ДАДАТОК А

Перелік посилань відповідно до наукових досліджень кафедри

13. Kachko, O., Makutonina, L., Akolzina, O. Similar algorithm optimization for asymmetric encryption with the «overstretched parameters».//NTRU 2017 4th International Scientific-Practical Conference Problems of Infocommunications Science and Technology. 2017. С. 330-333.

31. Медовой О.Л. Контекстно-онтологічна модель та методи обчислення метрик інформаційної якості веб-орієнтованих систем. Херсон, Вестник Херсонского національного технического университета, №34, С. 162-165. 2009 р.

ДАДАТОК Б

Слайди презентації

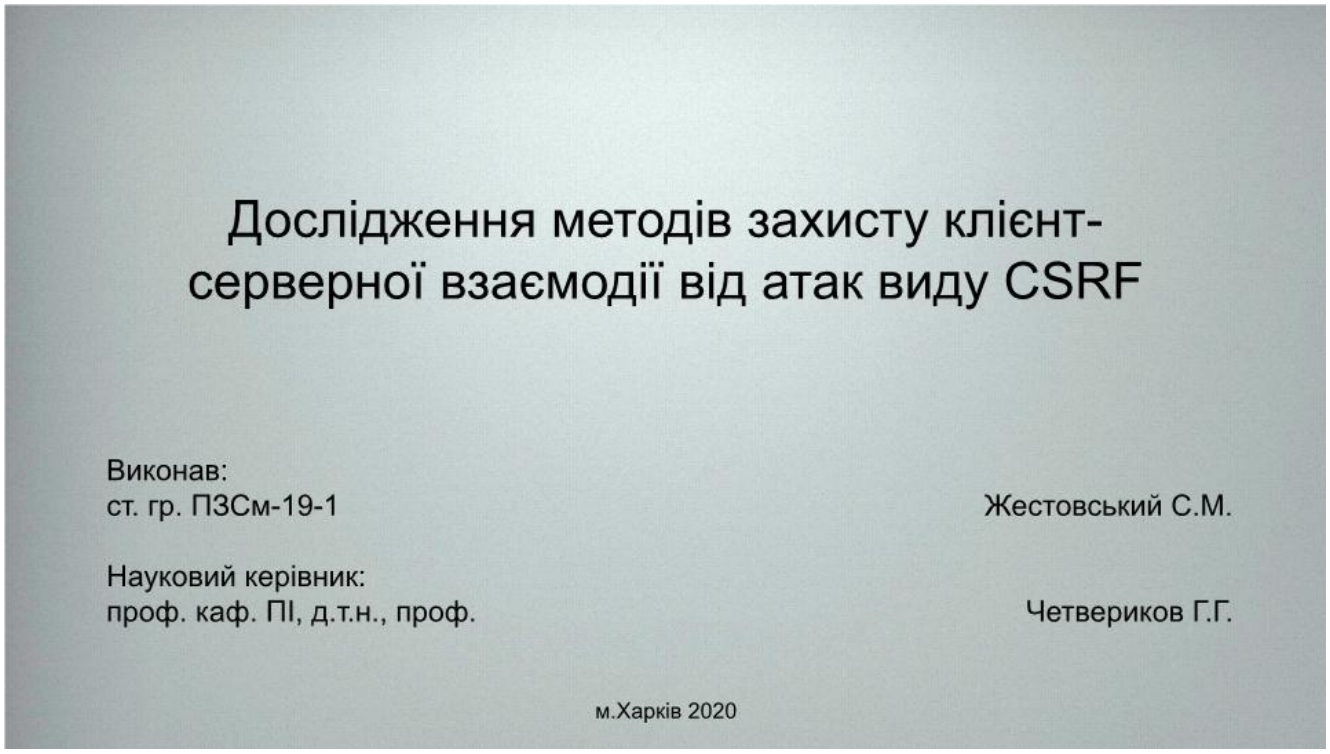

Рисунок Б.1 – Слайд №1

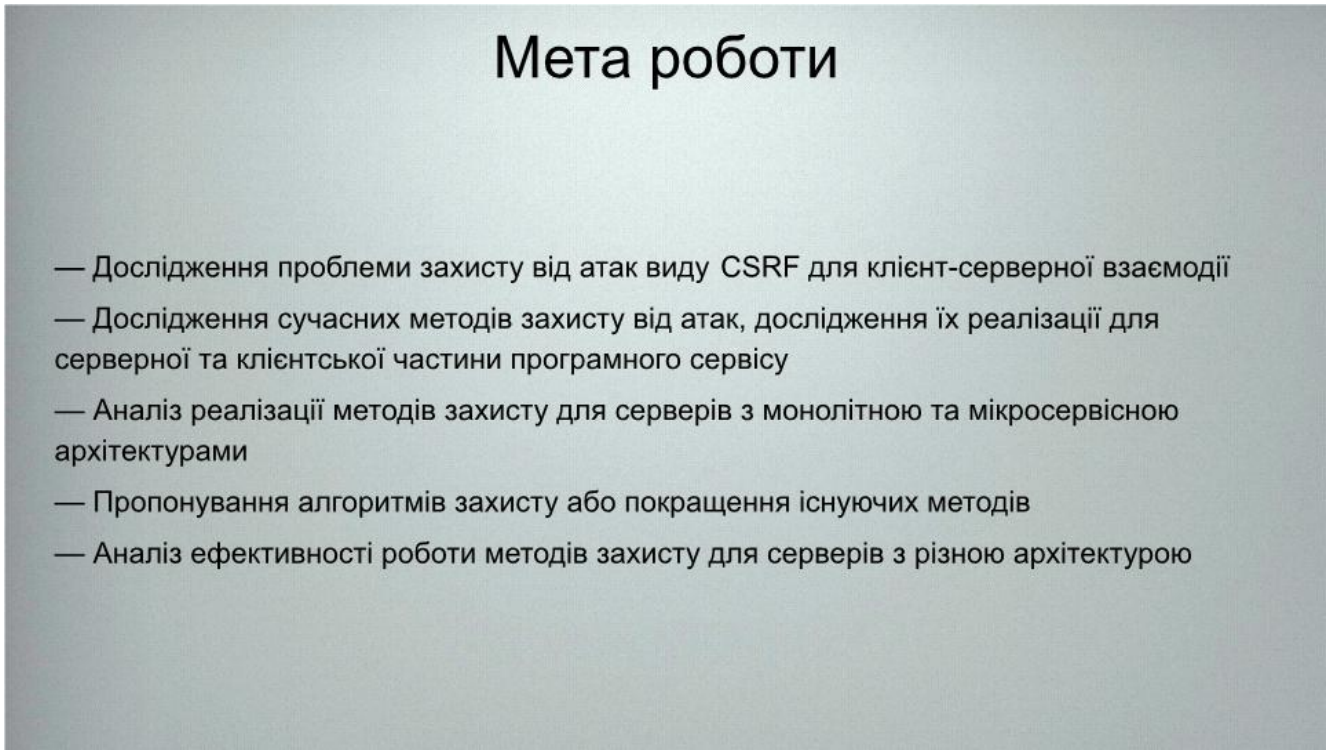

Рисунок Б.2 – Слайд №2

Актуальність проблеми

— Атаки виду SCRF уходять у першу п'ятірку найбільш розповсюджених атак

— Слабкий захист серверів: близько 60% серверів у мережі Інтернет частково або зовсім не захищенні від атак виду SCRF

— Поява нових підвидів SCRF атак, обхід старих реалізацій алгоритмів захисту

— Складність вибору серед наданих методів захисту для відповідних серверних рішень

Рисунок Б.3 – Слайд №3

Атака виду CSRF

Атака виду CSRF (міжсайтова підробка запиту) – це тип зловмисного використання веб-сайту, де несанкціоновані команди подаються від користувача, якому веб-система, що підтверджена атаці, довіряє.

Основним прикладом такої атаки слугує ситуація, де користувач переходить на заздалегідь підготовлений злочинцем веб-сайт (вірусний сайт), де знаходиться спеціальний запит до веб-сервісу, який являється ціллю для злочинця (цільовий сайт). При вході жертви до вірусного сайту, непомітно виконується вірусний запит, що надсилається до цільового сайту.

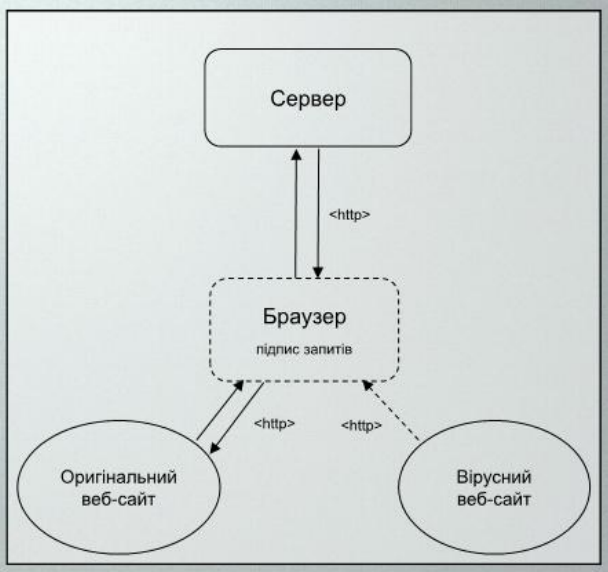

Рисунок Б.4 – Слайд №4

Аналіз існуючих методів захисту

Синхронний токен

Метод синхронного токена використовує згенерований персональний токен до кожної сесії для розпізнавання користувача. Такий токен, як і сам ідентифікатор сесії, зберігається на серверній частині.

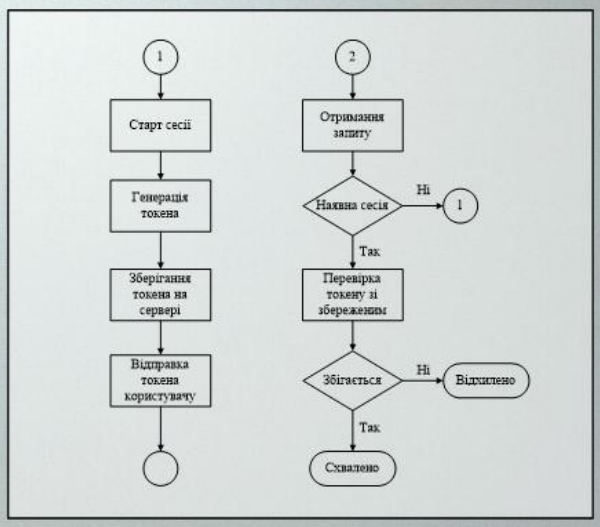

Рисунок Б.5 – Слайд №5

Аналіз існуючих методів захисту

Cookie-файл двійної відправки

Метод cookie-файлу двійної відправки використовує двійний підпис запиту за допомогою токена для перевірки оригінальності запиту.

Цей підхід не вимагає зберігання даних на стороні сервера, тим самим надаючи контроль сесії і токена до користувача.

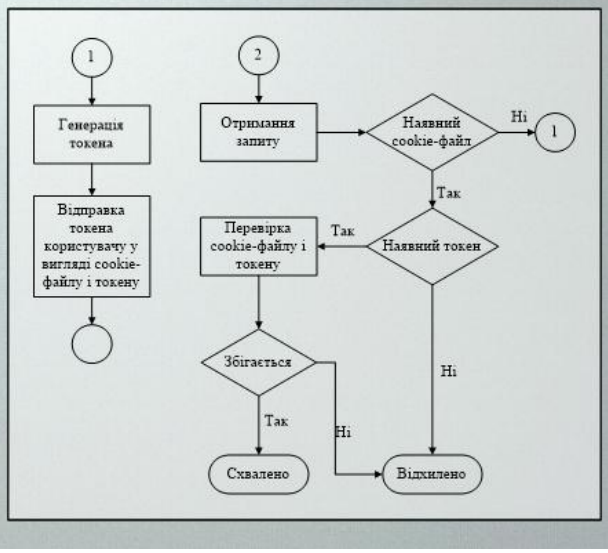

Рисунок Б.6 – Слайд №6

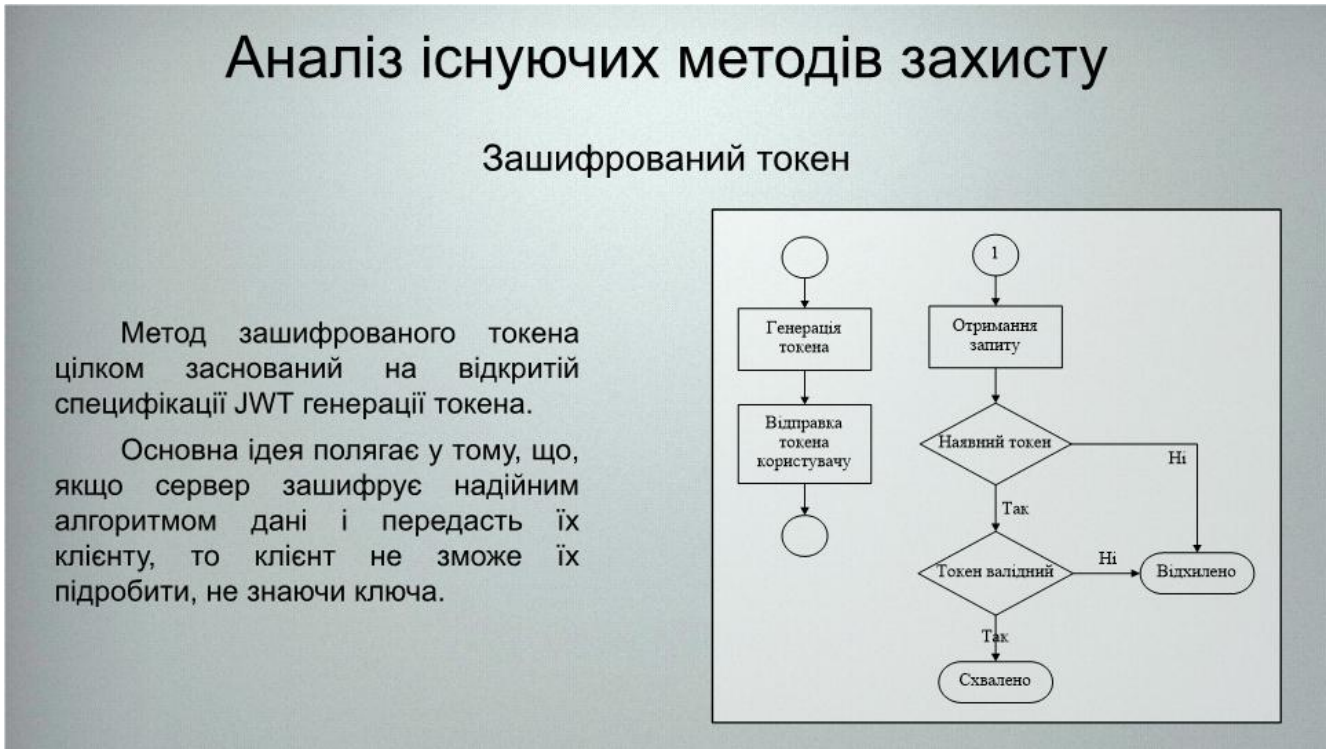

Рисунок Б.7 – Слайд №7

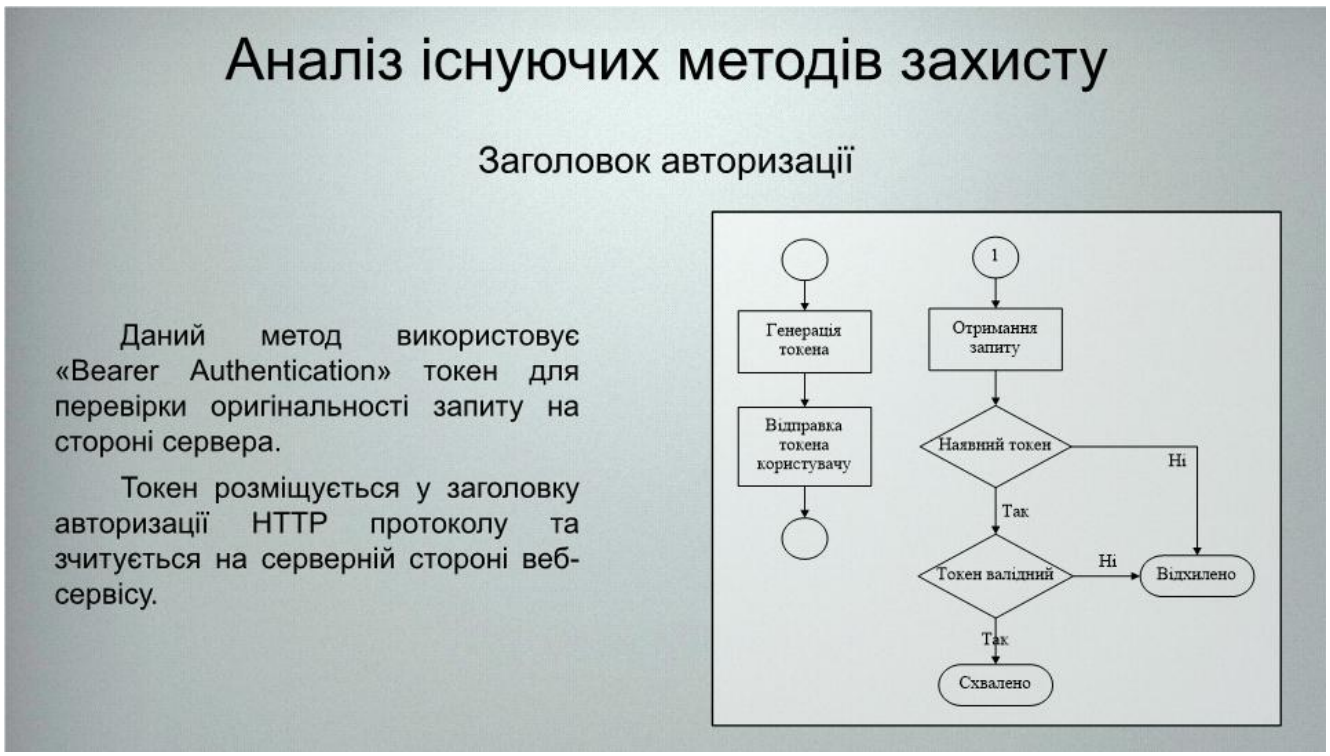

Рисунок Б.8 – Слайд №8

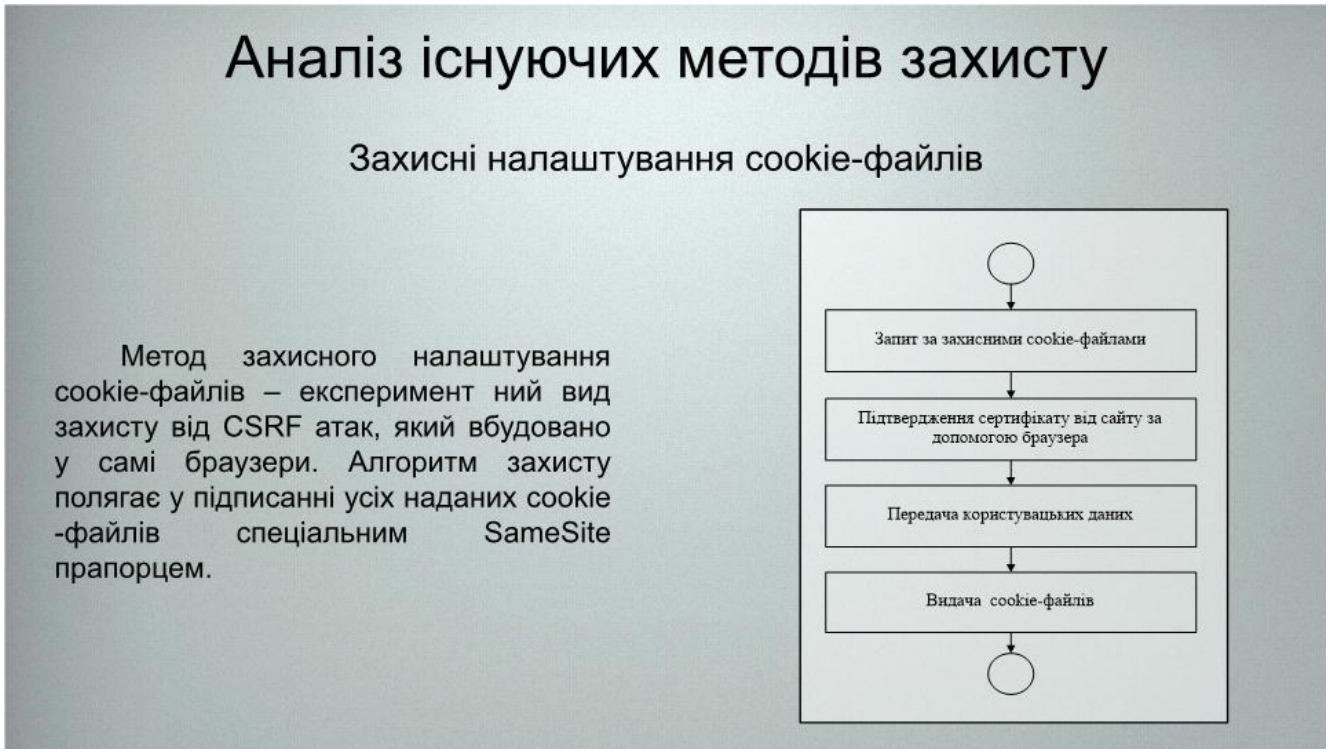

Рисунок Б.9 – Слайд №9

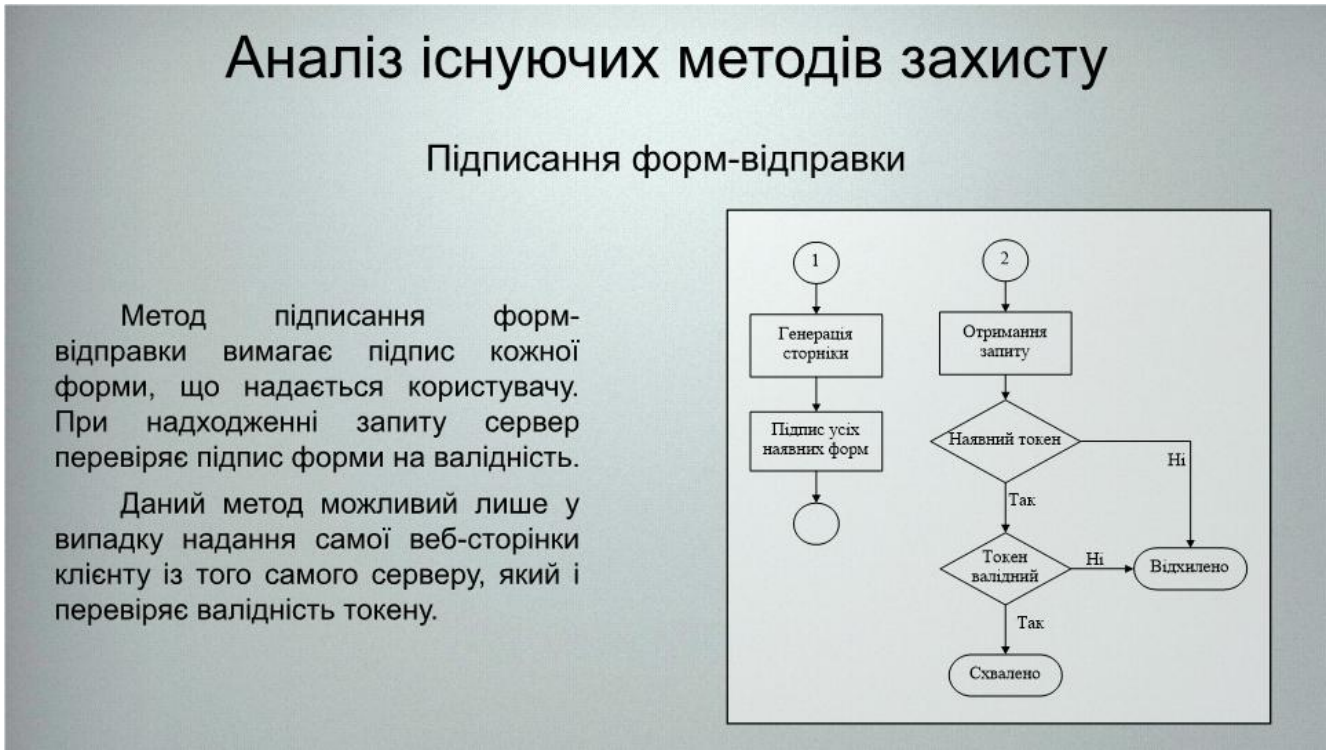

Рисунок Б.10 – Слайд №10

Аналіз існуючих методів захисту

Таблиця доменів

Таблиця доменів – це таблиця довірених ресурсів, що мають право на з'єднання з цільовим сервером.

Така таблиця розташована на сервері у місці, де виконується контроль усіх запитів на сервер.

При надходженні запиту, пакет даних вміщує в собі назву домену з якого було виконано запит. Якщо запит було виконано з оригінального сайту (тобто цільової веб-сторінки), то назва домену збігається з поточною назвою домену сервера.

Рисунок Б.11 – Слайд №11

Постановка задачі

— Дослідити сучасні методи захисту від атак виду CSRF для клієнт-серверної взаємодії з урахуванням серверів з різною архітектурою

— Створити алгоритми захисту або покращити працездатність існуючих методів

—Проаналізувати реалізацію методів захисту, вивести основні критерії для порівняння алгоритмів

— Побудувати тестову середу та провести тестування наданих методів захисту з урахуванням особливостей серверних архітектур

Рисунок Б.12 – Слайд №12

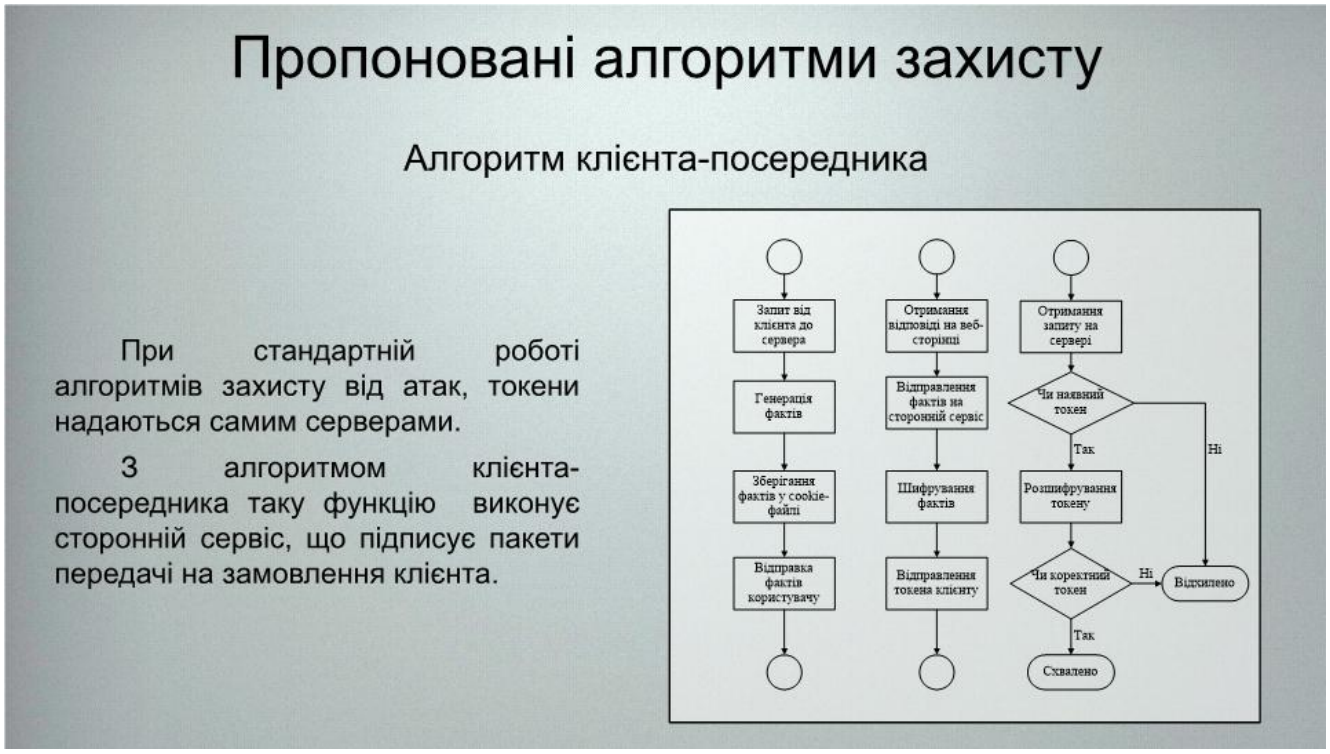

Рисунок Б.13 – Слайд №13

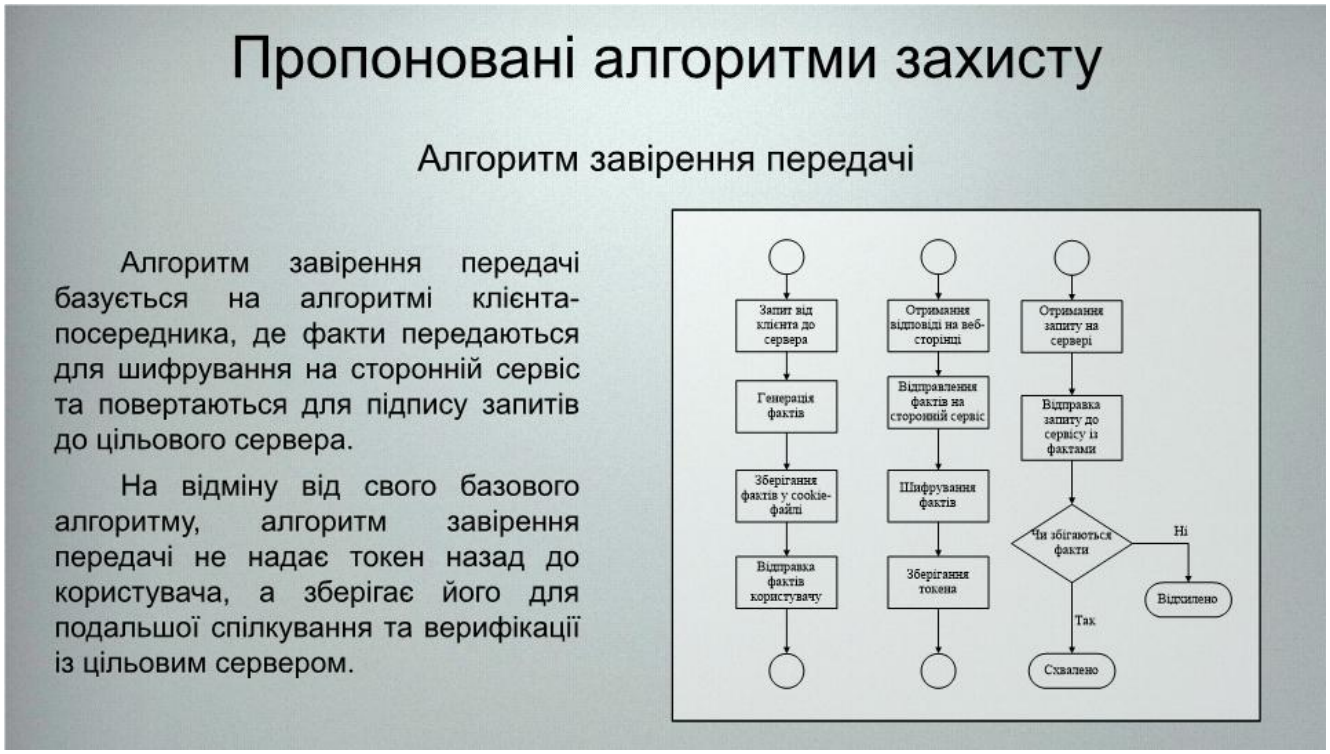

Рисунок Б.14 – Слайд №14

Рисунок Б.15 – Слайд №15

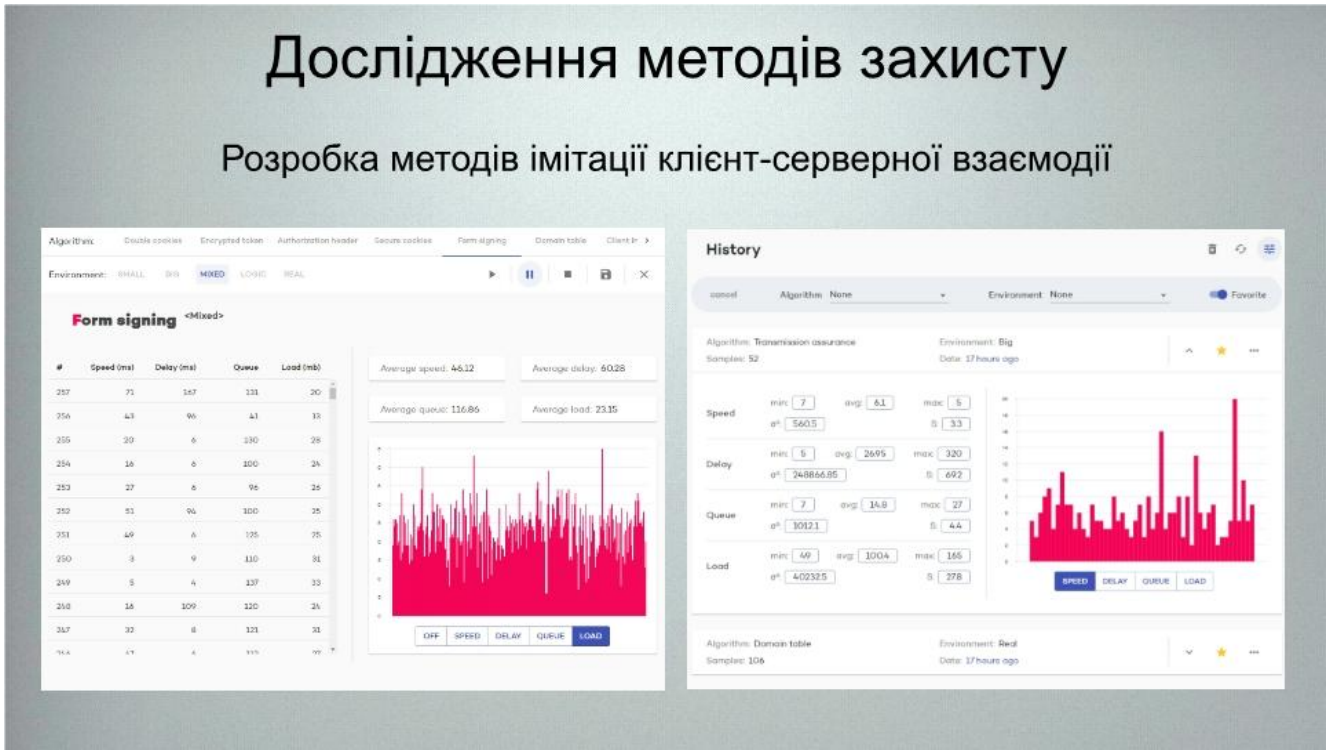

Рисунок Б.16 – Слайд №16

Дослідження методів захисту

Аналіз методів та алгоритмів захисту

Методи захисту	Критерії ефективності				
	Швидкість	Об'єм оброблюваних даних	Навантаження	Розмір коду	Безпека
Cookie-файл двійної відправки	59,4	15,6	149,2	252	6
Зашифрований токен	31,8	4,6	96,4	103	8
Заголовок авторизації	27,8	3,4	82,8	102	8
Захисні налаштування cookie-файлів	28,6	**2**	60	**30**	4
Підписання форм-відправки	101,8	23,2	114,8	131	5
Таблиця доменів	**26,4**	4	175,8	210	6
Алгоритм клієнта-посередника	38,8	2,2	**56,8**	63	8
Алгоритм завірення передачі	49,4	6,8	59,4	63	**10**

Рисунок Б.17 – Слайд №17

Висновок

В роботі було досліджено показники ефективності методів захисту клієнт-серверної від атак виду CSRF.

За результатами проведеного аналізу:

— найкращим методом захисту є алгоритм завірення передачі;

— наступним за оцінкою методом захисту є алгоритм клієнта-посередника;

— третій по ефективності метод захисту – алгоритм заголовків авторизації.

Було створено алгоритми захисту на основі стороннього сервісу для серверів переважно з мікросервісною архітектурою.

Рисунок Б.18 – Слайд №18

ДАДАТОК В

Стаття «Порівняльна характеристика основних методів захисту клієнт-серверної взаємодії від мережевих атак виду CSRF»

Приведенные примеры – лишь частичные решения множества задач, которые нам с вами ещё предстоит изучить. Такая разработка как «дрон» дает возможность расширить не только возможности людей, но и целых организаций, работая на благо общества. Главное – суметь протолкнуть «очередную революцию дронов» в правильное русло.

Список использованных источников:

1. Интернет дронов (Internet of drones, IoD) — очередная революция [Електронний ресурс] – Режим доступу до ресурсу: https://www.it.ua/ru/knowledge-base/technology-innovation/internet-dronov-iod-tehnologicheskaja-revoljucija-x0.
2. Что такое дрон: какие виды бывают и зачем они? [Електронний ресурс] – Режим доступу до ресурсу: https://alb.aero/blog/chto-takoe-dron-kakie-vidy-byvayut-i-zachem-oni.html.
3. Дроны в сельском хозяйстве [Електронний ресурс] – Режим доступу до ресурсу: https://protocol.ua/ru/kakie_droni_ispolzovat_dlya_selskogo_hozyaystva/
4. Как дроны помогают бизнесу и людям [Електронний ресурс] – Режим доступу до ресурсу: https://www.vedomosti.ru/technology/articles/2017/10/23/739085-kak-droni-pomogayut-biznesu.

Жестовський Сергій Миколайович, здобувач вищої освіти факультету комп'ютерних наук
«Харківський національний університет радіоелектроніки», Україна

Науковий керівник: Четвериков Григорій Григорович, доктор технічних наук, професор, професор кафедри програмної інженерії
«Харківський національний університет радіоелектроніки», Україна

ПОРІВНЯЛЬНА ХАРАКТЕРИСТИКА ОСНОВНИХ МЕТОДІВ ЗАХИСТУ КЛІЄНТ-СЕРВЕРНОЇ ВЗАЄМОДІЇ ВІД МЕРЕЖЕВИХ АТАК ВИДУ CSRF

Атака виду CSRF (міжсайтова підробка запиту) – це тип зловмисного використання веб-сайту, де несанкціоновані команди подаються від користувача до серверної частини веб-системи, який користувачу довіряє [1]. Це означає, що даний вид атаки націлений на веб-систему через її довірених користувачів. Основним прикладом такої атаки слугує ситуація, де користувач переходить на заздалегідь підготовлений злочинцем веб-сайт, де знаходиться спеціальний запит до серверної частини на яку націлений злочинець. В момент потрапляння жертви до вірусного сайту, виконується вірусний запит, що надсилається до цільового сайту. Тут треба зауважити метод роботи браузерів в даній ситуації, який є одним із ключових місць вразливості при атаці даного виду: при відправці запиту, браузер підписує пакети, що передаються, користувацькими даними, які були видані веб-сервером (також називаються cookie-файлами). У результаті атаки на веб-сервіс, цільовий сервер виконує передані команди із вірусного сайту, вважаючи, що даний запит був надісланий оригінальним користувачем, хоча сам користувач не мав уявлення о факті передачі запиту.

Опис методів та алгоритмів захисту. Для захисту клієнт-серверної взаємодії від атак виду CSRF існує декілька методів та алгоритмів, описаних нижче. Кожен окремий метод вирішує основну проблему захисту мережевого з'єднання, однак має певні недоліки, та для більш чіткого розуміння потрібно розглянуть кожен з відомих методів захисту окремо. Перерахуємо основні методи захисту від атак наданого виду:

– синхронний токен – метод використовує згенерований персональний токен [2] до кожної сесії для розпізнавання користувача. Такий токен, як і сам ідентифікатор сесії, зберігається на серверній частині [3, 4];

– cookie-файл двійної відправки – метод використовує двійний підпис запиту за допомогою токена для перевірки оригінальності запиту [3]. Цей підхід не вимагає зберігання даних на стороні сервера, тим самим надаючи контроль сесії і токена до користувача;

– зашифрований токен – метод заснований на відкритій специфікації генерації JWT токена [2]. Основна ідея полягає у тому, що, якщо ви зашифруєте надійним алгоритмом дані і передасте їх клієнту, то клієнт не зможе їх підробити, не знаючи ключа. Цей підхід не вимагає використання cookie-файлів, токен передається клієнту тільки в параметрах відповіді [3, 4];

–заголовок авторизації – метод використовує «Bearer Authentication» токен для перевірки оригінальності запиту на стороні сервера [5]. Bearer Authentication Token, або токен авторизації – це токен, який містить ідентифікаційні дані користувача. Токен розміщується у заголовку авторизації http протоколу (найчастіше у Authorization заголовку) та зчитується на серверній стороні веб-сервісу;

–захисні налаштування cookie-файлів – експеримент ний вид захисту від CSRF атак, який вбудовано у самі браузери [3]. Алгоритм захисту полягає у тому, щоб усі надані cookie-файли підписувати спеціальним SameSite прапорцем. Такий прапорець дає

браузерам зрозуміти, що помічені cookie-файли потрібно відправляти з цільового веб-сайту, таким чином унеможливлюючи відправлення cookie-файлів з вірусного сайту;

–підписання форм-відправки – метод вимагає підпис кожної форми що надається користувачу [3, 4]. При надходженні запиту сервер перевіряє підпис форми на валідність. Даний метод можливий лише у випадку надання самої веб-сторінки клієнту із того самого серверу, який і перевіряє валідність токену, що часто не є правдою;

–таблиця доменів – це таблиця довірених ресурсів, що мають право на з'єднання з цільовим сервером [4]. Така таблиця розташована на сервері у місці, де виконується контроль усіх запитів на сервер. Завдяки звіренню кожного пакету даних з таблицею можна виконувати контроль надсилання даних і з інших, дозволених доменів.

Для перерахованих методів захисту від атак потрібно провести порівняльну характеристику (табл. 1) з метою встановлення переваг та недоліків кожного із методів.

Таблиця 1

Порівняльна характеристика методів захисту від атак виду CSRF

Метод захисту	Переваги	Недоліки
Синхронний токен	– Оновлюється синхронно із користувацькою сесією; – унікальність для кожного клієнта; – простота генерації.	– Зберігається на серверній частині; – вразливий для XSS атак; – прив'язаний до сесії.
Cookie-файл двійної відправки	– Швидкість генерації пари; – при правильній реалізації важко вразливий до XSS атак; – зберігається на клієнті.	– Навантаження при реалізації передачі; – вразливий до cookie ін'єкцій, що призведе до підробити токену.
Зашифрований токен	– Не зберігається на серверній стороні; – клієнт не бере участь у створенні токену; – може містити корисну інформацію про користувача.	– Швидкість створення залежить від бажаної складності токену – вразливий для XSS атак.
Заголовок авторизації	– Часто використовуваний метод; – слугує і як токен авторизації; – може містити корисну інформацію про користувача.	– Вразливий для XSS атак; – має великий час існування, що збільшує шанси на підробку.
Захисні налаштування cookie-файлів	– Прості в реалізації; – на вразливі до XSS атак.	– Експериментальна технологія; – слабко або зовсім не підтримуються певними браузерами.
Підписання форм-відправки	– Простота підпису та відправки; – кожен раз унікальний токен.	– Можливо реалізувати лише при генерації сторінки; – потребують пере генерації цілої сторінки після відправки. – особливо вразливі для XSS атак;
Таблиця доменів	– Не вразлива до субдомених атак; – не вразлива до XSS атак; – не потрібно реалізовувати на стороні клієнта.	– Складність реалізації для серверів із мікросервісної архітектури; – вразлива до спеціальних атак із підробкою домену відправки.

[авторська розробка]

Потрібно зауважити, що показники безпеки алгоритмів цілком залежать від способу реалізації. Тобто при некоректному створені та впровадженні алгоритмів для зловмисника

можуть бути доступні нові способи обходу методів захисту.

Результати порівняльної характеристики. З наданих методів захисту від атак виду CSRF можна поділити більш ефективні (здатні до належного захисту) та менш ефективні (яких слід уникати).

Найменш ефективними методами захисту будуть: метод *захисних налаштувань cookie-файлів*, адже дана технологія лише починає розвиватись, метод *таблиці доменів*, адже для його обходу можна використати методи, які ще простіші у реалізації аніж сама CSRF атака, метод *підписання форм-відправки*, який вимагає перезавантаження цілої сторінки для коректної роботи та потребує вшивання токену при самій генерації сторінки, що являється не самим ефективним способом клієнт-серверної взаємодії. Також тут можна зазначити і метод *cookie-файлів двійної відправки*, проблема якого полягає у швидкості встановлення та верифікації клієнтського запиту.

Ті методи захисту з наданих, що залишились, є більш ефективними для захисту від атак. Кожен з даних методів може бути використаний при вирішенні специфічних потреб: *синхронний токен* може бути обраний за свою прив'язку до сесії, якщо це необхідно, *зашифрований токен* – простий та ефективний алгоритм для захисту від атак та може зберігати у собі корисну інформацію, *заголовок авторизації* – метод, що заснований на методі зашифрованого токену, адже та корисна інформація, зо у ньому зберігається, і є ідентифікатором користувача. Тобто заголовок авторизації слугує як токеном ідентифікації так і токеном перевірки оригінальності запиту користувача.

Висновок. Перераховані методи захисту являються основним способом захисту від атак виду CSRF, яка спроможна підроблювати запити до цільового серверу та використовувати особу користувача для виконання власних запитів. Дані алгоритми спроможні в тій чи іншій міні захистити клієнт-серверну взаємодію від атак та мають свої відповідні переваги та недоліки, через які можуть бути обрані при реалізації певного серверу. З наданих методів захисту найбільш ефективними являються: синхронний токен, зашифрований токен та заголовок авторизації. Остаточний вибір алгоритму залежить від цільового серверу, однак потрібно зауважити, що ефективність методів та їх захисні можливості залежать лише від їх програмної реалізації.

Список використаних джерел:

1. Alexenko, T., Jennc, M., Suman, D. Roy & Zeng, W.J. (2010). Cross-Sitc Request Forgery: Attack and Defense. *2010 7th IEEE Consumer Communications and Networking Conference.* January 9-12, 2010, Las Vegas, NV, USA. https://doi.org/10.1109/CCNC.2010.5421782
2. Sebastián E. Peyrott. The JWT Handbook. (2018). Retrieved from https://assets.ctfassets.net/2ntc334xpx65/o5J4X472PQUI4ai6cAcqg/13a2611de03b2c8edbd09c3ca14ae86b/jwt-handbook-v0_14_1.pdf
3. Cross-Site Request Forgery Prevention Cheat Sheet. (2020). Retrieved from https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet
4. Lin, X. Zavarsky, P., Ruhl, R. & Lindskog, D. (2009). Threat Modeling for CSRF Attacks. *2009 International Conference on Computational Science and Engineering.* August 29-31, 2009, Vancouver, BC, Canada. https://doi.org/10.1109/CSE.2009.372
5. Ahmed, S. & Mahmood, Q. An authentication based scheme for applications using JSON web token. *2019 22nd International Multitopic Conference (INMIC).* November 29-30, 2019, Islamabad, Pakistan. https://doi.org/10.1109/INMIC48123.2019.9022766