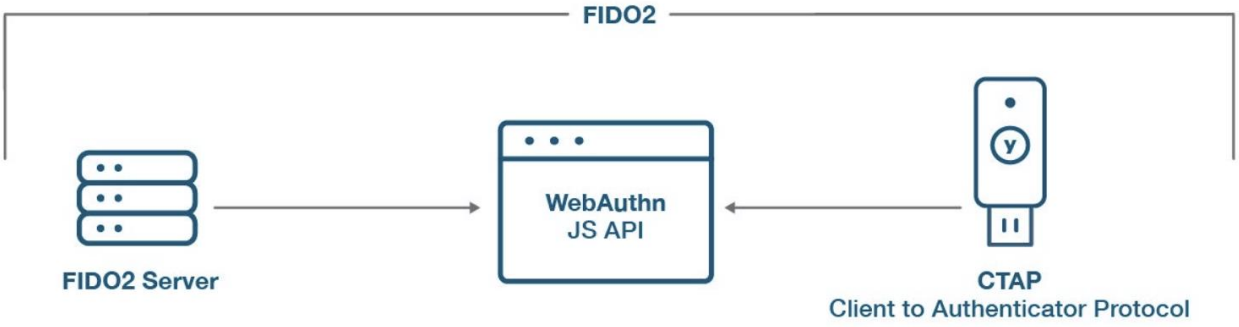

Рисунок 4.2 – WebAuthn, основа захисту від фішингу у протоколі FIDO2

Таким чином YubiKey демонструє високу стійкість до основних векторів атак: – завдяки протоколу FIDO2/WebAuthn він забезпечує ефективний захист від фішингу [2-4,36], а вбудована функція перевірки домену, унеможливлює підпис запитів із шахрайських сайтів. В умовах експлуатації критичних середовищ (критичних ІС) слід використовувати лише оновлені токени (після v.5.7), що усувають можливість експлуатації вразливості до *Side-Channel* атак. Атаки через соціальну інженерію теоретично можливі [4, 47], але їх реалізація сильно ускладнена завдяки багаторівневій перевірці контексту автентифікації.

4. 4 Практичне впровадження YubiKey для шифрування та автентифікації

Покроково розглянемо основні етапи з налаштування YubiKey для використання в корпоративному середовищі. Слід підкреслити, що налаштування охоплює генерацію ключів, автентифікацію через SSH, менеджмент ключів та передачу пристрою співробітникам. Для прикладу буде використано інструменти Kleopatra, OpenPGP та WSL2 *(Windows Subsystem for Linux)*, що дозволяє працювати з інструментами Linux безпосередньо у ОС Windows.

Дії, що виконуються IT-спеціалістом:

1) Налаштування YubiKey: *генерація ключів*

За допомогою ПЗ Kleopatra IT-спеціаліст ініціалізує YubiKey, створюючи пару ключів (публічний/приватний) безпосередньо на пристрої. Це гарантує, що ПК не покидає YubiKey та не може бути зчитаний ззовні. Ключі включають наступну інформацію:

- Ключ для підпису;
- Ключ для шифрування;
- Ключ для автентифікації (використовується для SSH-доступу).

2) Налаштування автентифікації через SSH: *експорт публічного ключа*

Після створення ключів IT-спеціаліст експортує публічний SSH-ключ із YubiKey за допомогою команди `ssh-add -L` (рис. 4.4). Цей ключ додається до відповідного облікового запису (наприклад, GitLab, сервер доступу тощо), що дозволяє персоні використовувати апаратну автентифікацію при підключеннях.

3) Менеджмент ключів та видача YubiKey:

IT-спеціаліст фіксує інформацію про ключ у внутрішній системі (реєстр). При цьому, до кожного YubiKey:

- прив’язується унікальний серійний номер пристрою;
- здійснюється прив’язка до конкретного користувача;
- прив’язується дата його видачі;
- формується контрольний хеш публічних ключів.

Після завершення цих етапів YubiKey передається співробітнику разом із первинним *PIN*-кодом та інструкціями з його зміни (розглянуто нижче).

Дії, що виконуються користувачем *(співробітником)*:

1) Початкове використання: *зміна PIN-коду:*
   - Підключити YubiKey до USB-порту;
   - Відкрити програму Kleopatra (див. рис.4.3):
     a. Перейти до розділу *"Smartcards"*;
     b. Переконатись, що вибрана вкладка *"OpenPGP"*;
     c. Обрати *"Change PIN"*;
     d. Ввести старий PIN-код, отриманий від IT-спеціаліста;
     e. Двічі ввести новий PIN-код (дозволено використовувати всі літери, шифри та спец. символи).
   - Підтвердити IT-спеціалісту, що ви змінили свій *PIN*-код.

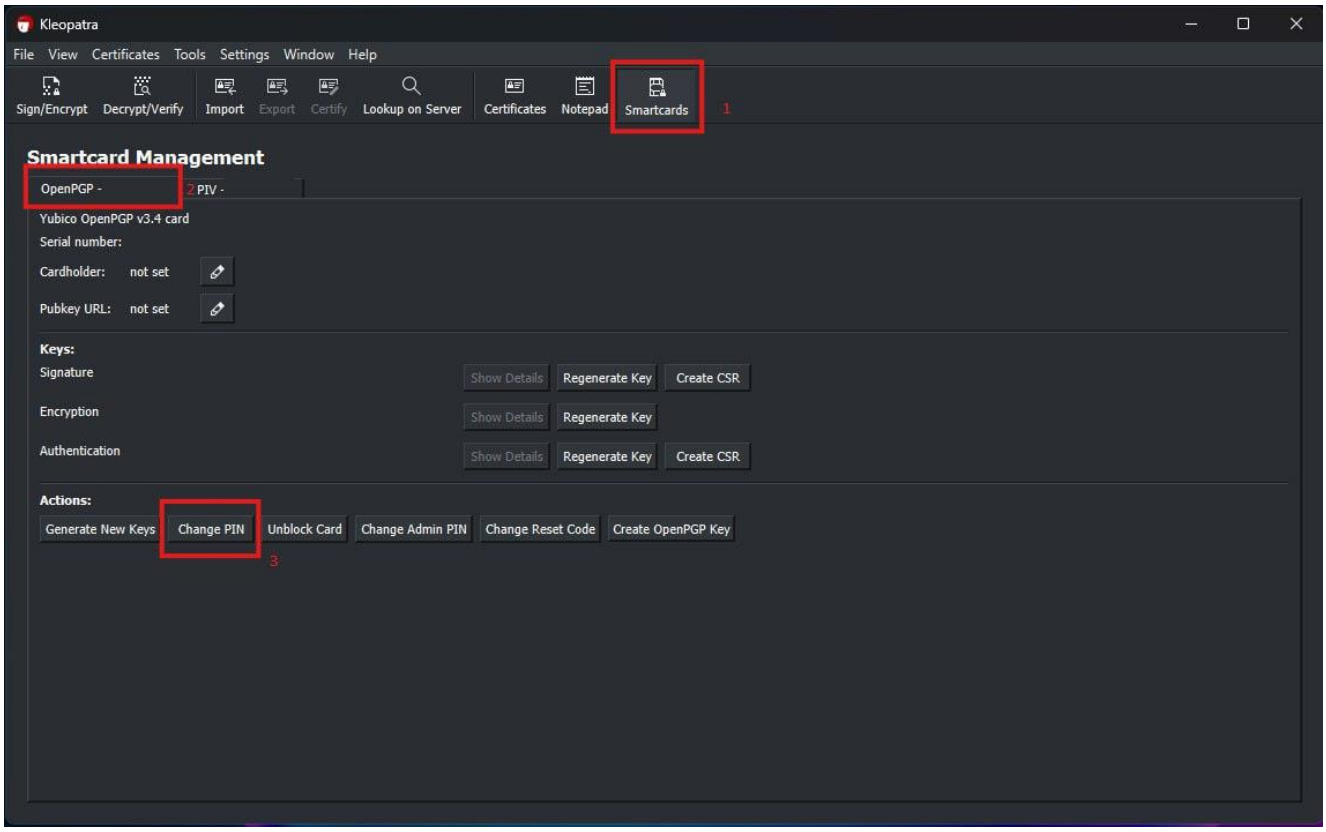

Рисунок 4.3 – Зміна *PIN*-коду до YubiKey з використанням ПЗ *Kleopatra*

Перевірка доступу: *термінали і підключення:*

Після налаштування *PIN*, токен готовий до роботи. Для підключення можна використовувати наступні інструменти (жодних додаткових налаштувань для цього не потрібно):

- MobaXterm;
- PowerShell;
- Звичайний cmd.exe.

Також можливе використання середовища WSL2, однак в цьому разі для коректної роботи з YubiKey у ньому потрібне додаткове налаштування (див. Додаток А, рис. А.1).

Щоб переконатися, що система розпізнає YubiKey і ключ є доступний, можна використати команду `ssh-add -L` (рис. 4.4).

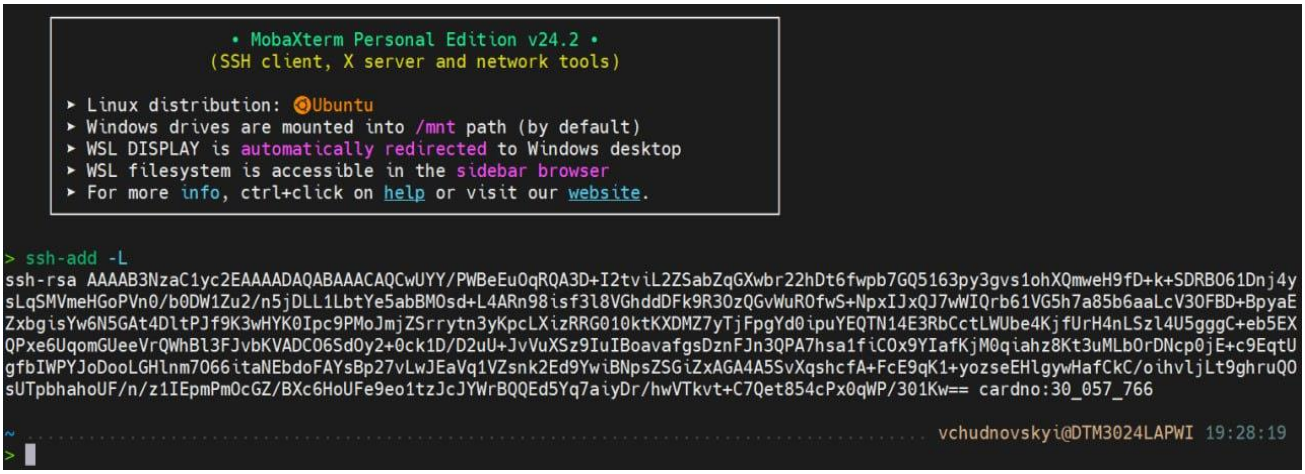

Рисунок 4.4 – Перевірка доступності публічного SSH-ключа на YubiKey у середовищі *MobaXterm*

2) Автентифікація через «дотик» *(тобто тактильне торкання)*:

- Під час автентифікації:
  a. Підключити YubiKey;
  b. Ввести новий PIN;
  c. Після запиту доторкнутися до пристрою – це активує ключ на 15 сек.

Без тактильного дотику ключ не активується навіть після введення правильного *PIN*-коду, що є заходом захисту від несанкціонованого використання пристрою [6], що потребує додаткового підтвердження цільової процедури.

Після виконання всіх вищезазначених кроків у ПЗ *Kleopatra* на вкладці *Smartcards* відображатимуться відбитки ключів (*Fingerprints*) для підпису, шифрування та автентифікації (див. рис.4.5).

Fingerprint – це унікальний короткий хеш публічного ключа. Ці відбитки, а також сам публічний ключ можна безпечно демонструвати або публікувати, оскільки вони призначені для поширення: – з їх допомогою інші користувачі можуть шифрувати дані для власника чи перевіряти його підписи, але не можуть отримати доступ до приватної інформації чи розшифрувати дані власника.

Водночас, серійний номер смарткарти не варто показувати публічно. Він є унікальним та потенційно може використовуватися для ідентифікації пристрою або побудови таргетованих атак, особливо у великій організації. Тому у відкритій документації та/або презентаціях бажано його приховувати.

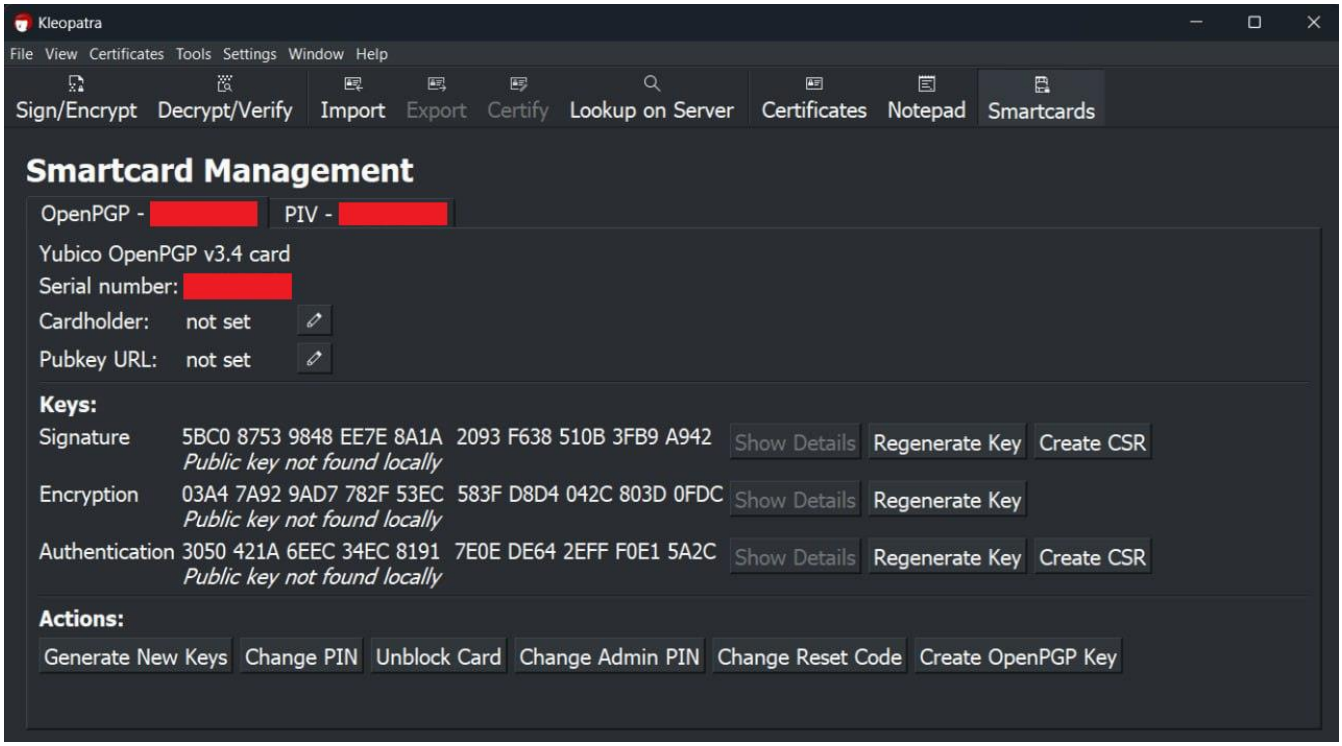

Рисунок 4.5 – Відображення *Fingerprints* ключів у ПЗ Kleopatra

4. 5 Рекомендації щодо впровадження YubiKey в існуючі IT-системи замість RSA-файлів

За результатами аналізу досвіду використання та моделювання процедур розгортання YubiKey, розглянемо покрокову стратегію впровадження цих апаратних ключів у корпоративне середовище, замість практиці традиційного збереження приватних ключів у вигляді файлів. В цьому сенсі, охоплюються як

технічні, так і організаційні аспекти, включаючи навчання персоналу, мінімізацію ризиків та забезпечення безперервності роботи самої ІС (див. табл.4.2).

Таблиця 4.2 – Узагальнені ризики використання YubiKey та способи їх вирішення

Ризик	**Рішення**
Втрата YubiKey	Миттєве відкликання ключа у системі, видача нового пристрою
Забутий PIN/PUK	Відновлення через ІТ-відділ (PUK повинен зберігатись у сейфі)
Неможливість автентифікації	Тимчасове використання резервного облікового запису
Несумісність з деякими системами	Перед впровадженням провести тестування з усіма платформами

1) Інформаційне повідомлення співробітникам: До початку технічного налаштування, ІТ-відділ розсилає внутрішнє повідомлення про заплановані зміни. Мета – підготувати персонал до впровадження YubiKey, роз’яснити його переваги та цільові очікування;
2) Первинне налаштування YubiKey для кожного співробітника: На цьому етапі ІТ-спеціаліст ініціалізує пристрій, генерує ключі та реєструє відповідні публічні ключі у внутрішній системі (див. п.п. 4.4);
3) Фізична видача пристроїв YubiKey: Кожному співробітнику видається ініціалізований YubiKey разом з первинним PIN-кодом, короткою інструкцією з налаштування та базовими правилами безпеки;
4) Навчання персоналу: ІТ-відділ проводить короткий тренінг або розсилає покрокову інструкцію для ознайомлення з базовим використанням YubiKey: входом через SSH, підписом, тощо;
5) Зміна PIN-коду та підтвердження готовності до роботи: Після отримання пристрою працівник змінює *PIN*-код відповідно до інструкції (див. п.п. 4.4). Після цього підтверджує ІТ-відділу про успішне налаштування;
6) Розгортання публічних SSH-ключів на серверах: Зібрані під час ініціалізації публічні ключі додаються до серверів або систем контролю версій, таких як *GitLab*, для кожного співробітника;

7) Перехідний період з паралельним використанням: Рекомендується протягом перших 4 тижнів дозволити паралельне використання як старого RSA-файлу, так і YubiKey, щоб уникнути збоїв у роботі;
8) Видалення старих SSH-ключів: Після закінчення перехідного періоду IT-відділ видаляє всі застарілі публічні ключі, що прив'язані до RSA-файлів, із серверів.

Організаційні та юридичні аспекти:

- Прозорість: Заздалегідь інформуйте персонал про зміни, причини впровадження, нові вимоги до безпеки та терміни;
- Політики безпеки: Уточніть або доповніть політику безпечного доступу (*SSH, VPN* тощо), включивши пункт про заборону зберігання приватних ключів у вигляді файлів;
- Юридичні аспекти: Варто документувати факт передачі YubiKey в користування працівнику, його серійний номер і повідомити про особисту відповідальність за втрату пристрою.

Навчання персоналу: Навчання персоналу має бути коротким, прикладним і мати формат інструкції з ілюстраціями. Основні теми навчання:

- Як підключати і використовувати YubiKey;
- Як змінити PIN;
- Що таке дотик для активації токену;
- Як переконатись, що ключ вже активний (команда `ssh-add -L`);
- Як повідомити про втрату токену.

4. 6 Порівняння ефективності досліджених методів автентифікації за результатами модельованих сценаріїв атак

За результатами розгляду можливих сценаріїв атак на розглянуті методи автентифікації (традиційне зберігання приватного ключа на комп'ютері користувача; апаратні ключі YubiKey; використання паролів чи біометричних даних), можна зробити певні узагальнення для кожного із зазначених вище підходів, що є принциповими, перш за все, з точки зору питань безпеки (табл.4.3).

У змодельованих сценаріях* було продемонстровано, як можуть відбуватись атаки типу «людина посередині» (MitM), фішинг, фізичне викрадення носія, атаки на комп'ютер жертви з метою отримання ключів або паролів, а також SE- атаки. Оцінка кожного методу проводилася за 4-ма наступними критеріями:

- Ймовірність атаки – наскільки часто подібні атаки трапляються в реальних умовах;
- Наслідки компрометації – які потенційні збитки може понести користувач у випадку «успішної» атаки;
- Складність реалізації атаки – які ресурси, знання та/чи рівень доступу потрібні для реалізації відповідної атаки;
- Засоби захисту – доступні механізми протидії.

Таблиця 4.3 – Узагальнення потенційних наслідків для різних сценаріїв атак

Метод автентифікації	**Ймовірність атаки**	**Наслідки компрометації**	**Складність реалізації атаки**	**Засоби захисту**
Парольна автентифікація	Висока	Повна компрометація доступу	Низька	Двофакторна автентифікація, менеджери паролів
Локальний приватний ключ *(SSH)*	Середня	Доступ до системи/серверу	Середня	Шифрування ключа, захищене зберігання
YubiKey *(апаратний токен)*	Низька	Обмежені, без PIN — мінімальні	Висока	Фізичний захист, PIN-код, політика блокувань
Біометрична автентифікація	Низька / Середня	Неможливість змінити дані біометрії	Висока	Локальне зберігання шаблонів, захист пристрою
Програмний OTP *(Google Authenticator, тощо)*	Середня	Можлива компрометація одноразових кодів	Середня	Захист телефону, резервні коди, шифрування

Висновки за Розділом:

1) Апаратні токени YubiKey забезпечують значно вищий рівень захисту приватного ключа, порівняно з традиційним зберіганням RSA-ключів на диску, зокрема завдяки ізоляції ключа, неможливості його клонування та потреби фізичної присутності користувача (власника).

2) Традиційні системи автентифікації (з файлами *«id_RSA»*) є вразливими до більшості найбільш розповсюджених атак, включаючи: – крадіжку ключа, фішинг, компрометацію клієнтського ПЗ та відсутність механізму швидкого відкликання ключів після їх компрометації.

3) Важливо чітко усвідомлювати, що апаратні токени не гарантують абсолютної безпеки: – наприклад, уразливість до *Side-Channel* атак була виявлена в YubiKey лише в 2024 році, тому критично важливо впроваджувати лише оновлені версії відповідних пристроїв та їх моделей.

4) Ефективне впровадження токенів YubiKey потребує не лише технічної інтеграції, а й імплементації певних організаційних заходів: – політики аудиту, інструктажів користувачів і врахування фактичного впливу SE атак, котрі обов’язково мають бути складовими корпоративної стратегії безпеки, та мати продовження у відповідних положеннях корпоративної політики безпеки.

ВИСНОВКИ

У ході виконання дипломної роботи було проаналізовано сучасні методи автентифікації, зокрема зосереджено увагу на апаратних засобах двофакторної автентифікації, таких як YubiKey. Проведений аналіз показав, що традиційні методи захисту, базовані лише на паролях або програмних токенах, в умовах постійного зростання складності атак, більше не забезпечують належного рівня ІБ, зокрема: - фішингових атак, MitM атак та перехоплення сесій. У пошуках можливих рішень на нові загрози [3,10,17], апаратні токени, що використовують криптографічні протоколи [14, 22], стали гідною альтернативою, яка дозволяє мінімізувати ризики, котрі пов'язані з компрометацією автентифікаційних даних користувачів сучасних ІКС .

Значна увага в роботі приділялася аналізу використовуваної криптографічної бази (методів й алгоритмів) апаратних ключів, зокрема таких алгоритмів, як RSA, ECDSA та EdDSA. Порівняння їх стійкості та продуктивності дозволило дійти висновку про перспективність використання EdDSA у сучасних токенах автентифікації. Виконаний аналіз принципів й властивостей протоколів U2F, FIDO2, CTAP та WebAuthn, дозволив певною мірою систематизувати практичні підходи до реалізації безпечного входу користувачів сучасних ІС, з різними рівнями взаємодії між клієнтом, сервером та апаратним токеном.

У рамках роботи було здійснено порівняння двох основних напрямів зберігання криптографічних ключів: 1 – локальне збереження приватного ключа у файловій системі користувача; 2 – збереження приватного ключа на апаратному пристрої, захищеному фізично та програмно. За результатами виконаних досліджень встановлено, що апаратний метод (тобто, апаратні токени) дозволяє значно підвищити безпеку процедуру автентифікації користувачів сучасних ІКС, виключаючи при цьому, можливість несанкціонованого копіювання даних ключа та зменшуючи ймовірність його злому/компрометації в разі зараження ОС пристрою користувача.

В ході реалізації практичної частини роботи проведено тестове моделювання процесу автентифікації користувачів за допомогою апаратних токенів YubiKey у віртуальному корпоративному середовищі з урахуванням типових сценаріїв входу персоналу, в умовах імітації спроб проведення фішингових атак, з оцінкою можливих наслідків для різних методів автентифікації. За результатами моделювання було доведено, що використання YubiKey як одного з факторів автентифікації (у поєднанні з паролем або біометрією) практично унеможливлює типові фішингові атаки [2-4] та значно підвищує стійкість системи до MitM-атак.

Узагальнення відомостей аналітичної і моделюючої (практичної) частин роботи дозволяє стверджувати, що незважаючи на високу ефективність апаратних токенів YubiKey, існують певні виклики, стосовно можливостей їх масового (безумовного) впровадження. Зокрема, до них належать потреба: - у врахуванні специфіки виконання процедур автентифікації персоналу критичних та/чи ізольованих ІС; - у навчанні користувачів; - наявність складнощів з інтеграцією у «застарілі» системи; - обмежена кількість відкритих інструментів для розробників; - необхідність загального адміністрування використання ключів (генерація, ранжування повноважень та деактивація) у великих організаціях. Також потребує уваги проблематика заходів з усунення наслідків втрати апаратного ключа, включаючи механізми резервного відновлення доступу.

В цілому, результати дослідження свідчать про доцільність та ефективність використання апаратних засобів автентифікації на основі відкритих криптографічних стандартів. Реалізація таких засобів у корпоративному середовищі дозволяє не лише підвищити загальний рівень ІБ, але й спрощує аудит дій персоналу завдяки вбудованим механізмам цифрового підпису та журналювання. Надалі перспективним напрямом є інтеграція таких засобів у структури PKI для централізованого управління доступом та сертифікатами.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Verizon *DBIR Report 2023*. Режим доступу: https://www.verizon.com/business/en-nl/resources/reports/dbir/2023/summary-of-findings/
2. Чорна Т., Лєсная Ю., Малахов С. Інсайд, фішинг та SE-атаки як складові проблематики доксінгу. *Proceedings of the XXII International Scientific and Practical Conference*, м. Хельсінки, 6–9 черв. 2023 р. Хельсінки, 2023. С. 506–510. Режим доступу: https://isg-konf.com/modern-theories-and-improvement-of-world-methods
3. Лєсная, Ю., & Малахов, С. (2023). *Аналіз розвитку, типові цілі та механізми здійснення фішингових атак. Комп'ютерні науки та кібербезпека*, (1), 6-27. Режим доступу: https://doi.org/10.26565/2519-2310-2023-1-01
4. Погоріла, К., Лєсная, Ю., Богданова, Є., & Малахов, С. (2022). *Соціальний інжиніринг, як фактор реалізації інсайдерських загроз*. Scientific Collection «InterConf», (111): with the Proceedings of the 1st International Scientific and Practical Conference «Scientific Community: Interdisciplinary Research» (June 6-8, 2022). Boston, USA; pp. 494-501. Режим доступу: https://archive.interconf.center/index.php/conference-proceeding/issue/view/6-8.06.2022
5. Мелкозерова, О., Нарежний , А., & Малахов , С. (2021). *Верификация отпечатков пальцев посредством декомпозиции минуций и решения задачи коммивояжера*. Режим доступу: https://ojs.ukrlogos.in.ua/index.php/scientia/article/view/12415
6. Лєсная Ю., Малахов С. *Бліц-огляд проблематики захисту від несанкціонованих дій на прикладах характерних реалізацій*. Problems of the development of modern science. Proceedings of the XXXIV International Scientific and Practical Conference, м. Мадрид, 30 серп. 2020 р. – 2 верес.

2022 р. Мадрид, 2022. С. 326–329. Режим доступу: https://isg-konf.com/problems-of-the-development-of-modern-science/

7. Колованова Є., Малахов С., Чорна Т. *Передумови та основні складові з протидії доксінгу персональних даних.* The 27th International scientific and practical conference «Trends of young scientists regarding the development of science», Едмонтон, 11–14 лип. 2023 р. Едмонтон, 2023. С. 194. Режим доступу: https://isg-konf.com/wp-content/uploads/2023/07/TRENDS-OF-YOUNG-SCIENTISTS-REGARDING-THE-DEVELOPMENT-OF-SCIENCE.pdf
8. NIST Special Publication 800-63B *Authentication and Lifecycle Management.* Режим доступу: https://pages.nist.gov/800-63-3/sp800-63b.html
9. Exploding Topics *40+ Multi-Factor Authentication Stats (2024)*. Режим доступу: https://explodingtopics.com/blog/multi-factor-authentication-stats
10. Чудновський, В., & Малахов, С. (2024). *Бліц-огляд сучасних методів автентифікації та особливості застосування MFA*. Proceedings of the XIV International Scientific and Practical Conference. Porto, Portugal. International Science Group. 2024. Pp. 422-425. Available at: DOI: 10.46299/ISG.2024.2.14. Режим доступу: https://isg-konf.com/the-latest-technologies-in-scientific-activity-and-the-educational-process/
11. DIY Investor *How are Smart Cards Useful in Financial Application*. Режим доступу: https://www.diyinvestor.net/how-are-smart-cards-useful-in-financial-application/
12. Apple *How to use Face ID with your iPhone*. Режим доступу: https://support.apple.com/en-us/HT208108
13. Microsoft *Multi-Factor Authentication.* Режим доступу: https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-howitworks
14. Yubico *YubiKey Overview.* Режим доступу: https://www.yubico.com/products/how-the-yubikey-works/

15. FIDO Alliance *Benefits of FIDO2 Authentication*. Режим доступу: https://fidoalliance.org/fido2/
16. Yubico: *What is a Sim Swap?* Режим доступу: https://www.yubico.com/resources/glossary/sim-swap/
17. Бойко, К., Чудновський, В. & Малахов, С. (2024). *Узагальнення напрямів програмної диверсності для покращення безпеки інформаційних систем*. Proceedings of the XIII International Scientific and Practical Conference. Valencia, Spain. International Science Group. 2024. Pp. 299-308. Режим доступу: https://isg-konf.com/cultural-and-artistic-processes-in-the-context-of-the-european-scientific-space
18. Barak, B. (2017). *The Complexity of Public-Key Cryptography*. Режим доступу: https://eprint.iacr.org/2017/365.pdf
19. National Institute of Standards and Technology (NIST). (2001). *Advanced Encryption Standard (AES)*. FIPS Publication 197. Режим доступу: https://doi.org/10.6028/NIST.FIPS.197
20. Qualys. *SSL Pulse (ISRG)*. Режим доступу: https://www.ssllabs.com/ssl-pulse/
21. RSA Laboratories. *Public-Key Cryptography*. Режим доступу: https://en.wikipedia.org/wiki/RSA_cryptosystem
22. Yubico. *YubiKey PIV Introduction*. Режим доступу: https://developers.yubico.com/PIV/
23. Microsoft *Key-based authentication in OpenSSH for Windows*. Режим доступу: https://learn.microsoft.com/en-us/windows-server/administration/openssh/openssh_keymanagement
24. RSA Community *RSA Governance & Lifecycle Integration: Microsoft Active Directory Summary*. Режим доступу: https://community.rsa.com/s/article/RSA-Governance--Lifecycle-Integration-Microsoft-Active-Directory-Summary
25. Oracle *Java Cryptography Architecture (JCA) Reference Guide*. Режим доступу: https://docs.oracle.com/javase/7/docs/technotes/guides/security/crypto/CryptoSpe

c.html

26. Yubico *FIDO2 Passwordless Authentication.* Режим доступу: https://www.yubico.com/authentication-standards/fido2/
27. Google *Titan Security Key*. Режим доступу: https://cloud.google.com/security/products/titan-security-key
28. Fido Alliance 2024 *Biometric Update*. Режим доступу: https://fidoalliance.org/biometric-update-passkeys-build-momentum-enabling-access-to-15-billion-online-accounts/
29. FIDO Alliance *87% of enterprises in the U.S. and UK are deploying passkeys*. Режим доступу: https://identityweek.net/new-fido-alliance-report-87-of-enterprises-in-the-u-s-and-uk-are-deploying-passkeys/
30. Yubico *Authentication standards*. Режим доступу: https://www.yubico.com/authentication-standards/
31. YubiKey *Implementation Guide.* Режим доступу: https://www.idmanagement.gov/implement/yubikey-guide/
32. Wikipedia *RSA SecurID.* Режим доступу: https://en.wikipedia.org/wiki/RSA_SecurID
33. Yubico *Financial services case study*. Режим доступу: https://www.yubico.com/resources/reference-customers/financial-services-case-study/
34. Yubico *Simplified authentication Collège de Paris*. Режим доступу: https://www.yubico.com/resources/reference-customers/college-de-paris
35. Yubico *City of Southgate levels up cybersecurity with password less authentication and the YubiKey.* Режим доступу: https://www.yubico.com/resources/reference-customers/city-of-southgate-case-study
36. Скибун, О. (2023). *Фішинг та фішери в сучасному світі*. *Grail of Science*, (23), 259–264. Режим доступу: https://archive.journal-grail.science/index.php/2710-3056/article/view/780

37. Yubico *Set up your YubiKey*. Режим доступу: https://www.yubico.com/setup/
38. Yubico *Works with YubiKey*. Режим доступу: https://www.yubico.com/works-with-yubikey/catalog
39. OWASP *Authentication Cheat Sheet*. Режим доступу: https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html
40. Yubico *Product Documentation*. Режим доступу: https://docs.yubico.com/
41. FIDO *User Authentication Specifications Overview*. Режим доступу: https://fidoalliance.org/specifications/
42. Yubico *PIV Compatible Smart Cards*. Режим доступу: https://www.yubico.com/authentication-standards/smart-card/
43. *A Tale of Two Studies: The Best and Worst of YubiKey Usability*. Режим доступу: https://ieeexplore.ieee.org/document/8418643
44. Arstechnica *YubiKeys are vulnerable to cloning attacks thanks to newly discovered side channel.* Режим доступу: https://arstechnica.com/security/2024/09/yubikeys-are-vulnerable-to-cloning-attacks-thanks-to-newly-discovered-side-channel/
45. Yubico *Securing SSH with the YubiKey*. Режим доступу: https://developers.yubico.com/SSH/
46. Wired *The Full Story of the Stunning RSA Hack Can Finally Be Told*. Режим доступу: https://www.wired.com/story/the-full-story-of-the-stunning-rsa-hack-can-finally-be-told
47. Гайкова, В., & Малахов, С. (2021). *Аналіз факторів і умов реалізації кібербулінгу з урахуванням можливостей сучасних інформаційних систем. Комп'ютерні науки та кібербезпека*, (1), 50-59. Режим доступу: https://doi.org/10.26565/2519-2310-2021-1-04
48. Teramind *10 Indicators of Compromise (IOC) Examples To Look Out For*. Режим доступу: https://www.teramind.co/blog/how-to-recognize-indicators-of-compromise/
49. OpenSSH *Security Best Practices*. Режим доступу:

https://www.openssh.com/security.html

50. RedHat *Eight ways to protect SSH access on your system*. Режим доступу: https://www.redhat.com/en/blog/eight-ways-secure-ssh
51. *How to Fix the "Warning: Remote Host Identification Has Changed" Error*. Режим доступу: https://ultahost.com/knowledge-base/fix-warning-remote-host-identification-has-changed-error/
52. *Compromised Credentials: Examples & Mitigation Strategies*. Режим доступу: https://www.reco.ai/learn/credential-compromise
53. Yubico *What is Phishing-Resistant MFA?* Режим доступу: https://www.yubico.com/resources/glossary/phishing-resistant-mfa/

ДОДАТОК А

Yubikey with WSL2

Install socat in your WSL Linux:

```
# In WSL
sudo apt install socat
```

Now let's install wsl-ssh-pageant. Check first that your "~/.ssh" directory exist, if not you need to create it first: "mkdir ~/.ssh".

```
# In WSL
windows_destination="/mnt/c/Users/Public/Downloads/wsl2-ssh-pageant.exe"
linux_destination="$HOME/.ssh/wsl2-ssh-pageant.exe"
wget -O "$windows_destination" "https://github.com/BlackReloaded/wsl2-ssh-pageant/releases/latest/download/wsl2-ssh-pageant.exe"
# Set the executable bit.
chmod +x "$windows_destination"
# Symlink to linux for ease of use later
ln -s $windows_destination $linux_destination
```

Finally, add the following config to your .bashrc file.

```
export SSH_AUTH_SOCK="$HOME/.ssh/agent.sock"
if ! ss -a | grep -q "$SSH_AUTH_SOCK"; then
   rm -f "$SSH_AUTH_SOCK"
   wsl2_ssh_pageant_bin="$HOME/.ssh/wsl2-ssh-pageant.exe"
   if test -x "$wsl2_ssh_pageant_bin"; then
      (setsid nohup socat UNIX-LISTEN:"$SSH_AUTH_SOCK,fork" EXEC:"$wsl2_ssh_pageant_bin" >/dev/null 2>&1 &)
   else
      echo >&2 "WARNING: $wsl2_ssh_pageant_bin is not executable."
   fi
   unset wsl2_ssh_pageant_bin
fi

export GPG_AGENT_SOCK="$HOME/.gnupg/S.gpg-agent"
if ! ss -a | grep -q "$GPG_AGENT_SOCK"; then
   rm -rf "$GPG_AGENT_SOCK"
   wsl2_ssh_pageant_bin="$HOME/.ssh/wsl2-ssh-pageant.exe"
   if test -x "$wsl2_ssh_pageant_bin"; then
      (setsid nohup socat UNIX-LISTEN:"$GPG_AGENT_SOCK,fork" EXEC:"$wsl2_ssh_pageant_bin -gpgConfigBasepath 'C:/Users/YOUR-WINDOWS-USERNAME-HERE/AppData/Local/gnupg' -gpg S.gpg-agent" >/dev/null 2>&1 &)
   else
      echo >&2 "WARNING: $wsl2_ssh_pageant_bin is not executable."
   fi
   unset wsl2_ssh_pageant_bin
fi
```

Now restart your PC just to be sure (or just restart WSL with "wsl --shutdown" from Powershell)

Рисунок А.1 – Приклад інструкції з налаштування YubiKey для середовища WSL2 *(Windows Subsystem for Linux)*