Державна служба України з надзвичайних ситуацій
Львівський державний університет безпеки життєдіяльності
Навчально-науковий інститут цивільного захисту
Кафедра інформаційних технологій та телекомунікаційних систем

«Допущено до захисту»
Начальник кафедри ІТтаТС
підполковник служби цивільного захисту
_____ Олександр ПРИДАТКО
“____” _____20___ року

ДИПЛОМНА РОБОТА МАГІСТРА

на тему **«Алгоритмізація процесу інтеграції сучасних методів автентифікації в системах управління взаємодією користувачів»**

Виконала:
студентка VI курсу, групи КН-61м
спеціальності (освітньої програми)
122 "Комп’ютерні науки" (Комп'ютерні науки)
(шифр і назва спеціальності (освітньої програми)
Наталія САМАРА
(ім’я та прізвище)
Керівник Назарій БУРАК
(ім’я та прізвище)
Рецензент Павло ЛУБ
(ім’я та прізвище

Львів – 2021 року

АНОТАЦІЯ

Наталія САМАРА «Алгоритмізація процесу інтеграції сучасних методів автентифікації в системах управління взаємодією користувачів». Дипломна робота за спеціальністю 122 “Комп’ютерні науки ” складається з текстової частини, що містить 3 розділи, 65 с., 17 рис., 6 табл., 39 джерел, 5 додатків.

Об’єкт дослідження – сучасні багатокористувацькі системи реалізовані на клієнт-серверній архітектурі.

Мета роботи – дослідження сучасних підходів ідентифікації користувачів при роботі із віддаленими серверами та розробка методу безпечної автентифікації із використання двох факторів, а також алгоритму його інтеграції в існуючі інформаційні системи.

Магістерська кваліфікаційна робота спрямована на дослідження сучасних методів захисту конфіденційної інформації на етапі авторизації користувачів у системи, які реалізовані на базі віддалених серверів та використовують клієнт-серверний вид з'єднання.

Проведено аналіз сучасних методів автентифікації користувачів у багатокористувацьких системах. Здійснено визначення основних їх переваг та досліджено можливі шляхи реалізації загроз безпеці даних.

Здійснено дослідження основних принципів ідентифікації та алгоритмів функціонування методу двофакторної автентифікації користувачів. Проведено аналіз сучасного стану програмної реалізації даних методів автентифікації.

Обґрунтовано доцільність використання у багатокористувацьких системах методу двофакторної автентифікації та описано архітектуру проектованої системи.

Розроблено алгоритм інтеграції методу двофакторної автентифікації в системах із взаємодією декількох користувачів.

АВТЕНТИФІКАЦІЯ, БАГАТОКОРИСТУВАЦЬКІ СИСТЕМИ, СЕРВІСИ ДВОФАКТОРНОЇ АВТЕНТИФІКАЦІЇ, БЕЗПЕКА, ІНФОРМАЦІЯ

ВИСНОВКИ

В наш час автентифікація є важливою процедурою для забезпечення конфіденційності, цілісності та доступності інформації користувачів у будь-яких системах чи ресурсах. Вона використовується повсякчас та всюди для обмеження та здійснення контролю, як фізичного доступу до об'єкту, так і доступу до інформації в самій системі.

Зростання кількості використовуваних застосунків та стрімкий розвиток технологій сьогодення зумовлюють необхідність пошуку нових, якісніших методів захисту особистих даних в інформаційних системах. Умовна безпечність та необізнаність користувачів в сфері інформаційної безпеки, збільшує ризик несанкціонованого доступу до розміщеної на захищеному ресурсі інформації. Науково та практично доведено, що користувач є найбільш уразливим елементом системи.

За сучасного розвитку інформаційних технологій існує велика кількість можливих атак зі сторони зловмисників, та найлегшою та найдієвішою лишається загроза саме за участі користувачів системи – використанням методів соціальної інженерії. Таким чином, дослідження шляхів посилення автентифікації в розроблюваних застосунках є пріоритетним завданням сьогодення.

У процесі виконання магістерської роботи, отримано наступні результати.

Проведено аналіз сучасних методів і засобів автентифікації, наявних державних та міжнародних стандартів автентифікації та авторизації, який вказав на необхідність використання у сучасних додатках двофакторну автентифікацію, яка є обов'язковою та виконує функцію основного фактору, який забезпечує підвищення надійності процедури авторизації користувача в системі та посилення захисту персональних даних користувачів.

Здійснено огляд та порівняльний аналіз існуючих найпопулярніших застосунків двофакторної автентифікації, які побудовані згідно розглянутих міжнародних стандартів, який вказав на відсутність універсальної моделі та

алгоритму їх інтеграції у вже існуючі інформаційні системи та актуальність дослідження. Також було досліджено шляхи отримання верифікації наданих користувачем даних. Використовуючи генератор одноразових паролів, на відміну від усіх інших наявних факторів, виключає необхідності у приєднанні пристрою на якому встановлено застосунок двофакторної автентифікації до глобальної мережі інтернет.

Проведено детальний огляд протоколу авторизації OAuth 2.0 з точки зору зручності у використанні та підсилення за допомогою першого фактору автентифікації. Обґрунтовано доцільність його використання в двофакторній автентифікації, замість перевірки фактору знання шляхом запиту паролю користувача.

На основі здійснених досліджень, виконано відбір оптимальних факторів та розроблено алгоритм автентифікації, що включає в себе використання протоколу авторизації OAuth 2.0, одноразовий пароль згенерований у розробленому веб-застосунку та у застосунку на смартфоні. У якості стороннього сервісу було обрано Google. Також розроблено рекомендації щодо інтеграції засобів запропонованого алгоритму двофакторної автентифікації в уже існуючі інформаційні системи, що забезпечить вищий рівень захищеності у порівнянні із існуючими підходами авторизації користувачів.

Побудовано блок-схему роботи та детально описано алгоритм роботи, розробленого веб-застосунку у який імплементовано обрану схему автентифікації. Виконано апробацію розробленого алгоритму, на прикладі веб-застосунку, що використовує результуючу схему автентифікації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Authentication using the Google APIs Client [Електронний ресурс] – Режим доступу до ресурсу: https://developers.google.com/api-client-library/javascript/start/start-js.
2. Dominic, Ehiwe & Kayode, Akinola & Ominike, Akpovi. (2018). Social Network Application User Authentication: 2FA with Encrypted Image. American Journal of Computing and Engineering Vol.3, Issue 1 No.1, pp 1 – 10
3. Features [Електронний ресурс] // authy. – 2019. – Режим доступу до ресурсу: https://authy.com/features/.
4. FreeOTP [Електронний ресурс] – Режим доступу до ресурсу: https://freeotp.github.io/.
5. Getting Started [Електронний ресурс] – Режим доступу до ресурсу: https://developers.google.com/api-client-library/javascript/start/start-js.
6. Getting Started [Електронний ресурс] – Режим доступу до ресурсу: https://developers.google.com/api-client-library/javascript/start/start-js.
7. HOTP: An HMAC-Based One-Time Password Algorithm [Електронний ресурс] // Network Working Group. – 2005. – Режим доступу до ресурсу: https://tools.ietf.org/html/rfc4226.
8. OATH Certification [Електронний ресурс] // OATH Authentication. – 2019. – Режим доступу до ресурсу: https://openauthentication.org/oath-certification/.
9. OCRA: OATH Challenge-Response Algorithm [Електронний ресурс] // Internet Engineering Task Force. – 2011. – Режим доступу до ресурсу: https://tools.ietf.org/html/rfc6287.
10. Open source version of Google Authenticator [Електронний ресурс] – Режим доступу до ресурсу: https://github.com/google/google-authenticator.
11. Segoro, Mauli & Putro, Prasetyo. (2020). Implementation of Two Factor Authentication (2FA) and Hybrid Encryption to Reduce the Impact of Account Theft

on Android-Based Instant Messaging (IM) Applications. 115-120. DOI:10.1109/IWBIS50925.2020.9255501.

12. Smotr, O., Burak, N., Borzov,Yu., Ljaskovska, S.:Implementation of Information Technologies in the organization of Forest Fire Suppression Process. In: Proceedings of the 2018 IEEE Second International Conference on Data Stream Mining & Processing (DSMP), pp. 157-161. Lviv, Ukraine, August 21-25, 2018

13. Specifications Overview [Електронний ресурс] // FIDO Alliance. – 2018. – Режим доступу до ресурсу: https://fidoalliance.org/specifications/.

14. The State of Strong Authentication [Електронний ресурс] // Javelin Strategy & Research. – 2019. – Режим доступу до ресурсу: https://1nmqmp2u9dgf3jo9centu6rq-wpengine.netdna-ssl.com/wp-content/uploads/2019/01/The-State-of-Strong-Authentication-2019-Report.pdf.

15. TOTP: Time-Based One-Time Password Algorithm [Електронний ресурс] // Internet Engineering Task Force. – 2008. – Режим доступу до ресурсу: https://tools.ietf.org/html/rfc6238.

16. TouchID, PIN, Password, Encryption [Електронний ресурс] // Authy. – 2019. – Режим доступу до ресурсу: https://authy.com/features/secure/.

17. Watts, Steve. (2015). NFC and 2FA: the death of the password?. Network Security. 2015. 19-20. DOI: 10.1016/S1353-4858(15)30061-1.

18. What is the Microsoft Authenticator app? [Електронний ресурс] – Режим доступу до ресурсу: https://docs.microsoft.com/en-us/azure/active-directory/user-help/user-help-auth-app-overview.

19. Y. Martyn, O. Smotr, N. Burak, O. Prydatko and I. Malets, "Informational Graphic Technologies for Fire Safety Level Determination in Special Purpose Buildings", Proceedings of the 2020 IEEE Third International Conference on Data Stream Mining & Processing (DSMP), Lviv, Ukraine, 2020, pp. 398-403. doi: 10.1109/DSMP47368.2020.9204180.

20. Антонов А.О. Особливості впровадження систем електронного документообігу в підрозділах ДСНС України / А.О. Антонов, Н.Є. Бурак //

Проблеми та перспективи забезпечення цивільного захисту: матеріали міжнар. наук.-практ. конф. молодих учених. – Харків: НУЦЗ України, 2018. – С. 12.

21. Березніков А. Cloud services [Електронний ресурс] / Андрій Березніков // denovo. – 2018. – Режим доступу до ресурсу: https://www.de-novo.biz/blog/vidi-hmarnih-servisiv-yakij-obrati-ta-oglyad-hmarnih-provajd-8.

22. Бурак Н.Є. Модель інформаційної архітектури мобільного додатку фіксації порушень правил дорожнього руху // Використання сучасних інформаційних технологій в діяльності національної поліції України: Мат. Всеукр. наук.-практ. сем. – Дніпро: ДДУВС, 2019. – С. 17-19.

23. Впровадження автоматизованих інформаційно-аналітичних систем в роботу служб доставки товарів / О.О. Смотр, Н.Є. Бурак, Р.Р. Головатий, І.О. Антоненко // Матеріали IX міжнародної школи-семінару «Теорія прийняття рішень». – Ужгород, 2019. – С. 194–195.

24. Жовтянський М. С. Моделювання проектного середовища впровадження «хмарних сервісів» у вищі навчальні заклади системи цивільного захисту / М. С. Жовтянський, Н. Є. Бурак // Управління проектами, програмами, портфелями : Тези доповідей І Міжнар. наук.-практ. конф.: [у 2т.]. – Одеса, 2016. – Том 1. – С. 54–56.

25. Иванов Вадим Вадимович, Лубова Елена Сергеевна, and Черкасов Денис Юрьевич. "Аутентификация и авторизация" Проблемы современной науки и образования, no. 2 (84), 2017, pp. 31-33.

26. Комп'ютерні мережі: [навчальний посібник] / А. Г. Микитишин, М. М. Митник, П. Д. Стухляк, В. В. Пасічник. – Львів: «Магнолія 2006», 2013. – 256 с.

27. Конахович Г. Ф. Захист інформації в мережах передачі даних: підручник /Г. Ф. Конахович, О. Т. Корченко, О. К. Юдін. - К: Видавництво ТОВ НЕП “ШТЕРСЕРВІС”, 2009. - 714 с.

28. Кошева Н.А., Мазниченко Н.І. Ідентифікація користувачів інформаційно-комп’ютерних систем: аналіз і прогнозування підходів // Системи обробки інформації. Випуск 6 (113). – Харків: Харківський університет Повітряних Сил імені Івана Кожедуба, 2013. – 320 с. С 215-223.

29. Кульчицький О.С. Аналіз існуючих підходів при ідентифікації і аутентифікації користувачів в телекомунікаційних системах / Грицюк В.В., Зотова І.Г., Кульчицький О.С. // Нац. ун-т оборони ім. Івана Черняховського, 2016. [Електронний ресурс]. – Режим доступу: http://znp-cvsd.nuou.org.ua/article/download/126048/120738.

30. Лосев Ю. І. Комп'ютерні мережі: навчальний посібник / Ю. І. Лосев, К. М. Руккас, С. І. Шматков / За редакцією Ю. І. Лосева. – Х. : ХНУ імені В. Н. Каразіна, 2013. – 248 с.

31. Ляшенко, Г.Є & Астраханцев, А.А. (2017). Дослідження ефективності методів біометричної автентифікації. Системи обробки інформації. 2(148). 111-114. https://doi.org/10.30748/soi.2017.148.20

32. Мушинський А.О. Інформаційна безпека пристроїв IoT // Проблеми та перспективи розвитку системи безпеки життєдіяльності: Зб. наук. праць XV Міжнар. наук.-практ. конф. молодих вчених, курсантів та студентів. – Львів: ЛДУ БЖД, 2020. – С. 214-216.

33. Придатко О. В., Бурак Н. Є., Дзень В. Є., Кунинець М. С. Адаптивна інформаційно-довідкова система "UniBell" як складова частина проєкту "Smart-університет". Науковий вісник НЛТУ України. 2020, т. 30, № 5. С. 105–113

34. Самара Н.М. Аналіз принципів реалізації методів двофакторної автентифікації в сучасних програмних додатках / Н.М. Самара, Н.Є. Бурак // Захист інформації в інформаційно-комунікаційних системах : збірних тез доповідей IV Всеукраїнської науково-практичної конференції молодих вчених, курсантів та студентів 27 листопада 2020 року. – Львів, ЛДУ БЖД, 2020. – С.54-56.

35. Термін «Автентифікація» [Електронний ресурс] // КАБІНЕТ МІНІСТРІВ УКРАЇНИ. – 1997. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/40-97-%D0%BF/ed20060315/find?text=%C0%E2%F2%E5%ED%F2%E8%F4%B3%EA%E0%F6%B3%FF.

36. Хом'як М.І. Інтеграція технології «Інтернет речей» в процес підготовки сучасного рятувальника/ М.І. Хом'як, Н.Є. Бурак // Проблеми та перспективи розвитку системи безпеки життєдіяльності: Зб. наук. праць XII Міжнар. наук.-практ. конф. молодих вчених, курсантів та студентів. – Львів: ЛДУ БЖД, 2017. – Ч.–2., С. 80-81.

37. Чмир П.О. Аналіз сучасних хмарних серверів зберігання даних / П.О. Чмир, Н.Є. Бурак // Проблеми та перспективи розвитку системи безпеки життєдіяльності: Зб. наук. праць XIII Міжнар. наук.-практ. конф. молодих вчених, курсантів та студентів. – Львів: ЛДУ БЖД, 2018. – С. 257-258.

38. Чмир П.О. Особливості використання хмарних серверів зберігання інформації / П.О. Чмир, Н.Є. Бурак // Захист інформації в інформаційно-комунікаційних системах: збірник тез доповідей II Міжвузівської науково - практичної конференції студентів і курсантів. – Львів: ЛДУ БЖД, 2017. – С. 61-62.

39. Чунарьова А. В. Аналіз існуючих шаблонів систем автентифікації в інформаційно-комунікаційних системах та мережах / А. В. Чунарьова, А. В. Чунарьов // Безпека інформації: наук.-практ. журнал. – 2012. – № 2 (18). – С. 65–70.