https://doi.org/10.31891/2219-9365-2023-74-7
УДК 004.056.5

ЦАВОЛИК Тарас
Західноукраїнський національний університет
https://orcid.org/0000-0002-1136-5705
e-mail: calisto2292@gmail.com
ЯЦКІВ Василь
Західноукраїнський національний університет
https://orcid.org/0000-0001-9778-6625
e-mail: jazkiv@ukr.net
ЯЦКІВ Наталія
Західноукраїнський національний університет
https://orcid.org/0000-0003-2421-4217
e-mail: jatskiv@ukr.net
ІВАСЬЄВ Степан
Західноукраїнський національний університет
https://orcid.org/0000-0003-2243-5956
e-mail: isv@wunu.edu.ua

ВИЯВЛЕННЯ НЕДОЛІКІВ У МЕХАНІЗМАХ АУТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ В SAAS-СЕРВІСАХ НА ОСНОВІ MITRE ATT&CK

У сучасному світі більшість бізнесів використовують SaaS-сервіси для зберігання та обробки конфіденційної інформації, що створює великий потік даних, який потребує захисту. Запобігання зловживанню даними є однією з ключових проблем у бізнесі. Для вирішення цієї проблеми важливо розуміти потенційні загрози, які можуть виникнути, та вживати відповідні заходи для їх запобігання.

Забезпечення надійного та безпечного доступу користувачів до SaaS-сервісів є важливою складовою інформаційної безпеки. Механізми аутентифікації відіграють ключову роль у перевірці ідентичності користувачів і забезпеченні їхньої авторизованої доступності. Однак, недоліки в цих механізмах можуть створювати потенційні шляхи для зловживань та несанкціонованого доступу.

MITRE ATT&CK є потужним інструментом, який може бути використаний для виявлення потенційних недоліків у механізмах аутентифікації користувачів в SaaS-сервісах. ATT&CK надає детальний опис злочинних тактик та технік, які можуть бути використані зловмисниками для атак на системи аутентифікації користувачів. Це дозволяє компаніям аналізувати свої механізми аутентифікації та вживати заходи для їх покращення та запобігання можливих атак.

Цей підхід дозволяє організаціям не лише ідентифікувати потенційні недоліки в механізмах аутентифікації, але й розробляти ефективні заходи для їхнього виявлення, запобігання та усунення. Застосування матриці MITRE ATT&CK для виявлення недоліків у механізмах аутентифікації стає все більш актуальним у контексті зростаючих загроз та необхідності захищати конфіденційні дані користувачів.

Ключові слова: SaaS-сервіси, матриця MITRE ATT&CK, аутентифікація користувачів, фреймворк MITRE.

TSAVOLYK Taras, YATSKIV Vasyl, YATSKIV Nataliia, IVASIEV Stepan
West Ukrainian National University

DETECTION OF VULNERABILITIES IN USER AUTHENTICATION MECHANISMS IN SAAS SERVICES BASED ON MITRE ATT&CK

In the modern world, the majority of businesses use SaaS services for storing and processing confidential information, creating a large flow of data that requires protection. Preventing data abuse is one of the key challenges in business. To achieve this goal, it is important to understand potential threats that may arise and take appropriate measures to prevent them.

Ensuring reliable and secure user access to SaaS services is an important component of information security. Authentication mechanisms play a crucial role in verifying the identity of users and ensuring their authorized access. However, vulnerabilities in these mechanisms can create potential avenues for abuse and unauthorized access.

MITRE ATT&CK is a powerful tool that can be used to identify potential vulnerabilities in user authentication mechanisms in SaaS services. ATT&CK provides a detailed description of criminal tactics and techniques that can be used by attackers to target user authentication systems. This enables companies to analyse their authentication mechanisms and take measures to improve them and prevent potential attacks.

This approach allows organizations not only to identify potential weaknesses in authentication mechanisms but also to develop effective measures for their detection, prevention, and mitigation. The use of the MITRE ATT&CK Matrix for identifying vulnerabilities in authentication mechanisms is becoming increasingly relevant in the context of growing threats and the need to protect users' confidential data.

Keywords: SaaS services, MITRE ATT&CK matrix, user authentication, MITRE framework.

Аналіз фреймворка MITRE ATT&CK

MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) є фреймворком для опису поведінки кіберзагроз та їхніх методів, що використовуються для здійснення атак на комп'ютерні

системи. ATT&CK розроблений MITRE Corporation з метою створення універсального мовного засобу для спілкування та аналізу в сфері кібербезпеки [1 – 3].

Фреймворк MITRE ATT&CK охоплює широкий спектр тактик, технік і процедур (TTP) зловмисників, що використовуються під час кібератак. ATT&CK надає детальний опис кожної тактики та пов'язаних з нею технік, а також інформацію про інструменти, джерела даних та інші корисні відомості. Основні цілі фреймворку ATT&CK:

1. Опис атак. ATT&CK надає детальні описи тактик, технік та процедур, що використовуються зловмисниками, щоб зрозуміти їх наміри та методи дії.

2. Виявлення атак. ATT&CK допомагає встановити і покращити механізми виявлення кібератак шляхом ідентифікації загроз та встановлення відповідних сигнатур та показників компрометації.

3. Аналіз та відповідь на інциденти. ATT&CK надає важливі вказівки щодо розслідування інцидентів та відповіді на атаки, допомагаючи розуміти поведінку загроз та їх можливі наслідки.

ATT&CK розширюється на різні області, включаючи розробку програмного забезпечення, інформаційну безпеку та кібербезпеку в загальному. Цей фреймворк широко використовується в індустрії кібербезпеки, в тому числі організаціями, які займаються аналізом загроз, розробкою програмного забезпечення, відповіддю на інциденти та навчанням фахівців з кібербезпеки [7, 11, 12].

ATT&CK допомагає організаціям покращити свою обороноздатність та здатність виявляти та реагувати на кібератаки, використовуючи інформацію про загрози, що використовуються в реальних атаках. Це цінний ресурс для розуміння методів зловмисників та покращення загальної кібербезпеки організації.

Аналіз механізмів аутентифікації користувачів в SaaS-сервісах

Оскільки в SaaS сервісах є багато важливої інформації про користувачів і все більше сервісів переходять в хмару було б доцільно використовувати для протидії загрозам SaaS Matrix (рис. 1), яка є одним з розширень фреймворку MITRE ATT&CK, спеціально розробленим для оцінки загроз безпеці, пов'язаних з SaaS-сервісами. Ця матриця доповнює основну MITRE ATT&CK, зосереджуючись на загрозах, що впливають на цей тип хмарних сервісів.

SaaS Matrix включає тактики, техніки та інструменти, які можуть бути використані зловмисниками для атак на SaaS-сервіси. Вона допомагає організаціям та безпековим командам розуміти можливі загрози, ідентифікувати недоліки в механізмах аутентифікації та розробляти стратегії захисту [13, 14].

Рис. 1. Захист SaaS – сервісів на основі фреймворка MITRE ATT&CK

Матриця SaaS включає різні тактики, такі як отримання початкового доступу, виконання, збереження, ескалацію привілеїв, ухиляння від виявлення, доступ до облікових даних, відкриття, горизонтальний рух, збір інформації, виведення та вплив. Кожна тактика включає набір пов'язаних з нею технік, які можуть бути використані зловмисниками.

Оцінка рівня складності виконання технік відбувається на основі трьох рівнів: низький, середній та високий. Це вказує на складність та вимоги, які виникають для виконання кожної конкретної техніки.

SaaS Matrix допомагає організаціям зрозуміти потенційні загрози та недоліки, пов'язані з механізмами аутентифікації користувачів в SaaS-сервісах, і розробити ефективні заходи забезпечення безпеки. Вона слугує цінним інструментом для аналізу, виявлення та розробки стратегій захисту в контексті SaaS-середовища [9].

Матриця ATT&CK розділена на так звані "тактики" та "техніки" [4].

Тактики - це загальні категорії злочинних дій, які можуть бути застосовані хакерами для досягнення своїх цілей. Наприклад, тактика "Credential Access" описує методи, за допомогою яких зловмисники можуть отримати доступ до облікових даних користувачів.

Техніки - це конкретні методи, які використовуються зловмисниками для досягнення цілей в межах відповідної тактики. Наприклад, техніка "Password Spraying" описує спосіб атаки, при якому зловмисник спробує ввести кілька популярних паролів для багатьох облікових записів, щоб отримати доступ до системи.

В наведеній таблиці 1 наведені тактики та кількістю пов'язані з ними техніки, які можуть бути використані для злому механізмів аутентифікації в SaaS-сервісах [8].

Таблиця 1

Тактики та кількість пов'язаних технік
для тестування безпеки механізмів аутентифікації в SaaS-сервісах

Тактика	Кількість пов'язаних технік
Initial Access	9
Execution	14
Persistence	7
Privilege Escalation	7
Defense Evasion	6
Credential Access	6
Discovery	11
Lateral Movement	5
Collection	5
Exfiltration	4
Impact	5

Крім того, кожна техніка має рівень складності виконання (Рис. 2), який вказує на те, наскільки складно зловмисникам виконати конкретну техніку [8].

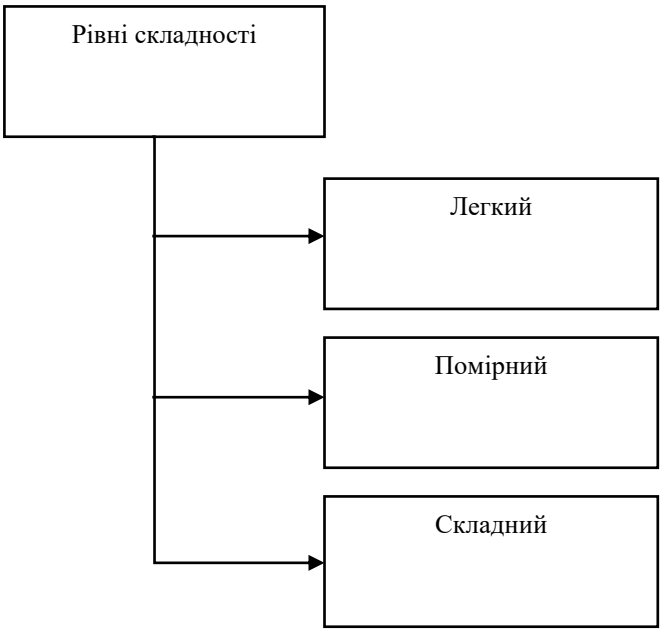

Рис. 2. Рівні складності технік в матриці MITRE ATT&CK

Основні механізми аутентифікації користувачів в SaaS-сервісах включають наступні методи [5, 6]:

1. Ідентифікація користувача і пароль. Це найпоширеніший механізм аутентифікації, де користувачі вводять свій ідентифікатор (наприклад, ім'я користувача або електронну пошту) та пароль для підтвердження своєї особи.

2. Багатофакторна аутентифікація. Цей механізм вимагає від користувачів надання двох або більше факторів для підтвердження своєї особи. Це може включати введення пароля, використання фізичного пристрою (такого як смартфон або токен доступу) або біометричну ідентифікацію (відбиток пальця, розпізнавання обличчя тощо).

3. Одноразові паролі (OTP - One Time Password). Цей механізм використовується для надання тимчасового пароля або коду, який використовується лише один раз для автентифікації користувача. Це може бути відправлення OTP на мобільний телефон або використання генератора OTP.

4. FIDO (Fast Identity Online). Цей відкритий стандарт використовується для сильної аутентифікації, включаючи використання фізичних пристроїв, таких як USB-ключі або біометричні сканери, для підтвердження особи користувача.

5. Сертифікати і цифрові підписи. Даний механізм використовується для аутентифікації користувачів за допомогою цифрових сертифікатів та підписів. Користувачі мають приватний ключ, що використовується для створення підпису, а сервери перевіряють цей підпис з використанням відповідного публічного ключа.

6. Синхронні токени. Даний механізм використовується для генерації унікального коду аутентифікації на основі спільного секретного ключа між сервером і фізичним пристроєм користувача. Цей код вводиться користувачем для підтвердження своєї особи.

В таблиці 2 наведені основні механізми аутентифікації, тактики, техніки та рівні складності виконання з якими може зіткнутися хакер при взломі SaaS систем [8].

Таблиця 2

Механізми аутентифікації, тактики та техніки в SaaS – сервісах

Механізм	Тактика	Техніки	Рівень складності виконання
Ідентифікація користувача і пароль	Зламання паролю	Відновлення пароля з використанням хешів	Середній
		Крадіжка паролів	
		Відновлення пароля через перехоплення трафіку	Високий
Багатофакторна аутентифікація	Фішинг та соціальний інженерінг	Фішинг аутентифікаційних даних	Середній-високий
		Викрадення другого фактора аутентифікації	
Одноразові паролі (OTP)	Фішинг та соціальний інженерінг	Викрадення OTP	Середній-високий
		Відновлення OTP з використанням перехопленого трафіку	Високий
FIDO (Fast Identity Online)	Викрадення фізичного пристрою	Соціальна інженерія для підміни FIDO-пристрою	Високий
		Використання краденого FIDO-пристрою	Середній-високий
Сертифікати і цифрові підписи	Викрадення приватного ключа	Використання викраденого приватного ключа	Високий
		Підробка підпису	Високий
Синхронні токени	Фішинг та соціальний інженерінг	Викрадення секретного ключа токена	Середній-високий
		Підробка синхронного коду	

Застосування MITRE ATT&CK для виявлення недоліків у механізмах аутентифікації користувачів в SaaS-сервісах.

Виявлення недоліків у механізмах аутентифікації в SaaS-сервісах є критично важливим завданням для забезпечення безпеки даних та запобігання несанкціонованому доступу. Існує кілька підходів до виявлення таких недоліків, які можуть бути використані організаціями для поліпшення своїх механізмів аутентифікації. В таблиці 3 наведені різні підходи до виявлення недоліків у механізмах аутентифікації в SaaS сервісах, а також порівняння їх переваги та недоліки.

Таблиця 3

Підходи до виявлення недоліків у механізмах аутентифікації в SaaS сервісах

Назва підходу	Опис підходу	Переваги	Недоліки
Аналіз журналів та моніторинг	Цей підхід полягає в аналізі журналів активності та моніторингу подій, пов'язаних з аутентифікацією.	Можливість виявлення підозрілої активності, нестандартних аутентифікаційних звернень або намагань несанкціонованого доступу.	Велика кількість згенерованих подій, що потребують ефективного моніторингу та аналізу.
Перевірка наявності актуальних патчів та вразливостей	Цей підхід передбачає оцінку наявності актуальних патчів і визначення потенційних вразливостей у механізмах аутентифікації	Дозволяє виявити відомі недоліки та вирішити їх шляхом встановлення патчів або розробки відповідних заходів безпеки.	Складність виявлення нових невідомих вразливостей та залежність від постачальників SaaS-сервісів для вирішення проблем безпеки
Тестування проникнення	Цей підхід полягає в проведенні спеціалізованих тестів проникнення для ідентифікації слабких місць у механізмах аутентифікації.	Виявлення потенційних проблем та використання реалістичних сценаріїв атак.	Висока вартість та потреба у висококваліфікованих спеціалістах для проведення тестування.
Аналіз вразливостей з використанням інструментів автоматичного сканування	Цей підхід використовує спеціалізовані інструменти для автоматичного сканування системи з метою виявлення вразливостей у механізмах аутентифікації.	Виявляє низькорівневі проблеми та надає широкий огляд стану безпеки системи.	Висока кількість фальшиво-позитивних результатів та потреба додаткової перевірки та підтвердження виявлених вразливостей.

Кожен з цих підходів має свої переваги та обмеження, і вибір підходу залежить від конкретних потреб та можливостей організації. Комбінація декількох підходів може бути ефективною стратегією для виявлення недоліків у механізмах аутентифікації в SaaS сервісах і забезпечення високого рівня безпеки.

Використання матриці MITRE ATT&CK для виявлення недоліків в SaaS-сервісах є важливим інструментом для забезпечення безпеки та захисту в цьому типі хмарних сервісів. MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) є фреймворком, який допомагає розуміти різні тактики та техніки, які зловмисники можуть використовувати для атак на системи.

Використовуючи MITRE ATT&CK в контексті SaaS-сервісів, можна ідентифікувати потенційні недоліки та вразливості в механізмах аутентифікації користувачів, які можуть бути використані зловмисниками для отримання несанкціонованого доступу до сервісів або компрометації даних. Фреймворк ATT&CK надає детальну структуру для аналізу та класифікації цих загроз.

За допомогою матриці ATT&CK можна виявити типові атаки та зловмисні дії, пов'язані з механізмами аутентифікації в SaaS-сервісах. Це допомагає розробити ефективні заходи безпеки та вдосконалити механізми аутентифікації для запобігання таким атакам.

Основною перевагою використання MITRE ATT&CK є його всебічність і гнучкість. Матриця ATT&CK надає широкий перелік тактик, технік та підходів, які можуть бути використані зловмисниками. Це дозволяє організаціям аналізувати і виявляти недоліки в механізмах аутентифікації та розробляти конкретні стратегії захисту.

Загалом, використання матриці MITRE ATT&CK для виявлення недоліків у механізмах аутентифікації користувачів в SaaS-сервісах є потужним інструментом для підвищення рівня безпеки і забезпечення захисту від потенційних загроз. Вона допомагає організаціям розуміти різні аспекти атак і розробляти ефективні стратегії захисту, що сприяє безпечному використанню SaaS-сервісів.

Методика застосування MITRE ATT&CK для виявлення недоліків у механізмах аутентифікації користувачів в SaaS-сервісах

Застосування матриці MITRE ATT&CK для виявлення недоліків у механізмах аутентифікації користувачів в SaaS-сервісах включає наступні кроки:

1. Визначення цілей. Організація встановлює свої цілі щодо безпеки аутентифікації користувачів у своїх SaaS-сервісах. Ці цілі можуть включати виявлення атак, захист від зловживання привілеями, забезпечення безпеки облікових записів та ін.

2. Аналіз загроз. Організація вивчає матрицю MITRE ATT&CK, специфічно фокусуючись на тактиках і техніках, пов'язаних з механізмами аутентифікації. Здійснюється аналіз потенційних загроз і ризиків, які можуть виникнути в цьому контексті.

3. Встановлення контрмір. Організація розробляє та впроваджує контрміри для виявлення та запобігання недолікам у механізмах аутентифікації. Це можуть бути технології моніторингу, системи реагування на інциденти, аналітичні інструменти тощо.

4. Моніторинг та виявлення. Застосовуються механізми моніторингу, щоб виявляти незвичайну або підозрілу активність, пов'язану з аутентифікацією користувачів. Наприклад, аналізується зловживання привілеями, спроби несанкціонованого доступу до облікових записів, використання недійсних аутентифікаційних даних тощо.

5. Відповідь на інциденти. У разі виявлення підозрілої активності або атаки на механізми аутентифікації, організація вживає відповідних заходів для припинення атаки, відновлення безпеки та запобігання подібним інцидентам у майбутньому.

6. Аналіз та вдосконалення. Організація аналізує результати виявлення недоліків у механізмах аутентифікації та вдосконалює свої заходи безпеки на основі отриманих даних. Це може включати оновлення політик безпеки, вдосконалення технологічних рішень або проведення навчань та свідомості користувачів.

В результаті застосування MITRE ATT&CK для виявлення недоліків у механізмах аутентифікації в SaaS-сервісах, організація може отримати краще розуміння потенційних загроз та вжити ефективні заходи для покращення безпеки своїх механізмів аутентифікації.

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямі

MITRE ATT&CK є важливим інструментом для виявлення недоліків у механізмах аутентифікації користувачів в SaaS-сервісах. Використання матриці дозволяє організаціям аналізувати потенційні загрози, ідентифікувати слабкі місця і приймати необхідні заходи для підвищення рівня безпеки.

Використання матриці MITRE ATT&CK полягає в тому, що вона надає систематичний підхід до оцінки аутентифікаційних механізмів в SaaS-сервісах. Матриця також надає повний огляд тактик і технік, які зловмисники можуть використовувати для порушення безпеки аутентифікації. Це дозволяє командам із кібербезпеки оцінювати і виявляти потенційні загрози та ризики.

Пропозиції щодо усунення виявлених недоліків та підвищення рівня безпеки в SaaS-сервісах включають:

- Забезпечення надійного механізму аутентифікації. Розробка та впровадження механізму аутентифікації, такого як багатофакторна аутентифікація або використання біометричних даних, може значно підвищити рівень безпеки в SaaS-сервісах.
- Застосування моніторингу та аналізу в реальному часі. Використання систем моніторингу та аналізу в реальному часі дозволяє виявляти незвичайну активність, спроби несанкціонованого доступу та аномалії у механізмах аутентифікації. Це дозволяє оперативно реагувати на потенційні загрози і запобігати їх впливу.
- Забезпечення регулярного оновлення. Потрібно постійно вдосконалювати свої механізми аутентифікації в SaaS-сервісах, враховуючи нові загрози та технології. Регулярні оновлення та вдосконалення допомагають уникнути застарілих недоліків і підвищують рівень безпеки.
- Навчання користувачів. Важливо проводити навчання користувачів щодо безпеки аутентифікації. Регулярні навчальні програми та посібники допоможуть користувачам бути більш свідомими щодо безпекових практик та уникати вразливостей.

Високий рівень безпеки аутентифікації в SaaS-сервісах вкрай важливий для захисту користувачів та конфіденційності даних. Використання матриці MITRE ATT&CK сприяє ідентифікації та виявленню недоліків у механізмах аутентифікації, дозволяючи організаціям розробити ефективні заходи безпеки. Постійний моніторинг, оновлення та навчання користувачів є ключовими елементами для підвищення безпеки в SaaS-сервісах і забезпечення надійної аутентифікації користувачів.

Література

1. B. Strom and A. Robertson, "The MITRE Corporation," 3 March 2020. [Електронний ресурс]. Режим доступу: https://medium.com/MITRE-attack/2020-attack-roadmap-4820d30b38ba (accessed on May 2023).
2. Caltagirone, S., Pendergast, A., & Betz, C. (2013). *The diamond model of intrusion analysis*. Center For Cyber Intelligence Analysis and Threat Research Hanover Md. [Електронний ресурс]. Режим доступу: https://apps.dtic.mil/sti/pdfs/ADA586960.pdf (accessed on May 2023).
3. Strom, B. E., Applebaum, A., Miller, D. P., Nickels, K. C., Pennington, A. G., & Thomas, C. B. (2018). MITRE att&ck: Design and philosophy. In *Technical report*. The MITRE Corporation. [Електронний ресурс]. Режим доступу: https://www.MITRE.org/sites/default/files/2021-11/prs-19-01075-28-MITRE-attack-design-and-philosophy.pdf
4. Al-Shaer, R.; Spring, J.M.; Christou, E. Learning the Associations of MITRE ATT&CK Adversarial Techniques. In Proceedings of the 2020 IEEE Conference on Communications and Network Security (CNS), Avignon, France, 29 June–1 July 2020. [Електронний ресурс]. Режим доступу: https://arxiv.org/pdf/2005.01654.pdf
5. Basra, J.; Kaushik, T. MITRE ATT&CK® as a Framework for Cloud Threat Investigation; Center for Long-Term Cybersecurity (CLTC): Berkeley, Italy, 2020.
6. Georgiadou, A., Mouzakitis, S., & Askounis, D. (2021). Assessing MITRE att&ck risk using a cyber-security culture framework. *Sensors*, *21*(9), 3267. [Електронний ресурс]. Режим доступу: https://www.mdpi.com/1424-8220/21/9/3267/pdf (accessed on May 2023).
7. The MITRE Corporation. “MITRE ATT&CK®”, The MITRE Corporation. 2023. [Електронний ресурс]. Режим доступу: https://attack.MITRE.org/ (accessed on May 2023).
8. The MITRE Corporation. “MITRE ATT&CK®”, The MITRE Corporation for SaaS platform. 2023. [Електронний ресурс]. Режим доступу: https://attack.MITRE.org/matrices/enterprise/cloud/saas/ (accessed on May 2023).
9. Heikki Jauhiainen. Designing End User Area Cybersecurity for Cloud-based Organization, 15 February 2021. [Електронний ресурс]. Режим доступу: https://www.theseus.fi/bitstream/handle/10024/467445/Designing%20End%20User%20Area%20Cybersecurity%20for%20Cloud-based%20Organization.pdf?sequence=2
10. Shahzaib Zahid, Muhammad Shoaib Mazhar, Syed Ghazanfar Abbas, Zahid Hanif, Sadaf Hina, Ghalib A. Shah, Threat modeling in smart firefighting systems: Aligning MITRE ATT&CK matrix and NIST security controls, Internet of Things, Volume 22, July 2023, 100766. DOI: https://doi.org/10.1016/j.iot.2023.100766
11. Ham, Jeroen Van Der. "Toward a better understanding of “Cybersecurity”." *Digital Threats: Research and Practice* 2.3 (2021): 1-3. DOI: https://doi.org/10.1145/3442445
12. Roy, S., Panaousis, E., Noakes, C., Laszka, A., Panda, S., & Loukas, G. (2023). SoK: The MITRE ATT&CK Framework in Research and Practice. *arXiv preprint arXiv:2304.07411*. [Електронний ресурс]. Режим доступу: https://arxiv.org/pdf/2304.07411.pdf
13. ACHAR, Sandesh. Software as a Service (SaaS) as Cloud Computing: Security and Risk vs. Technological Complexity. *Engineering International*, 2016, 4.2: 79-88.

14. PATEL, Navneet Singh; REKHA, B. S. Software as a Service (SaaS): security issues and solutions. *International Journal of Computational Engineering Research*, 2014, 4.6: 68-71.

References

1. B. Strom and A. Robertson, "The MITRE Corporation," 3 March 2020. [Online]. Available: https://medium.com/MITRE-attack/2020-attack-roadmap-4820d30b38ba (accessed on May 2023).
2. Caltagirone, S., Pendergast, A., & Betz, C. (2013). *The diamond model of intrusion analysis*. Center For Cyber Intelligence Analysis and Threat Research Hanover Md. [Online]. Available: https://apps.dtic.mil/sti/pdfs/ADA586960.pdf (accessed on May 2023).
3. Strom, B. E., Applebaum, A., Miller, D. P., Nickels, K. C., Pennington, A. G., & Thomas, C. B. (2018). MITRE att&ck: Design and philosophy. In *Technical report*. The MITRE Corporation. [Online]. Available: https://www.MITRE.org/sites/default/files/2021-11/prs-19-01075-28-MITRE-attack-design-and-philosophy.pdf
4. Al-Shaer, R.; Spring, J.M.; Christou, E. Learning the Associations of MITRE ATT&CK Adversarial Techniques. In Proceedings of the 2020 IEEE Conference on Communications and Network Security (CNS), Avignon, France, 29 June–1 July 2020. [Online]. Available: https://arxiv.org/pdf/2005.01654.pdf
5. Basra, J.; Kaushik, T. MITRE ATT&CK® as a Framework for Cloud Threat Investigation; Center for Long-Term Cybersecurity (CLTC): Berkeley, Italy, 2020.
6. Georgiadou, A., Mouzakitis, S., & Askounis, D. (2021). Assessing MITRE att&ck risk using a cyber-security culture framework. *Sensors*, *21*(9), 3267. [Online]. Available: https://www.mdpi.com/1424-8220/21/9/3267/pdf (accessed on May 2023).
7. The MITRE Corporation. "MITRE ATT&CK®", The MITRE Corporation. 2023. [Online]. Available: https://attack.MITRE.org/ (accessed on May 2023).
8. The MITRE Corporation. "MITRE ATT&CK®", The MITRE Corporation for SaaS platform. 2023. [Online]. Available: https://attack.MITRE.org/matrices/enterprise/cloud/saas/ (accessed on May 2023).
9. Heikki Jauhiainen. Designing End User Area Cybersecurity for Cloud-based Organization, 15 February 2021. [Online]. Available: https://www.theseus.fi/bitstream/handle/10024/467445/Designing%20End%20User%20Area%20Cybersecurity%20for%20Cloud-based%20Organization.pdf?sequence=2
10. Shahzaib Zahid, Muhammad Shoaib Mazhar, Syed Ghazanfar Abbas, Zahid Hanif, Sadaf Hina, Ghalib A. Shah, Threat modeling in smart firefighting systems: Aligning MITRE ATT&CK matrix and NIST security controls, Internet of Things, Volume 22, July 2023, 100766. DOI: https://doi.org/10.1016/j.iot.2023.100766
11. Ham, Jeroen Van Der. "Toward a better understanding of "Cybersecurity"." *Digital Threats: Research and Practice* 2.3 (2021): 1-3. DOI: https://doi.org/10.1145/3442445
12. Roy, S., Panaousis, E., Noakes, C., Laszka, A., Panda, S., & Loukas, G. (2023). SoK: The MITRE ATT&CK Framework in Research and Practice. *arXiv preprint arXiv:2304.07411*. [Online]. Available: https://arxiv.org/pdf/2304.07411.pdf
13. ACHAR, Sandesh. Software as a Service (SaaS) as Cloud Computing: Security and Risk vs. Technological Complexity. *Engineering International*, 2016, 4.2: 79-88.
14. PATEL, Navneet Singh; REKHA, B. S. Software as a Service (SaaS): security issues and solutions. *International Journal of Computational Engineering Research*, 2014, 4.6: 68-71.