НАЦІОНАЛЬНИЙ АЕРОКОСМІЧНИЙ УНІВЕРСИТЕТ
ІМ. М.Є. ЖУКОВСЬКОГО
„ХАРКІВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ"
Кафедра комп'ютерних систем, мереж і кібербезпеки

СТУДЕНТСЬКА КОНФЕРЕНЦІЯ ІНФОРМАЦІЙНА, ФУНЦІЙНА І КІБЕРБЕЗПЕКА

СКІФіК

Матеріали першої науково-технічної конференції

30 листопада 2021 року

ХАРКІВ - 2021

НАЦІОНАЛЬНИЙ АЕРОКОСМІЧНИЙ УНІВЕРСИТЕТ ІМ. М.Є. ЖУКОВСЬКОГО "ХАРКІВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ"

Кафедра комп'ютерних систем, мереж і кібербезпеки

СТУДЕНТСЬКА КОНФЕРЕНЦІЯ ІНФОРМАЦІЙНА, ФУНКЦІЙНА і КІБЕРБЕЗПЕКА

СКІФіК

Матеріали першої науково-технічної конференції

30 листопада 2021 року

Харків 2021

УДК 004.056

У збірнику подано тези доповідей першої науково-технічної студентської конференції «Студентська Конференція Інформаційна, Функційна і Кібербезпека». Розглянуті питання за такими напрямами: інформаційна безпека; функційна безпека; кібербезпека; методи атак та захисту за допомогою штучного інтелекту, смарт-системи, інтернет речей. Конференція поділена на дві секції: інформаційна безпека; функційна безпека.

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ КОНФЕРЕНЦІЇ

ISBN 978-966-1681-54-4

ПЛАН КОНФЕРЕНЦІЇ

<table>
<tr><td colspan="3">30 листопада 2021 року, Час: 15:00 – 19:00, онлайн</td></tr>
<tr><td>15:00
–
15:15</td><td colspan="2">Вітальне слово</td></tr>
<tr><td>15:15
–
15:30</td><td colspan="2">Виступ співробітників Управління кіберполіції в Харківській області, Сень Руслана та Северіна Максима. Тема: «Протидія кіберзлочинам підрозділами Департаменту кіберполіції України у сучасних реаліях»</td></tr>
<tr><td>15:30
–
15:45</td><td colspan="2">Виступ магістранта кафедри 503, НАУ "ХАІ", Юдіна Олеся Вікторович
Тема: Досвід навчання на міжнародних курсах з кибербезпеки</td></tr>
<tr><td>15:45
–
16:00</td><td colspan="2">Виступ студента кафедри 503, НАУ "ХАІ", Шипунова Микити Юрійовича
Тема: Студентський хакатон з кібербезпеки як можливість отримати досвід з розроблення та впровадження засобів захисту інформації</td></tr>
<tr><td rowspan="3">16:00
–
18:30</td><td>Секція 1</td><td>Секція 2</td></tr>
<tr><td>Інформаційна безпека</td><td>Функційна безпека</td></tr>
<tr><td>https://meet.google.com/uar-xuad-xvx</td><td>https://meet.google.com/bro-zava-sgx</td></tr>
<tr><td>18:30
–
18:45</td><td colspan="2">Перерва</td></tr>
<tr><td>18:45
–
19:00</td><td colspan="2">Підсумкове пленарне засідання</td></tr>
</table>

ПРОГРАМА КОНФЕРЕНЦІЇ

30 листопада 2021 року, Онлайн формат

Відкриття конференції, привітання учасників організаторами конференції та запрошеними гостями

Пленарні доклади:

Співробітники Управління кіберполіції в Харківській області, **Сень Руслан** та **Северін Максим**. Тема доповіді: «Протидія кіберзлочинам підрозділами Департаменту кіберполіції України у сучасних реаліях»

магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», **Юдін Олесь Вікторович**. Тема доповіді: «Досвід навчання на міжнародних курсах з кибербезпеки»

студент кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», **Шипунов Микита Юрійович**. Тема доповіді: «Студентський хакатон з кібербезпеки як можливість отримати досвід з розроблення та впровадження засобів захисту інформації»

Секція 1. Інформаційна безпека
Посилання: https://meet.google.com/uar-xuad-xvx
Модератор: Шипунов Микита Сергійович
Співмодератор: Цуранов Михайло Віталійович

Секція 2. Функційна безпека
Посилання: https://meet.google.com/bro-zava-sgx
Модератор: Юдін Олесь Вікторович
Співмодератор: Землянко Георгій Андрійович

ТЕЗИ ДОПОВІДЕЙ

Секція 1. Інформаційна безпека

Секція 1

РОЗРОБКА СИСТЕМИ «РОЗУМНИЙ БУДИНОК» ЗА ДОПОМОГОЮ ПЛАТФОРМИ OPENHAB

Бойков В.О.
Національний аерокосмічний університет ім. М. Е. Жуковського «ХАІ»
Науковий керівник Орехов О.О.

Актуальність. Сучасні темпи інформатизації змінюють розуміння самого змісті поняття "інформація". Сьогодні, в еру інформаційного суспільства, на арені цифрових послуг активними темпами рухається до першої позиції в лідерстві систем управління пристроями у будинках, офісах, закладах вищої освіти тощо. Аналіз ІТ ринку Україні свідчить, що технології "Інтернету речей" та системи на кшталт "Розумна кімната", "Розумний будинок", "Розумне місто" і т.д. тільки набирають популярності. Закордонна статистика, де інтелектуальний будинок - вже давно розглядається як повсякденна реальність, свідчить про високий рівень вигоди здійснення інвестування аналогічних проектів, окупність яких є досить швидкою.

Метою даної роботи є дослідження та реалізація системи розумного будинку за допомогою платформи openHab

Основні положення. Open Home Automation Bus (openHAB) — це програмне рішення, розроблене на Java, яке з'єднує компоненти для автоматизації будівель від широкого кола виробників в єдиній платформі, незалежно від виробника та протоколу. openHAB має багато співрозробників. На цей час розроблено друге покоління платформи, заснованої на спеціалізованому фреймворку Eclipse SmartHome.

На даний момент за допомогою платформи лише об’єднують різноманітні датчики та системи. Але потенціал забагато вище, та дозволяє зробити свою систему під свої потреби, тобто зробити та запрограмувати свої датчики та прилади.

Висновки. “Розумний будинок” забезпечує високий рівень безпеки: датчики, встановлені по периметру і в будинку, а також відео камери забезпечують моніторинг стану будинку. Система «Розумний будинок» надає можливість управління в режимі реального часу за допомогою

будь-якого мобільного пристрою або ПК, розташованого в локальній мережі та має доступ в Інтернет. “Розумний будинок” також забезпечує економію за рахунок оптимізації використання енергоресурсів. Орієнтована на користувача інфраструктура дозволяє позбавити людину від зайвих дій. Управління з телефону є візитною карткою систем розумного будинку.

Список літератури

1. An Overview of Home Automation Systems, IEEE Xplore. URL – https://ieeexplore.ieee.org/document/7791223 (дата звернення: 12.10.2021);
2. Are (IoT) Smart Homes of the Future As Smart As They Say? Panda Security. URL – https://www.pandasecurity.com/mediacenter/technology/iot-smart-homes-futuresmart-say. (дата звернення: 15.10.2021);
3. D. Evans, “The Internet of things: How the next evolution of the Internet is changing everything,” CISCO, San Jose, CA, USA, White Paper, 2011
4. Основні проблеми розумних будинків і як їх можна вирішити? Klaster. URL: https://klaster.ua/ua/stati-i-obzory/osnovnye-problemy-umnyhdomov-i-kak-ih-mozhno-reshit/ (дата звернення: 20.10.2021).

Відомості про авторів

Бойков Владислав Олександрович, магістрант кафедри комп’ютерних систем, мереж і кібербезпеки, м.т. 095-365-62-30, v.boikov@student.csn.khai.edu
Орехов Олександр Олександрович, ст. викладач кафедри комп’ютерних систем, мереж і кібербезпеки.

Секція 1

ДОСЛІДЖЕННЯ ЗАСОБІВ ЗАХИСТУ В МАГАЗИНАХ ЦИФРОВОЇ ДИСТРИБУЦІЇ

Бєлік Д. С.
Національний аерокосмічний університет ім. М. Е. Жуковського «ХАІ», Харків, Україна
Науковий керівник Цуранов М. В

Актуальність. З поширенням Covid-19 більшість звичайних магазинів (Allo,Сільпо,Comfy, Ашан) перейшли у онлайн режим роботи, а такі як Apple Store, Google Play Market (магазини для мобільних додатків), Steam, Epic Games Store, Origin (магазини, які продають комп'ютерні ігри), вже давно працюють лише в онлайні, що дозволило клієнтам не йти до магазина, а обирати потрібну їм річ не виходячи з дому [1]. У зв'язку з тим, що компанія Apple, задала тенденцію що гарні мобільні ігри можуть коштувати мінімальну ціну в 1 долар, велика частина населення почала покупати ігри в онлайн магазині Apple Store, що і вплинуло і на інші компанії, які почали експансію в мережу інтернет, заробіток Apple Store за 2020 рік склав 643 млрд долларів.

Метою даної роботи є аналіз засобів захисту магазинів цифрової дистрибуції.

Основні положення. Аналізуючи такі магазини як, Apple Store та Google Play Market, можна зробити висновок що Apple Store, звичайно є на сьогодні першим за показниками магазинів цифрової дистрибуції для мобільних гаджетів. Однією із причин цього є шалена популярність Iphone і тому у компаній розробників немає іншого вибору, як погодитися на усі правила Apple. Недоліком звичайно є відсутність кросплатоформеності, що цей магазин є дійсним тільки для гаджетів з операційною системою IOS, це приваблює тільки певне коло людей. Згідно з даних Steam, щоденно магазин відвідує близько 16 000 000 користувачів, у той час як у Epic Games Store приблизно 30 000 000 [2].

Зазвичай такі магазини мають недоліки у системі захисту [3]. Наприклад, корпорація Valve (компанія, що створила сервіс Steam), опублікувала звіт, згідно якого майже 77 тисяч користувачів Steam, щомісяця втрачають гроші, ігрові предмети та навіть облікові записи[4].

Слід зазначити, що захист у магазині Steam є більш безпечнішим, тому що там використовуються власно створене ПЗ – Steam Guard, яке

працює наступним чином: при авторизації до додатку, користувач має увімкнути функцію захисту, також при завершенні авторизації видається код на той випадок якщо телефон буде загублений, щоб можна було повернути доступ до облікового запису [5].

Також слід зазначити, що на сьогодні одним із найбезпечніших шляхів захисту для переведення коштів є оплата за допомогою QR-code. Тому що, у разі використання оплати за допомогою QR-code, магазини не зберігатимуть дані кредитової карточки та у разі злому облікового запису, доступ до них не буде отримано.

Висновки. Кожен із проаналізованих магазинів має свої функції захисту, однак вони не є повноцінним захистом, а також більшість із функцій захисту є незручними для користувачів, тому вони намагаються не використовувати їх взагалі, що в свою чергу ставить під загрозу їхні власні облікові записи.

Список літератури

1. Що таке магазин цифрової дистрибуції, *Wikipedia*. URL: https://uk.wikipedia.org/wiki/Інтернет-магазин (дата звернення: 03.10.2021);
2. Щоденний онлайн користувачів Steam та Epic Games Store, *Wikipedia*. URL:https://en.wikipedia.org/wiki/Epic_Games_Store#:~:text=Overall%2C%20Epic%20stated%20that%20overall,for%20third%2Dparty%20titles. (дата звернення: 15.10.2021);
3. Бєлік, Д.С. Цуранов М.В. Методи боротьби з кібершахраями в магазинах цифрової дистрибуції. // Протидія кіберзагрозам та торгівлі людьми : зб. матеріалів Міжнар. наук.-практ. конф. (26 листоп. 2019 р., м. Харків). - С. 221-223;
4. Опис методів захисту EGS. *Epic Game Store*. URL: https://www.epicgames.com/store/ru/news/epic-games-account-security?lang=ru (дата звернення: 30.10.2021);
5. Засоби захисту свого облікового запису та яким чином працює захист у Steam, *Steam*. URL: https://steamcommunity.com/sharedfiles/filedetails/?id=252672665 (дата звернення: 27.10.2021).

Відомості про авторів

Бєлік Данііл Сергійович, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, м.т. 099-645-84-20, d.belik@student.csn.khai.edu
Цуранов Михайло Віталійович, ст. викладач кафедри комп'ютерних систем, мереж і кібербезпеки. m.tsuranov@csn.khai.edu

Секція 1

ДОСЛІДЖЕННЯ АСПЕКТІВ БЕЗПЕКИ В AZURE COGNITIVE SERVICES

Боровик В.Ю.
Національний аерокосмічний університет ім. М. Е. Жуковського «ХАІ»
Науковий керівник Орєхов О.О.

Актуальність. Останнім часом, автоматизації піддається все більше аспектів життя. Складальні лінії заводів та фабрик в наш час повністю автоматизовані, лише невелика кількість людей підтримує їхню безперебійну роботу. Використання таких ресурсів економить час, трудові ресурси. Крім того, підвищується якість продукції. В наші дні, автоматизація та штучний інтелект дістались навіть таких аспектів як аналіз тексту, його переклад на різні мови та визначення емоційного забарвлення написанного абзацу, речення чи розділу. З іншої сторони, безпеку слід вважати першочерговим пріоритетом при розробці будь-яких програм, а з появою програм з підтримкою штучного інтелекту безпека стає ще важливішою. Саме Azure Cognitive Services вирішують як проблеми з наданням доступу до штучного інтелекту, так і з їх безпекою. Azure Cognitive Services включають різноманітні служби штучного інтелекту, які дозволяють створювати когнітивні рішення, які можуть бачити, чути, говорити, розуміти і навіть приймати рішення.

Метою даної роботи є дослідження безпеки служб Azure Cognitive Services

Основні положення. Служби Azure Cognitive Services підтримують такі аспекти безпеки, як використання безпеки транспортного рівня, аутентифікація, безпечне налаштування конфіденційних даних і Customer Lockbox для доступу до даних клієнтів. Безпека транспортного рівня. Усі кінцеві точки Cognitive Services, доступні через HTTP, застосовують TLS 1.2. З примусовим протоколом безпеки споживачі, які намагаються викликати кінцеву точку Cognitive Services, повинні дотримуватися цих вказівок:

1. Клієнтська операційна система (ОС) повинна підтримувати TLS 1.2;
2. Мова (і платформа), які використовуються для здійснення виклику HTTP, повинні вказати TLS 1.2 як частину запиту.

Аутентифікація. Деякі з пропозицій Cognitive Services включають контроль доступу на основі ролей (Azure RBAC). Azure RBAC можна використовувати, щоб спростити деякі церемонії, пов'язані з ручним керуванням принципалами. Безпечне налаштування конфіденційних даних. Для виконання цього аспекту Azure має підтримку змінних середовища, які виступають більш безпечною альтернативою використанню жорстко закодованих значень для конфіденційних даних. Customer Lockbox для Azure надає клієнтам інтерфейс для перегляду, схвалення або відхилення запитів на доступ до даних клієнтів. Він використовується у випадках, коли інженер Microsoft потребує доступу до даних клієнта під час запиту на підтримку.

Висновки. Azure Cognitive Services підримують багатогранні та зірзнорівневі аспекти безпеки, які, в большості, надаються разом зі службами. Отже, при використанні готового рішення штучного інтелекту від компанії Microsoft, не слід нехтувати такими можливостями, як використання безпеки транспортного рівня, аутентифікація, безпечне налаштування конфіденційних даних і Customer Lockbox для доступу до даних клієнтів.

Список літератури

1. Azure Cognitive Services: Exploring Cognitive Vision. *Towards Data Science*. URL – https://towardsdatascience.com/azure-cognitive-service-computer-vision-33ba62ce9d7e (дата звертання: 20.11.2021);
2. TLS Basics. *Internet Society*. URL – https://www.internetsociety.org/deploy360/tls/basics/ (дата звертання: 20.11.2021);
3. Authenticate requests to Azure Cognitive Services. *Microsoft*. URL – https://docs.microsoft.com/en-us/azure/cognitive-services/authentication (дата звертання: 20.11.2021);
4. Customer Lockbox for Microsoft Azure. *Microsoft*. URL – https://docs.microsoft.com/en-us/azure/security/fundamentals/customer-lockbox-overview (дата звертання: 20.11.2021);
5. Braband J., Schäbe Kh. On safety assessment of artificial intelligence. Dependability. 2020;20(4):25-34.

Відомості про авторів

Боровик Вадим Юрійович, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, м.т. 099-100-51-01, v.borovyk@student.csn.khai.edu
Орєхов Олександр Олександрович, доцент кафедри комп'ютерних систем, мереж і кібербезпеки, к.т.н., професор, a.orehov@csn.khai.edu

Секція 1

ВИБІР ТЕХНОЛОГІЙ ДЛЯ РОЗРОБКИ ЗАХИЩЕНОГО ТЕЛЕМЕДИЧНОГО ВЕБ-ДОДАТКУ

Бохан К.А.
Національний аерокосмічний університет ім. М. Е. Жуковського «ХАІ»
Науковий керівник Землянко Г. А.

Актуальність. З розвитком сучасних технологій все більше дій та процесів переносяться у віртуальне середовище. Тому, дуже важливо ці процеси реалізувати у захищеному вигляді. До таких процесів відносять ті, що можуть нанести шкоду користувачу, або системі у цілому. На веб-додаток, що пов'язаний з медициною є два види негативного впливу. Перший, це проблеми у самому додатку. До них відносять неякісний код, помилки у розрахунках, неправильне виведення інформації. До другої виду, відносять вплив ззовні. Наприклад, кібератаку або функціональну атаку. Так, як такі додатки мають великий роль у житті людей – необхідно зробити їх максимально захищеними для різних видів впливу. Найактуальніше, це робити для пандемій, та епідемій. Коли, попит на такі додатки – колосальний. А де великий попит – там великі навантаження, та лиходії. Зараз, постійно можна почути у ЗМІ, що десь через перенавантаження різні медичні установи працюють з перебоями. А від цього залежить життя людей.

Метою даної роботи є дослідження технологій створення захищених телемедичних веб-додатків.

Основні положення. Телемедицина - напрямок медицини, а саме комплекс дій, технологій та заходів, що застосовуються при наданні медичної допомоги, з використанням засобів дистанційного зв’язку у вигляді обміну електронними повідомленнями (у випадках, коли відстань є критичним чинником) [1]. Весь цей процес проходить у Інтернет-просторі. А через те, що медичні данні – це конфіденційна інформація. І увесь процес передачі проходить у відкритій мережі – необхідно його захистити від втручання ззовні. Адже, якщо це усе у відкритому доступі – не дуже складно пошкодити цей процес. З недавніх пір, в Україні провели реформу, через що, усі данні пов’язані з медициною усіх українців – знаходяться в електронному вигляді. Через що, ця сфера є дуже вразлива до атак.

Зв'язок пацієнта та лікаря можна реалізувати з допомогою ресурса Helsi. Це медична інформаційна система автоматизує роботу закладу охорони

здоров‘я, лікаря, лабораторії, стаціонару, ведення електронних медичних карток. Система має зручний та зрозумілий інтерфейс, допомагає формувати звіти, має вбудований конструктор бланків і форм медичних документів та функціонал для роботи за програмою медичних гарантій з Національною службою здоров'я України (НСЗУ) [2]. З допомогою цієї системи пацієнт може взаємодіяти с різними медичними ресурсами на відстані, що у сучасному світі – дуже важливо, та зручно. Як СУБД можливо використовувати продукти компаній Microsoft або Oracle як найбільш популярні та добре зарекомендовані себе в МІС [3]. Ще треба продумати варіант дистанційного зорового зв’язку пацієнта та лікаря. Адже, ці тезіси враховують сучасний період пандемії. Для цього можна реалізувати зв'язок через додатки дистанційного зв’язку. Гарний приклад – Google Meet. Це сервіс відеотелефонного зв'язку, розроблений компанією Google [4].

Висновки. У сучасному світі, та у період пандемії – захист медичних даних пацієнтів – важливий момент розроблення телемедичних веб-додатків. Для цього необхідно реалізувати безпечне середовище, для взаємодії пацієнтів з медичним середовищем. У України є такий ресурс, який зветься Helsi. Але з ним може взаємодіяти лише сімейний лікар. Через що, особиста присутність все ж необхідна. Якщо ж, дати доступ кожному пацієнту – це створить нові загрози для безпеки. Тому, треба знайти компромісний варіант, щоб зробити захищене середовище, і зменшити ризики для пацієнта, у період пандемії.

Список літератури

1. Телемедицина. *Wikipedia*. URL: https://goo.su/9aWm. (дата звернення: 12.11.2021);
2. Helsi. *Wikipedia.* URL: https://uk.wikipedia.org/wiki/Helsi (дата звернення: 12.11.2021);
3. Медичні інформаційні системи. *Комплексні медичні інформаційні системи.* URL – https://goo.su/9AWn (дата звернення: 12.11.2021);
4. Google Meet. *Wikipedia.* URL: https://uk.wikipedia.org/wiki/Google_Meet (дата звернення: 12.11.2021).

Відомості про авторів

Бохан Кирило Андрійович. Студент кафедри комп’ютерних систем, мереж і кібербезпеки, м.т. 050-600-86-03, k.a.bokhan@student.csn.khai.edu
Землянко Григорій Анатолійович, асистент кафедри комп’ютерних систем, мереж і кібербезпеки, g.zemlynko@csn.khai.edu

Секція 1

ПОРІВНЯЛЬНИЙ АНАЛІЗ ІСНУЮЧИХ АЛГОРИТМІВ ГЕШУВАННЯ

Бутенко С. І.
Національний аерокосмічний університет ім. М.Є. Жуковського «ХАІ»
Науковий керівник Пєвнєв В.Я.

Актуальність. З розвитком інформаційних технологій широкого розповсюдження набули задачі, які вирішуються з використанням геш-функцій. Серед задач можна виділити процес створення електронний цифровий підпис (ЕЦП) та системи зберігання паролів. ЕЦП використовується для контролю цілісності документа та ідентифікації особи, що його підписує [1]. При підписанні деякого набору даних вони обробляються за допомогою алгоритму гешування. У загальному випадку геш-функція - це математичний алгоритм, який перетворює дані довільного розміру в бітовий масив фіксованого розміру [2]. Це одна з вимог до геш-функції.

При організації систем зберігання паролів алгоритми гешування використовуються для того щоб не зберігати паролі у відкритому вигляді. Після обробки отримується бітова послідовність заданої довжини яка не може бути напряму конвертована у сам пароль. У разі викрадення паролів з системи даний метод захистить від миттєвої компрометації. В обох випадках швидкодія алгоритмів гешування корелюється з ефективністю використання ресурсів пристроїв на яких вони виконуються.

Для збільшення швидкості роботи алгоритмів потрібно підвищувати ефективність використання ресурсів. Висока швидкодія та пов'язана з нею висока ефективність дозволяє реалізовувати системи з їх застосуванням на пристроях з невеликими або сильно обмеженими обчислювальними можливостями.

Метою даної роботи є порівняння алгоритмів гешування за критерієм швидкодії.

Основні положення. У доповіді надано результаті порівняльного аналізу алгоритмів SHA-2(256) – зараз самий розповсюджений алгоритм гешування, Kupyna – національний стандарт гешування в України, Стрібог – міждержавний стандарт, с - останній з алгоритмів серії Message Digest (приймав участь в конкурсі на новий стандарт SHA-3) [3]. Задля досягнення повноти та коректності при проведенні

досліджень було враховувано фактори, які вплинути на отримані результати. Тестування швидкодії алгоритмів проводилось в рамках однієї системи з чітко визначеними параметрами, був мінімізоване вплив інших програмних засобів на ресурси системи, тестування алгоритмів проводилось на процесорах з різною архітектурою (x86 та ARM). Також слід брати до уваги те, що різні реалізації одного і того самого алгоритму можуть мати різний показник швидкодії. Під час проведення тестування було виявлено, що виконання сучасних алгоритмів гешування може бути розділено на декілька потоків. На результати тестування значно впливав доступний об'єм кеш-пам'яті процесора. Також було виявлено, що для виключення впливу інших програмних засобів потрібно за допомогою засобів операційної системи задати процесу, що виконує алгоритм, максимальний з доступних пріоритетів.

Висновки. При виборі алгоритмів для сучасних комп'ютерних систем слід звертати основну увагу на можливість виконання алгоритму у багато потоковому режимі, а також те, наскільки ефективно він може використовувати доступні ресурси системи.

Список літератури

1. Пєвнєв В. Я. Моделі загроз і забезпечення цілісності інформації. *Системи та технології*. 2018. №2 (56/1). С. 79–94.

2. Хеш-функция, что это такое? *Habr*. URL: https://habr.com/ru/post/534596/ (дата звернення 11.11.2021).

3. ДСТУ 7564:2014. Інформаційні технології. Криптографічний захист інформації. Функція гешування. Вид. офіц. Київ : Мінекономрозвитку України, 2015. 5 с.

Відомості про авторів

Бутенко Сергій Ігорович, студент кафедри комп'ютерних систем, мереж і кібербезпеки, м.т. 068-395-71-04, s.butenko@student.csn.khai.edu

Пєвнєв Володимир Яковлевич, доцент кафедри комп'ютерних систем, мереж і кібербезпеки, д.т.н., доцент, v.pevnev@csn.khai.edu

Секція 1

МОДЕЛІ ТА МЕТОДИ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ МЕДИЧНИХ ЗАКЛАДІВ

Герасимов Д. Р.
Національний аерокосмічний університет ім. М. Е. Жуковського «ХАІ»
Науковий керівник Орєхов О. О.

Актуальність. Найважливіша умова ефективної роботи сучасної лікарні є збільшення кількості вилікуваних пацієнтів, що обумовлює підвищення ефективності не тільки медичного діагностування, але й подальшого лікування хворих, що складається як з надання різноманітних терапевтичних процедур та методів лікування, а також перебування пацієнтів у палатах. Таким чином, розроблення методів підвищення ефективності функціонування закладів охорони здоров'я є актуальним.

Метою роботи є підвищення ефективності закладів охорони здоров'я шляхом зниження ризику прийняття некоректних рішень під час медичного діагностування та керування ресурсами. Об'єктом дослідження є процеси діагностування та лікування. Предметом дослідження є методи та моделі діагностування пацієнтів та розподілу медичних ресурсів, що забезпечують інформаційну безпеку медичних даних.

Основні положення. Для диверсифікованого діагностування та розподілу ресурсів запропоновано застосувати методи: функціонального аналізу [1], кластерного аналізу [2], теорії ймовірностей [3], теорії множин [4] та нечіткої логіки [5], що дозволило автоматизувати використання протоколів під час лікування та прийнятті контрольних і діагностичних рішень лікарем та автоматизувати медичні процеси, що є надзвичайно актуальним та цінним у час пандемії. Запропоновано багаторівневу архітектуру системи, яка дозволяє автоматизувати процеси реєстрації медичної інформації та вдосконалити процеси оптимального вибору лікування та розподілу медичних ресурсів.

Висновки. Проаналізовано сучасний стан проблем у закладах охорони здоров'я. Сформовані принципи побудови універсальної медичної інформаційної системи, що базуються на диверсності, адаптованості та сервіс-орієнтованій архітектурі, та забезпечують

універсальність діагностування, адміністрування та інформаційну безпеку. Запропоновано: математичну модель діагностування на підставі Протоколу надання медичної допомоги, що дозволило досягнути високих показників точності (0,98) при діагностуванні; математичну модель розподілу ліжок (адміністрування), що дозволило досягнути високих показників ефективності (0,90) під час лікування. Удосконалено методи: діагностування пацієнтів на основі принципів диверсифікації та ідентифікації біомедичних ознак із застосуванням математичного апарату теорії ймовірностей, що дозволило скоротити обсяг (у 4 рази) та час оброблення (у 2,5 рази) даних; адміністрування на основі принципів диверсифікації та ідентифікації біомедичних ознак із застосуванням математичного апарату теорії ймовірностей, що дозволило скоротити час перебування пацієнтів у палатах (на 20 %). Розроблено: моделі даних для ефективного діагностування, лікування та адміністрування, що забезпечило автоматизацію цих процесів у закладі охорони здоров'я.

Список літератури

1. Reed M. Methods of Modern Mathematical Physics. Functional Analysis. / M. Reed S. Barry.— Academic Press, 1980. — 400 p;
2. An Efficient Data Clustering Methodpfor Very Large Databases. Tian Zhang , Raghu Ramakrishnan, Miron Livny. // In: Proc. Int'l Conf. on Management of Data, ACM SIGMOD, pp. 103–114;
3. Теорія ймовірностей, математична статистика та імовірнісні процес и: навч. посіб. / [Ю. М. Слюсарчук, Й. Я. Хром'як, Л. Л. Джавала, В. М. Цимбал]; М-во освіти і науки України, Нац. ун-т «Львів. політехніка». — Львів: Вид-во Львів. політехніки, 2015. — 364 с;
4. Jech T. *Set Theory, Springer Monographs in Mathematics (Third Millennium ed.)/ T.* Jech, *Berlin, New York:* Springer-Verlag*, 2003. — p. 642*;
5. Zadeh, L. A. Fuzzy logic = computing with words / L. A. Zadeh. // IEEE Transactions on Fuzzy Systems. – 1996 – №4 (2): P.15 – 54.

Відомості про авторів

Герасимов Даніїл Русланович, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, м.т. 099-287-80-82, d.gerasimov@student.csn.khai.edu
Орєхов Олександр Олександрович, доцент кафедри комп'ютерних систем, мереж і кібербезпеки, к.т.н., професор, a.orehov@csn.khai.edu

Секція 1

ДОСЛІДЖЕННЯ ІСНУЮЧИХ МЕТОДІВ СТЕГОАНАЛІЗУ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

Дука І. О
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник Пєвнєв В.Я.

Актуальність. Завдання захисту цінної інформації від несанкціонованого доступу вирішувалося в усі часи історії людства. Серед методів захисту виділяється стеганографічний, через можливість зберігати та передавати інформацію у всіх перед очима, тобто стеганографія приховує сам факт передачі. За допомогою стеганографії можливо одночасно забезпечити конфіденційність і цілісність інформації [1]. Використання комп'ютерів дозволило зробити якісний стрибок у розвитку стеганографії. Її використання передбачає наявність контейнера - файлу, в якому розміщується інформація, що передається. В даний час це можуть бути текстові, графічні, аудіо- та відеофайли.

Методи стеганографії можуть бути як корисними так і небезпечними. Це залежить від того, хто користується та для чого. Коли мова йде про таємну комунікацію між хакерами, терористами, продавцями наркотичних речовин, вірусна програма для передачі конфіденційною інформації – ці приклади демонструють небезпечні дії, але важливо відмітити й корисні, наприклад цифрові водяні знаки на зображеннях та у фреймах фільму чи відео, - допомагають боротися із піратством та крадіжкою інтелектуальної власності[2]. Але частково стеганографію використовують із недобрим наміром. Одночасно з розвитком стеганографії розвивається й стегоаналіз.

Метою роботи є дослідження існуючих стеганографічних методів та методи стегоаналізу цифрових контейнерів.

Основні положення. В доповіді освітлюються особливості методів стеганографії та стегоаналізу. З аналізу наявних методів стегоаналізу випливає, що їх можна умовно поділити на дві основні групи. Перша група призначена для роботи з відомими стеганографічними алгоритмами; друга - для всіх інших алгоритмів стеганографії [3]. Методи обох груп побудовані з урахуванням припущення про недоступність початкового порожнього контейнера, який було використано для розміщення інформації в досліджуваний

стегоконтейнер.

У доповіді наведено аналіз існуючих методів стегоаналізу. Метод візуального аналізу є найпростішим способом аналізу графічних файлів, оскільки для цього досить просто поглянути на перехоплене зображення. Статистичні методи базуються на понятті «природного» контейнера. Суть методів полягає в оцінюванні ймовірності існування стеганографічного вкладення зі стегосистеми, яка є невідомою, на основі критерію оцінювання близькості досліджуваного контейнера до «природного». До переваг цієї групи методів належить необмежена сфера застосування, що є досить істотним як під час перевірки гіпотези про наявність стеганографічного вкладення з невідомої стегосистеми, так і під час розроблення схемних методів стегоаналізу. Основним недоліком методів цього класу є саме припущення про існування "природного" контейнера.

Висновок. Основним висновком по поданій роботі можна вважати те, що незважаючи на актуальність розробки систем стегоаналізу, в інтернеті мало інформації про можливі алгоритми їх застосування з теоретичної точки зору та практичної реалізації.

Список літератури

1. Пєвнєв В. Я. Моделі загроз і забезпечення цілісності інформації. *Системи та технології*. 2018. №2 (56/1). С. 79–94.

2. Цифровая стеганография как продвинутая техника уклонения от обнаружения вредоносных программ. URL: https://ichi.pro/ru/cifrovaa-steganografia-kak-prodvinutaa-tehnika-uklonenia-ot-obnaruzenia-vredonosnyh-programm-218817175139967

3. Кустов В. Н., Параскевопуло А. Ю. Простые тайны стегоанализа *Защита информации*. INSIDE. 2005. № 4. С. 72-78.

Відомості про авторів

Дука Ігор Олександрович, магістрант кафедри комп’ютерних систем, мереж і кібербезпеки, м.т. 066-420-15-30, i.o.duka@student.csn.khai.edu

Пєвнєв Володимир Яковлевич, доцент кафедри комп'ютерних систем, мереж і кібербезпеки, д.т.н., доцент, v.pevnev@csn.khai.edu

Секція 1

АНАЛІЗ БЕЗПЕКИ ДАНИХ В ОНЛАЙН-СЕРВІСІ ДЕРЖАВНИХ ПОСЛУГ «ДІЯ»

Запара М. О.
Національний аерокосмічний університет ім. М. Е. Жуковського «ХАІ» Науковий керівник Цуранов М. В.

Актуальність. З розвитком цифрових технологій ціна на мобільні пристрої суттєво зменшилася, що призвело до росту кількості користувачів. Через пандемію коронавірусу збільшився попит на різноманітні онлайн сервіси. Це призвело до прискорення цифрової трансформації, завдяки якій різноманітні структури почали створювати онлайн сервіси. На відміну від фізичних офісів, онлайн сервіси відкриті цілодобово та без вихідних. У зв'язку з цим, чимала кількість країн почали розробляти проекти у цій сфері. Найбільш успішними з них є: Польща, Китай, Естонія, ОАЄ та Великобританія — які запустили свої проекти впродовж 2019-го року [1]. Також до цього списку, у лютому 2020-го року, приєдналась Україна, у рамках проекту «Держава у смартфоні».

Метою цієї роботи є проведення аналізу безпеки даних в онлайн-сервісі державних послуг «Дія». В рамках цієї роботи буде проведено аналіз мобільного застосунку «Дія».

Основні положення. «Держава і Я» — український електронний сервіс державних послуг, розроблений Міністерством цифрової трансформації, в рамках проекту «Держава у смартфоні». Розглянемо складові даного сервісу: Портал — онлайн-сервіс державних послуг. [2] Застосунок — мобільний застосунок з електронними документами. Освіта — портал з онлайн-курсами. Бізнес — портал з допомоги малому та середньому бізнесу. Дія City — спеціальний правовий режим для IT-індустрії.

В даний час користувачу доступні наступні цифрові документи: водійські права, свідоцтво про реєстрацію транспортного засобу, поліс страховки авто, закордонний паспорт, ID-картка, Цифровий студентський, картка платника податків. Таким чином станом на 17 серпня 2021 року кількість активних користувачів онлайн-сервісу державних послуг «Дія» перевищила 6 млн осіб [3].

Для того, щоб скористатися цифровими документами користувач повинен пройти процес ідентифікації. Для цього у додатку існують наступні варіанти авторизації з використанням: BankID, технології NFC та ЕЦП. Перший варіант є основним, оскільки авторизація з NFC є

неможливою у випадку, якщо у користувача немає ID картки, а ЕЦП має лише незначна кількість користувачів.

Авторизація за допомогою BankID для користувача доволі зручна, оскільки він проходить цей процес використовуючи свої дані для авторизації у банківському клієнті.

У подібних застосунках інших держав основними засобами ідентифікації є Mobile-ID. Mobile-ID – це рішення цифрового підпису на базі SIM-карти (для якого необхідна спеціальна SIM картка) [4]. Такий ідентифікатор є надійним завдяки тому, що це ЕЦП яке зберігається на спеціальній SIM картці контрактних абонентів.

Останнє оновлення надало можливість зробити знімок екрану, який дозволяє надати інформацію зі своїх документів іншій людині. Але таким чином виникає неконтрольоване поширення персональних даних.

Висновки. Додаток «Дія» на даний момент продовжує розроблятися та оновлюватися, оскільки, має чи малу кількість недоліків відносно світових аналогів. До цих недоліків відноситься: використання менш надійного BankID замість Mobile-ID; відсутність технічної документації та закритість системи. Значно зменшити кількість недоліків можна лише за умови проведення аудиту незалежними експертами.

Список літератури

1. Ukraine’s digital revolution continues with enhanced legal status for e-passports. *Atlantic Coubcil.* URL — https://www.atlanticcouncil.org/blogs/ukrainealert/ukraines-digital-revolution-continues-with-enhanced-legal-status-for-e-passports/ (дата звернення: 23.10.2021);

2. Державні послуги онлайн. *Дія.* URL: https://plan2.diia.gov.ua/ (дата звернення: 23.10.2021);

3. Телеграм канал «FEDOROV». *Telegram.* URL: https://t.me/zedigital/766 (дата звернення: 23.10.2021);

4. «Smart-ID» — интеллектуальный способ идентификации личности. Как пользоваться Mobile-ID для регистрации учетной записи Smart-ID. *Smart-ID.* URL: https://www.smart-id.com/ru/spravka/voprosy-otvety/registratsiya/kak-polzovatsya-mobile-id-dlya-registratsii-uchetnoj-zapisi-smart-id/ (дата звернення: 30.10.2021).

Відомості про авторів

Запара Михайло Олександрович, студент кафедри комп’ютерних систем, мереж і кібербезпеки, м.т. 050-555-16-08, m.zapara@student.csn.khai.edu

Цуранов Михайло Віталійович, ст. викладач кафедри комп’ютерних систем, мереж і кібербезпеки, m.tsuranov@csn.khai.edu

Секція 1

ЗАГРОЗИ РОЗПОДІЛЕНИХ БАЗ ДАНИХ

Кирина Д. В.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник Цуранов М. В.

Актуальність. За останні кілька років концепція хмарних обчислень і віртуалізації закріпилась та стала популярною у сфері інформаційних технологій. Мільйони користувачів та різноманітних організацій по всьому світу користуються хмарними технологіями для зберігання, обробки, використання чималої кількості даних. Оскільки, хмарні технології напряму пов’язані з Інтернетом, то для роботи з даними використовуються розподілені бази даних (РБД). Однією із важливих перевагою таких БД перед іншими є те, що РБД автоматично масштабують пропускну здатність для відповідей поточного робочого навантаження і здатні багатократно розбивати дані по мірі розширення таблиць, що значно підвищує доступність даних [1]. Найбільш популярними прикладами РБД можна вважати Torrent, Amazon DynamoDB, Azure Cosmos DB.

Метою даної роботи є аналіз вразливостей розподіленої бази даних.

Основні положення. Серед багатьох визначень РБД найбільш влучним є: розподілена база даних складається з двох чи більше частин, розташованих на різних серверах. Така база даних може зберігатися на кількох комп'ютерах [2].

РБД насправді є віртуальною базою даних, компоненти якої фізично зберігаються в декількох різних реальних базах даних на декількох різних вузлах (по суті, будучи логічним об'єднанням цих реальних баз даних). Фундаментальний принцип РБД ґрунтується на тому, що користувачі розподіленої системи повинні мати можливість діяти так, ніби система не є розподіленою [3]. Всі проблеми розподілених систем відносяться до проблем реалізації, а не до проблем рівня користувача.

Розподілена система має декілька точок входу, через які здійснюється доступ до даних. Чим більше в системі таких входів, тим гостріша проблема безпеки. При обробці інформації порушення її цілісності може виникнути внаслідок технічних несправностей, алгоритмічних та програмних помилок, помилок та деструктивних дій обслуговуючого персоналу, зовнішнього втручання, дії руйнівних та шкідливих програм (вірусів, експлойтів, черв'яків, логічних бомб) [4].

Аналізуючи функціональність РБД, було виявлено найчастіші загрози. Більшість загроз пов'язані з некоректною установкою та налаштуванням СУРБД адміністратором БД. СУРБД складається з

єдиної логічної БД, розділеної на кілька фрагментів [5]. Прикладами найбільш розвинутих СУРБД є система R*, SDD-1, Distributed Ingres, BigTable.

Найпоширеніші з них: загрози перехоплення інформації у незахищених каналах зв'язку та мережах загального доступу; загрози впливу ШПЗ; загрози в системах автентифікації та авторизації; атака 51%; віддалені атаки на інфраструктуру (під інфраструктурою мережі слід розуміти сформовану систему організації відносин між об'єктами мережі та сервісні служби, що використовуються в мережі) і протоколи мережі (2PC, протокол двухфазної фіксації транзакцій, Frame Relay); атака на один із вузлів мережі (атака Eclipse).

Висновки. Оскільки, РБД не може існувати без мережі, тому атаки на мережу мають ключове значення. Також, при аналізі загроз РБД та причин їх виникнення було виявлено те, що більшість з них, пов’язані з організацією, установкою та налаштуванням СУРБД адміністратором баз даних. Тому система безпеки має одне із найважливіших значень в проектування та налаштуванні РБД.

Список літератури

1. Amazon RDS. *Amazon.* URL –https://aws.amazon.com/ru/rds/ (дата звернення: 18.10.2021);
2. Что такое база даних? *Oracle.* URL – https://www.oracle.com/ru/database/what-is-database/ (дата звернення: 22.11.2021);
3. Investigation of information security issues for graph databases suitable for big data processing while detecting money laundering and terrorism financing cases. *Безопасность информационных технологий*. URL - https://bit.mephi.ru/index.php/bit/article/view/1306 (дата звернення: 17.11.2021);
4. Певнев В. Я. Методы обеспечения целостности информации в инфокоммуникационных системах/ В.Я. Певнев // Вісник Національного технічного університету ХПІ. Серія: Техніка та електрофізика високих напруг. – 2015. - № 51. – С. 74-77;
5. Системы управления базами данных – коротко о главном. *OSP*. URL: https://www.osp.ru/dbms/1995/03/13031428#part_1 (дата звернення: 20.11.2021).

Відомості про авторів

Кирина Діана Віталіївна, студент кафедри комп’ютерних систем, мереж і кібербезпеки, м.т. 099-030-56-18, d.kyryna@student.csn.khai.edu
Цуранов Михайло Віталійович, ст. викладач кафедри комп’ютерних систем, мереж і кібербезпеки. m.tsuranov@csn.khai.edu

Секція 1

ДОСЛІДЖЕННЯ МЕТОДІВ БЕЗПЕЧНОГО ПРОГРАМУВАННЯ МОБІЛЬНИХ ДОДАТКІВ

Кійко О. Д.
Національний аерокосмічний університет ім. М.Є Жуковського
«Харківський авіаційний інститут»
Науковий керівник Морозова О. І.

Актуальність. В наш час використання мобільних пристроїв стає все популярнішим. Пов'язано це в першу чергу з тим, що сучасні смартфони стали в деяких випадках навіть потужнішими за персональний комп'ютер, а їх собівартість з кожним роком падає через розвиток технологій виробництва. Станом на 2021 рік близько 67% світового населення використовують мобільні телефони [1], при цьому з 2020 року кількість унікальних користувачів збільшилася на 1.8% (майже 93 мільйони осіб). За статистикою, більшість часу використання пристроїв припадає на соціальні мережі (44%) і додатки для розваг (22%). Під час пандемії Covid-19 особливого поширення набули програми для проведення відео-конференції та нарад [2]. Також велике поширення набули банківські додатки, оскільки і натомість запровадження карантинних заходів люди почали користуватися безготівковою оплатою товарів та послуг. У зв'язку з цим виникає питання забезпечення інформаційної та кібербезпеки, яким чином розробити додаток так, щоб ним було безпечно користуватися, щоб дані, які використовуються та обробляються програмою, не були пошкоджені або вкрадені. Як одним із рішень цієї проблеми може бути введення методів безпечного програмування [3]. Безпечне програмування — одна з форм безпечного проектування програм, мета якої забезпечити тривале функціонування певної частини коду програми під впливом непередбачуваних обставин[4].

Метою доповіді є представлення підходів до техніки безпечного програмування. Основною метою є покращення вихідного коду в таких аспектах як: підвищення зрозумілості коду та архітектури програми у цілому, кількість корисного коду, відмовостійкість програми, безпека даних, що зберігаються у програмі.

Основні положення. Методи безпечного програмування можуть бути поділені на дві групи: технічні та організаційні.

Під технічними методами мається на увазі методи написання коду таким чином, щоб його підтримка, пошук помилок та їх виправлення, а також масштабування займало мінімально можливий час. До групи технічних методів входить: перевірка вхідних даних, обробка помилок під час виконання та їх логування, написання надійного коду, написання тестів. Під організаційними методами маються на увазі методи перевірки нового і вже існуючого коду автором та членами команди для того, щоб знайти слабкі місця та можливі вразливості. У групу організаційних методів входять: тестування, код ревью, запровадження обов'язкового аналізу коду спеціальними інструментами, наприклад з допомогою SonarQube[5].

Висновок. Необхідно зауважити, що методи безпечного програмування працюватимуть повною мірою тільки в тому випадку, коли вони застосовані комплексно. Наприклад, можна перевірити всі вхідні дані, але якщо забути про обробку можливих помилок під час виконання, то поведінка програми в реальних умовах не можна передбачити.

Список літератури

1. Вся статистика интернета и соцсетей на 2021 год. *LYNX*. URL: https://www.lynx.in.ua/вся-статистика-интернета-и-соцсетей-н/ (дата звернення: 10.11.2021)

2. Videoconferencing app usage «hits 21 times pre-Covid levels». *Avinteractive*. URL – https://www.avinteractive.com/news/collaboration/usage-mobile-video-conferencing-apps-including-zoom-grew-150-first-half-2021-05-08-2021/ (дата звернення: 12.11.2021)

3. Pevnev V., Tsuranov M., Zemlianko H., Amelina O. Conceptual Model of Information Security: Integrated Computer Technologies in Mechanical Engineering - 2020. ICTM 2020. Lecture Notes in Networks and Systems, vol 188. Springer, Cham. H. 158 - 168

4. Pevnev V., Trehub Yu. Analysis and research of well-known orchestration systems for the construction of microservice infrastructure/ Advanced Information Systems. 2020. Vol. 4, No. 2, p.142 -147.

5. Sonarqube: What it is and why to use it? *Loginradius*. URL – https://www.loginradius.com/blog/async/sonarqube/

Відомості про авторів

Кійко Олег Дмитрович, магістрант кафедри комп’ютерних систем, мереж і кібербезпеки, м.т. 095-783-56-95, o.kiyko@student.csn.khai.edu

Морозова Ольга Ігорівна, професор кафедри комп’ютерних систем, мереж і кібербезпеки. д.т.н., доцент, o.morozova@khai.edu

Секція 1

ДЕЦЕНТРАЛІЗОВАНА СИСТЕМА ДЛЯ ЕЛЕКТРОННОГО ГОЛОСУВАННЯ З ВИКОРИСТАННЯМ БЛОКЧЕЙН: АНАЛІЗ РІШЕНЬ ТА ОБҐРУНТУВАННЯ ВИМОГ

Кошелик В. О.
Національний аерокосмічний університет ім. М.Є. Жуковського
«Харківський авіаційний інститут»
Науковий керівник Харченко В.С.

Актуальність. Вибори є важливою процедурою формування представницьких органів державної влади (президентські, парламентські вибори) та місцевого самоврядування (місцеві вибори) шляхом голосування. Із фальсифікацією виборів стикається багато країн. Фальсифікація виборів Президента України у 2004 році призвела до Помаранчевої революції. Одним із напрямів зменшення або навіть виключення ризиків фальсифікації та забезпечення безпеки виборів є створення доказово захищених систем для дистанційного електронного голосування (інтернет-голосування).

Мета роботи – дослідження і виявлення недоліків існуючих рішень, формулювання вимог до системи інтернет-голосування з використанням технології блокчейн (СІГБ).

Основні положення. Існуючі рішення мають схожі недоліки. Південно-корейське [1] і російське [2] рішення зберігають у блокчейн-системі дані, які можна використати від імені виборця. Турецьке [3] та польське [4] рішення покладаються на чесність органів, які видають виборцям дані для голосування. Українське рішення [5] має вади щодо способу відділити дані для автентифікації виборця від його голосу. Всі системи мають певні вразливості для «вкидання» бюлетенів, реєстрації та голосування «мертвих душ», порушення таємниці голосування та передчасного розголошення результатів.

На підставі порівняння та аналізу існуючих рішень, сформульовано вимоги до СІГБ: система має підтримувати голосування через інтернет, бути логічно та фізично децентралізованою, має перевіряти коректність даних перед реєстрацією, не допускати змінення зареєстрованих даних; забезпечувати органам влади можливість встановлення етапів виборів і не допускати реєстрацію даних, строки подання яких не дотримані; забезпечувати відкриту реєстрацію виборців, яку можна перевірити; не допускати реєстрацію одного виборця більше одного разу, голосування

незареєстрованих виборців та голосування одного зареєстрованого виборця більше одного разу; забезпечувати таємність голосування та надавати можливість виборцю перевірити коректність зарахування голосу; оприлюднити результати після закінчення термінів голосування, не допускати їх передчасного оприлюднення та втручання органів влади до процесу голосування; надати можливість зареєстрованим спостерігачам перевіряти коректність результатів.

Висновки. На сьогодні відсутні рішення СІГБ, які б відповідали всім вимогам. На підставі сформульованих вимог та надання їм певної ваги можливо запропонувати комплексний показник якості та безпеки СІГБ. З урахуванням результатів аналізу обґрунтовано архітектуру СІГБ.

Список літератури

1. Seiwoong Choi, Jihun Kang, Kwang Sik Chung. Design of Blockchain based e-Voting System for Vote Requirements // *J. Phys.: Conf. Ser. 1944 012002*. 2021;
2. Н. К. Трубочкина, С. К. Поляков. Система электронного голосования на основе технологии блокчейн с использованием смарт-контракта. // *Информационные технологии*. 2019. №2. Том 25. С. 75-85;
3. Ruhi Taş, Ömer Özgür Tanrıöver, A Manipulation Prevention Model for Blockchain-Based E-Voting Systems // *Security and Communication Networks*, vol. 2021, Article ID 6673691, 16 p.
4. Javaid, Muhammad Adeel, Electronic Voting System Security, 2014;
5. Букраба О.М., Мазепа Ф.С., Карнишов К.Р., Яковенко О.О., Кушніренко Н.І. Система електронного голосування на основі технології Блокчейн // *Обробка інформації в складних організаційних системах*. 2018. Вип. 4 (155). С. 41–46.

Відомості про авторів

Кошелик Владислав Олегович, студент кафедри комп'ютерних систем, мереж і кібербезпеки, м.т. 095-347-62-36, v.koshelik@student.csn.khai.edu

Харченко Вячеслав Сергійович, завідуючий кафедри комп'ютерних систем, мереж і кібербезпеки, Лауреат Державної премії України в галузі науки і техніки, заслужений винахідник України, д.т.н., професор, v.kharchenko@csn.khai.edu

Секція 1

ДОСЛІДЖЕННЯ ТА АНАЛІЗ IAC ПІДХОДУ ДЛЯ ПОБУДОВИ БЕЗПЕЧНОЇ ПРИВАТНОЇ ХМАРНОЇ ІНФРАСТРУКТУРИ

Лоцман Є. Р.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Цуранов М. В.

Актуальність. За результатами опитування USAID-Internews, популярність Інтернет технологій зросла на 30 відсотків за останні 5 років. Пікові показники зростання були зафіксовані під час всесвітньої пандемії вірусу Коронавірус [1]. Більшість населення планети зіткнулася з незвичними їй новими реаліями – зросла необхідність безконтактної оплати, з'явилися обмеження пересування та час перебування на вулиці, що призвело до зростання популярності онлайн сервісів.

Метою даної роботи є дослідження IAC подходу при побудові приватної хмарної інфраструктури.

В рамках проведеної роботи було проаналізовано підхід побудови інфраструктури на віртуальних серверах. До роботи було виділено визначення віртуалізації. Віртуалізація – це технологія, яка створює віртуальне представлення декількох комп'ютерів або серверів на апаратній базі одного фізичного комп'ютера, або кластера серверів. Ця апаратна база називається хостом; котрий має центральний процесор, оперативну пам'ять, накопичувальний простір та інше. Місткість фізичних ресурсів, диверсифікована гіпервізором, який забезпечує незалежність віртуальних машин одна від одної [2].

Основні положення. Документація сервісів та інформація про надійність та безпеку даних в рамках публічної хмари, яку публікують хмарні провайдери більше нагадують рекламні постери. Опублікована інформація може бути недостовірною та не дає змогу оцінити весь спектор вразливостей, загроз та надійність публічної хмари. Закрита політика хмарних провайдерів, стосовно питаннь інфраструктури та безпеки даних, демонструє обмеженність можливостей аналізу безпеки публічних хмар в порівнянні з приватними хмарами. За угодою з хмарним провайдером, клієнт має змогу запросити своїх експертів з інформаційної безпеки і провести часткове тестування системи для оцінки її на предмет взразливостей та можливих загроз безпеки.

Часткове тестування не дозволяє виявити всі можливі загрози і вразливості. Провайдер не може надати повний доступ до фізичних ресурсів, так як це приведе до компрометації даних інших користувачів хмари. Так як концепт публічної хмари передбачає використання фізичних ресурсів хмари одразу двома та більше клієнтами.

Безперервне зростання попиту на хмарні послуги потребує великих людських ресурсів для адміністрування та супроводу інфраструктури. Для спрощення адміністрування та масштабування було розроблено новий підхід до побудови інфраструктури – інфраструктура як код [3].

Висновки. В ході аналізу було виявлено, що IaC-обробка забезпечує більший контроль та прозорість, ніж адміністрування систем вручну. Файли конфігурації інфраструктури передаються до центрального репозиторію з контролем версій, де будь-який учасник команди може переглядати та редагувати дані інфраструктури. Це дозволяє проводити ефективний аудит. Наприклад, якщо команда проходить аудит відповідності стандартам безпеки PCI, та потрібно буде знати, чи використовується у відповідній частині інфраструктури шифрування SSL. За допомогою IaC-обробки можна швидко побачити налаштування SSL і виконати код, щоб переконатися, що інфраструктура, що діє, відповідає файлам конфігурації, що визначають використання SSL. Історія коммітів у системі контролю версій також є журналом з відомостями про час додавання або видалення налаштувань.

Список літератури

1. Лоцман Є. Р. Методи деанонимізації як засіб виявлення правопорушників. Протидія кіберзагрозам та торгівлі людьми: тези доп., м. Харків, 26 листоп. 2019 р. ХНУВС, 2019. С. 259 – 261;

2. Лоцман Є. Р., Цуранов М.В., Аналіз методів побудови приватної хмари. Проблеми інформатизації: тези доп., м. Харків, 26-27 листопада. 2020 р. ХПІ, 2020. С. 74;

3. Лоцман Є. Р., Цуранов М.В., Аналіз механізмів забезпечення кібербезпеки методології DevOps. Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління: тези доп., м. Харків, 9-10 квітня. 2020 р. ХПІ, 2020. С. 59.

Відомості про авторів

Лоцман Євгеній Романович, магістрант кафедри комп’ютерних систем, мереж і кібербезпеки, м.т. 097-546-49-43, e.lotsman@student.csn.khai.edu
Цуранов Михайло Віталійович, ст. викладач кафедри комп’ютерних систем, мереж і кібербезпеки, m.tsuranov@csn.khai.edu

Секція 1

ЗАСТОСУВАННЯ АЛГОРИТМІВ ІНТЕЛЕКТУАЛЬНОГО АНАЛІЗУ ДАНИХ У СИСТЕМАХ ВИЯВЛЕННЯ ВТОРГНЕНЬ

Луханін Б. Ю.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник Землянко Г.А.

Актуальність. В останні роки йде зростання потреби на мережеві системи. Програмне забезпечення стає більш складним, що призвело до ускладнення виявлення помилок та вразливих місць. Зловмисники стають все більш витонченими. Через це системи потребують більш ефективного захисту. Механізми виявлення вторгнень повинні мати більш якісні алгоритми аналізу даних для того, щоб покращити свою результативність. Тож чи є алгоритм, що здатний відповідати всім потребам.

Метою даної роботи є: розглянути алгоритми інтелектуального аналізу даних та зробити висновки щодо проблематики їх використання.

Основні положення.

Зробимо порівняльний аналіз переваг та недоліків 4 алгоритмів інтелектуального аналізу даних у системах виявлення вторгнення. Це метод опорних векторів, метод k-найближчих сусідів, дерево прийняття рішень та нейронна мережа.

1. Метод опорних векторів (SupportVectorMachine, SVM) — набір подібних алгоритмів навчання з учителем, застосовуваних у задачах класифікації та регресійного аналізу.Як переваги SVM можна відзначити здатність до узагальнення, високу точність і низьку обчислювальну складність прийняття рішення. Недоліком методу є відносно велика обчислювальна складність побудови моделі, що класифікує [2].
2. Метод k-найближчих сусідів (k-nearestneighbors, k-NN) — метричний алгоритм автоматичної класифікації об'єктів чи регресії. Об'єкт, що класифікується, відноситься до того класу, якому належать найближчі до нього об'єкти навчальної вибірки [3]. Метод k-NN є одним із найпростіших методів ІАД. Результати застосування методу легко піддаються інтерпретації. Недолік методу – його чутливість до локальної структури даних [2].
3. Дерево прийняття рішень - засіб підтримки прийняття рішень, що використовується в статистиці та аналіз даних для прогнозних моделей [4].Перевагами дерев прийняття рішень є простий принцип їх побудови та хороша інтерпретованість результатів, недоліком – невисока точність класифікації [2].
4. Нейронна мережа (або штучна нейронна мережа) — математична

модель, а також її програмне або апаратне втілення, побудована за принципом організації та функціонування біологічних нейронних мереж — мереж нервових клітин живого організму. Нейронні мережі не програмуються у звичному значенні цього слова, вони навчаються. Навчання мережі відбувається шляхом коригування значень ваги нейронів для мінімізації помилки класифікації [5]. Переваги нейронних мереж виражаються в їх здатності автоматично набувати знань під час навчання, а також здатності до узагальнення, основний недолік полягає у чутливості до шуму у вхідних даних [2]. Отже високу точність мають лише нейронні мережі та метод опорних векторів, який також має високу масштабованість разом із деревом прийняття рішень. Окрім високої масштабованості, вони також мають високу трудомісткість. У той же час метод k-найближчих сусідів має дуже низьку масштабованість, нейтральну трудомісткість та дуже низьку швидкість. А метод опорних векторів та дерево прийняття рішень мають високу швидкість та високу популярність

Висновки. Після порівняння їх переваг та недоліків стає зрозуміло, що кожен алгоритм має свої сильні та слабкі сторони. Але жоден з них немає можливості вирішити весь спектр задач, які потребує інтелектуальний аналіз даних.

Список літератури

1. Nefedov A. SupportVectorMachines: A SimpleTutorial. *Svmtutorial*. URL: https://svmtutorial.online/ (дата звернення: 27.10.2021);
2. Шарабыров И. В. Система обнаружения атак в локальных беспроводных вычислительных сетях на основе технологий интеллектуального анализа данных : дис. канд. тех. наук. Уфа, 2016. 144 с;
3. Hastie T., Tibshirani R., Friedman J. The Elements of Statistical Learning: guide book. Springer, 2001, 745 p;
4. Microsoft DecisionTreesAlgorithm. *Microsoft.* URL: https://docs.microsoft.com/en-us/sql/analysis-services/data-mining/micro-soft-decision-trees-algorithm (дата звернення: 12.11.2021)
5. Philip D. Wasserman Neural Computing: Theory and Practice: guide book. Van Nostrand Reinhold, 1989, 230 p.

Відомості про авторів

Луханін Богдан Юрійович, студент кафедри комп'ютерних систем, мереж і кібербезпеки, м.т. 096-875-81-12, b.lukhanin@student.csn.khai.edu
Землянко Георгій Андрійович, асистент кафедри комп'ютерних систем, мереж і кібербезпеки, g.zemlynko@khai.edu

Секція 1

АНАЛІЗ БЕЗПЕКИ ПЕРСОНАЛЬНИХ ДАНИХ КОРИСТУВАЧІВ СОЦІАЛЬНИХ МЕРЕЖ

Малєєва З.-Т. О.
Національний аерокосмічний університет ім. М.Є. Жуковського «ХАІ»
Науковий керівник Цуранов М.В.

Актуальність. За даними компаній «We are social» та «Hootsuite» за січень 2021 року аудиторія соціальних мереж налічує 4, 66 млрд осіб, що на 316 мільйонів (7,3 відсотка) більше, ніж в 2020 [1]. Загалом, приблизно 59,5 відсотка населення планети використовує соціальні мережі. Станом на січень 2021 р. у Facebook налічується більше 2,7 мілрд. користувачів, на другому місці вже декілька років незмінно залишається YouTube – з більше ніж 2 мілрд. користувачів [1]. За даними Kantar Україна, протягом останніх п'яти років найшвидше в країні розвиваються соціальні мережі Facebook та Instagram — насамперед завдяки забороні російських сайтів [2].

Мета роботи полягає в аналізі безпеки персональної інформації, розміщеної користувачами в соціальних мережах.

Основні положення. Існує багато визначень поняття «Соціальні мережі». Розглянемо одне з найбільш вживаних понять.

Соціальна мережа - інтерактивний розрахований на багато користувачів веб-сайт, контент якого наповнюється самими учасниками [3].

Соціальні мережі за своїм функціоналом поділяються на: соціальні мережі для спілкування (Одноклассники, Вконтакте, Facebook); професійні соціальні мережі (LinkedIn, Xing); соціальні мережі для обміну медіа-контентом (Instagram, YouTube, Tik Tok); соціальні мережі для авторських записів (Twitter, Tumblr); соціальні мережі для відгуків та оглядів (TripAdvisor, Foursquare); соціальні мережі для колективних обговорень (Reddit, 4PDA); соціальні мережі для знайомств (Badoo, Tinder).

Майже кожна соціальна мережа виступає оператором персональних даних користувачів, які збираються та обробляються, так як при реєстрації нового облікового запису, необхідно вказувати інформацію про особу, такі як: ПІБ, вік, освіта, номер контактного телефону та інші. Зазвичай, користувачі залишають відкриті профілі для інших. Користуючись цим зловмисники можуть аналізуючи повідомлення та дані, якими люди діляться в мережі, та здатні вивести конфіденційну інформацію, якої може бути достатньо, щоб, наприклад, отримати інформацію для відновлення паролю.

За даними компанії Le Journal du Web, можна побачити, що у соціальних мережах завантажується величезна кількість даних, а саме,

за день розміщаються близько 8 млн. записів на «стіні» та 70 млн. фотографій [4]. Нині майже всі мобільні телефони мають GPS-модуль, завдяки якому до фотографій одразу прикріпляється геомітка. Ця функція може розкривати особисту інформацію.

Якщо проаналізувати ліцензійні угоди соціальних мереж, то можна з'ясувати що відповідальність за конфіденційні дані несе сам користувач. Тому було розроблено політику безпеки в соціальних мережах: при реєстрації в соціальних мережах завжди читати політику конфіденційності; використовувати надійний пароль; використовувати двофакторну автентифікацію для додаткового захисту акаунту; не розкривати важливу інформацію в особистих повідомленнях; звертати увагу на те, хто додається у друзі; налаштувати доступ до конфіденційних даних в особистому профілі.

Висновки. Повністю убезпечити персональну інформацію в мережі означає загалом від неї відмовитися, що не є можливим, для сучасної людини. На даний момент немає технічних засобів захисту даних в соціальних мережах, а є тільки організаційні.

Список літератури

1. DIGITAL 2021: GLOBAL OVERVIEW REPORT. *Slideshare*. URL – https://www.slideshare.net/DataReportal/digital-2021-global-overview-report-january-2021-v03 (дата звернення 26.10.2021);
2. Як змінилося користування мобільними застосунками за 5 років: соцмережі та месенджери. *Tns*. URL: https://tns-ua.com/news/yak-zminilosya-koristuvannya-mobilnimi-zastosunkami-za-5-rokiv-sotsmerezhi-ta-mesendzheri (дата звернення 12.11.2021);
3. Цуранов М.В. Методи та засоби боротьби з правопорушеннями в інформаційній сфері: навчальний посібник / М.В. Цуранов, В.М. Струков, В.Я. Пєвнєв. – Харків: ХНУВС, 2015. – 256 с.;
4. Інтернет-статистика в реальному часі. *Internetlivestats*. URL: https://www.internetlivestats.com/ (дата звернення 12.11.2021).

Відомості про авторів

Малєєва Злата-Тіна Олександрівна, студентка кафедри комп'ютерних систем, мереж і кібербезпеки, м.т. 050-275-80-95, z.malieieva@student.csn.khai.edu
Цуранов Михайло Віталійович, ст. викладач студентка кафедри комп'ютерних систем, мереж і кібербезпеки. m.tsuranov@csn.khai.edu

Секція 1

ЗАХИСТ ВЕБ-САЙТУ

Оганян В. Ю.
Національний аерокосмічний університет ім. М. Е. Жуковського
«Харківський авіаційний інститут»
Науковий керівник Пєвнєв В. Я.

Актуальність. Одним з найважливіших завдань при розробці сайтів є їх захист. Адже інтернет є небезпечним місцем, а незахищений сайт може бути легко відключений зловмисниками, через несанкціонований доступ, що призведе до втрати довіри, репутації, часу і грошей людини або компанії, яка володіє тим чи іншим сайтом [1]. У зв'язку з цим захист веб-додатків від різних загроз стає актуальною проблемою.

Метою даної роботи є аналіз існуючих в даний час різних загроз, які можуть викликати некоректну роботу сайту, і розглянути сучасні способи захисту від шкідливого програмного забезпечення.

У доповіді наведені найбільш відомі і поширені засоби захисту, такі як [2,3]:

- Web Application Firewall (WAF);
- засоби захисту від DDoS-атак;
- сканери захищеності веб-додатків (WASS);
- засоби аналізу веб-сайтів на віруси.

Основні положення. Для захисту від втрати даних, SQL-ін'єкцій, отруєння файлами cookie, підбору паролів і використання різних вразливостей в веб-додатках використовується WAF – це файрволл, який сьогодні використовується як універсальний засіб захисту від багатьох видів загроз. Для захисту від DDoS-атак, спрямованих на так званий вид атак на відмову в обслуговуванні, які призводять до відсутності доступу до певного веб-сайту або сервісу на невизначений термін, до декількох тижнів, і, як наслідок, до втрати часу і грошових ресурсів, використовуються різні засоби захисту від DDoS. Захист здійснюється декількома способами: на краю мережі, через локальний центр очищення або шляхом перенаправлення трафіку в хмару. WASS-сканери та інструменти для аналізу сайтів на наявність вірусів, як випливає з назви, сканують сайти на наявність певних вразливостей, помилок, вірусів, сторонніх рекламних та інших шкідливих програм.

У доповіді також наведені існуючи вразливості. До кожного наведеного виду уразливості був розглянутий сценарій можливої атаки

з боку зловмисника. Також були запропоновані методи для розробників, які дозволяють утилізувати дані уразливості та розробити безпечний веб-застосунок [4].

Висновки. Підводячи підсумки, можна побачити, що без засобів захисту зловмисники можуть легко нашкодити сайту. А уникнути цього допоможе спільне використання всіх раніше перерахованих технологій і методів захисту сайтів. Такий підхід, використовуючи різні доступні засоби захисту, забезпечить найвищий і багаторівневий рівень безпеки, і заподіяти будь-яку шкоду буде набагато складніше. І навіть якщо це вдасться, вона не буде такою великою, як могла б бути без цих захистів, що, до того ж, допоможе швидко виявити проблему, якщо вона з'явиться, і усунути її. Тому всі власники різноманітних сайтів і ресурсів повинні ознайомитися з сучасними засобами захисту і використовувати їх.

Список літератури

1. Захист веб-додатків: чому це важливо? *Itbiz*. URL: https://itbiz.ua/ru/stati-i-obzory/ruzashhita-veb-prilozhenij-pochemu-eto-vazhnozaxist-veb-dodatkiv-chomu-ce-vazhlivo/ (дата звернення: 12.11.2021)

2. Hoffman A. Web Application Security : Exploitation and Countermeasures for Modern Web Applications. Sebastopol: O'Reilly Media, Inc, 2020. 450 p.

3. Welling Uk., Thomson L. PHP and MySQL Web Development. Hoboken, New Jersey: Addison-Wesley Professional, 2016. — 688 p.

4. Pevnev V., Popovichenko O., Tsokota Ya. Web application protection technologies Advanced Information Systems. 2020. Vol. 4, No.1. 2020, P. 219-223

Відомості про авторів

Оганян Вячеслав Юрійович, бакалавр кафедри комп'ютерних систем, мереж і кібербезпеки, м.т. 096-313-58-16, v.ohanian@student.csn.khai.edu

Пєвнєв Володимир Яковлевич, доцент кафедри комп'ютерних систем, мереж і кібербезпеки, д.т.н., доцент, v.pevnev@csn.khai.edu

Секція 1

ПОЛІМОРФНІ ВІРУСИ ТА МЕТОДИ ЇХ ВИЯВЛЕННЯ

Родіонов Д. В.
Національний аерокосмічний університет ім. М. Е. Жуковського «ХАІ»
Науковий керівник Пєвнєв В. Я.

Актуальність. Тема вірусів стає все більш актуальною з кожним роком, тому що кількість користувачів комп'ютерами та мережею Інтернет збільшується. Дуже часто у інтернеті разом із корисним матеріалом можна підхопити багато різноманітних вірусів. Відповідно до популяризації комп'ютерів, спеціалісти з кібербезпеки турбуються про безпечність користування Інтернетом та відповідні протидії вірусам. На даний момент є багато антивірусних програм, які знаходять та видаляють віруси [1]. Але з кожним роком створюється безліч нових вірусів, і модифікуються старі, саме тому антивірусні програми просто не встигають за ними. Одним із типів захищеності вірусів є поліморфізм вірусів.

Метою даної роботи є дослідження поліморфних вірусів та методів їх виявлення.

Основні положення. Поліморфні віруси запрограмовані таким чином, що вони можуть змінювати тіло вірусу після чергового зараження [2]. Найчастіше зміна коду досягається шляхом додавання операторів, які не змінюють принцип роботи вірусу. Підхід до виявлення саме поліморфних вірусів суттєво відрізняється від виявлення інших типів вірусів. Для того щоб знайти та ліквідувати поліморфний вірус, потрібно знати як він працює.

Кожен вірус має характерні ознаки. Такими ознаками можуть бути дії, що виконуються самим вірусом, характерними ознаками є ціль вірусу та методи її досягнення. На основі такої інформації і складаються сигнатури вірусів, використовуючи які антивірус шукає шкідливі програми. Також антивірус може ізолювати вірус (запуск в режимі sandbox) і вже там спостерігати за його поведінкою [3].

Існує багато технологій виявлення вірусів. Їх можна поділити на 2 групи [4].: технології сигнатурного аналізу та технології імовірнісного аналізу: сигнатурний аналіз - метод виявлення вірусів , що полягає в перевірці наявності в файлах сигнатур вірусів; евристичний аналіз -

технологія, заснована на імовірнісних алгоритмах, результатом роботи яких є виявлення підозрілих об'єктів.

У процесі евристичного аналізу перевіряється структура файлу, його відповідність вірусним шаблонах. Найбільш популярною евристичної технологією є перевірка вмісту файлу на предмет наявності модифікацій уже відомих сигнатур вірусів та їх комбінацій. Це допомагає визначати гібриди і нові версії раніше відомих вірусів без додаткового оновлення антивірусної бази. Евристичний аналіз - один із методів виявлення поліморфних вірусів.

Аналіз контрольних сум - це спосіб відстеження змін в об'єктах комп'ютерної системи. На підставі аналізу характеру змін - одночасність, масовість, ідентичні зміни довжин файлів - можна робити висновок про зараження системи.

Висновки. Поліморфні віруси майже неможливо виявити сигнатурними антивірусами. Для виявлення даного виду зловмисних програм потрібно відстежувати поведінку вірусу та фіксувати усі види підозрілої активності. Найкраще для цього підходить евристичний аналіз та аналіз контрольних сум. Як один із варіантів захисту від потрапляння поліморфних вірусів є резидентні монітори.

Список літератури

1. Новаков Е.О., Цуранов М.В. Использование обучаемых HIPS-антивирусов для противодействия киберпреступности. Системи управління, навігації та зв'язку, 2017, випуск 1(41);

2. Цуранов М.В. Методи та засоби боротьби з правопорушеннями в інформаційній сфері: навчальний посібник / М.В. Цуранов, В.М. Струков, В.Я. Пєвнєв. – Харків: ХНУВС, 2015. – 256 с.;

3. Polymorphic virus. *Cyber Hoot*. URL – https://cyberhoot.com/cybrary/polymorphic-virus/ (дата звернення: 20.11.2021);

4. Полиморфизм компьютерных вирусов. *Рус наука*. URL: http://www.rusnauka.com/14_NPRT_2010/Informatica/66880.doc.htm (дата звернення: 20.11.2021).

Відомості про авторів

Родіонов Дмитро Валерійович, студент кафедри комп'ютерних систем, мереж і кібербезпеки, м.т. 098-026-47-48, d.rodionov@student.csn.khai.edu

Пєвнєв Володимир Яковлевич, доцент кафедри комп'ютерних систем, мереж і кібербезпеки, д.т.н., доцент, v.pevnev@csn.khai.edu

Секція 1

ДОСЛІДЖЕННЯ МОЖЛИВОСТЕЙ ПРИХОВУВАННЯ ІНФОРМАЦІЇ В АУДІОФАЙЛАХ

Руєва А. В.
Національний аерокосмічний університет ім. М. Е. Жуковського «Харківський авіаційний інститут»
Науковий керівник Пєвнєв В. Я.

Актуальність. Розвиток інформаційних технологій спричинило різке збільшення можливостей незаконного доступу до інформації. У зв'язку із цим на перший план виходить інформаційна безпека, яка є складовою безпеки будь-якої держави. Одночасно зростає роль кібербезпеки. Використання комп'ютерної техніки дозволяє зробити прорив у багатьох галузях науки та техніки, медицині, виробництві та інших галузях. Водночас зростають загрози від незаконного отримання інформації, її зміни. Існуючі способи забезпечення конфіденційності, цілісності та доступності не здатні повністю усунути загрози для інформації, що передається. Багато фахівців вважають основним способом вирішення більшості завдань, що виникають при забезпеченні інформаційної безпеки, використання криптографії [1].

Одним із найбільш перспективним методом забезпечення конфіденційності та цілісності інформації є стеганографія, яка приховує сам факт передачі інформації [2]. Як контейнер, в якому розміщується повідомлення, що передається, можуть використовуватися текстові, графічні, аудіо- та відеофайли. Надійність такого способу передачі зростає, коли одночасно використовуються криптографічні та стеганографічні методи приховування інформації [3].

Метою даної роботи є дослідження можливостей приховування інформації в аудіофайлах, розробка блоків одно- та двобітового приховування.

Основні положення. У доповіді наведені наступні методи приховування інформації в аудіофайлах: вбудовування з розширенням спектра, вбудовування за рахунок модифікації фази аудіосигналу, вбудовування за рахунок зміни часу затримки echo-сигналу, вбудовування інформації в найменший біт. Порівняльний аналіз цих методів показав, що кожен з них має свої недоліки та переваги, а методи фазового кодування та луна-метод є найкращими для приховування даних (зберігають якість аудіофайлу, стійкі до модифікацій). Але на

відміну від методу фазового кодування, луна-метод є не так глибоко вивченим та однозначним як фазовий [4]. В доповіді представлено алгоритм з розробкою блоків побітового та двобітового приховування та визначено «формуючі величини» для луна-методу. Також було показано можливості луна методу шляхом проведення експериментів з різними контейнерами та різною довжиною приховуваної інформації. Результати експериментів демонструються за допомогою аудіофайлів.

Висновки. В доповіді було проаналізовано можливість вбудовування інформації луна-методом з використання блоків інформаційного приховування. Відмінні риси луна-методу дозволяють приховувати інформацію в аудіофайли, переслідуючи різні цілі, такі як: захист авторських прав, прав інтелектуальної власності або конфіденційних даних а також захист від НСД. Для цього в роботі було показано різні модифікації алгоритму. Було визначено, що ефективність використання двобітового блоку зростає з і збільшенням самого приховуваного тексту.

Список літератури

1. Урбанович П. П. Защита информации методами криптографии, стеганографии и обфускации: навч.-метод. посіб. Мінськ : БДТУ, 2016. 220 с.

2. Пєвнєв В. Я. Моделі загроз і забезпечення цілісності інформації. *Системи та технології*. 2018. №2 (56/1). С. 79–94.

3. Pevnev V., Voikov Yu. Research and Prototyping Methods of Steganography Using Mosaic. *Advanced Information Systems*. 2020. Vol. 4, No.2. P.137-141

4. Singh P. A Comparative Study of Audio Steganography Techniques. *IRJET*. 2016. Том 3, Випуск 4. с. 580-585.

Відомості про авторів

Руєва Анастасія Володимирівна, магістрант кафедри комп’ютерних систем, мереж і кібербезпеки, м.т. 095-25-82-148, a.ruieva@student.csn.khai.edu

Пєвнєв Володимир Яковлевич, доцент кафедри комп'ютерних систем, мереж і кібербезпеки, д.т.н., доцент, v.pevnev@csn.khai.edu

Секція 1

КРИПТОГРАФІЧНИЙ ЗАХИСТ IoT ПРИСТРОЇВ

Тяпко М. В.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник Пєвнєв В. Я.

Актуальність. Впродовж останніх років з розвитком технології Інтернет Речей (IoT) збільшується кількість пристроїв підключених до мережі Інтернет [1]. До пристроїв інтернет речей можна віднести розумні годинники, смарт-TV, пристрої голосового керування, камери, смарт-картки та інші. Деякі рішення зберігають та передають критично важливу інформацію. Для забезпечення конфіденційності та контролю цілісності даних використовується криптографія [2].

Метою даної роботи є дослідження існуючих рішень криптографічних алгоритмів для IoT девайсів.

Основні положення. Через те що більшість криптографічних алгоритмів було розроблено для використання серверами та звичайними комп'ютерами користувачів, багато з алгоритмів не підходять для пристроїв зі слабкими процесорами, низьким рівнем живленням та обмеженою пам'яттю, що є характеристиками пристроїв інтернет речей. Малоресурсна криптографія — це підгалузь криптографії, яка спрямована на надання рішень, розроблених для пристроїв із обмеженими можливостями [3], її мета полягає в розробці алгоритмів з низьким вмістом як апаратного, так і програмного забезпечення. Потреба оптимізації спонукає людей, що займаються криптографією, змінювати існуючі та створювати нові алгоритми. Таким чином з'явилися видозмінені версії AES, 3-DES, ГОСТ 28147-89, де були зменшені розміри блоку та відкритого ключу. Також з'явились нові шифри як Present, LEA, Simon, Speck та інші [4]. В 2015 році підрозділ Управління з технологій США National Institute of Standards and Technology (NIST) розпочав процес стандартизації та закликав компанії приєднатися до розробки криптографічних алгоритмів придатних для використання в обмежених середовищах [5]. Таким чином після завершення першого раунду відбору 32 із 56 запропонованих рішень було залишено для продовження розгляду, а після закінчення другого раунду в 2021 році після порівняння швидкості

шифрування та розміру коду алгоритмів залишилося лише 9 алгоритмів [5].

Висновки. Після порівняння результатів роботи алгоритмів та їх конфігурації можна зробити висновок, що AES не є універсальним рішенням тому що його апаратна реалізація має велике значення одиниці вимірювання Gate Equivalents (GE), ГОСТ 28147-89 займає менше місця, але може бути підвержений криптоаналізу. В тому числі, як і велика кількість нових шифрів, таких як SPECK, SIMON, через маленький розмір інформаційного блоку.

Список літератури

1. Internel of Thinks (IoT) market – growth, trends, COVID-19 impact and forecasts (2021-2026). *Mordon Intelligence*. URL – https://www.mordorintelligence.com/industry-reports/internet-of-things-moving-towards-a-smarter-tomorrow-market-industry (дата звернення: 18.11.2021);
2. Пєвнєв В.Я. Методи забезпечення цілосності інформації в інфокомунікаційних системах. Харків 2015 – с. 4. URL: http://repository.kpi.kharkov.ua/handle/KhPI-Press/19120 (дата звернення: 20.11.2021);
3. Report on Lightweight Cryptography, March 2017 – с. 1. *NIST*. URL – https://csrc.nist.gov/CSRC/media/Publications/nistir/8114/draft/documents/nistir_8114_draft.pdf (дата звернення: 19.11.2021);
4. An ultra light-weight cryptography scheme for IoT. *HAL*. URL – https://hal.archives-ouvertes.fr/hal-03359990/document (дата звернення: 18.11.2021);
5. Lightweigth Cryptography. *NIST*. URL – https://csrc.nist.gov/Projects/Lightweight-Cryptography (дата звернення: 18.11.2021).

Відомості про авторів

Тяпко Михайло Вікторович, бакалавр кафедри комп'ютерних систем, мереж і кібербезпеки, м.т. 099-494-57-95, m.tiapko@student.csn.khai.edu
Пєвнєв Володимир Яковлевич, доцент кафедри комп'ютерних систем, мереж і кібербезпеки, д.т.н., доцент, v.pevnev@csn.khai.edu

Секція 1

ДОСЛІДЖЕННЯ БЕЗПЕКИ СУЧАСНИХ ORM ФРЕЙМВОРКІВ .NET

Чишкала С.А.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник Орєхов О. О.

Актуальність. При розробці сучасних додатків часто виникає питання як додаток буде працювати з даними. З одного боку простішим для програмістів та дешевшим для власника продукту рішенням є використання сучасних ORM фреймворків, з іншого боку не все так однозначно, адже є багато «але» [1]. На етапі обговорення замовник та бізнес аналітик визначають список задач та всі вимоги до проекту. Все залежить від розмірів планується проєкту. Тема ORM завжди була і буде актуальною в розробці сучасних додатків, адже майже кожен додаток має свою базу даних і з цього постає питання, як цей додаток буде спілкуватися з базою і на скільки це безпечно [2].

Метою даної роботи є дослідження безпеки сучасних ORM бібліотек для .NET.

Основні положення. SQL-ін'єкція – це метод використання даних користувача через поле введення веб-сторінок [3]. Шкідливі дані, коли вони приймаються сервером або програмою, можуть використовуватися для маніпулювання даними користувача та компанії. Це одна з найпростіших і водночас найруйнівніших атакуючих ідей. Тисячі веб-серверів страждають щодня, завдаючи мільйони доларів збитків.

SQL-ін'єкція, залежно від типу використовуваної СУБД та умов впровадження, може дати можливість атакуючому виконати довільний запит до бази даних (наприклад, прочитати вміст будь-яких таблиць, видалити, змінити або додати дані), отримати можливість читання та/або запису локальних файлів та виконання довільних команд на сервері, що атакується. Атака типу ін'єкції SQL може бути можлива через некоректну обробку вхідних даних, що використовуються в SQL-запитах [4]. Зловмисники можуть використовувати цю вразливість для отримання облікових даних користувачів з бази даних. Після чого вони можуть видавати себе за реальних користувачів та красти їхні гроші чи дані.

Зловмисники можуть отримати права адміністратора у базі даних, щоб стерти, скопіювати чи пошкодити всі дані на сервері. У деяких випадках SQL ін'єкція також дозволяє зловмисникам отримати доступ до операційної системи. Це призводить до атаки на внутрішню мережу вашого бізнесу. Розробники сайтів та додатків, що працюють з реляційними базами даних, повинні знати про такі вразливості та вживати заходів протидії. В роботі були розглянуті способи захисту впроваджені в ORM бібліотеках від подібного роду атак.

Висновки. Entity Framework дуже популярна бібліотека в розробці сучасних комерційних додатків. Однак, багато розробників навіть не підозрюють про те на скільки потужний функціонал бібліотека пропонує. Багато хто ігнорує безпечні підходи при використанні фрейморку, або не підозрює про їх існування. На практиці, це відбувається через брак знань розробників. Використання ORM недостатньо, щоб запобігти атакам, таким як ін’єкції SQL [5]. Розробники повинні коректно використовувати фреймворк, щоб уникати небезпечний коду.

Список літератури

1. Security Considerations. *Microsoft*. URL – https://docs.microsoft.com/en-us/dotnet/framework/data/adonet/ef/security-considerations (дата звернення: 18.11.2021);
2. Secure Data Access. *Microsoft*. URL – https://docs.microsoft.com/en-us/dotnet/framework/data/adonet/secure-data-access (дата звернення: 18.11.2021);
3. SQL injection. *Wikipedia*. URL – https://en.wikipedia.org/wiki/SQL_injection (дата звернення: 19.11.2021);
4. SQL Injection attacks in Entity Framework Core. *Adrientorris*. URL – https://adrientorris.github.io/entity-framework-core/SQL-Injection-attacks-in-Entity-Framework-Core-2-0.html (дата звернення: 19.11.2021);
5. Fixing SQL Injection: ORM is not enough. *Snyk*. URL – https://snyk.io/blog/sql-injection-orm-vulnerabilities/ (дата звернення: 20.11.2021).

Відомості про авторів

Чишкала Сергій Андрійович, магістрант кафедри комп’ютерних систем, мереж і кібербезпеки, м.т. 066-237-33-39, s.chyshkala@student.csn.khai.edu

Орєхов Олександр Олександрович, доцент кафедри комп’ютерних систем, мереж і кібербезпеки, к.т.н., професор, a.orehov@csn.khai.edu

Секція 1

СИСТЕМА ЗАХИСТУ ЕЛЕКТРОННОГО КАБІНЕТУ МЕНЕДЖЕРА

Чоломбитько М. Ю.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник Пєвнєв В. Я.

Актуальність. Широке використання інформаційних технологій у всіх сферах життя суспільства робить досить актуальною проблему захисту інформації, інформаційних ресурсів, каналів передачі даних від злочинних дій зловмисників. У міру розвитку технологій електронних платежів та документообігу є велика небезпека втручання сторонніх осіб, з метою завдання шкоди підприємству [1].

Метою даної роботи є дослідження методів забезпечення безпеки електронного кабінету менеджера.

Основні положення. В електронному кабінеті менеджера міститься інформація про постачальників та покупців. Також в кабінеті зберігаються актуальні ціни фірми. Використання електронних документів значно спрощує роботу з документацією між різними установами і дозволяє досягти величезного економічного ефекту.

У даній системі не можна забувати про безпеку всієї системи, адже вона містить конфіденційну інформацію, втрата якої може завдати збитків фірмі. Однією з найважливіших вимог є забезпечення безпеки електронного обміну документами. Основними загрозами безпеки для роботи з електронними документами є:

- загроза цілісності інформації;
- загроза конфіденційності;
- загроза роботі системи;
- загроза доступності.

Для організації захисту інформації в системі, яка працює з електронними документами, додаткову увагу потрібно звернути на забезпечення доступності публічної інформації та блокування несанкціонованого доступу [1]. Якщо передбачається, що з кабінетом будуть працювати працівники підприємства з відповідними повноваженнями, то варто звернути увагу на питання, пов’язані з розмежуванням прав доступу користувачів до інформації. Людина, що працює на ділянці занесення в програму даних, не повинен мати

можливості ознайомлюватися з результатами бухгалтерської звітності (якщо це не передбачено його посадовими обов'язками).

Ще одна проблема, яка пов'язана доступністю є захисту електронних документів і його реквізитів від випадкових чи навмисних змін, а також захист електронного документа під час його зберігання в електронному архіві [2].

Висновки. Робота з електронними документами зараз стає все більш поширеною. Електроні кабінети полегшують роботу між різними фірмами та установами. Але, будь-яка конфіденційна інформація, яка передається в електронній формі повинна бути добре захищена. Як показує аналіз практики, найбільш поширеним злочином у сфері високих інформаційних технологій є неправомірний доступ до інформації. Системи, в якій зберігається інформація, має бути захищена від неправомірного доступу та мати обмеження на внесення та зміну даних.

Список літератури

1. Заводянський В.О. Захист інформації в електронному документообігу. У кн.: Матеріали VI Міжнародної науково технічної конференції молодих учених та студентів. Актуальні задачі сучасних технологій., 16-17 листопада 2017 р., м. Тернопіль / Терн. нац. техн. ун-т ім. Івана Пулюя, Україна;

2. Проблеми електронного документообігу та шляхи їх вирішення. *Magazine*. URL: http://magazine.faaf.org.ua/problemi-elektronnogo-dokumentoobigu-ta-shlyahi-ih-virishennya.html (дата звернення: 20.11.2021).

Відомості про авторів

Чоломбитько Маргарита Юріївна, студент кафедри комп'ютерних систем, мереж і кібербезпеки, м.т. 099-678-97-79, m.cholombytko@student.csn.khai.edu

Пєвнєв Володимир Яковлевич, доцент кафедри комп'ютерних систем, мереж і кібербезпеки, д.т.н., доцент, v.pevnev@csn.khai.edu

Секція 1

АНТИВІРУСНИЙ ЗАСІБ ДЛЯ ВИЯВЛЕННЯ СТЕЛС-ВІРУСІВ

Шипунов М.Ю.
Національний аерокосмічний університет ім. М. Е. Жуковського «ХАІ»
Науковий керівник: ст. викладач Цуранов М. В.

Актуальність. На сьогоднішній день, завдяки розповсюдженості мережі Інтернет, все частіше відбуваються масові вірусні зараження інфокомунікаційних систем, що наносить величезні збитки. Лише кількість атак з використанням вірусів типу Ransomware збільшилось на 46% [1]. Кількість знайдених вірусів-майнерів збільшилась на 8500% [1]. На 80% збільшилася кількість знайдених вірусів під MacOS [1]. Згідно звіту компанії Symantec, кількість офіційно зареєстрованих вразливостей збільшилася на 13% [1]. На 92% збільшилась кількість заблокованих завантажувальних вірусів [1]. У 2017 році найбільш серйозна атака проводилася з використанням вірусу WannaCry (> $1 млрд збитків) [2].

Мета роботи: полягає у аналізі механізмів роботи стелс вірусів та існуючих засобів для боротьби з ними.

Основні положення. За особливостями алгоритму роботи, віруси поділяються на наступні категорії: резидентні, поліморфні та стелс [3]. Найбільш небезпечні віруси мають стелс елементи, тому що найбільші збитки були нанесені саме шкідливим програмним забезпеченням, яке використовувало цю технологію.

Проблема виявлення стелс-вірусів полягає в тому, що вони активно ховають свою присутність у системі шляхом перехоплення системних повідомлень або підміни деяких компонентів операційної системи [3]. Через це, коли виконується системний виклик або відкриття файлу, вірус перехоплює контроль та окрім реальних функцій системи, виконує свої [3]. Для того, щоб знайти та деактивувати вірус, потрібен антивірус, який буде ефективний проти стелс вірусів. За технологіями захисту класифікують наступні антивірусні засоби: сигнатурні, проактивні та комбіновані [3].

Сигнатурні антивіруси під час пошуку використовують для виявлення вірусів бази даних, та здебільшого не є ефективними під час пошуку вірусів зі стелс елементами [3]. Це зумовлено тим, що процес оновлення та додавання нових сигнатур у бази потребує часу.

У свою чергу проактивні антивіруси намагаються запобігти зараженню комп'ютера, замість того, щоб шукати вірус у вже зараженій системі. Ефективність такого антивірусу залежить від проактивної компоненти яка

в ньому використовується. Найпоширенішими алгоритмами проактивного захисту є: евристичний аналіз, емуляція коду, виконання коду у пісочниці та віртуалізація робочого оточення для аналізу поведінки [4]. Найбільш дійовою вважається виконання програм у пісочниці, так як програма виконується в ізольованому місці та не може завдати шкоди системі. Основним недоліком проактивних антивірусів є помилкові спрацювання. Через це користувач може заблокувати роботу антивірусного програмного забезпечення після декількох повідомлень про зараження.

Комбіновані антивіруси поєднують різні підходи. До них відносяться як сигнатурний пошук так і проактивні технології, які було розглянуто вище. Наразі більшість антивірусного програмного забезпечення використовують комплексний підхід для захисту комп'ютера. Прикладом таких антивірусів є: Zillya! Total Security, Kaspersky Internet Security та Avast! Antivirus.

Висновки. Аналіз особливостей роботи стелс вірусів та антивірусного програмного забезпечення показав, що існуючі методи захисту не можуть гарантовано виявляти стелс віруси. Найбільш ефективними себе показали антивіруси з проактивними компонентами, але і вони не можуть безпомилково знешкодити віруси даного типу. Саме тому є необхідність в створенні спеціального антивірусного засобу, який комбінував використання декількох проактивних компонент для збільшення ймовірності виявлення та знешкодження в системі стелс вірусів.

Список літератури

1. Symantec Internet Security Thread Report. Volume 38. *Symantec*. URL – https://docs.broadcom.com/doc/istr-23-2018-en (дата звернення: 20.10.2021);
2. Убытки от WannaCry оценили в миллиард долларов. *Економічна правда.* URL: https://www.epravda.com.ua/rus/news/2017/05/25/625286/ (дата звернення: 2.11.2021);
3. Цуранов М.В. Методи та засоби боротьби з правопорушеннями в інформаційній сфері: навчальний посібник / М.В. Цуранов, В.М. Струков, В.Я. Пєвнєв. – Харків: ХНУВС, 2015. – 256 с.;
4. Новаков Е.О., Цуранов М.В. Использование обучаемых hips-антивирусов и для противодействия киберпреступности. Системи управління, навігації та зв'язку, 2017, випуск 1(41).

Відомості про авторів

Шипунов Микита Юрійович, студент кафедри комп'ютерних систем, мереж і кібербезпеки, м.т. 098-034-43-88, m.shypunov@student.csn.khai.edu
Цуранов Михайло Віталійович, старший викладач кафедри комп'ютерних систем, мереж і кібербезпеки, m.tsuranov@csn.khai.edu

Секція 1

ПОЛІТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЯК ВАЖЛИВА СКЛАДОВА ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

Шорский О. Е.
Національний аерокосмічний університет ім. М.Є Жуковського
«Харківський авіаційний інститут»
Науковий керівник Пєвнєв В.Я.

Актуальність. Комп'ютерні та інформаційні технології сьогодні охопили усі галузі економіки. Рівень технологічного розвитку визначає не лише економічний потенціал країни та якість життя її громадян, але й роль і місце цієї країни в глобальному суспільстві, масштаби та перспективи її економічної та політичної інтеграції з усім світом [1]. Для будь-якої сучасної компанії інформація стає одним із головних ресурсів, збереження та правильне розпорядження яких має ключове значення для розвитку бізнесу та зниження рівня різноманітних ризиків. Актуальною проблемою для підприємства стає забезпечення інформаційної безпеки. Інформаційна безпека – властивість системи протягом заданого часу протистояти несанкціонованому зняттю та модифікації інформації [2].

Метою доповіді є визначення вимог до формування інформаційної політики, яка повинна відповідати існуючим законодавчим, нормативно-правовим актам, міжнародним зобов'язанням та внутрішнім документам.

Основні положення. Інформаційна безпека являє собою комплекс заходів, основним завданням якого є забезпечення таких властивостей інформації як конфіденційність, цілісність, доступність, а також неспростовність, апелювання, спостережність, облік й автентифікація [3].

Політика безпеки визначається як сукупність документованих управлінських рішень, спрямованих на захист інформації та асоційованих із нею ресурсів. Політика безпеки включає аналіз можливих загроз і вибір відповідних заходів протидії, які є сукупністю тих норм, правил поведінки, якими користується конкретна організація при обробці інформації та її захисту [4]. Метою політики безпеки є мінімізація ризиків при використанні інформаційних технологій за допомогою систем забезпечення кібербезпеки

Висновки. У доповіді розглядається політика інформаційної безпеки, яка повинна давати чітке уявлення про необхідну поведінку користувачів, адміністраторів та інших фахівців при впровадженні та використанні інформаційних систем та засобів захисту інформації, а

також під час здійснення інформаційного обміну та виконання операцій з обробки інформації. Важливою функцією політики є чітке розмежування відповідальностей у процедурах інформаційного обміну: усі зацікавлені особи повинні ясно усвідомлювати межі як своєї відповідальності, так і відповідальності інших учасників відповідних процедур і процесів. Надано принципи забезпечення політики інформаційної безпеки, до яких відносяться принципи системності, комплексності, ешелонування, рівноміцності, безперервності, розумової достатності, законності, керування та персональної відповідальності. Також одним із завдань формування політики безпеки є розробка критеріїв її оцінки, за допомогою яких можливо та потрібно визначити найбільш загрозливі напрямки можливих атак на існуючу систему забезпечення кібербезпеки як інформаційних систем, так і захист самих користувачів (співробітників підприємства та його клієнтів та контрагентів), захист інформаційних активів організації, забезпечення стабільної та ефективної діяльності підприємств й організацій.

Список літератури

1. Про Рекомендації парламентських слухань на тему: "Реформи галузі інформаційно-комунікаційних технологій та розвиток інформаційного простору України". *Відомості Верховної Ради України*, від 22.04.2016. 2016 р. № 17. С.9, С.191;

2. Певнев В. Я., Цуранов М. В. Математическая модель информационной безопасности. *Системи обробки інформації*. 2010. № 3 (84). С. 62-64;

3. Пєвнєв В. Я. Моделі загроз і забезпечення цілісності інформації. *Системи та технології*. 2018. №2 (56/1). С. 79–94;

4. Кібальник Л.О., Напора І.Ю. Впровадження політики інформаційної безпеки банківських установ. *Причорноморські економічні студії*. 2016. №12-2. С.119-122.

Відомості про авторів

Шорский Олександр Едуардович, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, м.т. 098-733-94-62, a.shorskiy@student.csn.khai.edu

Пєвнєв Володимир Яковлевич, доцент кафедри комп'ютерних систем, мереж і кібербезпеки, д.т.н., доцент, v.pevnev@csn.khai.edu

Секція 1

ДОСЛІДЖЕННЯ ІНСТРУМЕНТІВ ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ DOCKER-КОНТЕЙНЕРІВ

Юдін О. В.
Національний аерокосмічний університет ім. М. Е. Жуковського «ХАІ»
Науковий керівник Цуранов М. В.

Актуальність. З розвитком хмарних технологій, ціна на зберігання та обслуговування даних істотно зменшилась [1]. Що призвело до стрімкого росту використання послуг хмарних провайдерів бізнесом. Для зменшення витрат ресурсів у хмарному сховищі, розробники почали використовувати технологію контейнеризації. Контейнер – це стандартна одиниця ПЗ, яка упаковує код та всі його модулі, тому додаток швидко і надійно переміщається з одного обчислювального середовища в інше [2]. Серед багатьох ПЗ для контейнеризації, 36 % ринку займає «Docker», станом на 2021 рік, це найбільший відсоток використання для ПЗ з контейнеризації [3]. Однак, через зріст попиту на хмарну інфраструктуру, дана галузь привернула увагу зловмисників, які в тому числі намагаються отримати доступ до керуючої машини через вразливості «Docker». У своєму звіті компанія Aqua Security стверджує, що 50% нових неправильно налаштованих екземплярів Docker піддаються атакам ботнетів протягом 56 хвилин після установки [4]. Статистичні дані збираються за допомогою сканерів вразливостей, які не тільки сканують контейнер на предмет безпечності його використання, а й відправляють статистику вразливостей на сервер, для формування аналітики.

Метою даної роботи є дослідження безпеки сучасних Docker-контейнерів.

Аналізуючи ринок хмарних технологій, дослідники компанії Trend Micro виявили новий шифрувальник DarkRadiation. Дане шкідливе ПЗ є bash-скриптом, та призначене для ураження серверної частини Docker контейнерів, які розташовані на дистрибутивах Red Hat, CentOS. Шкідливий скрипт, має змогу зупинити або відключити всі запущені Docker-контейнери. Способом поширення вірусу є скомпрометовані облікові записи та втрачені SSH-ключі [5].

Основні положення. Для своєчасного виявлення НСД до контейнера, використовуються два типи сканерів вразливостей:

статичні та динамічні. Серед статичних сканерів, ефективним є Anchore, це утиліта для перевірки наявності вразливостей в образі по базі «CVE». При перевірці контейнера, утиліта сканує відкриті порти, конфігурацію екземпляра. База CVE – є одною з найбільших баз вразливостей в комп'ютерної мережі. В роботі розглянуто переваги та недоліки сканерів вразливостей для ПЗ контейнеризації.

Висновки. Програмне забезпечення «Docker» є невід'ємною частиною DevOps-технології та має багатогранні інструменти захисту. Однак, більшість інструментів не інстальовані за замовчуванням. Більшість розробників не орієнтовані на безпечну конфігурацію контейнеру. На практиці, це відбувається через брак знань розробників та адміністраторів. Зменшити ризик НСД до чутливих об'єктів можна за допомогою сканерів вразливостей, однак даний метод є лише емпіричним тестом безпеки і не гарантує безпечність екземпляра.

Список літератури

1. Савчук В. О., Цуранов М. В. Аналіз засобів безпеки хмарних платформ. У кн.: Проблеми інформатизації: тези доп. 8-ї міжнар. наук.-техн. конф., 26-27 листопада 2020 р., м. Черкаси, м. Харків, м. Баку, м. Бельсько-Бяла : [у 3 т.]. Т. 1 / Черк. держ. технолог. ун-т [та ін.]. – Харків : Петров В. В., 2020. – 83 с.;

2. Use containers to Build, Share and Run your applications. *Docker*. URL – https://www.docker.com/resources/what-container (дата звернення: 17.10.2021);

3. Sysdig 2021 container security and usage report. *Sysdig*. URL – https://sysdig.com/blog/sysdig-2021-container-security-usage-report/ (дата звернення: 29.02.2021);

4. Aqua Security protects containerized apps and infrastructure, raises $135M. *Venture Beat*. URL – https://venturebeat.com/2021/03/10/aqua-security-protects-containerized-apps-and-infrastructure-raises-135m/ (дата звернення: 18.10.2021);

5. Актуальные киберугрозы: II квартал 2021 года. *Positive Technologies*. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2021-q2/ (дата звернення: 18.10.2021).

Відомості про авторів

Юдін Олесь Вікторович, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, м.т. 066-554-94-07, o.yudin@student.csn.khai.edu

Цуранов Михайло Віталійович, ст. викладач кафедри комп'ютерних систем, мереж і кібербезпеки, m.tsurabov@csn.khai.edu

ТЕЗИ ДОПОВІДЕЙ

Секція 2. Функційна безпека

Секція 2

ДОСЛІДЖЕННЯ СИСТЕМИ ДОСТУПУ ДО КЕРУВАННЯ АВТОМОБІЛЕМ ЗА ТЕРМОГРАМОЮ ОБЛИЧЧЯ

Воронько В. О.
Національний аерокосмічний університет ім. М. Е. Жуковського «ХАІ»
Науковий керівник Желтухін О.В.

Актуальність. З кожним роком (приблизно на 25.5% на рік) стрімко зростає ринок біометричних технологій. Серед тих респондентів, підприємства яких застосовують або планують застосовувати біометричні технології, високою популярністю користується технології ідентифікації особистості за райдужною оболонкою ока, ідентифікації з геометрії обличчя – 2D та 3D-фотографії, термограма обличчя [1].

З розвитком біометричних технологій, ціна та надійність ідентифікації користувача біометричних технологій обмеження доступу до керування автомобілем істотно зменшилась. Що призвело до стрімкого росту використання біометричних параметрів людини у системах обмеження доступу до різних об'єктів. Для зменшення витрат ресурсів у системах обмеження доступу до об'єкта, розробники почали використовувати технології ідентифікації людини з використанням його індивідуальних біометричних характеристик, таких як: відбитки пальців, відбитки долоні, сітківка ока, 2D та 3D зображення обличчя, також термограма обличчя [2]. Серед багатьох технологій ідентифікації, ідентифікація особи за термограмою обличчя є досить перспективною, тому, що ця технологія окрім функції ідентифікації здатна виконувати ще додатково функцію контролю стану особи таку як алкогольне, або наркотичне сп'яніння, втрата свідомості внаслідок інфаркту, або інсульту, лихоманки, або стану афекту, які призводять до зміну термограми ідентифікуємої людини.. На сьогоднішній день, ця технологія є найбільш перспективною, тому що дозволяє ідентифікувати особистість з високою ймовірністю і здійснює знімання біометричних параметрів людини, що ідентифікується, безконтактним способом.

Метою даної роботи є дослідження безпеки ідентифікації за термограмою обличчя.

Основні положення. Аналізуючи ринок біометричних технологій, дослідники компаній Toshiba та BMW виявили що, ідентифікація особи за 2D та 3D зображенням обличчя, а також термограмою обличчя є досить перспективними. Використання ідентифікації за термограмою обличчя окрім функції ідентифікації особи може також проводити контроль стану користувача системи. Світовий автопром впроваджує у нові автомобілі алкозамок для запобігання керуванням автомобілем у стані сп'яніння. Наявність інфаркту, інсульту , або лихоманки у водія зараз контролюється тільки лікарем і тільки у професійних водіїв перед робочою зміною, а у протязі робочої зміни стан водія не контролюється зовсім. Протягом останнього року у країні сталося кілька ДТП внаслідок того, що водію стало зле під час керування транспортним засобом.

Для своєчасного виявлення критичного стану воді транспортного засобу може бути застосована система, що проектується для ідентифікації водія за термограмою обличчя яка може бути використана не тільки для ідентифікації особи водія, а і для безконтактного контролю його стану при керуванні автомобілем.

Висновки. Ідентифікація людини з використанням його індивідуальних біометричних характеристик є досить актуальною у системах функціональної безпеки потенційно небезпечних об'єктів.

Список літератури

1. Біометрична ідентифікація (світовий ринок). *ITRN*. URL: http://www.itrn.ru (дата звернення: 29.10.2021);

2. Особливості технології розізнання осіб toshiba. *Toshiba*. URL – http://www.toshiba.ru/products/products-for-business/sistema-raspoznavaniya-lits/ (дата звернення: 18.11.2021).

Відомості про авторів

Воронько Владислав Олегович, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, м.т. 050-95-93-859, v.voronko@student.csn.khai.edu

Желтухін Олександр Васильович, ст. викладач кафедри комп'ютерних систем, мереж і кібербезпеки, a.zheltukhin@csn.khai.edu

Секція 2

БЕЗПЕКА ТЕХНОЛОГІЇ RFID

Волобуєва Д. М.
Національний аерокосмічний університет ім. М. Е. Жуковського «ХАІ»
Науковий керівник Землянко Г. А.

Актуальність. В останні роки RFID технології набирають популярність серед крупних компаній в сфері торгівлі, транспорту, контролю доступу. Також у різних медичних системах починають активно впроваджувати дану технологію. RFID використовують для маркування лікарських препаратів та аналізів. Одночасно з цим, з'являється багато проблем з виходом з ладу цієї технології [1].

Метою роботи є дослідження безпеки сучасних RFID-міток.

Основні положення. На даний час, RFID-мітки використовують у більшості випадків для відстеження переміщення об'єктів, для контролю у системах інвентарного обліку, для захисту від крадіжок тощо.

Радіочастотна ідентифікація (Radio Frequency Identification) – це технологія, яка дозволяє ідентифікувати різноманітні об'єкти [2]. Система радіочастотної ідентифікації RFID включає в себе RFID-мітку, яка складається з мікрочіпа, де зберігається інформація, та антени, за допомогою якої передає та отримує дані. RFID-зчитувачі, необхідні для розпізнання та отримання відомостей, які переносяться у базу даних [3].

Протоколи, за якими найчастіше використовуються RFID-мітки в Україні – це ISO 14443(A), ISO 15693, ISO 18000. Перші два протоколи мають проблеми з колізією, а у останнього проблеми з зчитуванням міток.

На даний час у продажу маються різноманітні зчитувачі та записуючі прилади. RFID-мітки працюють на різноманітних частотах: 134,2 кГц (LF), 13,56 МГц (HF), 860-960 МГц (UHF) [4]. Мітки бувають активними та пасивними. Пасивна мітка працює без джерела живлення, отримуючи живлення лише за допомогою сигналу сканеру. Недолік активної мітки – для неї потрібен сканер великої потужності, вбудоване або зовнішнє живлення. Перевагами RFID-міток перед штрих-кодом є многократне змінення інформації, швидкість занесення даних та розмір [5].

В процесі роботи було розглянуто протокол EM4100 працюючий на частоті 125 кГц. У пасивній мітці як тільки зростає напруга до рівня спрацьовування, RFID-ключ передає 64 біта даних. Перевірка цілісності даних здійснюється мікроконтролером за допомогою обчислення бітів

контролю парності для кожної «строки» і «стовбця» та порівняння з отриманими даними від RFID-ключа [4, 5].

Для захисту від функційних загроз RFID-міток потрібно використовувати спеціальні захисні чохли, які блокують RFID-сигнали. Для запобігання копіювання RFID-міток можливо використання криптографії. Для більш складних пристроїв можливо використати автентифікацію методом «запит-відповідь», тобто сканер подає запит мітці, яка у свою чергу відповідає секретним цифровим ключем. Ключ можна отримати завдяки симетричній або асиметричній криптографії.

Висновки. Розглянута технологія RFID потребує доопрацювання, в зв'язку с тим, що вона не є досить безпечною в плані збереженості даних, які розташовані на мітці, також потребується переробка протоколів або створення нового. Але дана технологія може замінити штрих-коди, так як може перезаписуватись та бути скритна. Мітки вміщують набагато більше інформації в меншому розмірі, та можуть бути зчитані з більшої відстані. Через це вони можуть бути використані також для логістики.

Список літератури

1. V. Borodavka, M. Tsuranov, Biometrics: analysis and multi-criterion selection. *2018 IEEE 9th Internationa*l *Conference on Dependable Systems, Services and Technologies (DESSERT).* (дата звернення: 20.11.2021);

2. Технологія RFID – що це? *Go RFID*. URL: https://go-rfid.ru/novosti-i-statiy/novosti-tehnologiy/chto-takoe-tehnologiya-rfid (дата звернення: 02.10.2021);

3. Де застосовується RFID? *IDS*. URL: https://ids.by/index.php?option=com_content&view=article&id=14%3Agde-primenyaetsya-rfid-&catid=4%3Arfidinfo&Itemid=10 (дата звернення: 12.10.2021);

4. Радіочастотна ідентифікація (RFID): принцип роботи та застосування .*Electrik Info*. URL: http://electrik.info/device/1247-radiochastotnaya-identifikaciya-rfid.html (дата звернення: 14.10.2021);

5. Атаки на RFID. *Хабр*. URL: https://habr.com/ru/post/148663/ (дата звернення: 24.10.2021).

Відомості про авторів

Волобуєва Дар'я Михайлівна, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, м.т. 099-970-74-72, d.volobueva@student.csn.khai.edu

Землянко Георгій Андрійович, асистент кафедри комп'ютерних систем, мереж і кібербезпеки, g.zemlynko@csn.khai.edu

Секція 2

АНАЛІЗ ВРАЗЛИВОСТЕЙ SCADA-СИСТЕМ

Єлюхін Р. В.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»,
Харків, Україна
Науковий керівник Землянко Г. А.

Актуальність. Об'єм ринку SCADA-систем у 2019 році привісив 30 мільярдів доларів та, по оцінкам, буде зростати у період до 2026 року по 7.5% на рік. Такий стрімкий ріст обумовлюється широким впровадженням SCADA-систем у інфраструктуру промислового, міського та транспортного IoT. Основний попит на SCADA-системи, все також, йде від критично-важливих інфраструктур, таких як: енергетика, нафтова та газова промисловість, телекомунікації, хімічна та фармацевтична промисловості [1]. Однак з розвитком ринку розвивається і загальна кількість вразливостей, виявлених у компонентах АСУ ТП, так у 2017 році ця кількість досягала 197, а вже у 2018 році зросла до 257 виявлених вразливостей, серед яких найбільшу частку у 23% займають вразливості SCADA-систем [2]. З сучасних загроз можна відмітити атаку на українське обленерго у 2016 році, водоочисну станцію у Флориді та енергопостачання Мумбаю у 2021 році [3].

Також на даний момент не існує єдиного методу визначення рівня захищеності SCADA-систем, який би дозволяв визначати проблеми з різних сторін [4].

Метою даної роботи є виявлення слабких місць SCADA-системи та оцінки рівня її захищеності.

Основні положення. Огляд стану безпеки АСУ ТП, проведений компанією Positive Technologies показує, що кожна п'ята вразливість усувається довше за місяць. 50% вразливостей дозволяють хакеру запустити виконання коду. Для 35% вразливостей є експлойти. Серед усіх вразливостей АСУ ТП SCADA-вразливості займають найвищу долю [5].

Аналізуючи типи вразливостей SCADA-систем серед найбільш застосовуваних можна відмітити:

− Вразливості автентифікації, які зв'язані з "слабким" парольним захистом. До таких вразливостей відносять - використання стандартних інженерних паролів, встановлених виробниками на приладах промислової автоматики, використання простих паролей, зберігання паролей у відкритих джерелах.

– Вразливості програмно-апаратних компонентів, зв'язані з використанням відкритих портів системи та проведенням DoS-атаки для переповнення розміру буферів.

Висновки. Основною ціллю атаки на АСУ ТП стають SCADA-системи, тому забезпечення безпеки SCADA-систем одне із головних завдань, яке стоїть перед підприємством, в якому функціонує така система. Серед проблем захищеності SCADA-систем можна відмітити те, що для атаки зловмиснику часто не потрібно володіти складними навичками, бо серед найпоширеніших SCADA-вразливостей найбільші частки займають вразливості поганого захисту паролей. Також слід відмітити, що у більшості випадків актуального захисту від проникнення в програмне забезпечення АСУ ТП не дозволяє побудувати не відсутність інформації про вразливості ПЗ, а відсутність регламентуючої законодавчої бази, єдиних міжнародних стандартів, щоб несли обов'язковий, а не рекомендаційний характер.

Список літератури

1. A. Bhutani, P. Wadhwani. SCADA Market Size By Component, By Applic ation, Industry Analysis Report, Regional Outlook, Growth Potential, Competiti ve Market Share & Forecast, 2020 – 2026, 2020. – 160 с. *Global Market Insights.* URL – https://www.gminsights.com/industry-analysis/scada-supervisory-control-and-data-acquisition-market (дата звернення: 17.11.2021);

2. Вразливості в АСУ ТП, за 2018 рік. *Positive technologies.* URL – https://www.ptsecurity.com/ru-ru/research/analytics/ics-vulnerabilities-2019 (дата звернення: 18.11.2021);

3. Атаки за участю SCADA-систем. *SecurityLab.ru.* URL – https://www.securitylab.ru/news/tags/SCADA (дата звернення: 18.11.2021);

4. O. Syrotkina, M. Alekseyev, O. Aleksieiev. Evaluation to Determine the Efficiency for the Diagnosis Search Formation Method of Failures in Automated Systems. Eastern-European Journal of Enterprise Technologies. – 2017. – Vol. 4, Issue 9 (88). – P. 59-68. *PDF*. URL – https:// pdfs.semanticscholar.org/bde9/dab572e7cf8e57d17ee3fee344e0d51ad35c.pdf (дата звернення: 19.11.2021);

5. Сироткіна Є.І. Структурно-логічна модель діагностики відмов SCADA системи. Науковий вісник НГУ. – 2014. – № 4. – С. 52-57.

Відомості про авторів

Єлюхін Роман Валерійович, студент кафедри комп'ютерних систем, мереж і кібербезпеки, м.т. 068-756-69-94, r.yeliukhin@student.csn.khai.edu

Землянко Георгій Андрійович, асистент кафедри комп'ютерних систем, мереж і кібербезпеки. g.zemlynko@csn.khai.edu

Секція 2

БЕЗПЕКА БЕЗКОНТАКТНОЇ ОПЛАТИ

Жданкін А. В.
Національний аерокосмічний університет ім. М. Е. Жуковського «ХАІ»
Науковий керівник Землянко Г. А.

Актуальність. За останні п'ять років в Україні, як і у всьому світі, широке поширення набула технологія безконтактної оплати, що закономірно: вона спрощує процес оплати, дозволяючи використовувати для цих цілей пристрої, що носяться, такі як смарт-годинник або смартфон замість традиційної оплати пластиковою карткою. При цьому з'являється питанням: наскільки безпечно її використання.

Метою даної роботи є аналіз безпеки безконтактної форми оплати та її види і особливості.

Основні положення. Банківські картки є сьогодні поширеним платіжним засобом: переважна більшість українців (82 %) – власники банківських карток, причому за останні 11 років їхня частка зросла з 31 % до 82 %. Українці вважають технологію безконтактної оплати зручною. Ті, хто знайомий з цією технологією, частіше відзначали зручність платежів за допомогою банківської картки (80%) та смартфона (70%). Більшість людей впевнені, що оплату товарів та послуг зручно здійснювати за допомогою смарт-годинників (63%), браслетів (60%) та брелків (56%) [1].

Провівши аналіз було зрозуміло, що, наприклад, з банківською картою, що володіє тільки контактним способом оплати - зазвичай магнітна смуга та/або мікропроцесор, пластикова карта, що підтримує можливість безконтактного платежу більш вразлива [2]. Розглянувши це питання, було вирішено, що більшість переживань простих користувачів пов'язані з можливістю без підтвердження ПІН-кодом проводити так звані мікро-транзакції. Передбачається, що зловмисник, який використовує POS термінал для оплати, може зробити незаконне списання коштів з банківського рахунку без відома власника, наприклад, у громадському транспорті притулити термінал із запитом на списання до сумки чи кишені. Такий варіант розвитку подій, безумовно, можливий, проте на практиці складно реалізуємо через такі обставини: Для здійснення цієї операції необхідна невелика відстань

між платіжним терміналом та карткою – менше 10 см [3]. Завдання значно ускладняються, якщо в одному місці розташовано кілька карток з можливістю безконтактної оплати, у разі виявлення кількох карток у полі дії деякі види терміналів не здатні зробити списання коштів. Важливо розуміти, що термінал не можна так просто взяти – він має бути зареєстрований, підключений, мати доступ до Інтернету, на нього має бути відкритий рахунок, а організація, на яку відкрито рахунок, має пройти перевірку служби безпеки банку. Зловмисник може користуватися POS терміналом юридичної особи, оформленої на підставні особи, але все це, на чорному ринку, значно перевищить потенційні вигоди від цього виду шахрайства, що робить його недоцільним. Навіть у разі успішного списання коштів у законних власників їх зарахування на рахунок зловмисника відбудеться не відразу, а через кілька днів. При цьому ймовірність того, що ніхто з жертв не помітить зникнення і не звернеться до свого банку-емітенту карти, а той, у свою чергу, до банку-еквайєра з метою встановлення підозрілих операцій за рахунком, який буде після заблоковано, вкрай низька.

Висновки. Використання пристрою з одним із перелічених вище сервісів безпечніше, ніж користування звичайною карткою, що підтримує безконтактні платежі. Для виключення ймовірності несанкціонованого читання безконтактних карток можна застосувати екранування, обернувши картки фольгою або використовувати гаманець із RFID захистом.

Список літератури

1. Безконтактні платежі: повернення до готівки не буде. *Нафи*. URL: https://bit.ly/3p44ur0 (дата звернення: 14.11.2021);

2. Ідентифікаційні картки. Картки на інтегральних схемах безконтактні. Карти близької дії. Частина 1. Фізичні характеристики. *Электронный фонд ПНТД*. URL: http://docs.cntd.ru/document/1200108020 (дата звернення: 15.11.2021);

3. Як вкрасти гроші з безконтактної картки та Apple Pay. *Хабр*. URL: https://habr.com/ru/post/422551/ (дата звернення: 16.11.2021).

Відомості про авторів

Жданкін Артем Вікторович, студент кафедри комп'ютерних систем, мереж і кібербезпеки, м.т. 066-248-54-55, a.zhdankin@student.csn.khai.edu

Землянко Георгій Андрійович, асистент кафедри комп'ютерних систем, мереж і кібербезпеки, g.zemlynko@csn.khai.edu

Секція 2

ФУНКЦІЙНА БЕЗПЕКА СЕРВЕРІВ В КРИТИЧНІЙ ІНФРАСТРУКТУРІ

Кириченко Д. С.
Національний аерокосмічний університет ім. М. Е. Жуковського «ХАІ»
Науковий керівник Землянко Г. А.

Актуальність. В нинішньому світі безперебійна робота ряду високотехнологічних служб та сервісів є життєво необхідною. Захист критичної інфраструктури є важливою проблемою усіх країн. Високий рівень розвитку сучасного суспільства залежить від багатьох послуг, в значній мірі наданих приватним бізнесом. До критичної інфраструктури відносяться об'єкти, мережі, служби та системи, збій в роботі яких позначиться на здоров'ї, безпеці і добробуті громадян країни [1]. Як приклади життєво важливої матеріальної інфраструктури можна виділити мости та дороги, аеропорти, електростанції, споруди зв'язку та воєнні бази. Ці та інші види інфраструктури неможливі без комп'ютерів, серверів та мереж, представлених системами диспетчерського керування і збору даних (SCADA) [2]. За останні роки відбувся ряд атак на критичні інфраструктури, такі як трагедія 11 вересня в США та 11 березня в Мадриді, які стали поворотним пунктом в глобальній безпеці та чітко зазначили необхідність мати стратегію уникнення потенціальних загроз. Як приклад – "The European for Critical Infrastructure Protection" [1].

Метою даної роботи є виявлення загроз та вразливостей на системах критичної інфраструктури.

Основні положення. Провівши аналіз відомих атак на кіберфізичні системи, були виявлені основні загрози та найбільші вразливості критичної інфраструктури [3]. Більшість атак на інформаційну інфраструктуру відбувається віддалено. Ці атаки використовують вразливості програмного коду на підприємстві. Головні серед вразливостей – застарілі та більш вразливі системи. Приватні та державні підприємства на яких відсутні належні практики оновлення систем безпеки стають найбільш частою ціллю хакерів. Також в звітах піднімаються питання контролю над обліковими записами, такі як обмеження доступу співробітників лише до тих функцій, які необхідні їм для роботи, та видалення облікових записів після звільнення працівника. Так, за останні пів року у Європі було чотири випадки, коли звільнені працівники мали доступ до облікового запису

систем управління, наприклад – загальний аккаунт GoToMyPC використовувався для видаленого доступу до систем у позаробочий час. При атаці на державні системи, такі як залізні дороги та аеропорти, хакери використовують цілий ряд вразливостей – від можливості встановити шкідливе програмне забезпечення та злом облікових записів до халатності або низькій кваліфікації працівників [4].

Висновки. Підприємства критичної інфраструктури насьогодні мають плани та рішення стосовно забезпечення інформаційної безпеки. Використовується фізична ізоляція сервера у закритому приміщення під охороною, використання автентифікації по ключам SSH, використання технологій VPN та SSL та своєчасне оновлення програмного забезпечення. Якщо та хакерські атаки не знаходять вразливостей, необхідно проводити моніторинг вторгнень до системи для своєчасного вияву вразливостей. Звісно не тільки шкідливе ПО та хакерські атаки можуть бути загрозою системам критичної інфраструктури. Так, поломки зі сторони апаратної частини системи внаслідок несвоєчасної фізичної профілактики та заміну термопасти, пилу, зносу елементів та фізичного втручання є загрозою працездатності системи на рівні втручання сторонньої особи в систему [5].

Список літератури

1. Критична інфраструктура. *Panda Security*. URL: https://mont.com/Content/files/pad_pad360%20-%20whitepaper%20-%20критические%20инфраструктуры.pdf (дата звернення: 19.11.2021);
2. Захист критично важливої інфраструктури. *McAfee Enterprise*. URL: https://www.mcafee.com/enterprise/ru-ru/about/public-policy/critical-infrastructure.html (дата звернення: 19.11.2021);
3. Software and systems engineering — Capabilities of software safety and security verification. *Online Browsing Platform.* URL – https://www.iso.org/obp/ui/#iso:std:iso-iec:23643:ed -1:v1:en (дата звернення: 21.11.2021);
4. Віддалена атака на сервер компанії водопостачання. S*ecurityLab*. URL: https://www.securitylab.ru/news/526494.php (дата звернення: 20.11.2021);
5. Захист сервера від зламу URL: https://integrus.ru/blog/zashhita-servera-ot-vzloma.html (дата звернення: 21.11.2021).

Відомості про авторів

Кириченко Дмитро Сергійович, студент кафедри комп'ютерних систем, мереж і кібербезпеки, м.т. 073-325-95-06, d.kirichenko@student.csn.khai.edu
Землянко Георгій Андрійович, асистент кафедри комп'ютерних систем, мереж і кібербезпеки, g.zemlynko@csn.khai.edu

Секція 2

ДОСЛІДЖЕННЯ СИСТЕМИ СБОРУ ІНФОРМАЦІЇ СТАНУ СХОВИЩ БОРОШНОМЕЛЬНОГО КОМБІНАТУ.

Пилипенко І. С.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Желтухін О.В.

Актуальність. З кожним роком потреба в переробці і перевалці зернових стрімко зростає, що відбивається на кількості нових елеваторів і борошномельних комбінатів, а так само збільшення потужностей існуючих. Всі елеватори та зернопереробні підприємства, відносяться до класу підприємств з високим ступенем вибухо та пожежонебезпеки. Недотримання і порушення норм призводить до серйозних наслідків, від руйнування силосів і елеваторного обладнання, до загибелі співробітників.

Миттєве самозаймання дрібних частинок, викликане статичною електрикою або банальним перегрівом підшипника, миттєво створює тиск до 10 кг / см2, яке супроводжується різким зростанням температури до 3000С. Подібний вибух, що відбувається в будь-якому з вузлів називається «первинним пиловим вибухом» і часто він є причиною «вторинного пилового вибуху», при якому відбувається руйнування будівлі елеватора, силосів і призводить до катастрофічних наслідків [1].

З розвалом СРСР обстановка з вибухами на млинкомбінатах покращилася - в основному через те, що ці мелькомбінати масово позакривали. В цей час в США було теж не дуже - там на зернопереробному виробництві тільки в період з 1987 по 1997 рік відбулося 129 вибухів [2].

При тривалому зберіганні зерно само зігрівається, що призводить до його самозаймання, при якому в вільні обсяги силосів (бункерів) - в надсводний і підсводний простор, а також в приміщення надсилосного і підсилосного поверхів надходять горючі газоподібні продукти термоокислительной деструкції: водень, метан, оксид вуглецю в концентраціях, що перевищують значення нижніхконцентраційних меж поширення полум'я (НКПР) цих газів (значення НКПР,% об .: H2 - 4,08; CH4 - 5,24; CO - 12,50) [3].

Метою даної роботи є дослідження безпеки системи збору і передачі інформації на вибухонебезпечних виробництвах.

Основні положення. В ході даної розробки необхідно реалізувати систему збору інформації про наповненість, та стан сховищ готової продукції, та сировини борошномельного комбінату, або іншого подібного за масштабами промислового підприємства. Дана система повинна забезпечити: оперативність передачі даних, визначення місця розташування сховища на території підприємства, ефективне використання наявних вимірювальних приладів, значною мірою скорочення кількості обслуговуючого персоналу, у зв'язку з автоматизацією процесу контролю стану сховищ, контроль цілісності контактної мережі.

Для вирішення поставленого завдання необхідно: обґрунтувати і вибрати спосіб передачі інформації, обґрунтувати і вибрати дротову, або бездротову технологію передачі інформації, обґрунтувати і вибрати тип інформаційної мережі для передачі інформації.

Висновки. Розробка безпечної високоефективної системі збору і передачі інформації про стан об’єктів вибухонебезпечних є досить актуальною у сучасному світі для поліпшення безпеки виробництва на потенційно небезпечних підприємствах.

Список літератури

1. Вибухи на елеваторах - їх можна уникнути! *Зернова Столиця.* URL: https://zeo.ua/press-center/bez-rubriki/vzryivyi-na-elevatorax. (дата звернення: 19.10.2021);
2. Взрывающиеся мельницы! *Disgustingmen*. URL: https://disgustingmen.com/history/vzryvayushhiesya-melnitsy/. (дата звернення: 20.10.2021);
3. Вопросы пожарной безопасности на объектах хранения, переработки и использования растительного сырья. *Ervist*. URL: http://www.ervist.ru/stati/voprosy-obespecheniya-pozharnoy-bezopasnosti-na-obektah-hraneniya-pererabotki-i-ispolzovaniya-rastitel.html (дата звернення: 21.10.2021).

Відомості про авторів

Пилипенко Ігор Станіславович, магістрант кафедри комп’ютерних систем, мереж і кібербезпеки, м.т. 093-628-04-64, i.pilipenko@student.csn.khai.edu

Желтухін Олександр Васильович, ст. викладач кафедри комп’ютерних систем, мереж і кібербезпеки, a.zheltukhin@csn.khai.edu

Секція 2

АВТЕНТИФІКАЦІЯ КОРИСТУВАЧІВ НА ОСНОВІ СТІЙКОГО КЛАВІАТУРНОГО ПОЧЕРКУ

Резніков А.О.
Національний аерокосмічний університет ім. М. Е. Жуковського «ХАІ»
Науковий керівник Землянко Г.А.

Актуальність. З розвитком мережевих ресурсів та появою великої кількості мережевих сервісів, гостро постало завдання автентифікації та ідентифікації користувачів. Як відомо, правоохоронці тривалий час працюють успішно з одним із типів поведінкових біометричних даних — рукописним почерком. Висота, довжина, кути букв — це повний перелік характеристик, якими можна ідентифікувати людини, який написав той чи інший текст [1].

Проте прогрес не стоїть на місці, і глобальна інформатизація ознаменувала перехід до нового суспільства – інформаційного. Те, що робилося вручну або механічно, почало здійснюватися автоматично за участю оператора. Проте робота людини і машини аналогічно характеризується поведінковими біометричними даними. Одними з таких характеристик є біометричні характеристики введення з тексту клавіатури, інакше кажучи, клавіатурний почерк.

Метою даної роботи є дослідження процесу автентифікації користувачів за допомогою стійкого клавіатурного почерку.

Основні положення. Можливість автентифікувати клавіатурний почерк людини з'являється при введенні парольної фрази, що складається з достатньо великої кількості букв. Клавіатурний почерк, також званий ритмом друкування, відображає спосіб друкування користувачем тієї або іншої фрази. Це зумовлено тим, що кожна людина набирає текст на клавіатурі по-різному, тому за певними характеристиках можна ідентифікувати користувача з досить високою точністю [2]. Головний недолік використання клавіатурного почерку для ідентифікації особи – тимчасова зміна почерку у користувачів під впливом стресових ситуацій, яке може призвести до відмови в доступі людині, що має на це право [3].

Метод роботи системи складається з кількох етапів. Для реєстрації користувач вводить спеціальний та персональний текст із клавіатури. Система аналізу отримує дані про підкреслення користувача. Отримані дані зберігаються у базі, подальшим завданням якої є автентифікувати

оператора, виходячи з наявного масиву даних [4]. У перспективі розглядається розробка системи, що діє за даним алгоритмом, а також запровадження аналізу характеристик маніпулятора «миша».

У ході перших експериментів із цією системою участь взяли п’ять піддослідних. Завдання кожного оператора було ввести п'ять разів фразу «У хащах півдня жив би цитрус? Так, але фальшивий екземпляр!» [4]. Подальше завдання – аналіз кореляції певної тривалості: скільки разів зустрічається та чи інша тривалість введення з урахуванням похибки 30 мс. Ці значення прийняті за індивідуальну характеристику оператора. При тестуванні на 200 мс виявлено велику кількість збігів. Це можна пояснити досвідченістю операторів. Для подальшого розвитку системи варто відзначити цей факт і розглядати часові показники з більш точним фільтром.

Висновки. Таким чином, підбиваючи підсумки, можна відзначити, що найпростішим, а також надійним, за дотримання певних вимог, і найбільш популярним засобом автентифікації в даний момент є пароль. Однак прогрес не стоїть на місці, і, можливо, пароль як такий поступиться місцем іншим засобам автентифікації, які не будуть мати таких істотних недоліків, як його втрата або зберігання в доступному місці, записаному на будь-що. І сам процес автентифікації відбуватиметься непомітно для користувача.

Список літератури

1. Ross, A. An introduction to biometric systems [Text]/ A. Ross, A.K. Jain, S. Prabhakar // *IEEE Trans Circuits Syst Video Technol*. – 2004. – №14. – P. 4–20

2. Трушіна Є.А. Ідентифікація користувача ЕОМ за клавіатурним почерком, як метод захисту від несанкціонованого доступу [Текст]. – 1997. – 27 с.

3. Мартинова, Л.Є. Дослідження та порівняльний аналіз методів автентифікації [Текст]/ Л. Є. Мартинова, М.Ю. Умніцин, К.Є. Назарова // *Молодий вчений*. - 2016. - № 19. - С. 90-93

4. Ложников, П.С. Автентифікація користувачів комп'ютера по клавіатурного почерку і особливостям особи [Текст]/ П.С. Ложников, А.Е. Сулавко, Е.В. Бура // *Питання кібербезпеки*. - 2017. - № 4. - С. 24-34.

Відомості про авторів

Резніков Андрій Олександрович, студент кафедри комп’ютерних систем, мереж і кібербезпеки, м.т. 097-541-86-08, a.reznikov@student.csn.khai.edu
Землянко Георгій Андрійович, асистент кафедри комп’ютерних систем, мереж і кібербезпеки, g.zemlynko@csn.khai.edu

АЛФАВІТНИЙ ВКАЗІВНИК

ЗМІСТ

СТУДЕНТСЬКА КОНФЕРЕНЦІЯ
ІНФОРМАЦІЙНА, ФУНКЦІЙНА і КІБЕРБЕЗПЕКА
СКІФіК

Відповідальний за випуск М.В. Цуранов

Підписано до друку: 29.11.2021
Формат 60×84 1/16. Папір офіс. №2. Офс. Друк
Ум. друк. арк. 3,89. Обл.-вид. арк. 4,08. Наклад 100пр.
Замовлення 88. Ціна вільна

Віддруковано ФОП Лисенко І.Б.
61070, Харків – 70, вул. Чкалова, 17, моторник корпус, к. 147.
Свідоцтво про внесення суб'єкта видавничої справи до державного реєстру видавців, виготовлювачів і розповсюджувачів ДКК №2607 від 11.09.06 р.