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 третьої
науково-технічної конференції

30 листопада, 1 грудня 2023 року

ХАРКІВ - 2023

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 третьої
науково-технічної конференції
30 листопада, 1 грудня 2023 року

Харків 2023

УДК 004.056
С 88

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

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ КОНФЕРЕНЦІЇ

Співголови оргкомітету:

ХАРЧЕНКО В'ячеслав Сергійович (д.т.н., проф., кафедра комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», Харків, Україна);

ЮДІН Олесь Вікторович (аспірант кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», Харків, Україна).

Члени оргкомітету:

ПЄВНЄВ Володимир Яковлевич (д.т.н., доцент, кафедра комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ»);

ЗЕМЛЯНКО Георгій Андрійович (аспірант, кафедра комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ»);

ШИПУНОВ Микита Юрійович (магістрант 565-іМ групи, кафедра комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ»);

СЕЛІВАНОВА Марія Олександрівна (магістрантка 555-іМ групи, кафедра комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ»);

СТАЦИШИНА Ірина Павлівна (магістрантка 555-іМ групи, кафедра комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ»);

ПРОЦЕНКО Єгор Сергійович (студент 545-і групи, кафедра комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ»).

С 88 Студентська конференція інформаційна, функційна і кібербезпека СКІФіК : матеріали третьої науково-технічної конференції 30 листопада, 1 грудня 2023 року. – Харків: ФОП Бровін О.В., 2023. – 130 с.
ISBN 978-617-8238-26-1

©Національний аерокосмічний університет ім. М.Є. Жуковського «Харківський авіаційний інститут», Харків, Україна, 2023

ПЛАН ПЕРШОГО ДНЯ КОНФЕРЕНЦІЇ

30 листопада 2023 року, Час: 15:00 – 19:00, онлайн		
15:00 – 15:10	Вітальне слово	
15:10 – 15:20	Вітальне слово спонсора конференції «Харківський ІТ Кластер».	
15:20 – 15:45	Виступ аспірантки кафедри 503, НАУ «ХАІ»; Software Developer, Grid Dynamics, Веприцької Олени Юріївни Тема: Систематизація варіантів застосування штучного інтелекту в контексті кібербезпеки	
15:45 – 15:50	Перерва	
15:50 – 18:30	**Секція 1**	**Секція 2**
	Інформаційна безпека	Функційна безпека
	https://meet.google.com/viy-wshy-ssg	https://meet.google.com/fky-yioa-fkh
18:45 – 19:00	Обговорення результатів роботи секцій	

ПЛАН ДРУГОГО ДНЯ КОНФЕРЕНЦІЇ

1 грудня 2023 року, Час: 15:00 – 19:00, онлайн		
15:00 – 15:05	Оголошення Оргкомітету	
15:05 – 15:10	Вітальне слово спонсора конференції «Distributed Lab»	
15:10 – 15:30	Виступ дослідника Distributed Lab, Дениса Рябцева Тема: Zero Knowledge Proof	
15:30 – 15:35	Перерва	
15:35 – 18:30	**Секція 1**	**Секція 2**
	Інформаційна безпека	Функційна безпека
	https://meet.google.com/viy-wshy-ssg	https://meet.google.com/fky-yioa-fkh
18:30 – 18:45	Перерва	
18:45 – 19:00	Підсумкове пленарне засідання	

ПРОГРАМА КОНФЕРЕНЦІЇ

30 листопада, 1 грудня 2023 року, Онлайн формат

Відкриття конференції, привітання учасників організаторами конференції та запрошеними гостями

Пленарні доповіді:

Аспірантка кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», **Веприцька Олена Юріївна**. Тема доповіді: «Систематизація варіантів застосування штучного інтелекту в контексті кібербезпеки».

Дослідник Distributed Lab, **Денис Рябцев**. Тема доповіді: «Zero Knowledge Proof».

Секція 1. Інформаційна безпека
Посилання: https://meet.google.com/viy-wshy-ssg
Модератор: Юдін Олесь Вікторович
Спів модератори: Стацишина Ірина Павлівна, Проценко Єгор Сергійович

Секція 2. Функційна безпека
Посилання: https://meet.google.com/fky-yioa-fkh
Модератор: Землянко Георгій Андрійович
Спів модератор: Селіванова Марія Олександрівна, Шипунов Микита Юрійович

ТЕЗИ ДОПОВІДЕЙ

Секція 1. Інформаційна безпека

Секція 1

ПЕРСОНАЛЬНА КІБЕРБЕЗПЕКА

Андренко К. В.
Харківський національний університет імені В. Н. Каразіна
Науковий керівник: Філатова Л. Д.

Актуальність. Проблема персональної кібербезпеки є надзвичайно актуальною в сучасному цифровому світі. З кожним днем все більше людей користується інтернетом і цифровими пристроями в своєму повсякденному житті. Смартфони, планшети, комп'ютери використовуються для спілкування, роботи, фінансових операцій та зберігання особистої інформації. Однак, разом з цим вдосконалюються і методи та техніки кіберзлочинності [1]. Несанкціонований доступ до наших особистих даних, викрадення фінансових ресурсів, фішингові атаки та інші види шахрайства стрімко поширюються і спричиняють серйозні наслідки.

Мета. Мета персональної кібербезпеки полягає у забезпеченні захисту особистих даних, приватності та цифрового життя кожного користувача. Вона спрямована на запобігання кібератак, крадіжки ідентичності, фінансових втрат, та інших негативних наслідків, пов'язаних з кіберзагрозами.

Основні положення. Забезпечити персональну кібербезпеку допоможе низка простих заходів: регулярне оновлення програмного забезпечення, антивірусного захисту тощо. Персональна кібербезпека включає усвідомлення загроз, використання сильних та унікальних паролів, актуалізацію програмного забезпечення, обережність при відкриванні посилань та вкладень електронної пошти, обмеження розголошення особистої інформації, безпечне підключення до мереж Wi-Fi, використання двох факторної аутентифікації, регулярне створення резервних копій даних, освіту щодо кібербезпеки та використання захисних програм [2].

Усвідомлення загроз передбачає розуміння різних типів кіберзагроз, таких як фішинг, шкідливе програмне забезпечення, соціальний інжиніринг тощо. Використання сильних та унікальних паролів є важливим аспектом персональної кібербезпеки. Рекомендується використовувати паролі, які складаються з комбінації великих і малих літер, цифр та спеціальних символів. Крім того, важливо мати окремий пароль для кожного облікового запису. Актуалізація програмного забезпечення є необхідною, оскільки виробники регулярно випускають оновлення, які виправляють виявлені вразливості. Регулярне оновлення програмного забезпечення допомагає забезпечити оптимальний рівень безпеки. При

відкриванні посилань та вкладень електронної пошти важливо бути обережним. Необхідно перевіряти посилання на достовірність та впевнитися, що вони не містять шкідливого вмісту або фішингових спроб. Обмеження розголошення особистої інформації є важливим аспектом персональної кібербезпеки. Необхідно оберігати конфіденційну інформацію, таку як паролі, номери соціального страхування, фінансові дані тощо. Безпечне підключення до мереж Wi-Fi включає використання захищених мереж з шифруванням WPA2 або WPA3. Використання ненадійних або відкритих мереж може призвести до несанкціонованого доступу ваших особистих даних.

Висновок. Забезпечення персональної кібербезпеки є надзвичайно важливим. Розуміння загроз, використання сильних паролів, актуалізація програмного забезпечення, обережність при відкриванні посилань та вкладень, обмеження розголошення особистих даних, безпечне підключення до мережі та інші заходи допоможуть зменшити ризики стати жертвою кіберзлочинів.

Список літератури

1. Information security, Cybersecurity and the IEC 62443 series of standards. *Instytut Kształcenia Menadżerów Jakości*. URL – https://ikmj.com/en/information-security-cybersecurity-and-the-iec-62443-series-of-standards (дата звернення: 30.10.2023);
2. Безпека ваших пристроїв. *Довідка.info*. URL: https://dovidka.info/kiberbezpeka (дата звернення: 31.10.2023).

Відомості про авторів

Андренко Катерина Віталіївна, студентка 3 курсу, ННІ «Каразінський банківський інститут» ХНУ ім. В.Н. Каразіна, andrenko2021.9511523@student.karazin.ua
Філатова Любов Дмитрівна, доцент кафедри інформаційних технологій та математичного моделювання, ННІ «Каразінський банківський інститут» ХНУ ім. В.Н. Каразіна, к. ф.-м. н., доцент, liubov.filatova@karazin.ua

Секція 1

ПОРІВНЯЛЬНИЙ АНАЛІЗ МЕТОДІВ ШИФРУВАННЯ ДАНИХ

Абрамова В. Д.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Брежнєв Є. В.

Актуальність порівняльного аналізу методів шифрування даних зберігається через постійний розвиток технологій і необхідність забезпечення безпеки інформації та захисту від нових загроз. Кіберзагрози та методи злому вимагають від методів шифрування адаптації до нових умов. Комплексна система захисту інформації вимагає виявлення раціональної комбінації методів захисту для зниження ризиків кібербезпеки.

Метою порівняльного аналізу методів шифрування даних є виявлення відповідного методу для забезпечення необхідного рівня захисту інформації при оптимальній потужності та дотриманням вимог безпеки.

Основні положення. Існує декілька основних методів шифрування даних які мають свої переваги та недоліки. Симетричне шифрування – це метод, коли один ключ використовується як для шифрування, так і для розшифрування даних [1]. Перевага метода – швидке шифрування, тож він підходить для роботи з великим обсягом інформації. Недоліком є необхідність вирішення проблеми безпечної передачі ключа та неможливість використовування в ЕЦП через відомість ключа для обох сторін. Приклади: AES (Advanced Encryption Standard), DES (Data Encryption Standard). Асиметричне шифрування – для шифрування даних використовують відкритий ключ, а для розшифровування – закритий [2]. Розшифрування відбувається тільки за допомогою закритого ключа. Цей ключ не може бути визначеним з ключа зашифровування. Перевагою є забезпечення високого рівня безпеки та зручність обміну ключами, але при роботі з невеликим обсягом даних – є менш продуктивним. Приклади: RSA, ECC. Хешування – перетворення вхідного масиву даних довільної довжини у вихідний бітовий рядок фіксованої довжини (хеш-функцію) [3]. Використовується тільки для перевірки цілісності даних через необоротність перетворення. Приклади: SHA-256, MD5. Гібридне шифрування – комбінація симетричного та асиметричного шифрування для забезпечення безпеки обміну ключами та ефективності шифрування [4]. Симетричний ключ використовується для шифрування даних, а асиметричний для шифрування самого симетричного ключа. Недолік - Може вимагати більше обчислювальних ресурсів. Квантове шифрування – цей метод використовується для передачі ключа симетричного шифрування [5]. Він заснований на принципах квантової фізики, що забезпечує високий рівень захисту від злому за допомогою квантових

обчислень. Перевагою методу є можливість виявлення втручання до процесу квантового розподілу ключа, але на даний час передача неможлива на великі відстані.

В роботі виконаний порівняльний аналіз таких методів шифрування даних: AES, DES, RSA, ECC SHA-256, MD5, гібридне шифрування, квантове шифрування. Були висвітлені їх переваги, недоліки та принципи використання.

Висновки. Розвиток технологій зумовлює збільшення обсягів оброблюваних даних, які треба захистити та появу нових методів шифрування. Отже, порівняльний аналіз методів шифрування даних залишається вкрай важливими для підтримки безпеки інформації, захисту від нових загроз та підтримання актуальності в галузі криптографії. Для вибору необхідного методу шифрування пропонується використовувати їх показники щодо рівня безпеки, швидкості роботи, контексту застосування та дотримання галузевих стандартів та нормативних вимог.

Список літератури

1. Hlynchuk L., Hryshanovych T., Stupin A. (2021). Реалізація стандарту симетричного шифрування DES мовою програмування C та порівняння часу його роботи з відомими утилітами. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(14), 118–130. DOI: https://doi.org/10.28925/2663-4023.2021.14.118130;
2. Що таке шифрування та як воно працює? *Kingston Technology*. URL: https://www.kingston.com/ua/blog/data-security/what-is-encryption (дата звернення: 10.11.2023);
3. Hash функції. *Medium*. URL: https://medium.com/techmaker/hash-функції-90bf2be2af1e (дата звернення: 09.11.2023);
4. Воробйов В.Г. Теоретичні основи побудови гібридних криптографічних систем захисту інформації. Сучасні Інформаційні Технології / 4. Інформаційна безпека. URL: https://www.rusnauka.com/18_NPRT_2017/Informatica/4_227128.doc.htm (дата звернення: 10.11.2023);
5. Квантова криптографія. *Енциклопедія сучасної України*. URL: https://esu.com.ua/article-11921 (дата звернення: 11.11.2023);

Відомості про авторів

Абрамова Валерія Денисівна, студентка кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», v.d.abramova@student.csn.khai.edu
Брежнєв Євген Віталійович, професор кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», д.т.н., старший науковий співробітник, e.brezhnev@csn.khai.edu

Секція 1

КІБЕРБЕЗПЕКА У БІЗНЕСІ: ВІДНОВЛЕННЯ ПІСЛЯ КІБЕРАТАК

Азманов І. П.
Національний університет «Запорізька політехніка»
Науковий керівник: Зайко Т. А.

Актуальність. У наш час, коли технологічний прогрес проникає в усі сфери життя, питання кібербезпеки набувають особливої важливості. Загрози з боку кіберзлочинців стають все більш витонченими, вимагаючи постійної уваги до захисту даних та інформаційних ресурсів. Без належного захисту, організації та приватні особи можуть опинитися під загрозою серйозних наслідків, починаючи від фінансових втрат до втрати довіри.

Мета роботи. Вивчення та узагальнення ключових аспектів відновлення бізнесу після кібератак для забезпечення надійної кібербезпеки.

Основні положення. Кібербезпека відіграє ключову роль у захисті від безлічі загроз, включаючи віруси, фішинг, шкідливе програмне забезпечення, DDoS-атаки та різні кіберризики. Ці вразливості часто виникають через слабке програмне забезпечення, мережеві налаштування та людські помилки, створюючи потенційні точки входу для зловмисників [1].

Для сучасного підприємства неодмінно необхідна надійна система кібербезпеки. Її роль одна з найголовніших, адже вона виступає охоронцем цілісності даних, гарантуючи конфіденційність як для клієнтів, так і для компанії. Ба більше, вона забезпечує безперервність бізнес-процесів, запобігаючи неприємним збоям у критично важливих операціях. При цьому, не забуває стежити за дотриманням усіх необхідних норм і стандартів, що стосуються безпеки даних.

Однак варто пам'ятати, що втрата важливих даних, фінансові труднощі, шкода репутації, юридичні складнощі, а також потреба в додаткових ресурсах для відновлення і зміцнення бізнесу – усі ці фактори являють собою довгострокові наслідки кібератак [2]. Недостатня увага до цього питання може мати вкрай серйозні наслідки, аж до припинення діяльності компанії.

Важливо посилити засоби захисту, запобігаючи майбутнім інцидентам. Оновлення програмного забезпечення, впровадження нових технологій і моніторингу загроз – без виконання цих дій ви ризикуєте знову бути скомпроментованими [4].

Не менш важливою складовою є прозоре спілкування із зацікавленими сторонами – клієнтами, партнерами та регулюючими органами. Надавши всебічну інформаційну підтримку, ми демонструємо відповідальний підхід до забезпечення кібербезпеки і прагнемо до відновлення довіри.

Додатково, рекомендується провести аудит поточних кібербезпек. Це включає в себе перевірку всіх систем і мереж на предмет вразливостей, а також оцінку ефективності наявних заходів захисту. Результати аудиту допоможуть точково поліпшити системи безпеки і запобігти аналогічним інцидентам у майбутньому.

Необхідно також навчити співробітників основ кібербезпеки. Регулярні тренінги та тестування допоможуть підвищити обізнаність співробітників про можливі загрози та правила безпечної поведінки в мережі. Долучення співробітників до процесу забезпечення кібербезпеки створить додатковий рівень захисту.

Висновки. Під час мого дослідження я заглибився у вивчення ключових аспектів відновлення бізнесу після кібератак з метою забезпечення надійної кібербезпеки. Розглянувши різні види кібератак, я усвідомив, наскільки серйозною загрозою вони можуть бути для бізнесу. Розроблений алгоритм дій після кібератаки, починаючи з аналізу ситуації та закінчуючи впровадженням проактивних заходів із забезпечення безпеки, стає невід'ємною частиною стратегії забезпечення кібербезпеки. Моє дослідження підкреслює важливість готовності до інцидентів і доводить, що комплексний і систематичний підхід до відновлення бізнесу після кібератак є фундаментальним елементом забезпечення надійної кібербезпеки.

Список літератури

1. Cybersecurity Essentials (1st Edition) / [Charles J. Brooks, Christopher Grow, Philip A. Craig Jr.]. – Canada, 2018. – 591 p.;
2. Кібератака — Що Це Таке І Які Її Наслідки?. *Biz.* URL: https://biz.nv.ua/ukr/experts/kiberataka-shcho-ce-take-i-yaki-jiji-naslidki-50036682.html (дата звернення: 12.10.23);
3. Що таке кібератака? | Захисний комплекс Microsoft. *Microsoft.* URL: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-a-cyberattack (дата звернення: 13.10.23);
4. Cybercrime Aftermath: How to Recover From a Cyber Attack? *Embroker.* URL – https://www.embroker.com/blog/how-to-recover-from-a-cyber-attack/ (дата звернення: 15.10.23).

Відомості про авторів

Азманов Ілля Павлович, студент кафедри програмних засобів, Національний університет «Запорізька політехніка», azmanoff20@gmail.com
Зайко Тетяна Анатоліївна, доцент кафедри програмних засобів, Національний університет «Запорізька політехніка», к.т.н., доцент, nika270202@gmail.com

Секція 1

РОЗРОБКА ПОЛІТИКИ БЕЗПЕКИ ВЕБ САЙТУ

Акчурін М. О.
Національний аерокосмічний університет ім. М.Є. Жуковського «ХАІ»
Науковий керівник: Годунов О. С.

Актуальність. Стійкість до кіберзагроз та атак: Загрозами можуть бути атаки на авторизацію, витік особистих даних користувачів, DDoS-атаки, злами, а також можливість втрати чи порушення цілісності даних. Зростаюча кількість користувачів та їх очікування: Користувачі очікують, що їхні дані будуть захищені та матимуть високий рівень конфіденційності. Регулярні вимоги: Законодавство щодо захисту персональних даних (GDPR, CCPA та ін.) накладає строгі вимоги на зберігання, обробку та захист особистої інформації.

Розвиток нових технологій та стандартів безпеки: Постійний розвиток цифрових технологій означає необхідність постійного оновлення підходів до захисту.

Поява нових стандартів безпеки та методів аутентифікації потребує постійного вдосконалення політики безпеки.

Мета. Створення системи захисту конфіденційності та особистих даних користувачів, цілісності інформації в інтернет магазині, а також запобігання несанкціонованому доступу та втраті цих даних.

Основні положення. У доповіді розглянуто JWT токени та їх безпека:

1. Створення безпечних токенів: Використання надійних механізмів створення та перевірки JWT токенів для авторизації користувачів та забезпечення їхньої безпеки під час передачі та зберігання.
2. Встановлення строку дії токенів: Обмеження терміну дії токенів для зменшення ризику злому через втрату чи крадіжку.

У доповіді наведені протокол авторизації через Google OAuth та методи аутентифікації та авторизації

Протокол авторизації через Google OAuth 2.0:

1. Керування доступом до даних: Захист від несанкціонованого доступу до даних користувачів, використовуючи протокол OAuth 2.0 для сторонньої авторизації через Google та інші платформи.
2. Безпека взаємодії з Google API: Забезпечення безпеки під час взаємодії з API Google через OAuth 2.0 протокол.

У доповіді особливу увагу надано питанням забезпечення аутентифікації та авторизації. Розглянути вимоги до створення до цих складових забезпечення безпеки.

1. Складність паролів та двофакторна аутентифікація: Встановлення вимог до складності паролів, використання двофакторної аутентифікації, обмеження прав доступу та впровадження аудиту активності користувачів.

2. Обмеження прав доступу: Встановлення привілеїв доступу залежно від ролі користувача для мінімізації ризику несанкціонованого доступу до важливих функцій магазину чи даних.

У доповіді наводяться вимоги до проведення моніторингу та реагування на можливі порушення та шкідливі події. Постійний моніторинг активності, виявлення потенційних порушень безпеки та швидка реакція на них.

Висновки. Безпека інтернет-магазину є основною складовою успіху та довіри користувачів. Захист конфіденційної інформації, цілісності даних та доступності сервісів для легітимних користувачів є вельми важливим.

Основними принципами безпеки є: Комплексний захист даних: Розробка та впровадження стратегії захисту, яка охоплює всі аспекти обробки даних від створення та передачі токенів до зберігання особистої інформації. Застосування найкращих практик забезпечення безпеки відповідно до стандартів безпеки даних.

Системи аутентифікації та авторизації: Впровадження сильних механізмів аутентифікації та авторизації, що включають надійні паролі, двофакторну аутентифікацію та обмеження прав доступу для запобігання несанкціонованому використанню системи.

Валідація та безпека JWT токенів та протоколу OAuth 2.0: Постійна перевірка цілісності та безпеки JWT токенів, а також впровадження механізмів безпеки при використанні протоколу OAuth 2.0 для стороннього авторизації через Google та інші платформи.

Моніторинг та реагування: Постійний моніторинг системи для вчасного виявлення аномальних активностей та швидкої реакції на потенційні загрози для запобігання втрати даних або порушень безпеки.

Успішна реалізація цих принципів дозволить інтернет-магазину забезпечити надійний захист особистих даних користувачів, підвищити рівень довіри споживачів та забезпечити стабільну та безпечну роботу платформи. Такий підхід до безпеки є важливим у світі, де загрози кібербезпеки постійно зростають.

Список літератури

1. Стандарт GDPR. *GDPR.* URL: https://gdpr-text.com/uk (дата звернення: 10.11.2023);
2. Стандарт OAuth 2.0. *Oauth.* URL: https://oauth.net/2 (дата звернення: 10.11.2023);
3. Рекомендації щодо безпеки веб-додатків. *OWASP*. URL: https://owasp.org (дата звернення: 10.11.2023).

Відомості про авторів

Акчурін Максим Олександрович, студент кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», m.akchurin@student.csn.khai.edu
Годунов Олександр Сергійович, ст. викладач кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», a.godunov@csn.khai.edu

Секція 1

АНАЛІЗ ЗАХИСТУ ПЛАТІЖНОЇ СИСТЕМИ GOOGLE PAY

Бейник А. О.
Національний Університет «Запорізька Політехніка»
Науковий керівник: Зайко Т. А.

Актуальність. Тенденція діджиталізації також поширилась і на сферу банкінгу. Майже кожен власник смартфону з чипом NFC має доступ до безконтактних платіжних систем таких як: Apple Pay, Google Pay та Easy Pay. Для своєї роботи системам необхідно отримати конфіденційні дані банківських карток. Але наскільки такі дані знаходяться під захистом? Для аналізу було обрано додаток Google Гаманець, що працює на основі системи Google Pay так як він налічує понад 500 мільйонів завантажень.

Метою даної роботи є аналіз існуючих засобів захисту в платіжній системі Google Pay.

Основні положення. Першим та найголовнішим ключем до захисту даних є токенізація. Імплементація цього процесу полягає в декількох етапах:

– Зберігання даних картки за допомогою технології HCE (Host Card emulation)
– При додаванні картки створюється віртуальний номер акаунту, що зберігається на серверах Гугл
– Під час транзакції, Google Pay створює тимчасовий одноразовий токен, що репрезентує користувацький віртуальний акаунт
– Цей токен далі відправляється на Гугл Сервер, де токен має збігатися з зашифрованими даними і далі передано банку, що робить Google посередником в процесі транзакції [1].

Другий засіб – це захист телефону паролем, пін-кодом або біометрією. Для використання Google гаманця ви повинні захистити телефон одним з вище перерахованих методів, так для того щоб провести транзакцію користувач має пройти захист телефону. Якщо прибрати захист з телефона, що має платіжні карти в Google гаманці, вони всі автоматично видаляються.

Ще одним методом захисту, що використовується Google гаманцем є верифікація картки. Коли користувач додає нову картку або ж було помічено підозрілу активність, необхідно підтвердити свою особистість. Верифікація може відбуватися різними шляхам [2]:

– надсилання коду для підтвердження на пошту або за номером телефону;
– повідомлення коду за дзвінком;
– через банківський додаток або веб-сайт;

– надсилання коду зі списанням з картки.

Окрім безпеки на пристрої Google також забезпечує захист на серверах завдяки використання протоколів безпеки. Наприклад:

– Encryption in transit (захищає дані при транспортуванні, розшифровуючи їх після налагодження зв'язку з серверами та автентифікацією, перевіряю недоторкіність);

– Encryption at rest (захищає дані під час зберігання на серверах);

Також Google Pay відповідає двом найважливішим захисними вимогам:

– PCI DSS – сукупність 12 вимог до компаній, щодо забезпечення безпеки даних платіжних карток, які передаються, зберігаються й обробляються;

– SCA – забезпечення безпеки електронних платежів, завдяки використання багатофакторної автентифікація.

Висновки. Google Pay використовує багатошарову систему безпеки та протоколів аби надійно захистити платіжні дані своїх користувачів. Але завжди варто пам'ятати, про захист вашого смартфону такий як використання надійного паролю, так як з наявністю пристрою з примітивним паролем зловмисник може з легкістю отримати доступ до ваших коштів..

Список літератури

1. A Deep Dive into Google Pay and Apple Pay. *Medium.* URL – https://medium.com/mobilepeople/a-deep-dive-into-google-pay-and-apple-pay-d56dab7194a0 (дата звернення: 13.11.2023);

2. Is Google Pay Safe? Here's How Google Protects Your Payments. *Getmoss.* URL – https://www.getmoss.com/guide/en/is-google-pay-safe/ (дата звернення: 13.11.2023).

Відомості про авторів

Бейник Анастасія Олексіївна, студентка кафедри програмних засобів, Нціональний університет «Запорізька Політехніка», abeynik21@gmail.com

Зайко Тетяна Анатоліївна, доцент кафедри програмних засобів, Національний університет «Запорізька Політехніка», к.т.н., доцент, nika270202@gmail.com

Секція 1

ЗАХИСТ КОНФІДЕНЦІЙНИХ ДАНИХ У СНЕПШОТАХ EBS

Бригинець А. А.
Державний університет інформаційно-комунікаційних технологій
Науковий керівник: Гайдур Г. І.

Актуальність. Amazon Web Services (AWS) надає потужну платформу для хмарних обчислень з численними функціями та послугами. Однією з таких послуг є снепшоти Elastic Block Store (EBS), яка дозволяє створювати та зберігати томи даних для віртуальних машин інстансів EC2.

Снепшоти EBS представляють собою знімки цих томів, які можна створювати для забезпечення резервного копіювання даних, відновлення до попередніх станів і обміну даними між регіонами та обліковими записами AWS. Однак неуважне керування снепшотами може призвести до серйозних проблем безпеки та витоку конфіденційних даних.

У 2018 році компанія Duo Security опублікувала статтю, в якій йдеться про те, що вони знайшли 116 386 загальнодоступних снепшотів EBS з 3 213 облікових записів [1]. На конференції DEFCON 27 (2019) Бен Морріс представив дослідження про загальнодоступні обсяги EBS, в якому він підтвердив 50 витоків даних і оцінив загальну кількість вразливостей у 750-1250 шт. у всіх регіонах AWS. При цьому витоку постраждав широкий перелік галузей, включно з великими компаніями у сфері технологій та охорони здоров'я. Витік даних включав несанкціонований доступ до вихідного коду, приватні SSH-ключі, персональні дані та паролі, а також інші різноманітні форми облікових даних [2].

Метою цієї роботи є підвищення безпеки використання AWS через конкретні заходи. Зроблено акцент на розгляді безпеки AWS, зосереджуючись на загрозах публічних снепшотів EBS. Надання рекомендацій щодо моніторингу снепшотів, зміни дозволів та політики конфіденційності.

Основні положення. При створенні образу машини Amazon Machine Image (AMI) з інстансу EC2 та використанні Amazon Elastic Block Store (EBS), AWS автоматично створює снепшоти прикріплених до інстансу томів EBS, які асоціюються з AMI. Снепшоти EBS служать для швидкого відновлення томів до попереднього стану та можуть бути використані для передачі даних між регіонами та обліковими записами AWS.

Такі процеси часто можуть нести загрозу для конфіденційності даних, адже снепшоти віртуальних машин можуть містити дані такого типу. У разі, якщо снепшот буде завантажено у відкритий доступ з налаштованим пунктом «Публічний», то будь-хто охочий зможе монтувати такий снепшот і отримати доступ до інформації.

У гіпотетичному сценарії експлуатації вразливості, атакуюча сторона спочатку визначає користувача IAM та унікальний ідентифікатор облікового запису AWS. Далі перевіряє прикріплені користувацькі політики щоб визначити їх дозволи. Слідом переглядаються всі снепшоти EBS та визначається, хто має дозвіл createVolumePermission на конкретному снепшоті. Якщо снепшот є загальнодоступним, є можливість створення тому з цього снепшоту та його прикріплення до EC2 у обліковому записі AWS. У разі успішного приєднання тому до EC2 можна під'єднатися до снепшоту по SSH, монтувати том та отримувати доступ до конфіденційних даних.

У випадку виявлення загальнодоступного снепшоту, можна вжити наступних заходів: змінити дозволи, щоб зробити снепшот приватним; змінити облікові дані, у випадку якщо снепшот містив КД; провести розслідування для виявлення причин інциденту; використання подій CloudTrail для моніторингу та реагування на інциденти, такі як оприлюднення або копіювання снепшотів зловмисником.

Висновки. Використання EBS снепшотів ефективно забезпечує резервне копіювання даних для інстансів EC2. Недбале керування снепшотами може призвести до серйозних ризиків витоку інформації. Робота виявляє ці загрози та пропонує заходи для підвищення безпеки через зміну дозволів та моніторинг подій, наголошуючи на важливості реагування на сповіщення від AWS та своєчасного розуміння розробниками можливих ризиків.

Список літератури

1. Piper S. Beyond S3: Exposed Resources on AWS. Duo Security. *Duo*. URL – https://duo.com/blog/beyond-s3-exposed-resources-on-aws (date of access: 08.11.2023).
2. DEFCONConference. xBen Benmap Morris - Finding Secrets in Publicly Exposed Ebs Volumes – DEF CON 27 Conference, 2019. *YouTube*. URL – https://www.youtube.com/watch?v=HXM1rBk_wXs (date of access: 08.11.2023).

Відомості про авторів

Бригинець Анастасія Андріївна, студентка кафедри інформаційної та кібернетичної безпеки, Державний університет інформаційно-комунікаційних технологій, anastasiyka.br@gmail.com
Гайдур Галина Іванівна, завідувач кафедри інформаційної та кібернетичної безпеки, Державний університет інформаційно-комунікаційних технологій, д.т.н., професор, gaydurg@gmail.com

Секція 1

АНАЛІЗ АЛГОРИТМІВ ПОБУДОВИ НАЙКОРОТШИХ ШЛЯХІВ

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

Актуальність. Сучасне використання алгоритмів побудови найкоротших шляхів розширюється на багато галузей, визначаючи ефективність та оптимізацію ключових систем. В галузі інформаційних технологій та мережевих систем алгоритми найкоротших шляхів відіграють важливу роль у забезпеченні оптимального маршруту передачі даних через глобальні мережі. Це є критичним для розвитку швидких та ефективних мережевих рішень, що впливають на функціонування сучасних технологій зв'язку [1]. У сфері інформаційної безпеки за допомогою алгоритмів пошуку найкоротших шляхів можна побудувати оптимальну конфігурацію системи захисту. У сферах транспорту та логістики алгоритми найкоротших шляхів стають невід'ємною частиною вирішення завдань планування маршрутів та аналізу транспортних потоків. Вони допомагають оптимізувати шляхи перевезень, зменшуючи час та вартість доставки. У геологічному моделюванні ці алгоритми застосовуються для визначення оптимальних маршрутів досліджень та видобутку ресурсів, що впливає на ефективність видобутку та охорону навколишнього середовища [2]. Алгоритми найкоротших шляхів також використовуються у задачах, пов'язаних з аналізом екологічних систем. Вони дозволяють визначити оптимальні маршрути для моніторингу та дослідження екосистем, сприяючи ефективному управлінню ресурсами та збереженню природних об'єктів.

Мета роботи. Провести аналіз та порівняння алгоритмів побудови найкоротших шляхів у графах.

Основні положення. В доповіді розглянуто алгоритмів побудови найкоротших шляхів у графах. У дослідженні зосередимося на ключових аспектах кожного алгоритму, таких як швидкість виконання, ефективність у різних умовах графів, а також їх математичне обґрунтування.

В доповіді наведено: алгоритм Дейкстри – це алгоритм, який є найпоширенішим алгоритмом пошуку найкоротших шляхів у графах з відсутністю від'ємних ваг. Цей алгоритм відноситься до типу індексних алгоритмів та використовується для знаходження найкоротших шляхів від вершини до інших вершин. Наступним індексним алгоритмом, розглянутим в доповіді, є алгоритм Белмана-Форда, відмінністю від алгоритму Дейкстри є можливість працювати з графами, які містять ребра від'ємної ваги [3]. Наступними в доповіді були розглянуті матричні алгоритми. Було розглянуто алгоритм Флойда-Уоршела, який дозволяє

знайти відстані від всіх вершин в графі та дозволяє працювати з від'ємними ребрами. Також було розглянуто матричний алгоритм Джонсона, який, використовуючи додавання фіктивної вершини та перезважування робер, дозволяє застосувати алгоритм Дейкстри до графів з від'ємними вагами робер [4]. Особлива увага доповіді приділяється ранговому алгоритму. Ранговий алгоритм дуже легко розпаралелюється, дозволяє працювати з ребрами та циклами від'ємної ваги, несе в собі інформацію про знаходження найкоротших шляхів та прокладає шлях у вигляді переліка вершин.

У доповіді приведено дослідження, які включатимуть значення ефективності та здатності алгоритмів враховувати різні ваги робер, можливість працювати з від'ємними циклами та знаходити зворотній шлях.

Висновки. Робота присвячена порівняльному аналізу алгоритмів визначення найкоротших шляхів. Було проведено аналіз кожного з алгоритмів, та порівняння кожного з кожним в якому було досліджено недоліки та переваги кожного з алгоритмів.

Список літератури

1. Shortest Path Algorithms. URL – https://www.hackerearth.com/practice/algorithms/graphs/shortest-path-algorithms/tutorial/ (дата звернення: 10.10.2023);
2. Rajeev A. A Comparison of the 3 Shortest Path Algorithms. URL – https://medium.com/@adithjrajeev/a-comparison-of-the-3-shortest-path-algorithms-b49f02736901 (дата звернення: 12.10.2023);
3. Diestel R. Graph Theory. Berlin : Springer Nature, 2010. 447с.
4. Sedgewick R., Wayne K. Algorithms. Массачусетс : Addison-Wesley, 2011. 976с.

Відомості про авторів

Булгаков Гліб Юрійович, студент кафедри комп’ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», h.bulhakov@student.csn.khai.edu
Пєвнєв Володимир Яковлевич, професор кафедри комп’ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», д.т.н., доцент, v.pevnev@csn.khai.edu

Секція 1

РОЗРОБКА ТЕХНОЛОГІЇ ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ В КОРПОРАТИВНІЙ ІНФОРМАЦІЙНІЙ СИСТЕМІ

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

Актуальність. Корпоративні інформаційні системи (КІС) стали невід'ємною складовою сучасного бізнесу, прискорюючи його розвиток та полегшуючи управління багатьма процесами. Проте, зростання комплексності КІС породжує загрозу вразливостей, які можуть призвести до незаконного доступу до інформації, порушення конфіденційності та цілісності даних. Тому розробка технології виявлення вразливостей в корпоративній інформаційній системі є актуальною та важливою задачею. Корпоративні інформаційні системи великих компаній регулярно зазнають змін - оновлюється конфігурація обладнання, змінюється топологія мереж, з'являються нові вузли і цілі системи [1].

На сьогодні не існує єдиного алгоритму виявлення вразливостей в корпоративних інформаційних системах. Подібна ситуація виникає через те, що кожна з досліджуваних систем має свої особливості та потребує індивідуального підходу [2]. Тому розробка технології виявлення вразливостей стає надзвичайно важливою задачею для забезпечення безпеки корпоративних інформаційних систем.

Метою є дослідити існуючі підходи до виявлення вразливостей в корпоративних інформаційних системах та визначити вимоги до технології, що буде розроблятися.

Основні положення. Розглядаючи найрозповсюджені типи загроз, що виникають в інформаційних системах можна виділити рад тих, що зустрічаються найчастіше: Недоліки захисту службових протоколів, словникові паролі, недостатній рівень захисту привілейованих облікових записів, зберігання важливої інформації у відкритому вигляді, вразливі версії програмного забезпечення, недостатня освіченість персоналу системи з приводу можливих дій зловмисників [3]. Виходячи з описаного висче можна зазначити, що джерелом більшості з описаних загроз є недбалість персоналу системи на етапі її створення або обслуговування.

У доповіді розглядаються різні підходи для виявлення вразливостей та різні підходи. Більшість з них потребує використання в комплексі з іншими та під керуванням досвідченого експерта. Основні з низ подані нижче.

Сканування вразливостей. Це процес автоматичного сканування мережі та систем на наявність вразливостей. Існують спеціальні програмні засоби які виявляють вразливості, аналізуючи порти, служби, програмне забезпечення та конфігурації систем.

Аудит безпеки. Це процес систематичного перевірки безпеки системи, включаючи перевірку наявності вразливостей. Він включає огляд конфігурацій, перевірку політик безпеки, перевірку прав доступу, аналіз журналів подій та інші процедури.

Пенетраційне тестування. Це процес активного тестування системи шляхом моделювання атак та спроб проникнення з боку зловмисників.

Моніторинг безпеки. Це неперервне спостереження за системою з метою виявлення потенційних вразливостей або зловмисної діяльності. автоматизовані системи управління вразливостями.

Висновки. Виявлення вразливостей корпоративних інформаційних систем потребує комплексного підходу з урахуванням особливостей конкретної досліджуваної системи. Будь який процес виявлення вразливостей в даному типі систем є сильно залежним від рівня допуску до компонентів, що надається особі, що проводить аналіз, та її рівня експертності. Важливим є те, щоб експерт, що проводить аналіз корпоративної інформаційної системи компанії, яка працює в певній галузі мав високий рівень досвідченості не лише в принципах побудови систем безпеки, а й особливостях даної галузі.

Не існує конкретних стандартизованих алгоритмів виявлення вразливостей через те, що кожна система має власні особливості, які важко урахувати в стандартизованому алгоритмі. Можуть бути використані комплексні підходи на базі методик аналізу. Але набір інструментів буде відрізнятися в залежності від обраної системи та вимог до рівня безпеки.

Список літератури

1. Дмитро Мехед, Юлія Ткач, Володимир Базилевич, Володимир Гур'єв, Ярослав Усов. АНАЛІЗ ВРАЗЛИВОСТЕЙ КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ СИСТЕМ. *Jrnl.* URL – https://jrnl.nau.edu.ua/index.php/ZI/article/view/12453/17051(дата звернення: 01.06.2023);
2. А.І. Андрухів, Д.О. Тарасов. Порівняння методів оцінки захищеності корпоративних інформаційних систем. *Lpnu.* URL – https://science.lpnu.ua/sites/default/files/journal-paper/2017/dec/7287/013-9vis573.pdf (дата звернення: 01.06.2023);
3. Вразливості корпоративних інформаційних систем, 2019. *Ptsecurity.* URL – https://www.ptsecurity.com/ru-ru/research/analytics/corporate-vulnerabilities-2019/#id1 (дата звернення: 01.06.2023).

Відомості про авторів

Бутенко Сергій Ігорович, студент кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», s.butenko@student.csn.khai.edu
Пєвнєв Володимир Яковлевич, професор кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», д.т.н., доцент, v.pevnev@csn.khai.edu

Секція 1

РОЗРОБЛЕННЯ МЕТОДИКИ ТА ЗАСОБІВ ОЦІНЮВАННЯ ІНФОРМАЦІЙНОЇ ТА КІБЕРБЕЗПЕКИ ДЛЯ КОМПАНІЙ СЕРЕДНЬОГО ТА МАЛОГО РОЗМІРУ ПРАЦЮЮЧИХ У СФЕРІ ІТ. ЗАБЕЗПЕЧЕННЯ ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ ТА СЕРЕДОВИЩА

Бутирін Д. О.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Пєвнєв В. Я.

Актуальність. Загрози кібербезпеці швидко зростають, викликаючи серйозні виклики для компаній незалежно від їхнього розміру. Але компанії середнього та малого розміру особливо вразливі через обмежені ресурси та фінансові можливості. Тому виникає необхідність розроблення ефективної методики та засобів, спеціально адаптованих до їхніх потреб і здатних забезпечити надійний рівень захисту інформації та середовища [1].

За даними репорту KHARKIV IT RESEARCH 2021, станом на середину 2021 року тільки в Харкові вели активну діяльність 511 IT-компаній, які співпрацюють з 45 тисячами фахівців різних спеціалізацій. З 2019 року IT-індустрія в Харкові зросла на 29 %, при цьому загалом в Україні працюють 2234 IT-компанії, що зазначено у дашборді технологічної екосистеми України, опублікованому Міністерством цифрової трансформації [2].

З огляду на кількість компаній, які вже працюють та появу нових компаній в сфері IT, та зростаючу кількість загроз, актуальність питання захисту інформації та кібернетичного середовища таких компаній неможливо переоцінити [3,4].

Метою даної роботи є дослідження та визначення основних загроз, ризиків та потреби у засобах захисту інформації та безпеки середовища де ця інформація зберігається, для компаній середнього та малого розміру, які працюють у сфері IT. Також важливим є розроблення комплексного підходу до оцінювання інформаційної та кібербезпеки в таких компаніях, а також створення відповідних засобів захисту.

Основні положення. Під час доповіді зазначається то, що IT компанії отримують від замовників та працюють з великими обсягами інформації. У більшості випадків ця інформація є конфіденційною та дуже вразливою.

Наведені у доповіді результати аналізу потреб компаній, виявлення актуальних загроз і ризиків, дасть змогу ідентифікувати необхідність розроблення інноваційних методик оцінювання, які враховують особливості компаній середнього та малого розміру.

У доповіді визначені критерії оцінювання та наведені розроблені шкали оцінювання, які допоможуть виміряти рівень безпеки та визначити пріоритетні напрямки дій.

У доповіді наведені результати впровадження розробленої методики оцінювання та засобів захисту, яка є ключовим кроком у покращенні безпеки інформації та кібернетичного середовища в компаніях середнього та малого розміру. Її впровадження допоможе зменшити рівень вразливості та ризики, підвищити свідомість та культуру безпеки, а також забезпечити ефективне використання обмежених ресурсів.

Висновки. Беручі до уваги зростання ринку IT в Україні та світі, додавання все більшої кількості IT компаній, які працюють з конфіденційною та вразливою інформацією, можна дійти висновку про абсолютну необхідність розроблення методики та засобів оцінювання інформаційної та кібербезпеки для компаній середнього та малого розміру у сфері IT. Це є дуже важливим завданням та стає дуже актуальним з огляду на стрімке зростання кількості та якості загроз. Такі рішення допоможуть забезпечити надійний рівень захисту інформації та кібернетичного середовища в умовах обмежених ресурсів, а також підвищити відповідність компаній вимогам кібербезпеки.

Список літератури

1. NIST Special Publication 800-53: Security and Privacy Controls for Federal Information Systems and Organizations. *NIST*. URL – https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final (дата звернення 10.09.2023).
2. Kharkiv IT research 2021 — третє масштабне дослідження українського IT-ринку. *IT-Kharkiv*. URL: https://it-kharkiv.com/projects/kharkiv-it-research-2021 (дата звернення 10.09.2023);
3. Cybersecurity Framework - National Institute of Standards and Technology *NIST*. URL – https://www.nist.gov/cyberframework (дата звернення 10.09.2023);
4. CIS Critical Security Controls, Prioritized & simplified best practices, Follow our prioritized set of actions to protect your organization and data from cyber-attack vectors. *Cisecurity*. URL – https://www.cisecurity.org/controls (дата звернення 11.09.2023).

Відомості про авторів

Бутирін Дмитро Олександрович, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», d.o.butyrin@student.csn.khai.edu
Пєвнєв Володимир Яковлевич, професор кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», д.т.н., доцент, v.pevnev@csn.khai.edu

Секція 1

РОЗРОБЛЕННЯ ТА ДОСЛІДЖЕННЯ ЗАСОБІВ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ КОМУНІКАЦІЇ РОЮ ДРОНІВ З ВИКОРИСТАННЯМ ШТУЧНОГО ІНТЕЛЕКТУ

Васильєв О. В.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Клюшніков І. М.

Актуальність. В наш час для виконання комплексних завдань, де можуть застосовуватися безпілотні літальні апарати (БПЛА) як, наприклад, для проведення військової розвідки, або моніторингу об'єктів критичної інфраструктури є доцільним використання не одного, а рою БПЛА для підвищення гарантоздатності виконання завдань [1]. Проте збільшення кількості БПЛА для виконання завдання суттєво збільшує ризик бути атакованим, що в свою чергу підвищує актуальність питань пов'язаних з безпекою, надійністю та гарантоздатністю як всього рою, так і окремих БПЛА, що його формують.

Метою даної роботи є розробка програмно-апаратного комплексу для забезпечення безпеки комунікації БПЛА між собою та стацією керування, а також створення системи виявлення та запобігання вторгнень на основі технологій штучного інтелекту, розміщених на станції керування та на борту БПЛА для ефективної протидії атакам різного типу, наприклад: Denial of Service attack (DoS); Packet sniffing attack; Man-in-the-middle attack; Spoofing (GPS spoofing) attack; Jamming attack, і Wormhole attack [2]. І у разі загрози втрати зв'язку з оператором, навчити систему приймати рішення в умовах автономності БПЛА для продовження виконання завдань та проведення процедур на відновлення зв'язку з оператором.

Основні положення. Якщо проаналізувати існуючі рішення, то можна зробити висновок, що одні з них можуть добре працювати проти одних видів атак, але бути недієвими проти інших видів атак [2]. Наприклад, використання протоколу WPA2 може захисти канал зв'язку від перехоплення інформації, наприклад логіну та паролю від БПЛА [3], проте цей протокол не захистить від таких атак як Jamming які можуть створювати завади на будь-які радіочастоті, що робить неможливим комунікації з БПЛА, який потрапив в зону дії радіоелектронної боротьби (РЕБ) [4]. Слід зазначити, що атаки можуть комбінуватися, наприклад, після проведення атаки Jamming яка змусить БПЛА увімкнути режим «Return to home» - функція повернення додому, буде задіяна атака GPS spoofing, за допомогою якої зловмисник може коректувати траєкторію польоту БПЛА, який буде намагатися рухатися у напрямку станції керування за сигналами системи супутникової навігації [2].

Висновки. Тому виникає задача створення та розгортання апаратно-програмного комплексу з інтелектуальною системою виявлення та запобігання атак як на станції керування так і на БПЛА з застосуванням засобів штучного інтелекту – системи прийняття рішень, що забезпечить адаптивну автономність БПЛА у разі втрати зв'язку з станцією керування. Та для підвищення ефективності протидії атакам на рій БПЛА планується розроблення БПЛА-приманок [5], які будуть мати визначені точки вразливості та задачею цих БПЛА є навмисне ініціювання кібератаки, з метою визначення методів атаки та викриття порушника.

Список літератури

1. Securing Against DoS/DDoS Attacks in Internet of Flying Things using Experience-based Deep Learning Algorithm. *Researchgate*. URL – https://www.researchgate.net/publication/350171510_Securing_Against_DoSDDoS_Attacks_in_Internet_of_Flying_Things_using_Experience-based_Deep_Learning_Algorithm (дата звернення: 29.04.2023);
2. Fast, Reliable, and Secure Drone Communication: A Comprehensive Survey.*Researchgate*.URL:https://www.researchgate.net/publication/353212475_Fast_Reliable_and_Secure_Drone_Communication_A_Comprehensive_Survey (дата звернення: 30.04.2023);
3. Defense Techniques Against Cyber Attacks on Unmanned Aerial Vehicles. *Researchgate*.URL: https://www.researchgate.net/publication/328135272_Defense_Techniques_Against_Cyber_Attacks_on_Unmanned_Aerial_Vehicles (дата звернення: 30.04.2023);
4. A Survey on the Use of Deep Learning Techniques for UAV Jamming and Deception. *MDPI*. URL: https://www.mdpi.com/2079-9292/11/19/3025 (дата звернення: 29.04.2023);
5. HoneyDrone: A medium-interaction unmanned aerial vehicle honeypot.*Researchgate*. URL: https://www.researchgate.net/publication/326280510HoneyDrone_A_mediuminteraction_unmanned_aerial_vehicle_honeypot (дата звернення: 15.04.2023).

Відомості про авторів

Васильєв Олексій Вадимович, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», o.v.vasyliev@student.csn.khai.edu

Клюшніков Ігор Миколайович, доцент кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», к.т.н., старший науковий співробітник, i.kliushnikov@csh.khai.edu

Секція 1

ДОСЛІДЖЕННЯ ВАРІАНТІВ ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В КОНТЕКСТІ КІБЕРБЕЗПЕКИ: СИСТЕМАТИЗАЦІЯ БАЗОВИХ СЦЕНАРІЇВ І КОНТРЗАХОДІВ

Веприцька О. Ю.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Харченко В. С.

Актуальність. Незважаючи на те що, розвиток штучного інтелекту (ШІ) вплинув на зростання рівня автоматизації та інновацій, він також відкрив нові можливості для зловмисників. Використання ШІ як зброї через «вепонізацію» технологій дозволяє здійснювати більш ефективні атаки. Окрім того, виникають нові загрози – «атаки на штучний інтелект», які дозволяють зловмисникам маніпулювати системами штучного інтелекту (СШІ) та змінювати їхню поведінку [1].

Метою даної роботи є класифікація та аналіз сценаріїв, де ШІ розглядається як: об'єкт (система або актив), що має бути захищеним; засоби (технологія) для здійснення атаки, засоби (технологія) захисту від кібератак, а також систематизація контрзаходів для кібератак для визначення їх впливу на цілісність, конфіденційність та доступність. Дослідження базується на принципах і моделях, описаних в [2, 3], та розвиває їх задля зменшення ризиків успішних атак.

Основні положення. В дослідженні використовуються визначення, пов'язані з кібератаками та ШІ, зокрема:

- атака на ШІ – цілеспрямована маніпуляція СШІ з кінцевою метою спричинення її непрацездатності;
- атака, підсилена ШІ (AI powered attack) – атака з використанням технологій ШІ для підвищення дієвості поточних кібератак та створення нових сервісів з використанням ШІ;
- засоби захисту підсилені ШІ (AI powered protection) – програмно-апаратні засоби, які побудовані з використанням технологій ШІ та забезпечують проактивний захист від кібератак.

В рамках проведеної роботи досліджено загрози/атаки на:

- традиційні системи: DDoS атака, генерація DGA, атаки вторгнення, генерація фейкових даних (текстових, аудіо, зображень, відео), генерація фішингових посилань, автоматизоване CAPTCHA-проходження;
- системи ШІ: змагальні атаки (фізичні, цифрові), атаки отруєння (цільові, невибіркові, backdoor), спонж-атака, атаки на моделі ШІ (кража та інверсія моделі, визначення належності до тренувальних даних тощо).

Розглянуто можливі заходи безпеки для попередження і толерування кожної з атак, їхні переваги, недоліки та виклики, пов'язані з обмеженнями

для впровадження. Для оцінювання запропоновано використовувати ризик орієнтований метод, що базується на розширеній техніці IMECA.

Висновки. В доповіді представлено таксономію кібератак з урахуванням аспекту ШІ, надано рекомендації щодо впровадження контрзаходів, базуючись на результатах IMECA-оцінювання ризиків.

Основним науковим результатом є розширена множина сценаріїв, що описується декартовим добутком множин систем ШІ, засобів їх захисту з використанням ШІ та атак, підсилених ШІ. Це надає змогу підвищити повноту оцінювання загроз і атак, а також перейти до глибшого кількісного аналізу з використанням, наприклад, методів теорії ігор і марковських випадкових процесів. Крім того, важливими напрямами подальших досліджень є: розроблення та аналіз сценаріїв з послідовностями атак, підсилених ШІ, з різними просторово-часовими моделями реалізації, а також з огляду на природну резильєнтність засобів штучного інтелекту [4].

Список літератури

1. Kaloudi N., Li J. The AI-Based Cyber Threat Landscape. ACM Computing Surveys. 2020. Vol. 53, no. 1. P. 1–34. URL: https://doi.org/10.1145/3372823;
2. Security-Informed Safety Analysis of Autonomous Transport Systems Considering AI-Powered Cyberattacks and Protection / O. Illiashenko et al. Entropy. 2023. Vol. 25, no. 8. P. 1123. URL: https://doi.org/10.3390/e25081123;
3. Veprytska O., Kharchenko V. AI powered attacks against AI powered protection: classification, scenarios and risk analysis. 2022 12th International Conference on Dependable Systems, Services and Technologies (DESSERT), Athens, Greece, 9–11 December 2022. 2022. URL: https://doi.org/10.1109/dessert58054.2022.10018770;
4. Resilience and Resilient Systems of Artificial Intelligence: Taxonomy, Models and Methods / V. Moskalenko et al. Algorithms. 2023. Vol. 16, no. 3. P. 165. URL: https://doi.org/10.3390/a16030165.

Відомості про авторів

Веприцька Олена Юріївна, аспірантка кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», o.veprytska@csn.khai.edu
Харченко Вячеслав Сергійович, завідувач кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», д.т.н., професор, v.kharchenko@csn.khai.edu

Секція 1

АНАЛІЗ ХАКЕРСЬКИХ АТАК НА МІНІСТЕРСТВО ЗАКОРДОНИХ СПРАВ

Вірський Я. М.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Тецький А. Г.

Актуальність. Атаки з боку зловмисників на державні установи, в тому числі на Міністерство закордонних справ (МЗС), є серйозною загрозою національній безпеці. Вони можуть призвести до витоку конфіденційної інформації, порушення роботи державних систем та навіть до дестабілізації ситуації в країні. Хакерські атаки на МЗС є все більш поширеними. У 2022 році було зафіксовано низку таких атак, зокрема на офіційні сайти МЗС США, Великобританії та України [1]. Атаки на МЗС можуть мати далекосяжні наслідки. Наприклад, виток конфіденційної інформації може призвести до витоку державної таємниці, а порушення роботи державних систем може призвести до перебоїв у дипломатичній діяльності [2].Тому дослідження хакерських атак на МЗС є важливим напрямком наукових досліджень. Воно дозволяє підвищити рівень розуміння цієї загрози та розробити ефективні методи її протидії. Тема є актуальною та перспективною для наукової конференції.

Метою даної роботи є дослідження принципів «безпечного» кодування. даної роботи є обговорення актуальних проблем безпеки, пов'язаних із кібератаками на Міністерство закордонних справ. Конференція дозволить обмінятися досвідом і знаннями в галузі кібербезпеки, сприяти розвитку наукових досліджень у цій галузі та розробці ефективних методів протидії кібератакам.

Покращити розуміння хакерських атак на МЗС. Це дозволить учасникам обговорити різні типи кібератак на МЗС, їхні мотиви та наслідки. Розробити ефективні методи протидії кібератакам на МЗС. Конференція дозволить обговорити актуальні дослідження та розробки в галузі кібербезпеки, спрямовані на підвищення рівня захисту МЗС від кібератак [3].

Основні положення. Безпечне Для своєчасної протидії загрозам використовуються антивірус та мережевий екран. Серед популярних та ефективним антивірусів є Microsoft Defender, це потужний автономний інструмент перевірки, який можна запустити із довіреного середовища без завантаження ОС. Також віддається перевага такому міжмережевий екран як FortiClient. Це програмний продукт, що забезпечує безпеку настільних комп'ютерів, ноутбуків та мобільних пристроїв. FortiClient включає антивірус, захист від шпигунського програмного забезпечення, персональний міжмережевий екран, фільтр для web-контенту і антиспам.

Форензіка є важливим інструментом для аналізу кібератак на МЗС. Вона дозволяє зібрати та зберегти докази, які можуть бути використані для ідентифікації хакерів, розуміння їхніх мотивів та запобігання майбутнім атакам [4].

Висновки. Швидкі зміни технологій та методів кібератак вимагають постійного моніторингу та адаптації заходів безпеки. Аналіз минулих атак може слугувати важливим інструментом для покращення існуючих стратегій та запобігання майбутнім загрозам. Хакерські атаки на МЗС можуть мати міжнародний характер, і співпраця на міжнародному рівні стає критично важливою для виявлення та припинення подібних загроз. Це стає серйозною загрозою для національної безпеки, оскільки це може призвести до втрати чутливої інформації, порушення дипломатичних відносин та інших наслідків, що можуть шкодити інтересам країни. Розробка та впровадження ефективних заходів протидії хакерським атакам є невід'ємною частиною стратегії національної безпеки. На основі аналізу можна розробити конкретні рекомендації для удосконалення захисту інформації та інфраструктури МЗС.

Список літератури

1. 2022 Ukraine cyberattacks. *Wikipedia*. URL – https://en.wikipedia.org/wiki/2022_Ukraine_cyberattacks (дата звернення: 14.10.2023);
2. Bad Magic's Extended Reign in Cyber Espionage Goes Back Over a Decade. *Hacker News*. URL – https://thehackernews.com/2023/05/bad-magics-extended-reign-in-cyber.html (дата звернення: 15.10.2023);
3. Кібербезпека: Все Що Необхідно Знати Кожному Користувачу Мережі Інтернет. *Ukraine lifehacker*. URL – https://www.ukraine-lifehacker.com/kiberbezpeka-vse-shcho-neobkhidno-znaty (дата звернення: 15.10.2023);
4. Carier B. File System Forensic Analysis. 2005. Page 511. URL – https://repo.zenksecurity.com/Forensic/File%20System%20Forensic%20Analysis.pdf (дата звернення: 16.10.2023).

Відомості про авторів

Вірський Ярослав Михайлович, студент кафедри комп’ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», y.m.virsjkyy@student.csn.khai.edu
Тецький Артем Григорович, доцент кафедри комп’ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», к.т.н., a.tetskiy@csn.khai.edu

Секція 1

ЗАХИСТ СИСТЕМ РОЗПІЗНАВАННЯ ДОРОЖНІХ ЗНАКІВ ВІД АТАК ТА ВТРУЧАННЯ

Ганжа Д. Є.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Шостак А. В.

Актуальність. З розвитком технологій машинного навчання, штучного інтелекту та автономних транспортних засобів системи розпізнавання дорожніх знаків стали невід'ємною частиною сучасної транспортної інфраструктури. Вони дозволяють автомобілям "читати" і розуміти дорожні знаки, дотримуватись правил дорожнього руху і, таким чином, підвищувати безпеку на дорогах [1]. Однак із зростанням значущості цих систем зростає й потенційна загроза їхній безпеці. У цьому контексті аналіз та захист від уразливостей у системах розпізнавання дорожніх знаків стають актуальними завданнями, які потребують серйозної уваги та досліджень. Як і багато інших комп'ютерних систем, системи розпізнавання дорожніх знаків стають об'єктами уваги кіберзлочинців.[2] Злом і втручання в такі системи можуть призвести до створення хибних знаків, зміни дорожніх інструкцій та підвищення ризику аварій. З появою нових технологій, таких як нейронні мережі та комп'ютерний зір, системи розпізнавання дорожніх знаків стають все більш точними та здатними. Однак із зростанням їхньої складності зростає і потенційна вразливість.

Метою даної роботи є аналіз та дослідження методів захисту систем розпізнавання дорожніх знаків від атак та втручання.

Автори дослідження провели ряд експериментів, націлених на обхід моделей, заснованих на обмеженні глибокого навчання, та продемонстрували їхню здатність обманювати системи "зору" при розпізнаванні дорожніх знаків. В рамках експерименту було обрано знак "STOP", і за допомогою внесених змін зловмисники змогли скласифікувати його моделлю як «SPEED LIMIT 45» [3]. Основним методом було виявлення таких областей на дорожньому знаку, які найбільше вносять спотворення та призводять до помилок у роботі класифікатора. Цікаво, що запропонований підхід до обману був успішно адаптований та перевірений на інших дорожніх знаках, що наголошує на його ефективності [4].

Основні положення. Для забезпечення своєчасного виявлення атак або втручання в систему розпізнавання дорожніх знаків рекомендується застосовувати комплексний підхід, що включає систему виявлення атак, механізм оповіщення та реагування, а також застосування додаткових заходів захисту на основі виявлених атак. Цей підхід сприяє ефективному

захисту системи від потенційних загроз та забезпечує надійне функціонування системи розпізнавання дорожніх знаків.

Висновки. Системи розпізнавання дорожніх знаків перебувають у стадії активного розвитку та інтеграції до сучасних автомобілів. У міру поширення розумних доріг та автономних автомобілів, забезпечення їхньої безпеки стає все більш актуальним завданням. Системи розпізнавання дорожніх знаків можуть також включати відеоспостереження і збір даних про дорожню обстановку. Захист цих даних від незаконного доступу та використання також є вкрай важливим. Виходячи з цих факторів, стає зрозумілим, що забезпечення безпеки та надійності систем розпізнавання дорожніх знаків – це необхідність, яка сприяє покращенню дорожньої безпеки та захисту даних користувача.

Список літератури

1. A. Geiger, P. Lenz, and R. Urtasun. Are we ready for autonomous driving? the KITTI vision benchmark suite. In Computer Vision and Pattern Recognition (CVPR), 2012 IEEE Conference on, pages 3354–3361. IEEE, 2012;
2. Безпека машинного навчання: чи ефективні методи захисту чи нові загрози? *Habr*. URL – https://habr.com/companies/pt/articles/416691/ (дата звернення: 11.10.2023);
3. A. Nguyen, J. Yosinski, and J. Clune. Deep neural networks are easily fooled: High confidence predictions for unrecognizable images. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pages 428–435, 2015;
4. Robust Physical-World Attacks on Deep Learning Visual Classification. *Arxiv*. URL – https://arxiv.org/pdf/1707.08945.pdf (дата звернення: 15.10.2023).

Відомості про авторів

Ганжа Дмитро Євгенійович, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», d.hanzha@student.csn.khai.edu
Шостак Анатолій Васильович, доцент кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», к.т.н., доцент, a.shostak@csn.khai.edu

Секція 1

ДОСЛІДЖЕННЯ ТА РОЗРОБКА МОДЕЛЕЙ ЗАСТОСУВАННЯ АІ ДЛЯ ЗАПОБІГАННЯ РИЗИКІВ ТРАВМУВАННЯ НА ВИРОБНИЦТВІ

Грисюк С. О.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Пєвнєв В. Я.

Актуальність. Дослідження та розробка моделей застосування штучного інтелекту (ШІ) для запобігання ризиків травмування на виробництві є дуже актуальними. Промислові травми та нещасні випадки на робочому місці можуть мати серйозні наслідки для працівників та підприємства в цілому. Використання ШІ може допомогти зменшити ймовірність виникнення таких ситуацій та покращити безпеку на робочому місці.

Одним з основних напрямків досліджень в цій області є розробка систем візуального спостереження з використанням комп'ютерного зору. ШІ може аналізувати відеозаписи з камер спостереження, виявляти потенційно небезпечні ситуації та надавати оперативне сповіщення працівникам та керівництву про можливі загрози.

Іншим напрямком є розробка моделей прогнозування ризиків на основі аналізу даних [1]. ШІ може аналізувати великі обсяги даних про травми, нещасні випадки та умови праці, враховуючи такі фактори, як тип робіт, використання обладнання, виробничі стандарти тощо. На основі цих даних можуть бути розроблені моделі, які дозволяють передбачити ризики травмування та приймати вчасні заходи для їх запобігання [2].

Метою даної роботи є дослідження та розробка моделей застосування штучного інтелекту (ШІ) для запобігання ризиків травмування на виробництві. Головною метою є забезпечення безпеки працівників і підвищення безпекових стандартів на робочих місцях.

Основні положення доповіді, у якої наводяться дослідження та результати розробки моделей застосування штучного інтелекту для запобігання ризиків травмування на виробництві включають наступне.

1. Аналіз даних: Вивчення та аналіз історичних даних про травми, нещасні випадки та умови праці для виявлення шаблонів травмування та ідентифікації факторів ризику.
2. Розробка моделей прогнозування: Розробка алгоритмів та моделей на основі аналізу даних для прогнозування ризиків травмування..
3. Розробка системи візуального спостереження: Розробка алгоритмів та моделей, які здатні аналізувати відеозаписи з камер спостереження та виявляти небезпечні ситуації.

4. Розробка системи попередження та реагування: Розробка системи, яка забезпечує оперативне сповіщення працівників та керівництва про потенційні загрози безпеці.

5. Валідація та впровадження: Перевірка ефективності розроблених моделей та систем через експерименти та пілотні проекти. Валідація може включати оцінку точності та надійності моделей, а також взаємодію з працівниками та керівництвом для забезпечення відповідності розробок їх потребам.

Висновки. Дослідження та розробка моделей застосування штучного інтелекту для запобігання ризиків травмування на виробництві має великий потенціал для покращення безпеки працівників, зниження кількості травм та покращення умов праці. Це може сприяти підвищенню продуктивності та зменшенню втрат на виробництві.

Список літератури

1. Тренди ШІ: які етичні загрози несе використання штучного інтелекту. *Центр економічної стратегії.* URL – https://ces.org.ua/yaki-eticni-zagrozi-nese-vikoristannya-stucnogo-intelektu (дата звернення: 05.09.2023);

2. Штучний інтелект у сфері безпеки праці: варто застосовувати чи ні? допоможе чи завадить? *Науково-виробничий журнал Охорона Праці*. URL: https://ohoronapraci.kiev.ua/article/anonsi/stucnij-intelekt-u-sferi-bezpeki-praci-varto-zastosovuvati-ci-ni-dopomoze-ci-zavadit (дата звернення: 08.09.2023).

Відомості про авторів

Грисюк Сергій Олександрович, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», s.o.hrysiuk@student.csn.khai.edu

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

Секція 1

ЗАСТОСУВАННЯ МЕТОДІВ І ЗАСОБІВ ШТУЧНОГО ІНТЕЛЕКТУ ПРИ ВИЯВЛЕННІ І РОЗСЛІДУВАННІ ЗЛОЧИНІВ У СФЕРІ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Губарєв І. О.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник Харченко В. С.

Актуальність. Застосування методів і засобів штучного інтелекту (ШІ) при виявленні і розслідуванні злочинів у сфері інформаційних технологій (ІТ) є дуже актуальною темою в сучасному світі. Злочини в сфері ІТ стають все більш поширеними і складними, вимагаючи нових підходів та інструментів для їх виявлення та розслідування.

Метою даної роботи є поглиблене розуміння сучасних тенденцій, проблем та потенційних переваг застосування ШІ в розслідуванні та виявленні злочинів у сфері ІТ та внесення внеску в цю галузь, яка активно розвивається.

До основних завдань даної роботи можна віднести наступне:

- дослідити сучасні методи і засоби ШІ, що використовуються для виявлення і розслідування злочинів у сфері ІТ;
- проаналізувати можливості та обмеження цих методів і засобів, оцінити їх ефективність та застосовність у реальних ситуаціях;
- вивчити проблеми, що виникають при використанні ШІ в сфері виявлення і розслідування кіберзлочинів, і запропонувати можливі шляхи їх вирішення;
- зробити огляд сучасних розробок, комерційних продуктів і дослідницьких робіт, пов'язаних з ШІ в кібербезпеці та розслідуванні злочинів у сфері ІТ;
- визначити перспективи подальшого розвитку цієї області, ідентифікувати потенційні виклики та можливості для досліджень і розвитку технологій ШІ.

Основні положення. Ці основні положення демонструють значущість та потенціал застосування методів і засобів ШІ для виявлення і розслідування злочинів у сфері ІТ, а також вказують на важливі аспекти, які потребують додаткової уваги та дослідження:

- ШІ є потужним інструментом для виявлення, аналізу і передбачення злочинних діянь у сфері ІТ;
- методи і засоби ШІ можуть бути застосовані для виявлення аномалій, виявлення шаблонів злочинної діяльності, прогнозування ризиків та автоматичного аналізу великих обсягів даних;
- ШІ може допомогти в розслідуванні злочинів шляхом автоматизації процесу збору доказів, аналізу великих обсягів інформації, виявлення

зв’язків між підозрюваними та ідентифікації деталей, що допоможуть розкрити злочин;

- використання ШІ спрощує виявлення і розслідування злочинів, дозволяє зменшити час, затрати та помилки, пов'язані з ручним аналізом даних, і покращує ефективність роботи правоохоронних органів і служб безпеки;
- проте, існують певні виклики та проблеми, пов’язані з використанням ШІ в цій сфері, такі як етичні питання, приватність даних, недостатня надійність алгоритмів, розуміння прийнятих рішень системами ШІ, а також необхідність постійного оновлення технологій і навчання персоналу.

Висновки. ШІ дозволяє швидко аналізувати великі обсяги даних і виявляти складні залежності та патерни, що допомагає виявити кримінальну активність, включаючи кіберзлочини. Застосування ШІ дозволяє автоматизувати аналіз, збір доказів та ідентифікацію злочинців, що прискорює розслідування та забезпечує кращі результати. ШІ може аналізувати дані та виявляти залежності, що допомагають передбачати можливі кримінальні діяння та приймати заходи для їх уникнення. ШІ сприяє об'єктивному та нейтральному розгляду кримінальних справ, оскільки алгоритми не піддаються емоційному впливу або упередженості. ШІ може виявляти та передбачати нові форми кіберзлочинності, що допомагає забезпечити кращу захист інформаційних систем та мереж.

Список літератури

1. Бегма А. П., Ховпун О. С. Розслідування злочинів в ІТ-сфері. Наукові праці Національного університету «Одеська юридична академія». Одеса, 2021. №28. С. 12-19. URL: https://tinyurl.com/yknbpxjv;
2. Шрамко С. С., Гальцова О. В. Використання технологій штучного інтелекту у протидії злочинності. Матеріали науково-практичного онлайн-семінару. Харків, 2020. С. 6-51. URL: http://surl.li/aijyb;
3. Демура М. І, Клепка Д. І. Перспективи застосування штучного інтелекту у галузі кримінального судочинства. Стаття Національного юридичного університету імені Ярослава Мудрого та Науково-дослідного інституту вивчення проблем злочинності імені академіка В.В. Сташиса Національної академії правових наук України. Харків, 2022. №5. С. 554-558. URL: http://lsej.org.ua/5_2022/133.pdf;
4. European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment. Матеріали пленарного засідання CEPEJ. Страсбург, 2018. С. 5-66.

Відомості про авторів

Губарєв Ігор Олександрович, магістрант кафедри комп’ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», i.o.hubariev@student.csn.khai.edu
Харченко Вячеслав Сергійович, завідувач кафедри комп’ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», д.т.н., професор, v.kharchenko@csn.khai.edu

Секція 1

РОЗРОБЛЕННЯ МЕТОДИКИ ТА ЗАСОБІВ АНАЛІЗУ ВРАЗЛИВОСТЕЙ, ВИБОРУ ТА АДАПТАЦІЇ VPN ПРОДУКТІВ ВІДПОВІДНО ДО ВИМОГ КОРИСТУВАЧІВ

Демура Р. І.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Харченко В. С.

Актуальність. VPN-продуктів в сучасному світі є вкрай важливою. VPN-продукти допомагають захистити приватність, захистити від кіберзагроз, обійти географічні обмеження, підсилюють безпеку підключення до громадських Wi-Fi та безпеку роботи з віддаленими ресурсами, відкривають доступ до заблокованих сайтів і сервісів і зберігають інтернет-анонімність [1].

Актуальність VPN-продуктів полягає в їх здатності забезпечувати приватність, безпеку та свободу під час користування Інтернетом. З урахуванням постійно зростаючої кількості кіберзагроз та необхідності збереження особистих даних, використання VPN стає важливим елементом для користувачів в будь-якому контексті, від індивідуального використання до комерційного застосування.

Метою даної роботи є розроблення методики дослідження та аналізу вразливостей VPN продуктів, а також, вибору VPN продуктів відповідно до вимог користувачів.

Основні положення. VPN (Virtual Private Network) – це віртуальна приватна мережа, яка забезпечує шифрування трафіку між клієнтом та VPN-сервером і зміну IP-адреси [2]. Ключові аргументи, що доводять необхідність використання VPN-сервісів в сучасному цифровому світі:

- захист даних: Використання VPN-сервісів дозволяє захистити дані, що передаються через Інтернет, від хакерських атак та інших вторгнень [3];
- анонімність: VPN-сервіси дозволяють приховати справжню IP-адресу користувача, що робить неможливим відстеження його дій в Інтернеті;
- обхід блокування: VPN-сервіси дозволяють обійти блокування сайтів та сервісів, які можуть бути заблоковані в певних регіонах [4];
- безпечне використання громадських Wi-Fi мереж: VPN-сервіси забезпечують безпечне підключення до громадських Wi-Fi мереж, які можуть бути небезпечними;
- зниження ризику витоку даних: Використання VPN-сервісів знижує ризик витоку даних при використанні громадських Wi-Fi мереж та інших відкритих мереж [5];

– збереження конфіденційності: VPN-сервіси допомагають зберігати конфіденційність при передачі даних, що важливо для захисту особистої інформації та комерційних секретів;

– захист від відстеження рекламодавців: VPN-сервіси захищають від відстеження рекламодавців та інших компаній, які можуть використовувати дані щодо поведінки користувача в Інтернеті для рекламних цілей.

Висновки. Отже, актуальність використання VPN-сервісів в сучасному цифровому світі важко переоцінити. Вони забезпечують захист особистої інформації, конфіденційності та анонімності в Інтернеті, дозволяють обходити обмеження цензури, захищають від кібератак та надають можливість отримувати доступ до геоблокованого контенту.

Список літератури

1. Що таке VPN, і як ним безпечно користуватись. *Український Південь*. URL: https://pivdenukraine.com.ua/2022/06/05/ukra%D1%97ncyam-na-timchasovo-okupovanix-teritoriyax-varto-koristuvatisya-vpn-derzhspeczvyazku (дата звернення: 19.10.2023);
2. Налаштування MikroTik VPN L2TP. *MikroTik*. URL: https://настройка-микротик.укр/nastrojka-mikrotik-vpn-server-l2tp (дата звернення: 22.10.2023);
3. Conceptual overview of VPN. *Wireguard*. URL – https://www.wireguard.com (дата звернення: 20.10.2023);
4. VPN for travelling abroad. *ProtonVPN*. URL – https://protonvpn.com/travelling (дата звернення: 20.10.2023);
5. Secure access and network connectivity reimagined. *OpenVPN*. URL – https://openvpn.net (дата звернення: 20.10.2023).

Відомості про авторів

Демура Руслан Іванович, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», r.i.demura@student.csn.khai.edu

Харченко Вячеслав Сергійович, завідувач кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», д.т.н., професор, v.kharchenko@csn.khai.edu

Section 1

AI - A NEW THREAT TO CYBERSECURITY

Daria Drakon
V.N. Karazin Kharkiv National University
Scientific advisor: Natalia Stiahlyk

Relevance. Cybersecurity is advancing in step with new technologies, never falling behind. Every day, new challenges arise, which either improve or reveal what still needs to be worked on in security systems.
Artificial Intelligence (AI) is evolving even faster than other technological developments. If, not long ago, there was no serious concern about its threat to modern cybersecurity, it has become an urgent issue now. Opinions on the impact of AI vary because, on one hand, it can help and enhance security, but on the other hand, in the wrong hands, it can only harm security systems.

Purpose. Hence, the pressing question today is the seriousness of AI threats to cybersecurity. In 2018, The New York Times reported that researchers from the United States and China successfully controlled AI systems developed by Amazon, Apple, and Google to perform various basic actions without the users of these AI systems knowing [1]. While there were no significant problems with transferring money, password cracking, or opening doors with AI systems back then, in 2023, this has become a problem for AI system users. Nowadays, most hackers use AI for intrusion, and security systems are slow to recognize or sometimes cannot counter this type of attack.

Principal provisions. AI-based security systems can also be hacked, and such incidents may go undetected for a long time. In April of this year, there were reports that criminals called a woman in Arizona, claiming her daughter was their hostage, and they perfectly imitated her daughter's voice using AI. A little earlier, in 2022, the FBI reported a series of complaints about people using «stolen information, as well as fake videos and voices to apply for remote technical positions». In 2019, AI was able to mimic the CEO's voice, complete with a distinct accent, convincing executives to transfer around $240,000 to a fake account [2].
As we can see, AI easily handles such tasks and is already widely used in criminal activities. Of course, more widely available AI systems like ChatGPT have rules embedded in their code that prevent them from directly participating in such actions. However, there has been information online suggesting that these safeguards can be easily circumvented by rephrasing requests. This is indeed true; for example, if you ask ChatGPT not just to generate a password for you but to help you remember your password, it will readily assist.
Experts have also categorized AI-related threats into three levels:

– low level: Bias exploitation, Bot hacking, AI evasion, AI-generated fake reviews, AI-driven harassment, Counterfeit content;

– medium level: Military robots, "Snake oil," Data poisoning, Machine learning cyberattacks, Autonomous combat drones, Online eviction, Facial recognition deception, Market bombardment;

– high level: Audio/video impersonation, Autonomous cars as weapons, Individual phishing, AI-controlled system breaches, Large-scale extortion, AI-generated fake news.

Conclusions. Based on all this, we can only conclude one thing: the threat of AI is real, and cybersecurity, along with everything else, is still at risk without the ability to counter it effectively.

References

1. Artificial Intelligence Is a Threat to Cybersecurity. It's Also a Solution. *BCG*. URL – https://www.bcg.com/publications/2018/artificial-intelligence-threat-cybersecurity-solution (date of access: 15.10.2023);
2. 20 ways AI enables criminals. *Mind Matters*. URL – https://mindmatters.ai/2023/04/20-ways-ai-enables-criminals (date of access: 19.10.2023);
3. Steve Wilson (CPO, Contrast Security) – with help from various AI technologies: «Cybersecurity and Artificial Intelligence: Threats and Opportunities». April 2023;
4. Centre for European Policy Studies (CEPS): «Artificial Intelligence and Cybersecurity». Brussels, May 2021. ISBN 978-94-6138-785-1;
5. ChatGPT. *OpenAi*. URL – https://chat.openai.com (date of access: 20.10.2023).

Author Information

Drakon Daria, ERI «Karazin Banking Institute», Cybersecurity in finance, daria.drakon@student.karazin.ua

Stiahlyk Natalia, Ph.D., Head of the Department of Information Technology and Mathematical Modeling Karazin Banking Institute, V.N. Karazin Kharkiv National University, natalia.stiahlyk@karazin.ua

Секція 1

БЕЗПЕКА ПЕРСОНАЛЬНИХ ДАНИХ КОРИСТУВАЧІВ ВЕБ-ЗАСТОСУНКІВ

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

Актуальність. В сучасному цифровому ландшафті, де веб-застосунки стають необхідною та незамінною складовою повсякденного життя, а активність онлайн зростає, актуальність забезпечення безпеки персональних даних користувачів стає критичною. З ростом технологічного прогресу збільшується ймовірність кіберзагроз, таких як хакерські атаки, фішинг, розкрадання даних, які можуть призвести до витоку конфіденційної інформації користувачів в веб-застосунках. Велика кількість людей використовує веб-застосунки для різноманітних цілей, включаючи фінансові операції «Mono Bank», покупки «Rozetka», обмін особистою інформацій. Це робить їх привабливою мішенню для кіберзлочинців. Законодавчі органи України впроваджують нові норми і стандарти щодо захисту особистої інформації [1]. Це вимагає від компаній та веб-застосунків дотримуватися строгих правил, що підсилює необхідність надійного захисту даних. Також були великі інциденти, такі як витоки даних у великих корпораціях, привертають значну увагу громадськості та підкреслюють необхідність покращення безпеки веб-застосунків. Забезпечення безпеки даних впливає на психологічний аспект споживачів. Користувачі виявляють більшу довіру та впевненість в використанні веб-сервісів, де їх данні належним чином захищені. Отже, розгляд та розробка стратегій для забезпечення безпеки персональних даних у веб-сервісах стає необхідністю для збереження довіри споживачів, стабільності онлайн-середовища та успішного функціонування цифрового суспільства.

Мета роботи полягає в тому що потрібно всебічно розглянути проблему несанкціонованого доступу до персональних даних та розробка стратегій для ефективного захисту цих персональних даних користувачів у веб-застосунках. Робота спрямована на аналіз існуючих загроз, визначення ключових принципів захисту даних, і розробку рекомендацій для забезпечення стабільності та конфіденційності в онлайн-сервісах.

Основні положення. В роботі встановлюються фундаментальні принципи та стратегії для ефективного захисту персональних даних в веб-застосунках. Враховуючи технічні та соціальні аспекти безпеки, щоб створити комплексний підхід для забезпечення безпеки. Приклад 1: Аналіз та дослідження останніх випадків атак на веб-застосунки, таких як атаки типу SQL ін’єкції, крос-сайтового сценаріювання (XSS) або викрадення

індентифікаторів сесій [2]. Приклад 2: Розгляд принципів енкрипції даних в покої, аутентифікації двофакторного типу, та систем моніторингу, таких як системи реєстрації подій, для виявлення непередбачуваних активностей. Приклад 3: Визначення конкретних процедур та політик безпеки, встановлення регулярних аудитів безпеки коду, підтримка систем патчінгу та імплементація функцій контролю доступу. Приклад 4: Створення веб-сайту або розділу в додатку, де користувачі можуть дізнатися про методи забезпечення своїх персональних даних та взаємодіяти з питаннями безпеки [3].

Висновки. В результаті проведеного аналізу вказують на важливість та актуальність заходів забезпечення безпеки персональних даних у веб-застосунках. Розроблені рекомендації та стратегії мають на меті сприяти створенню надійних та безпечних онлайн-сервісів для користувачів.

Список літератури

1. Політика безпеки персональних даних в Україні для веб-застосунків *Vlasne*. URL: https://www.vlasneua.com/policy (дата звернення 14.11.2023);
2. Найвідоміші вразливості веб-застосунків *XSS* та *SQL* ін'єкції, вразливості автентифікації. *DOU UA*. URL: https://dou.ua/forums/topic/40613/ (дата звернення 14.11.2023);
3. Забезпечення конфіденційності у компанії Apple. *Apple*. URL: https://support.apple.com/uk-ua/HT202303 (дата звернення 14.11.2023).

Відомості про авторів

Желтухіна Ірина Олександрівна, студентка кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», i.o.zheltukhina@student.csn.khai.edu
Желтухін Олександр Васильович, старший викладач кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», a.zheltukhin@csn.khai.edu

Секція 1

ЗАХИСТ МЕРЕЖЕВИХ ПРОТОКОЛІВ: ВАЖЛИВІСТЬ ТА СТРАТЕГІЇ ОБОРОНИ

Жмуцький М. А.
Національний університет «Запорізька політехніка»
Науковий керівник: Зайко Т. А.

Актуальність. Актуальність захисту мережевих протоколів у сучасному світі не може бути переоцінена. З кожним днем суспільство стає все більше цифровим, та залежність від мереж і технологій зростає. З цим зростанням збільшується і кількість потенційних кіберзагроз, з якими ми стикаємося. Ця актуальність посилюється щодня, бо мережеві протоколи є основними будівельними блоками всього цифрового світу – від корпоративних мереж до особистих комунікацій та публічних служб.

Зростання кількості зв'язаних пристроїв у мережі, таких як «Інтернет речей» (IoT), покладає ще більший тиск на захист мережевих протоколів. Ця нова хвиля підключених пристроїв створює додаткові можливості для зловмисників та ризики для приватності та безпеки. Відсутність належного захисту може призвести до серйозних наслідків, таких як витік особистої інформації, розповсюдження шкідливого програмного забезпечення та втрати доступу до систем. Тому актуальність захисту мережевих протоколів надзвичайно важлива в цьому епохальному переході до цифрового світу.

Метою даної доповіді є розгляд актуальних питань захисту мережевих протоколів, виявлення основних загроз та ризиків, а також надання рекомендацій щодо забезпечення безпеки при використанні мережевих протоколів.

Основні положення. Ключовим елементом забезпечення безпеки мережевих протоколів є поєднання аналізу загроз, шифрування даних, контролю доступу, регулярних оновлень та систем моніторингу для виявлення подій.

Щоб розробити ефективні заходи захисту мережевих протоколів, необхідно провести аналіз потенційних загроз і ризиків. Цей аналіз може включати в себе виявлення можливостей перехоплення пакетів, атак на протоколи авторизації та інших вразливостей на рівні транспортного та мережевого рівнів OSI моделі.

Шифрування є важливим способом захисту даних, що передаються по мережі. Протоколи, такі як TLS/SSL та IPSec, використовують шифрування для забезпечення конфіденційності та цілісності даних [1]. Важливо правильно налаштувати шифрування, щоб запобігти використанню застарілих алгоритмів та протоколів, які можуть бути легко зламані.

Аутентифікація та авторизація є важливими для захисту мережевих протоколів. Вони дозволяють ідентифікувати користувачів та надавати їм доступ до ресурсів лише в тому випадку, якщо вони мають на це право. Сильні методи аутентифікації, такі як двофакторна аутентифікація, і належно налаштовані правила доступу допомагають запобігти несанкціонованому доступу до ресурсів [1].

Розробники та вендори мережевих протоколів повинні регулярно випускати оновлення та патчі для усунення відомих вразливостей. Це допоможе запобігти експлуатації цих вразливостей зловмисниками [2].

Системи моніторингу та виявлення інцидентів допомагають виявити кібератаки на ранніх етапах, щоб можна було швидко відреагувати та мінімізувати збитки. Ці системи слід постійно оновлювати, щоб вони могли виявляти нові загрози [2].

Враховуючи ці основні положення та впроваджуючи їх на практиці, організації можуть підвищити захист даних, зменшити ризики кібератак і забезпечити безпеку мережевих протоколів.

Висновки. Мережеві протоколи є основою для передачі даних в Інтернеті. Їхній захист є критично важливим для забезпечення конфіденційності, цілісності та доступності даних. Зростаюча кількість загроз та ризиків вимагає постійного вдосконалення методів захисту мережевих протоколів. Правильно налаштований захист допоможе зменшити ймовірність кібератак та зберегти дані в безпеці.

Список літератури

1. Рівні та протоколи інформаційної безпеки. *UA5 ORG*. URL: https://ua5.org/protect/1688-rivni-ta-protokoly-informaczijnoyi-bezpeky.html (дата звернення: 27.09.2023);
2. Network Security Best Practices. *Netwrix*. URL: https://www.netwrix.com /network_security_best_practices.html (дата звернення: 28.09.2023).

Відомості про авторів

Жмуцький Максим Анатолійович, студент кафедри програмних засобів, Національний університету «Запорізька політехніка», maksym.zhmutskyi@gmail.com
Зайко Тетяна Анатоліївна, доцент кафедри програмних засобів, Національний університет «Запорізька політехніка», к.т.н., доцент, nika270202@gmail.com

Section 1

ONLINE BANKING INFORMATION SECURITY

Heorhii Zemlianko
National Aerospace University «Kharkiv Aviation Institute»
Scientific advisor: Vyacheslav Kharchenko

Relevance. In today's reality, the state of information security in online systems has become a global concern. In fact, the spread of cybercrime has transcended geographical boundaries and has become a critical international issue. It is noticeable that the fragile state of information security in financial institutions makes them increasingly vulnerable to potential cyber-attacks, which has raised alarm bells in the expert community [1].

There are numerous examples of online systems being disrupted. Intellectual property theft, for example, has become an alarmingly common occurrence in the digital world. Despite the universal nature of such incidents, banking institutions are still reluctant to publicly acknowledge such breaches. This reluctance is due, at least in part, to the profound impact that such admissions can have on customer confidence, which further complicates the situation.

Even in countries where e-business is at its peak, the volume of financial transactions conducted online is significantly limited. In practice, these transactions tend to involve relatively small amounts of money. This phenomenon is largely due to a lack of attention to information security in the complex environment of electronic systems [2].

A close analysis of the available data reveals a complex interaction between information security and the conduct of online business. For example, there have been numerous instances of major hacks and data breaches that have severely impacted organizations and limited their ability to conduct high-value financial transactions. These incidents are prime examples of deep information security issues.

Purpose. This study aims to comprehensively address key issues in the security of online banking systems by examining various aspects of information security. It aims to understand and evaluate the challenges faced by online systems in securing financial data and transactions. The research seeks to provide insights and recommendations to improve security measures in online banking. By analyzing emerging threats and technologies, it aims to provide a robust framework for protecting this critical financial infrastructure in the evolving digital landscape.

Principal provisions. Therefore, the issue of protecting online banking systems is of paramount importance in their development and operation. and operation. Information in online systems must be protected. At the same time, the cost of organizing protection should not exceed the losses that may arise from a breach of the protection system for the entire period of system operation. In addition, any elements of the protection system should not reduce the reliability of the on-line banking system.

An adequate level of information security of an on-line system is particularly relevant for open public systems that process classified information with limited access. After all, all devices and processes of the system (computer network) interact with each other according to a certain set of standards and are open to interaction with other systems (computer networks). This is due to the need to involve a large number of systems, a large number of technical means, and programs used in computer systems or networks. Therefore, a computer system that conforms to certain standards will be open to certain standards, will be open to interconnection with any other system that conforms to the same standards. This also applies to mechanisms for cryptographic protection of information or protection against unauthorized access to information.

Conclusions. Thus, the development of trends in the processing of banking information on the basis of modern automated technologies and the constant increase in the number of users of on-line systems are accompanied by the emergence of new threats, which are negative companions of scientific and technological progress. Therefore, the development of the security system of the on-line banking system should include the creation of a model of possible threats and the selection of effective security methods, which, in turn, should be an integral part of the on-line banking system at all stages of its operation.

List of references

1. Krebs on Security – In-depth security news and investigation. *Krebs on Security – In-depth security news and investigation*. URL – https://krebsonsecurity.com/ (date of access: 01.10.2023);
2. Scritube – publica fisierul tau pe internet, articole, documente, informatii online. *Scritube - publica fisierul tau pe internet, articole, documente, informatii online*. URL – https://www.scritub.com (date of access: 01.10.2023);
3. Як еволюціонує мобільний банкінг у світі та чому українські необанки на крок попереду. *PaySpace Magazine*. URL: https://psm7.com/ru/fintech/kak-evolyucioniruet-mobilnyj-banking-v-mire-i-pochemu-ukrainskie-neobanki-na-shag-vperedi.html (date of access: 01.10.2023).

Information about the authors

Heorhii Zemlianko, a PhD student from the Department of Computer Systems, Networks and Cybersecurity, National Aerospace University «Kharkiv Aviation Institute», g.zemlynko@student.csn.khai.edu
Vyacheslav Kharchenko, Dr. Sc., professor, Head of the Department of Computer Systems, Networks and Cybersecurity, National Aerospace University «Kharkiv Aviation Institute», v.kharchenko@csn.khai.edu

Секція 1

МЕТОДИ ЗАХИСТУ СУЧАСНИХ ВЕБСАЙТІВ ВІД XSS-АТАК

Канцібер Д. С.
Полтавський державний аграрний університет
Науковий керівник: Одарущенко О. М.

Актуальність. Практично кожна комерційна та державна організація має власний сайт, на якому зберігаються персональні дані інших людей, фінансова звітність та інша чутлива інформація, яка може бути цікава зловмисникам. Згідно дослідження [1] кількість XSS-атак збільшилася з 470 в 2011 році до 22,000 в 2022, і продовжує збільшуватися. Це складає близько 15% всіх атак на веб-сайти. Нажаль, більшість веб розробників та власників продуктів не надають достатньої уваги безпеці та протидії вразливостям. Для зменшення шкоди від XSS-атак потрібно використовувати сучасні методи захисту.

Метою роботи є вивчення та аналіз існуючих методів захисту сучасних веб-сайтів від XSS-атак.

Основні положення. XSS (Cross Site Scripting) – це атака, що полягає в введені шкідливого коду, що виконується в браузері клієнта (JavaScript) на веб сторінку, якою користуються інші люди. Ціллю таких атак зазвичай є перехват особистих даних, таких як cookies, або будь-яка інша інформація пов'язана з сеансом користувача.

Для захисту веб-сайту від XSS-атак існують наступні методи:

– шпаргалка по запобіганню XSS. Для попередження атак можна використовувати збірник правил. Наприклад: відхиляти все, зберігати ненадійні дані в таблицях стилів, body документа, популярних атрибутах (width, height тощо), або в значеннях GET запитів;

– перевірка вхідного тексту. Один з найпоширеніших методів захисту від XSS-атак. Його суть полягає в використанні спеціальних програмних модулів для аналізу та фільтрації вхідного тексту;

– CSP (Content Security Policy). Це політика безпеки, запроваджена для запобігання XSS, clickjaking та інших видів ін'єкційних атак. Розробники повинні встановити перелік довірених джерел, з яких на їх вебсайт можна завантажувати файли (JavaScript, CSS, аудіо та відео файли та інші)[2];

– HTTP-only cookies. Встановлення атрибуту «HttpOnly» для кукі, в яких міститься ідентифікатор сесії ускладнює доступ до кукі з боку скриптів, запущених у контексті сторінки;

– Xsser. Автоматизований фреймворк, що допомагає знаходити, впроваджувати та документувати XSS вразливості. Цей інструмент допомагає тестувати рівень захищеності веб-сайту [3];

– Інструменти глибокого навчання. Розробка таких інструментів розпочалась в 2018-2020 рр. В них застосовуються різноманітні методи такі як: RNN, CNN, CDNN. Окрім методів «чорного ящику», існує метод «сірого ящику». В такому підході використовувався HTML-вивід з чутливими до контексту XSS-дефектами на основі HTTP-запитів [4].

Висновки. Для захисту від XSS атак існують різноманітні методи та програмні засоби. Важливо розуміти, що в кожного методу і засобу є свої переваги та недоліки. Для забезпечення більш ефективного захисту можна комбінувати підходи, поєднуючи їх між собою. Розвиток технологій та поява нових загроз вимагають постійного вдосконалення методів захисту. Розробники повинні вдосконалювати свої підходи до безпеки, впроваджувати нові технології та методи захисту, а також систематично оновлювати вже існуючі заходи безпеки.

Список літератури

1. Increasing Trend of XSS Attacks. *ResearchGate.* URL: https://www.researchgate.net/figure/Increasing-trend-of-XSS-attacks_fig1_361539153 (дата звернення 11.11.2023);
2. Content Security Police (CSP). *Imperva* URL: https://www.imperva.com/learn/application-security/content-security-policy-csp-header (дата звернення 12.11.2023);
3. XSSer – Automated Web Pentesting Framework Tool to Detect And Exploit XSS Vulnerabilities. *GBHackers On Security.* URL: https://gbhackers.com/xsser-automated-framework-detectexploit-report-xss-vulnerabilities (дата звернення 11.11.2023);
4. V S Stency and N Mohanasundaram, A Study on XSS Attacks: Intelligent Detection Methods: 2021 J. Phys.: Conf. Ser. 1767 012047.

Відомості про авторів

Канцібер Дмитро Сергійович, студент кафедри інформаційних систем та технологій, Полтавський державний аграрний університет, dmytro.kantsiber@st.pdau.edu.ua
Одарущенко Олег Миколайович, професор кафедри інформаційних систем та технологій, Полтавський державний аграрний університет, д.т.н., професор, odarushchenko@gmail.com

Секція 1

РОЗРОБКА ПОЛІТИКИ БЕЗПЕКИ ФІНАНСОВОЇ УСТАНОВИ

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

Актуальність. Фінансова установа є об'єктом потенційних загроз, таких як кібератаки, шахрайства, внутрішні злочини, а також системні ризики, пов'язані зі змінами на фінансовому ринку. Розробка політики безпеки (ПБ) стає важливим інструментом для ідентифікації, управління та зменшення цих ризиків. Фінансові установи мають значний вплив на економіку та суспільство, тому забезпечення їх безпеки є надзвичайно важливою задачею [1].

Метою є дослідити існуючі види ПБ та різновидність фінансових установ. Визначити головні кроки для розробки політики безпеки фінансової установи.

Основні положення. Фінансова установа – юридична особа, яка відповідно до закону надає одну чи декілька фінансових послуг, а також інші послуги (операції), пов’язані з наданням фінансових послуг, у випадках, прямо визначених законом, та внесена до відповідного реєстру в установленому законом порядку [2]. Фінансові установи грають важливу роль у фінансовій системі, сприяючи економічному розвитку та забезпечуючи доступ до фінансових ресурсів для підприємств і особистого використання. До фінансових установ належать банки, кредитні спілки, ломбарди, лізингові компанії, довірчі товариства, страхові компанії, установи накопичувального пенсійного забезпечення, інвестиційні фонди і компанії та інші юридичні особи, виключним видом діяльності яких є надання фінансових послуг, а у випадках, прямо визначених законом, - інші послуги (операції), пов’язані з наданням фінансових послуг. [2]

У доповіді ПБ визначається як документований затверджений функціонуючий процес, який визначає загальні засади та цілі для безпечності організації та управління ризиками [3]. Вона включає в себе широкий спектр заходів, спрямованих на ідентифікацію, управління та мінімізацію ризиків, загроз та вразливостей, що можуть впливати на безпеку організації або її діяльність.

Види ПБ можуть розрізнятися залежно від контексту та сфери застосування, проте основні категорії включають наступні: інформаційна політика безпеки, фізична політика безпеки, кадрова політика безпеки, фінансова політика безпеки.

В даній роботі розглядаються всі вище вказані ПБ. Однак більш уваги приділяється інформаційної ПБ, оскільки це прямо стосується контексту.

Також не менше уваги слід приділити фінансовій ПБ, адже тема стосується саме фінансових установ.

Висновки. Отже, розробка політики безпеки фінансової установи є важливим процесом, який дозволяє організації визначити свої стратегії та підходи до забезпечення безпеки. Існує кілька кроків, які можуть бути включені до процесу розробки політики безпеки:

- аналіз ризиків: оцінка потенційних загроз та ризиків, якими зазвичай зіштовхується організація. Це може включати зовнішні загрози, такі як кібератаки, природні лиха, конкуренція, а також внутрішні загрози, такі як недостатня кваліфікація персоналу, внутрішнє шахрайство тощо;
- визначення цілей: формулювання конкретних цілей безпеки, які організація бажає досягти. Ці цілі повинні бути відповідними для організації та відображати її потреби та цінності;
- встановлення політичних принципів: формулювання принципів та цінностей, які організація відстоює в сфері безпеки. Це може включати принципи конфіденційності, цілісності, доступності, прозорості, відповідності законодавству та інших стандартів безпеки;
- розробка процедур та стандартів: створення конкретних процедур, стандартів та положень, які деталізують способи реалізації політики безпеки. Ці документи можуть включати процедури контролю доступу, управління ризиками, управління інцидентами, навчання та свідомості з питань безпеки;
- комунікація та навчання: забезпечення відповідного інформування та навчання працівників є важливими елементами розробки політики безпеки, оскільки залучення працівників та їх усвідомлення ролі та відповідальності в сфері безпеки є ключовим для її ефективного впровадження.

Список літератури

1. Принципи безпеки фінансових установ в Україні URL – http://psae-jrnl.nau.in.ua/journal/1_81_2021_ukr/18.pdf (дата звернення 27.06.2023);
2. Закон України «Про фінансові послуги та державне регулювання ринкув фінансових послуг» від 07.01.2023 №2664-III, Розділ I, стаття 1, пункт 1 URL – https://zakon.rada.gov.ua/laws/show/2664-14#Text (дата звернення 27.06.2023);
3. Міжнародний стандарт ISO/IEC 27001 URL – http://www.itref.ir/uploads /editor/2ef522.pdf (дата звернення 27.06.2023).

Відомості про авторів

Кирина Діана Віталіївна, магістрантка кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», d.kyryna@student.csn.khai.edu
Пєвнєв Володимир Яковлевич, професор кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», д.т.н., доцент, v.pevnev@csn.khai.edu

Секція 1

ДОСЛІДЖЕННЯ ТА РОЗРОБКА МОДЕЛІ ЗАГРОЗ КОМЕРЦІЙНОГО ВЕБ-СЕРВІСУ

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

Актуальність. Не можна заперечувати, що онлайн-шопінг популярний у наш час. Дослідження показують, що це більше, ніж просто тенденція. Клієнти продовжуватимуть звертатися до Інтернету щоразу, коли хочуть зробити роздрібну покупку. Згідно дослідженням Forbes Adviser очікується, що світовий ринок електронної комерції у 2023 році становитиме 6,3 трильйона доларів, та що до 2026 року ринок електронної комерції становитиме понад 8,1 трильйона доларів [1]. У той же час найуразливішою галуззю є електронна комерція, яка зазнає 32,4% атак у різних формах [2].

За останні кілька років у галузі електронної комерції сталася низка витоків даних. Ці порушення не тільки збільшують репутаційні, фінансові та операційні ризики, але й вічно переслідують бізнес електронної комерції, оскільки одне порушення даних коштує компанії в середньому 3,86 мільйона доларів і займає 280 днів для локалізації [3]. 10,5 трильйонів доларів. Саме стільки коштуватиме компаніям кіберзлочинність до 2025 року – за даними Cyber Ventures, це 15% ріст кожного року [4]. Тому актуальність кібербезпеки для поточних та нових комерційного веб-сервісу як ніколи висока.

Метою даної роботи є дослідження безпеки та розробка моделі загроз яка буде слугуватиме структурованим фреймворком, який ідентифікує, аналізує та класифікує потенційні загрози та вразливості, характерні для комерційних веб-сервісів.

Основні положення. Для розробки моделі загрози доступні кілька систем і методологій. Деякі широко використовувані фреймворки безпеки веб-служб включають: модель STRIDE – забезпечує структурований підхід до ідентифікації загроз з точки зору цих категорій, допомагаючи систематично оцінювати ризики; модель DREAD – це система оцінки ризиків, яка використовується для кількісного визначення серйозності виявлених загроз і визначення пріоритетів на основі їх потенційного впливу; методологія OCTAVE зосереджена на виявленні та оцінці ризиків з точки зору бізнес-цілей, інформаційних активів і вразливостей, надаючи цілісне уявлення про ризики безпеці; методологія PASTA – це методологія, орієнтована на ризик, яка об’єднує моделювання загроз, оцінку ризиків і симуляцію атак для систематичного аналізу загроз і визначення відповідних заходів безпеки.

Використовуючи ці фреймворки та методології, організації можуть прийняти структурований підхід до моделювання загроз і підвищити ефективність своїх заходів безпеки.

Висновки. У сучасному цифровому ландшафті комерційні веб-сервіси відіграють вирішальну роль у сприянні онлайн-транзакцій, комунікації та обміну інформацією. Однак із зростанням довіри до веб-сервісів зростає й потреба вирішувати постійну загрозу, яка створює значні ризики для їх безпеки. Щоб забезпечити захист цінних даних, важливо розробити ефективні моделі загроз, спеціально адаптовані до унікальних проблем, з якими стикаються комерційні веб-сервіси. Моделювання загроз має першочергове значення в сфері безпеки веб-служб. Воно забезпечує структурований підхід до виявлення та оцінки потенційних загроз, характерних для комерційних веб-служб, що дозволяє організаціям покращити розуміння ризиків безпеки та дати можливість постачальникам веб-послуг запровадити надійні заходи безпеки для захисту своїх систем, даних клієнтів і загальних бізнес-операцій.

Список літератури

1. 38 E-Commerce Statistics Of 2023. *Forbes Advisor*. URL – https://www.forbes.com/advisor/business/ecommerce-statistics (дата звернення: 08.02.2023);
2. E-Commerce Security Infographics – Statistic, Issues, And Solutions for 2022. *LinkenIn Nitesh Behani blog*. URL – https://www.linkedin.com/pulse/e-commercesecurity-infographics-statistic-issues-nitesh-behani- (дата звернення: 17.05.2022);
3. Major e-commerce data breaches: What we can learn from them. *DataQuest magazine*. URL – https://www.dqindia.com/major-e-commerce-data-breaches-whatwe-can-learn-from-them (дата звернення: 10.08.2022);
4. Cybercrime To Cost The World $10.5 Trillion Annually By 2025. *Cybercrime magazine*. URL – https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025 (дата звернення: 13.11.2020).

Відомості про авторів

Кислицин Олександр Олександрович, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», o.o.kyslytsyn@student.csn.khai.edu

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

Секція 1

АНАЛІЗ АНТИВІРУСНИХ СИСТЕМ ДЛЯ ЗАХИСТУ ІНФОКОМУНІКАЦІЙНИХ СИСТЕМ

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

Актуальність. Аналіз антивірусних систем для захисту інфокомунікаційних систем залишається критичним напрямком досліджень в контексті зростаючих загроз кібербезпеці. Застосування сучасних алгоритмів в цій галузі дозволяє не лише ефективно виявляти й блокувати нові види загроз, а й оптимізувати системи захисту, реагуючи на змінні та складні атаки. Це важливо не лише для захисту користувачів та їх даних, а й для забезпечення безпеки критичних інфраструктур та глобальних мереж, які використовуються у сферах фінансів, медицини, енергетики та інших важливих галузях. На фоні постійного розвитку технологій та зростаючої кількості пристроїв, що підключаються до мережі, проблема кібербезпеки набуває ще більшого значення.

Алгоритми антивірусних систем стають необхідним інструментом у протидії різноманітним загрозам, включаючи шкідливі програми, фішинг, атаки з використанням вразливостей та інші методи зловживання, що стали більш витонченими й складними. Ця тема не лише стосується сфери інформаційних технологій, але й має важливість для захисту особистої конфіденційної інформації, фінансових активів та важливих даних, що зберігаються у різних форматах та мережевих середовищах. Отже, дослідження та аналіз антивірусних систем для захисту інфокомунікаційних систем залишається актуальним та важливим у сучасному цифровому світі, де кібербезпека стає ключовим аспектом для функціонування різноманітних сфер діяльності.

Мета роботи. Провести аналіз та порівняння антивірусних систем для захисту інфокомунікаційних систем.

Основні положення. Для дослідження антивірусних систем для захисту інфокомунікаційних систем у доповіді розглянути найбільш поширені антивірусні програми:

Malwarebytes: Оцінка ефективності у виявленні та видаленні шкідливих програм різних типів, у тому числі вірусів, троянів, шпигунського ПЗ. Аналіз його здатності виявляти загрози в реальному часі та умови виявлення нових вірусів.

Avast Antivirus: Оцінка здатності програми виявляти та блокувати віруси та інші загрози, вплив програми на швидкодію системи та способи виявлення вірусів у віртуальних середовищах.

ESET NOD32 Antivirus: Аналіз системи виявлення нових вірусів та взаємодії з іншими захисними програмами. Оцінка ефективності виявлення та блокування загроз різного типу.

AVG Antivirus: Перевірка його здатності виявляти та блокувати віруси, співпраця з іншими захисними програмами та зручність у використанні для користувача.

У доповіді наведені результати дослідження для кожної з цих систем. Під час цих досліджень вимірювалась можливості та ефективності у виявленні та блокуванні вірусів, реакцію на нові загрози, вплив на продуктивність системи, можливості виявлення вірусів у реальному часі та на віртуальних платформах. Крім того розглядались можливості щодо доступності оновлень та взаємодію з різними операційними системами.

Висновки. Робота присвячена порівняльному аналізу антивірусних систем. Було проведено аналіз кожного з антивірусів, наведено результати порівняльного аналізу розглянутих антивірусів та досліджено недоліки та переваги кожного з антивірусів.

Список літератури

1. ANALYSIS AND RESEARCH OF THE CHARACTERISTICS OF STANDARDIZED IN UKRAINE ANTIVIRUS SOFTWARE. *Researchgate.* URL – https://www.researchgate.net/publication/334198724_analysis_and_research_of_the_characteristics_of_standardized_in_ukraine_antivirus_software (дата звернення: 10.11.2023);
2. Smith J. Introduction to Antivirus Systems. New York : PublisherX, 2015. 300 c.;
3. Salomon D. Computer Viruses and Malware. Miccypi : Springer, 2020. 420c.;
4. Kaspersky E. Antivirus Evolution: From Detection to Prevention. New York : Springer, 2019. 450c.

Відомості про авторів

Корпань Владислав Миколайович, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ»

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

Section 1

IMPACT OF CONTAINERIZATION ON SECURITY IN DEVOPS ARCHITECTURE

Bohdan Kosarevskyi
National Aerospace University «Kharkiv Aviation Institute»
Scientific advisor: Dmytro Uzun

Relevance. The integration of containerization into DevOps practices has ushered in a paradigm shift in software development and deployment. As organizations increasingly adopt container orchestration platforms like Kubernetes and Docker, it becomes imperative to scrutinize the impact of this technological evolution on the security landscape within DevOps architectures [1, 2]. This work explores the multifaceted relationship between containerization and security, shedding light on the challenges and opportunities it presents. By examining the nuances of this integration, we aim to provide a comprehensive understanding of how containerization influences security measures in DevOps workflows.

Purpose. The goal of this work is to examine how the advent of containerization technologies, exemplified by Docker, has transformed the landscape of software development, testing, and deployment. Containers, by encapsulating applications and their dependencies, aim to guarantee uniformity across diverse environments. Although this approach enhances agility and scalability, it simultaneously introduces novel security considerations. The primary objective is to initiate a comprehensive reevaluation of security practices within containerized DevOps environments, addressing vulnerabilities intrinsic to this architecture. Through this exploration, we seek to discern the nuanced impact of containerization on security in DevOps workflows.

Main provisions. One notable impact of containerization on DevOps security lies in the isolation of application components. Isolation offered by containers reduces the attack surface, limiting the potential impact of security breaches. However, this containment introduces challenges related to shared kernel vulnerabilities and the need for continuous monitoring to detect and respond to potential threats promptly.

To comprehend the full extent of the impact, a comparative analysis of security measures in traditional and containerized DevOps environments is crucial. Traditional DevOps often relies on virtual machines, each running a full operating system. In contrast, containers share the host system's kernel, making them more lightweight and efficient. This shift presents a trade-off between resource efficiency and security isolation.

Containerized DevOps environments benefit from rapid scaling and resource optimization, but they necessitate enhanced attention to container image security, orchestration vulnerabilities, and the secure configuration of container runtimes.

By contrasting the strengths and weaknesses of traditional and containerized DevOps, organizations can make informed decisions about their security postures.

A critical aspect of the impact of containerization on DevOps security is the identification and mitigation of risks within the continuous integration/continuous deployment (CI/CD) pipeline [3]. The dynamic nature of containerized microservices introduces challenges in maintaining a consistent and secure deployment environment. Security measures must be integrated seamlessly into the CI/CD pipeline, incorporating vulnerability scanning, image signing, and runtime protection to ensure the integrity of the entire software supply chain.

Conclusions. In conclusion, the impact of containerization on security in DevOps architecture is a nuanced and evolving topic that demands careful consideration. While containerization brings unprecedented agility and efficiency, it also introduces a new set of security challenges. The benefits of containers must be balanced with the need for robust isolation and continuous monitoring. A comparative analysis helps organizations make informed decisions about adopting containerization in their DevOps workflows, considering the specific security requirements of their applications.

The future of DevOps security lies in the ability to harness the advantages of containerization while proactively mitigating its inherent risks. Through ongoing research, collaboration, and the implementation of evolving security practices, organizations can navigate the evolving landscape of DevOps with confidence in the security of their containerized workflows.

List of references

1. Pod Security Standards. *Kubernetes*. URL – https://kubernetes.io/docs/concepts/security/pod-security-standards (date of access: 01.11.2023);
2. Security best practices. *Docker docs*. URL – https://docs.docker.com/develop/security-best-practices (date of access: 01.11.2023);
3. Adding Security Into CI/CD Pipeline *Ciklum*. URL – https://www.ciklum.com/blog/adding-security-into-ci-cd-pipeline (date of access: 02.11.2023).

Information about the authors

Bohdan Kosarevskyi, a master's student from the Department of Computer Systems, Networks and Cybersecurity, National Aerospace University «Kharkiv Aviation Institute», b.v.kosarevskyi@student.csn.khai.edu
Dmytro Uzun, PhD, Associate Professor from the Department of Computer Systems, Networks and Cybersecurity, National Aerospace University «Kharkiv Aviation Institute», d.uzun@csn.khai.edu

Секція 1

ОЦІНКА РЕЗИЛЬЄНТНОСТІ ЦЕНТРІВ ОБРОБКИ ІНФОРМАЦІЇ

Кривенко Д. О.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Брежнєв Є. В.

Актуальність. Простій в роботі центру обробки даних (ЦОД) в декілька хвилин може призвести до фінансових та репутаційних втрат якщо, було допущено втрату даних своїх клієнтів. Тому постає питання забезпечення резильєнтності роботи ЦОД. На роботу таких центрів можуть впливати різні аварійні ситуації. Це можуть бути: кібератаки, несправність обладнання, програми з вимогою викупу, вимкнення електроенергії, стихійні лиха та навіть людські помилки. ІТ-команди з питань аварійного відновлення ЦОД мають розглянути всі можливі загрози і розробити плани дій щодо підвищення резильєнтності ЦОД.

Метою даної роботи є оцінка резильєнтності, як інтегрального показника захисту ЦОД.

Основні положення. Типовий ЦОД включає декілька технічних майданчиків які складаються з серверних шаф, мережевого обладнання, які забезпечують роботу ЦОД та його клієнтів. Завдання полягає в тому щоби забезпечити кібербезпеку ЦОД. Оцінювати рівень резильєнтності можна декількома способами.

Існує спосіб оцінки за допомогою відповідності до стандартів. Перевага способу в тому, що використовуватимуться методи сумісні між собою та добре налагоджені. Але є недоліки, метод не гнучкий, кібер загрози швидко адаптуються на відміну від стандартів які можуть швидко стати не актуальними. Потрібен великий час на оновлення стандартів та атестацію.

Другий метод заснований на математичних моделях. Математична функція може включати декілька показників - наприклад, частка втраченої інформації, інвестиції в захист інформації, їх рентабельність. Ці показники не однорідні між собою. та Не має загального методу вимірювання цих параметрів. Пошук рішення для захисту ускладнюється також тим, що протистояння в інформаційній сфері ведеться в умовах невизначеності, коли дії суперника невідомі і можуть бути передбачені лише з певною ймовірністю на основі статистичних даних або з допомогою експертної оцінки.

В якості показника резильєнтності пропонується використовувати параметр цільовий час відновлення (RTO). Він зосереджується на доступності сервісів та даних, враховує всі аспекти ІТ-інфраструктури, покладається на best practice в побудові відмовостійкої інфраструктури та моніторинг. За час встановленим RTO застосовані методи захисту повинні

виявити проблему, відреагувати та застосувати інструменти відновлення поки це не стане критичною втратою часу для роботи ЦОД.

Для визначення РТО пропонується застосувати систему моніторингу «Nagios». Це програма моніторингу комп'ютерних систем і мереж. Вона призначена для спостереження, контролю стану обчислювальних вузлів і служб, оповіщення адміністратора, якщо якісь із служб припиняють свою роботу.

Висновок. Резильєнтність – це інтегральний показник захисту ЦОД. Він враховує багато аспектів захисту, стійкості та можливості відновлення, які працюють в комплексі. Розглянутий ілюстративний приклад визначення РТО для типового ЦОД підтверджує можливість практичного застосування даного показника для задач визначення раціонального варіанту побудови систем захисту.

Список літератури

1. Effective Risk Management in the Data Center. *Datacenterknowledge*. URL – https://www.datacenterknowledge.com/archives/2017/05/08/effective-risk-management-data-center#close-modal (дата звернення: 26.09.2023);
2. Designing and Managing Data Centers for Resilience: Demand Response and Microgrids. U.S. Department of Energy;
3. What is data center resiliency and why is it important?. *Techtarget.* URL – https://www.techtarget.com/searchdatacenter/definition/resiliency (дата звернення: 06.10.2023).

Відомості про авторів

Кривенко Дмитро Олександрович, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», d.o.kryvenko@student.csn.khai.edu

Брежнєв Євген Віталійович, професор кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», д.т.н, старший науковий співробітник, e.brezhnev@csn.khai.edu

Секція 1

РОЗРОБКА І ДОСЛІДЖЕННЯ ІНТЕГРОВАНИХ СИСТЕМ БЕЗПЕКИ ЦЕНТРІВ З ОБРОБКИ ДАНИХ

Кривенко Д. О.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Пєвнєв В. Я.

Актуальність. Центр обробки даних (ЦОД) виконує функції обробки, зберігання і розповсюдження інформації, як правило, в інтересах корпоративних клієнтів – він орієнтований на вирішення бізнес-завдань шляхом надання інформаційних послуг. Консолідація обчислювальних ресурсів і засобів зберігання даних в ЦОД дозволяє скоротити сукупну вартість володіння IT- інфраструктурою шляхом можливості ефективного використання технічних засобів, наприклад, перерозподілу навантажень, а також шляхом скорочення витрат на адміністрування.

Сьогодні немає єдиного закону, який би регулював створення ЦОД і послуги, які вони надають за допомогою своєї інфраструктури, і вимоги до їхньої якості. Тож ми можемо виділити декілька проблемних питань з цього приводу, а саме технічний і програмний аспект та також правовий який повинен регулювати ці питання у взаєминах між постачальником послуг ЦОД та замовником. В технічному плані повинно бути забезпечена належна інфраструктура, комунікації та обладнання які забезпечують виконання завдання ЦОД, а також вирішення питань з безпеки як фізичної, функціональної, так і кібербезпеки.

Мета. Розглянути як сучасні компанії в Україні вирішують завдання з постачання послуг дата-центру, які їх особливості у вирішенні цього питання, також дослідити як забезпечуватися безпека, цілісність та доступність такої складної системи як ЦОД.

Основні положення. Отже оцінюючи можливі ризики що зустрічаюся в таких масивних системах можна виділити DDoS-атаки — надсилання великих обсягів фальшивого трафіку до комп'ютерної системи доти, доки обсяг трафіку не переповнить її, позбавивши доступу законних користувачів, встановлення шпигунського ПО, проникнення та викрадення інформації з носіїв або її псування, варто відмітити що проникнення може відбутися як зсередини так і ззовні, також проблеми доступу до інформації та її конфіденційність. Так також може відбутися фізичне втручання в роботу обладнання чи його знищення, різноманітні надзвичайні ситуації як відключення світла, повені, землетруси.

Вирішуючи питання ризиків було створено міжнародний стандарти такі як Uptime Institute та TIA-942, які регулюють ці питання. Мережа центру обробки даних вимагає повного аналізу нульової довіри, щоб бути включеною в будь-яку архітектуру ЦОД. Брандмауери центрів обробки

даних, засоби контролю доступу до даних, системи запобігання вторгненням (IPS), WAF і їхні сучасні аналоги системи захисту веб-додатків і API (WAAP) повинні бути належним чином розроблені, щоб гарантувати їхнє масштабування відповідно до потреб мереж центрів обробки даних. Крім того, вибираючи сховище даних або постачальника хмарних послуг, дуже важливо розуміти запобіжні заходи, які вони застосовують для свого власного ЦОД. Проведення аудитів безпеки. Це процес систематичного перевірки безпеки системи, включаючи перевірку наявності вразливостей. Він включає огляд конфігурацій, перевірку політик безпеки, перевірку прав доступу, аналіз журналів подій та інші процедури.

Висновки. До вирішення питань безпеки дата-центрів треба підходити комплексно, бо компоненти тісно пов'язані між собою. Обробка великого масиву даних компаніям потрібує забезпечення багатьох вимоги до інфраструктури, об'єму, захисту, цілісності та доступності інформації.

Список літератури

1. Юридичні основи роботи дата-центрів. *Mklegalservice.* URL – https://mklegalservice.com/tpost/4plhynlcg1-yuridichn-osnovi-roboti-data-tsentrv (дата звернення: 9.10.23);
2. С.В. Батечко, О.Ю. Лебедєва, В.В. Зоріло Методика оцінки захищеності інформаційних систем (2021). *Immm.* URL – http://immm.op.edu.ua/files/archive/n3_v11_2021/2021_3(3).pdf (дата звернення: 10.10.23);
3. TIA-942 Data Center Standards Overview. *TE Connectivity.* URL – http://www.te.com/content/dam/te/global/english/industries/enterprise-network-solutions/knowledge-center/documents/enterprise-white-paper-tia-942-data-center-standards-overview-102264ae.pdf (дата звернення: 10.10.23).

Відомості про авторів

Кривенко Дмитро Олександрович, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», d.o.kryvenko@student.csn.khai.edu
Пєвнєв Володимир Яковлевич, професор кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», д.т.н, доцент, v.pevnev@csn.khai.edu

Секція 1

РОЗРОБЛЕННЯ ТА ДОСЛІДЖЕННЯ ЗАСОБІВ КІБЕРБЕЗПЕКИ ВЕБ-СИСТЕМИ ДОСТАВКИ ПОСИЛОК З ВИКОРИСТАННЯМ БПЛА

Крюченков О. І.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Морозова О. І.

Актуальність. У сучасному інформаційному суспільстві на сьогоднішній день веб-система є невід'ємною частиною в будь-якій сфері, вона забезпечує інформаційну підтримку, функціональні можливості та багато іншого. Веб-система має бути зручною та функціональною [1]. Розробка веб-застосунків в мережі інтернет є дуже актуальним напрямком. Тенденція розвитку сайті зростає з кожним роком. Така популярність зумовлена зручністю використання сучасних веб-систем [2].

Крім того, кібербезпека стає все важливішою в галузі веб-систем доставки посилок з використанням безпілотних літальних апаратів (БПЛА) 3]. Зі зростанням обсягів пересилання даних та електронних операцій у цій галузі, забезпечення безпеки є обов'язковим завданням. Це важливо з метою захисту конфіденційності даних, запобігання несанкціонованому доступу та забезпечення цілісності операцій.

Мета роботи полягає в розробленні та аналізі засобів кібербезпеки для веб-системи доставки посилок з використанням БПЛА, зокрема розгляданні методів і алгоритмів, які можуть забезпечити високий рівень безпеки в цій галузі.

Основні положення. Для досягнення поставленої мети, розглянемо основні аспекти кібербезпеки в контексті веб-систем доставки посилок з використанням БПЛА [4, 5]. Основні завдання для захисту даних та забезпечення безпеки операцій:

1. Аналіз загроз. Це може включати в себе атаки на мережевий рівень, а також можливі ризики, пов'язані з фізичним доступом до БПЛА.
2. Розроблення заходів забезпечення. Серед них є методи і технології кіберзахисту, які можуть бути використані для захисту веб-системи доставки посилок, зокрема шифрування даних, аутентифікацію користувачів, контроль доступу та моніторинг системи.
3. Використання БПЛА в забезпеченні кібербезпеки, зокрема в областях моніторингу та виявлення загроз, а також захисту даних під час транспортування посилок.

Процес проєктування веб-системи зазвичай складається з трьох частин:

– розробка концепції ресурсу, в якій представлені основні ідеї, та аналіз, спрямований на визначення потреб кінцевого користувача;

– логічне проектування, в якому формується сценарій майбутньої роботи з описом можливих сторінок порталу та гіпертекстових посилань між ними, розглядом способів активізації сторінок шляхом впровадження мультимедіа;

– фізичний дизайн, безпосереднє створення сайту.

Висновки. Робота присвячена розробленню та дослідженню засобів кібербезпеки веб-системи доставки посилок з використанням БПЛА. В ході роботи необхідно проаналізувати загрози, розробити та впровадити заходи забезпечення безпеки та використовувати переваги БПЛА у контексті кібербезпеки веб-системи доставки посилок.

Список літератури

1. Cybersecurity in the Field of Parcel Delivery Systems. *Atlanticcouncil.* URL – https://www.atlanticcouncil.org/blogs/geotech-cues/ (дата звернення: 10.10.23);
2. Cybersecurity Measures for Parcel Delivery Web Systems. *Postandparcel.* URL – https://postandparcel.info/122245/features/e-commerce-features/cyber-security-attacks/ (дата звернення: 11.10.23);
3. Utilizing UAVs for Enhancing Cybersecurity in Parcel Delivery. *isprs-annals.* URL – https://isprs-annals.copernicus.org/articles/IV-4-W4/73/2017/isprs-annals-IV-4-W4-73-2017.pdf (дата звернення: 12.10.23);
4. Cybersecurity in Transportation Systems. *Tamu.* URL – https://static.tti.tamu.edu/tti.tamu.edu/documents/TTI-2023-1.pdf (дата звернення: 12.10.23);
5. Web System Security: Key Aspects and Challenges. *Vaadata.* URL – https://www.vaadata.com/blog/how-to-secure-a-website (дата звернення: 15.10.23).

Відомості про авторів

Крюченков Олег Ілліч, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», o.kriuchenkov@student.csn.khai.edu
Морозова Ольга Ігорівна, професор кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», д.т.н., доцент, o.morozova@csn.khai.edu

Секція 1

КІБЕРАТАКИ НА БЕЗПІЛОТНІ ЛІТАЛЬНІ АПАРАТИ: КЛАСИФІКАЦІЯ ТА УРАЗЛИВОСТІ

Логачов М. Г.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Фесенко Г. В.

Актуальність. Використання БПЛА для розмінування стає важливою стратегією для зменшення ризиків, пов'язаних із мінно-вибуховими об'єктами в Україні. БПЛА дозволяють проводити швидку та безпечну розвідку та розмінування, що дозволяє знизити ризики для життя людей, оптимізувати час і ресурси, а також забезпечити більш точні та ефективні результати при розмінуванні [1].

Метою роботи є дослідження та аналіз методів збору та передачі даних з безпілотних літальних апаратів (БПЛА) з метою виявлення потенційних уразливих точок у процесі передачі цих даних.

Основні положення. БПЛА, також відомі як дрони, використовуються для різноманітних застосувань і поділяються на дві основні категорії: цивільні та військові.

Під час управління дронами оператор постійно обмінюється різноманітними пакетами даних через бездротовий зв'язок. Ці дані включають відео, аудіо, інформацію від датчиків та оброблені дані. Керуючі пакети містять команди, інструкції, інформацію про стан системи, позицію та інші дані для ефективного управління дронами та їхніми мережами [2]. Як високооптимізована кібер-фізична система, дрони піддаються широкому спектру можливих кібератак.

Кібератака – це агресивна дія з злочинними намірами, що впливає на функції обчислення та комунікації. Хоча атаки можуть призвести до деяких поступових збоїв у вимогах кібербезпеки, такі збої можуть не бути кінцевою метою зловмисника. Таким чином, кібератака може бути складним багатоетапним процесом. Наприклад, кібератака може складатися з трьох етапів. На першому етапі до БПЛА надсилають фальшиві навігаційні повідомлення, що призводить до неправильного розрахунку його координат. На другому етапі супротивник глушить канал управління, щоб БПЛА не отримував команди від наземної станції управління. І, нарешті, на третьому етапі за допомогою підроблених навігаційних повідомлень і без команди управління БПЛА може бути дезорієнтованим і зрештою впасти на землю [3].

Розглядаючи кібератаку як атомарну на кожному етапі, та классифікуючи ці атаки на основі їх точок входу, можна виділити три основні типи входу в атаку, а саме: радіоканал, повідомлення та бортова система, де на кожному з кількох етапів атомарна атака спричиняє

додатковий збій у системі кібербезпеки та приводить БПЛА до більш скомпрометованого стану, що ближче до кінцевої мети зловмисника [4].

На основі цих точок входу, можна розподілити кібератаки на БПЛА на такі шість категорій: блокування каналу (Channel Jamming), перехоплення повідомлень (Message Interception), видалення повідомлень (Message Deletion), впровадження повідомлень (Message Injection), фальсифікація повідомлень (Message Spoofing), атака на бортову систему (On-Board System Attack)

Висновки. У контексті кібербезпеки нам потрібно забезпечити конфіденційність, цілісність та автентичність інформації, якою керуються БПЛА. Крім того, ми повинні забезпечити доступність послуг, які використовуються або пропонуються БПЛА. Ця доступність послуг, в поєднанні з конфіденційністю, цілісністю та автентичністю інформації, узагальнюється вимогами кібербезпеки БПЛА.

Список літератури

1. Федоренко Г. Л., Фесенко Г. В., Харченко В. С. «Аналіз методів і розроблення концепції гарантованого виявлення та розпізнавання вибухонебезпечних предметів.» Сучасний стан наукових досліджень та технологій в промисловості. 2022. № 4 (22). С. 20–31. DOI: https://doi.org/10.30837/ITSSI.2022.22.020
2. Erdelj, M.; Saif, O.; Natalizio, E.; Fantoni, I. «UAVs that fly forever: Uninterrupted structural inspection through automatic UAV replacement.» Ad Hoc Netw. 2019, 94, 101612.
3. Kong, P.-Y. «A Survey of Cyberattack Countermeasures for UAV». November 2021.
4. Mohsen Riahi Manesh and Naima Kaabouch, «Cyber attacks on unmanned aerial system networks: Detection, countermeasure, and future research directions,» Computers & Security, vol. 85, pp. 386-401, August 2019.

Відомості про авторів

Логачов Михайло Геннадійович, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», m.h.lohachov@student.csn.khai.edu

Фесенко Герман Вікторович, професор кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», д.т.н., доцент, h.fesenko@csn.khai.edu

Секція 1

АНАЛІЗ МЕТОДІВ ВИЯВЛЕННЯ АВТОРІВ ФАЙЛУ, ЩО ДОСЛІДЖУЄТЬСЯ

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

Актуальність. З розвитком мережі Інтернет цифрові дані стали невід'ємною частиною повсякденного життя, проблема ідентифікації авторства файлів набула важливого значення в різних галузях, включно з комп'ютерною криміналістикою, кримінальним розслідуванням та авторським правом.

Ця проблема вимагає розробки ефективних методів ідентифікації авторства файлу, які допоможуть визначити, хто несе відповідальність за створення або редагування конкретного файлу. Аналіз авторства - це статистичне дослідження лінгвістичних та обчислювальних характеристик письмових документів окремих осіб [1].

Відомі дослідження аналізу авторства для текстової комунікації в Інтернеті є дуже обмеженим. Традиційні письмові твори є об'ємними і, як правило, добре структуровані відповідно до загальних синтаксичних і граматичних правил. На відміну від них, онлайн-документи, такі як електронні листи та миттєві повідомлення, короткі, погано структуровані і зазвичай написані мовою абзаців, що містить кілька орфографічних і граматичних помилок. Ці відмінності роблять деякі традиційні роботи з аналізу авторства неможливими для застосування до текстових даних в Інтернеті.

Метою даної роботи є дослідження методів виявлення авторства файлів, отриманих в мережі Інтернет.

Основні положення. У доповіді надано дослідження авторства, яке показують, що окремі особи часто залишають сліди їх особистості у своїх письмових роботах [2]. Наприклад, вибір слів, композиція речень і абзаців, а також відносна перевага одних мовних артефактів над іншими можуть допомогти відрізнити одну особу від іншої. Перехопивши та проаналізувавши «почерк» анонімних текстових повідомлень, є можливість виокремити певні характеристики одного автора повідомлень з вибірки.

При ідентифікації авторів файлів отриманих в інтернеті, використовують різні підходи та методи, а саме: стилістичний аналіз тексту, виявлення місця розташування відправника, експертна оцінка, порівняння зразків авторства, машинне навчання.

Наведені у доповіді методи визначення автора файлів показує, що це завданням є непростим і багато авторів намагаються приховати свою

особистість, змінюючи стиль [3]. Крім того, неможливо з упевненістю визначити автора файлу, аналізуючи тільки текст і метадані, оскільки інші автори можуть мати схожий стиль або доступ до аналогічної інформації. Але використовуючи поєднання деяких з цих методів може дати позитивний результат у визначенні автора конкретного файлу.

Висновки. Представлені у доповіді методи та їх комплексне використання можуть допомогти в ідентифікації автора. Однак, як на сьогодні не існує консенсусу щодо правильної методології. Майже кожен з представлених методів страждає від таких проблем, як сумнівний аналіз, непослідовність для одного і того ж набору авторів, невдала реплікація. У таких випадках головну роль починає відігравати кваліфікація експерта. Користувачі повинні дотримуватись організаційних методів безпеки та не відкривати файли невідомого походження.

Список літератури

1. R. H. Baayen, H. van Halteren, and F. J. Tweedie. Outside the cave of shadows: using syntactic annotation to enhance authorship attribution. URL - http://www.sfs.unituebingen.de/hbaayen/publications/BaayenHalterenTweedie1996.pdf (дата звернення: 12.11.2023);
2. O. de Vel, A. Anderson, M. Corney, and G. Mohay. Multi-topic e-mail authorship attribution forensics. URL – https://eprints.qut.edu.au/8039/1/8039.pdf (дата звернення: 13.11.2023);
3. A Unified Data Mining Solution for Authorship Analysis in Anonymous Textual Communications. URL – https://spectrum.library.concordia.ca/id/eprint/976945/1/fung2011b.pdf (дата звернення: 13.11.2023);

Відомості про авторів

Малєєва Злата-Тіна Олександрівна, магістрантка кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», z.malieieva@student.csn.khai.edu
Пєвнєв Володимир Яковлевич, професор кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», д.т.н., доцент, v.pevnev@csn.khai.edu

Секція 1

ДОСЛІДЖЕННЯ ТА РОЗРОБКА ПОЛІТИКИ БЕЗПЕКИ ПІДПРИЄМСТВА

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

Актуальність. Дослідження та розробка політики безпеки виробничого підприємства мають велику актуальність у сучасних умовах. Забезпечення безпеки на робочому місці як складової частини політики безпеки є одним із головних пріоритетів для будь-якого підприємства. Ось декілька причин, чому актуальність досліджень та розробки політики безпеки виробничого підприємства постійно зростає. Оптимізація витрат: Несприятливі події, пов'язані з безпекою, можуть призвести до значних фінансових втрат для підприємства. Наприклад, штрафи за порушення норм безпеки, виплати компенсацій працівникам через травми або хвороби, втрати виробництва через припинення роботи - все це може негативно вплинути на фінансовий стан підприємства. Дослідження та розробка політики безпеки дозволяють підприємству ідентифікувати потенційні ризики та приймати заходи для їх запобігання, що допомагає знизити витрати, пов'язані з безпекою. Збереження репутації: Підприємство, яке піклується про безпеку своїх працівників, буде мати кращу репутацію серед споживачів, інвесторів та інших зацікавлених сторін. Зацікавлені сторони все більше уважають питання безпеки як важливий аспект діяльності підприємства, тому вони активно стежать за тим, як виробничі підприємства впроваджують політику безпеки. Дослідження та розробка політики безпеки допомагають підприємству зберегти свою репутацію і впевненіше працювати на ринку.

Отже, дослідження та розробка політики безпеки виробничого підприємства мають велику актуальність і допомагають забезпечити безпеку працівників, підвищити продуктивність, знизити витрати та зберегти репутацію підприємства.

Мета дослідження та розробки політики безпеки підприємства полягає у створенні ефективної системи заходів та стратегій, спрямованих на забезпечення безпеки підприємства.

Основні положення дослідження та розробки політики безпеки підприємства буде включати наступні елементи. Оцінка загроз: Першим кроком є проведення оцінки загроз, яка включає ідентифікацію потенційних ризиків безпеки, таких як фізична вторгнення, кібератаки, природні катастрофи тощо. Дослідження дозволяє встановити, які загрози є найбільш імовірними і які можуть нанести найбільші збитки підприємству. Аналіз потенційних наслідків: Дослідження повинне включати аналіз можливих наслідків, які можуть виникнути внаслідок

зазначених загроз. Це можуть бути фінансові втрати, порушення конфіденційності даних, втрата репутації підприємства, порушення робочого процесу та інші наслідки. Визначення цілей безпеки: Після оцінки загроз і аналізу наслідків підприємство повинно визначити свої цілі безпеки. Це можуть бути, наприклад, забезпечення безпеки працівників, захист конфіденційності клієнтської інформації, зменшення ризику втрати даних тощо. Розробка стратегій та політик безпеки: Дослідження допомагає визначити оптимальні стратегії та політики безпеки для підприємства. Це може включати впровадження фізичних заходів безпеки, таких як контроль доступу до приміщень або використання відеоспостереження, а також кіберзаходи, такі як використання міцних паролів, шифрування даних та регулярне оновлення програмного забезпечення.

Висновки. Отже, дослідження та розробка політики безпеки підприємства є необхідними для ефективного управління ризиками, забезпечення відповідності, захисту активів та працівників, а також збереження репутації підприємства.

Список літератури

1. ISO 27001:2013 «Information technology – Security techniques – Information security management systems – Requirements». URL – https://certification.com.ua/iso27001?gclid=Cj0KCQiAr8eqBhD3ARIsAIe-buO231SMy2oO23E7KzrFqXX8mS3f3bH_Q3F8vspzLxqjwOesePgHkUQaAlA8EALw_wcB (дата звернення: 11.10.2023);

2. NIST SP 800-53 «Security and Privacy Controls for Federal Information Systems and Organizations». URL – https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final (дата звернення: 11.10.2023);

3. Control Objectives For Information And Related Technology, “COBIT”. *Emirsaleh*. URL – https://emirsaleh.wordpress.com/carrier-path/information-technology-world/control-objectives-for-information-and-related-technology-cobit (дата звернення: 11.10.2023);

4. Krag Brotby. Information Security Governance: A Practical Development and Implementation Approach. John Wiley & Sons Inc, 2009, Page 208.

Відомості про автора

Марченко Віктор Васильович, магістрант кафедри комп’ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», viktor.marchenko@student.csn.khai.edu

Пєвнєв Володимир Яковлевич, професор кафедри комп’ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», д.т.н., доцент, v.pevnev@csn.khai.edu

Секція 1

СИСТЕМИ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ: ПРОБЛЕМИ БЕЗПЕКИ

Міхайлова М. С.
Національний університет «Запорізька політехніка»
Науковий керівник: Зайко Т. А.

Актуальність. Значення електронного документообігу в Україні було визнане на законодавчому рівні в 2003 році, коли був прийнятий Закон «Про електронні документи та електронний документообіг» [1]. Пізніше було прийнято й інші нормативні акти, які розширили правову підтримку для електронного документообігу. Наприклад, Закон України «Про електронні довірчі послуги» закріпив юридичну силу електронного документообігу [1]. Системи електронного документообігу здобули популярність та стали невід'ємною частиною бізнес-процесів та адміністративного управління. Проте, разом із перевагами, виникають і проблеми в області безпеки, які варто ретельно аналізувати.

Метою даної роботи є дослідження та ідентифікації проблем в області систем електронного документообігу, якими користуються в Україні.

Основні положення. Електронний документообіг – це сукупність процесів створення, оброблення, відправлення, передавання, одержання, зберігання, використання та знищення електронних документів [2].

Система електронного документообігу – це програмне забезпечення для роботи з електронними документами на всіх стадіях їхнього життєвого циклу: створення, редагування, зберігання [3]. Український ринок програмного забезпечення електронного документообігу представлений низкою програмних продуктів: «M.E.Doc», «СОТА», «FREDO ДокМен», «Вчасно», «FlyDoc» тощо [4].

До найпоширеніших проблем безпеки в даній сфері можно віднести: відсутність двофакторної автентифікації, аудиту безпеки, низький рівень шифрації та контролю доступу, слабкий рівень захисту від вірусних програм, фішинг та соціальна інженерії. Для подальшого вдосконалення безпеки систем електронного документообігу в Україні, необхідно визначити стратегії для вирішення виявлених проблем.

Наприклад відсутність двофакторної автентифікації, яка може ставити під загрозу безпеку електронних документів та облікових записів користувачів, може бути вирішена впровадженням додаткових методів перевірки особи, таких як біометричні дані або одноразові паролі. Аудит безпеки є ключовим аспектом у дотриманні безпеки електронного документообігу. Тому важливо реалізовувати систему, яка дозволить вести запис та моніторити події, пов'язані з електронними документами, щоб мати можливість передбачити проблеми завчасно.

Щодо шифрування та контролю доступу, можна рекомендувати підняти рівень шифрації до сучасного військового рівня шифрування, як, наприклад, AES-256. Також треба звернути увагу на вдосконалення системи контроля доступу. Використання жорстких правил доступу може допомогти у забезпеченні конфіденційності електронних документів.

Окрім цього, необхідно звернути увагу на захист від вірусних програм, розвиваючи та впроваджуючи ефективні антивірусні заходи та механізми виявлення загроз. І нарешті, важливо враховувати такі загрози, як фішинг та соціальна інженерія. Необхідно проводити навчання користувачів, вдосконалювати системи виявлення фішингу та встановлювати ефективні методи захисту від соціально-інженерних атак.

Висновки. Безпека систем електронного документообігу в Україні є дуже важливою, особливо з огляду на обробку чутливої інформації та особистих даних. Помилки в цій сфері можуть призвести до серйозних наслідків, включаючи втрату конфіденційної інформації та порушенню законодавства. На поточний момент безпекова ситуація в сфері електронного документообігу в Україні не є стабільною через повномасштабне вторгнення Росії в Україну, але аналіз та усунення проблем з безпекою проводиться незважаючи на часті кібератаки.

Список літератури

1. Про електронні довірчі послуги: Закон України від 01 січня 2023 року, № 2801-IX. *zakon.rada.gov.ua.* URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text (дата звернення: 18.10.2023);
2. Про електронні документи та електронний документообіг: Закон України від 01 серпень 2022 року, № 851-IV. *zakon.rada.gov.ua.* URL: https://zakon.rada.gov.ua/laws/show/851-15#Text (дата звернення: 19.10.2023);
3. Електронний документообіг: види систем та їхні функції. *Deals*. URL: https://dealssign.com/blog/elektronnij-dokumentoobig-vidi-sistem-ta-yixni-funkciyi (дата звернення: 19.10.2023);
4. Редько М. О. Порівняння систем електронного документообігу. У кн.: Облік, оподаткування і контроль: теорія та методологія: тези доп. IV-ї міжнар. наук.-практ. конф., 28 грудня 2018 р., м.Тернопіль/Терноп. національ. економ. ун-т [та ін.]. –Тернопіль: Крисоватий А. І. 2018. – 182 с.

Відомості про авторів

Міхайлова Марія Сергіївна, студентка кафедри програмних засобів Національний університет «Запорізька політехніка», mariamihajlova31@gmail.com

Зайко Тетяна Анатоліївна, доцент кафедри програмних засобів Національний університет «Запорізька політехніка», к.т.н., доцент, nika270202@gmail.com

Секція 1

РОЗРОБЛЕННЯ ТА ДОСЛІДЖЕННЯ МЕТОДІВ І ЗАСОБІВ АНАЛІЗУ ВРАЗЛИВОСТЕЙ І ЗАХИСТУ СИСТЕМ ІНТЕРНЕТУ РЕЧЕЙ РОЗУМНИХ ОФІСІВ

Молчанов А. О.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Харченко В. С.

Актуальність. Збільшення кількості приладів на базі інтернет речей та прагнення зробити офіси більш енергоефективними призвело до тенденції різкого поширення систем розумних офісів останніми роками. Значну роль у цьому відіграло і збільшення інвестиції у цю сферу. Розумний офіс - це комбіноване використання розумних пристроїв, які з'єднані через мережу в одну систему [1]. Згідно з наведеними звітами компаній Allied Market Research і Data Bridge Market Research розмір світового ринку у сфері смарт-офісів та програмного забезпечення для смарт-офісів до 2028-2030 років сягне 90.63 мільярдів доларів [2]. Так з появою нових рішень збільшиться й актуальність питання безпеки, як фізичної так і кібербезпеки.

Метою даної роботи є дослідження проблем безпеки, функцій, архітектур, платформ, можливих атак і загроз, а також обґрунтування необхідності в їх захисті.

Згідно річного звіту Європейського ринку систем безпеки інтернету речей (IoT), протягом наступних років, аж до 2028 року, загальний середньорічний темп зростання інцидентів досягне відмітки 12.5% у Європейському регіоні. Основним напрямком з безпеки прогнозовано стане захист від витоку даних [3].

Основні положення. Структури смарт офісів, які побудовані на технологіях інтернету речей, включають в себе: датчики, що збирають інформацію; побутові пристрої; канали зв’язку; сервери; мобільні додатки; тощо [3]. Серед основних функцій розумних офісів слід виділити: контроль енергоефективності; контроль комфортних приладів для функціоналу офісу; контроль безпеки; контроль управління офісним середовищем; контроль зчитування лічильників [1]. Платформи для розумних будинків є зв’язуючим компонентом, до якого під’єднуються всі прилади і існують у трьох типах: програмні, апаратні та комбіновані. Оскільки до платформ підключаються усі розумні пристрої, то вони повинні бути універсальні і підтримувати основні стандарти зв’язку. Єдиної схеми архітектури для смарт офісів не існує[4].

Серед загроз і атак на системи смарт офісів можна виділити наступні: атаки на інформаційні активи, можливі загрози безпеки та атаки на архітектури [5].

Висновки. Через стрімке збільшення кількості розумних приладів, які можна інтегрувати у середу смарт офісів, збільшується і актуальність в їх захисті. Проаналізувавши основні функції, платформи та архітектури смарт офісів зроблено висновок, що за основу смарт офісів береться одна з трьох платформ: програмна, апаратна чи комбінована. Єдиної архітектури для таких систем не існує, оскільки у кожному офісі можуть бути різноманітні прилади чи системи комунікації. Отже після обрання платформи можна розробляти свою архітектуру. Аналізуючи атаки на системи інтернету речей виявлено, що зловмисники можуть проводити атаки як на самі контролери та сервери, так і на пристрої, які збирають, передають інформацію, та активно взаємодіють з актуаторами.

Список літератури

1. Smart Home: Architecture, Technologies and Systems. *Sciencedirect.* URL – https://www.sciencedirect.com/science/article/pii/S1877050918305994 (дата звернення: 23.04.2023);
2. Global Smart Office Market. *Alliedmarketresearch.* URL – https://www.alliedmarketresearch.com/smart-office-market-A13723 (дата звернення: 17.04.2023);
3. Європейський ринок безпеки інтернету речей (IoT) — зростання, тенденції, вплив COVID-19 і прогнози (2023–2028роки). *Mordorintelligence.* URL: https://www.mordorintelligence.com/ru/industry-reports/europe-internet-of-things-iot-security-market (дата звернення: 22.04.2023);
4. The best smart home systems 2023: Top ecosystems explained. *the-ambient.* URL – https://www.the-ambient.com/guides/smart-home-ecosystems-152#:~:text=Google,%20Amazon,%20Apple%20and%20SmartThings,make%20home%20automation%20a%20doddle (дата звернення: 24.04.2023);
5. Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes. *Mdpi.* URL – https://www.mdpi.com/1424-8220/18/3/817 (дата звернення: 27.04.2023).

Відомості про авторів

Молчанов Артем Олегович, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», a.o.molchanov@student.csn.khai.edu
Харченко Вячеслав Сергійович, завідувач кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», д.т.н, професор, v.kharchenko@csn.khai.edu

Секція 1

ДОСЛІДЖЕННЯ ВПЛИВУ ШТУЧНОГО ІНТЕЛЕКТУ НА КІБЕРБЕЗПЕКУ ВЕБ-ЗАСТОСУНКІВ

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

Актуальність дослідження впливу штучного інтелекту на кібербезпеку веб-застосунків проявляється у декількох аспектах. Штучний інтелект стає все більш поширеним у різних сферах, включаючи медицину, фінанси, транспорт, комунікації та інші. Застосування штучного інтелекту вимагає глибокого розуміння потенційних загроз для кібербезпеки веб-застосунків, щоб забезпечити їх безпеку та захист від можливих атак. Впровадження штучного інтелекту в кіберзлочинність може призвести до виникнення нових видів атак та методів обхіду захисту [1]. Атаки, які використовують штучний інтелект, можуть бути складнішими для виявлення та захисту, що ставить під загрозу безпеку веб- застосунків та приватність користувачів [2]. Штучний інтелект може використовуватися для аналізу великих обсягів персональних даних, що створює ризик порушення приватності та можливість зловживання цими даними. Захист персональних даних веб-застосунків від штучного інтелекту стає важливою задачею для забезпечення конфіденційності та довіри користувачів. Залежно від типу застосунку, штучний інтелект може бути використаний як інструмент для посилення кібербезпеки або для здійснення шкідливих дій [3]. Це ставить виклик перед розробниками та кібербезпековими експертами для розробки нових стратегій захисту, адаптивних систем та методів виявлення атак, що використовують штучний інтелект. Враховуючи ці аспекти, дослідження впливу штучного інтелекту на кібербезпеку веб-застосунків є актуальним завданням, що допомагає розуміти та адаптуватися до швидкого розвитку технологій, забезпечуючи безпеку, приватність та довіру в онлайн середовищі.

Метою є дослідження впливу штучного інтелекту на кібербезпеку веб-застосунків для розуміння загроз та розробки відповідних стратегій захисту, а також визначення основних проблем та викликів, пов'язаних з впливом штучного інтелекту на кібербезпеку веб-застосунків.

Основні положення. Штучний інтелект може використовуватися як засіб для покращення кібербезпеки веб-застосунків. Однак, він також може бути використаний зловмисниками для здійснення атак та обходу систем захисту, що ставить під загрозу безпеку веб-застосунків. Використання штучного інтелекту може створити нові види загроз для веб- застосунків. Крім того, штучний інтелект може використовуватися для генерації шкідливого коду, фішингу, соціального інжинірингу та інших атак, які

мають великий потенціал завдати шкоди веб-застосункам та користувачам. Для захисту веб-застосунків від впливу штучного інтелекту необхідно розробляти ефективні та адаптивні захисні механізми. Це може включати використання штучного інтелекту для виявлення та відповіді на атаки, розробку алгоритмів виявлення вразливостей та захисту, застосування аналізу поведінки для виявлення аномальних, шифрування та аутентифікації для забезпечення конфіденційності та цілісності даних, а також навчання на основі даних для адаптивного захисту. Впровадження штучного інтелекту в кібербезпеку вимагає врахування етичних та правових аспектів. Наприклад, необхідно уникати дискримінації та недостатньої прозорості в процесі використання штучного інтелекту. Також важливо розробляти стандарти та нормативи, які регулюють використання штучного інтелекту в кібербезпеці, забезпечуючи ефективність та безпеку веб- застосунків [3].

Висновки. Штучний інтелект має значний вплив на кібербезпеку веб-застосунків, вносячи як позитивні, так і негативні аспекти. Забезпечення кібербезпеки веб-застосунків є постійним завданням, яке вимагає постійного моніторингу, аналізу та оновлення захисних механізмів. Впровадження штучного інтелекту в кібербезпеку потребує балансу між використанням його для поліпшення захисту та захисту від нових видів атак, а також урахування етичних та правових аспектів.

Список літератури

1. Herping S. (2019). Securing Artificial Intelligence – Part I. *stiftung-nv*. URL – https://www.stiftung-nv.de/sites/default/files/securing_artificial_intelligence.pdf (дата звернення: 12.06.2023);
2. Pupillo L., Fantin S., Ferreira A., Polito C. (2021). Artificial Intelligence and Cybersecurity. CEPS Task Force Report. *Ceps*. URL – https://www.ceps.eu/wp-content/uploads/ 2021/05/CEPS-TFR-Artificial-Intelligence-and-Cybersecurity.pdf (дата звернення: 01.06.2023);
3. Hartmann K., Steup C. (2020). Hacking the AI – the Next Generation of Hijacked Systems. In 12 International Conference on Cyber Conflict (CyCon). *doi.org*. URL – https://doi.org/10.23919/CyCon49761.2020.9131724 (дата звернення: 12.06.2023).

Відомості про авторів

Момот Олег Олександрович, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», o.o.momot@student.csn.khai.edu
Пєвнєв Володимир Яковлевич, професор кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», д.т.н., доцент, v.pevnev@csn.khai.edu

Секція 1

СИСТЕМА ДВОФАКТОРНОЇ АУТЕНТИФІКАЦІЇ КОРИСТУВАЧА КОРПОРАТИВНОГО СЕРЕДОВИЩА З ВИКОРИСТАННЯМ QR-КОДУ

Мордас І. С.
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»
Науковий керівник: Отрох С. І.

Актуальність. На сьогоднішній день технології відіграють важливу роль в будь-якій сфері людського життя. І нагальною проблемою є захист конфіденційних даних користувача. Здійснення аутентифікації за допомогою логіну і паролю, є надзвичайно вразливим способом, адже кіберзлочинність стрімко розвинулася і отримати дані для доступу в несанкціонований спосіб вже не є тяжким викликом. Варто звернути увагу, що доволі часто самі користувачі використовують один і той же пароль для входу до різних систем, що збільшує ймовірність його викрадення.

Ключ до вирішення даної проблеми полягає в двофакторної аутентифікації за допомогою QR-коду, який є зручним у використання і безпечним для отримання токену, необхідного для генерації одноразового динамічного коду [1]. Дана система унеможливлює викрадення конфіденційних даних, також допомагає запобігти несанкціонованому доступу.

Метою даної роботи є дослідження та реалізація системи двофакторної аутентифікації користувача корпоративного середовища за допомогою QR-коду і алгоритму TOTP.

Основні положення. Для реалізації входу на основі двофакторної аутентифікації реалізовано алгоритм TOTP («Time-based One-Time Password») [2]. Основний принцип його роботи полягає в генерації унікального динамічного коду на основі секретного ключа і параметру часу.

Також для візуального відображення шести значного коду необхідний будь-який зчитувальний пристрій або звичайний персональний мобільний телефон, адже за допомогою нього відбувається сканування QR-коду [3].

Основний принцип його роботи полягає в створенні хешу за допомогою криптографічної методу SHA-1 (Secure Hash Algorithm) [4]. Дана функція приймає такі параметри: секретний ключ, що становить собою довільний набір байтів і час Unix, який вимірюється в секундах, які минули від початку епохи. В результаті виконання хешування, ми отримуємо рядок довжиною в 20 байтів, які в подальшому обрізається до 6-значного вигляду.

Згенерований код, є дійсним лише невеликий проміжок часу, що зазвичай становить 30 секунд [5]. Тобто це час необхідний для введення користувачем його до системи.

Висновки. Отже, було реалізовано і досліджено систему двофакторної аутентифікації за допомогою QR-коду і алгоритму TOTP з метою підвищення рівня безпеки захисту конфіденційних даних та унеможливлювання несанкціонованого доступу. Також було використано технологію QR-коду, для зручного використання і шифрування даних.

Список літератури

1. How does a QR code encode data?. URL – https://www.qr-code-generator.com/blog/how-does-a-qr-code-encode-data/ (дата звернення: 19.10.2023);
2. Time based One Time Password. URL – https://www.hypr.com/security-encyclopedia/time-based-time-password-totp-otp/ (дата звернення: 20.10.2023);
3. Що таке QR-код: як виник та для чого використовується. URL – https://nbookpart.com.ua/sho-take-qr-kod-iak-vinik-ta-dlia-chogo-vikoristovyetsia/ (дата звернення: 10.10.2023);
4. Secure Hash Algorithms. URL – https://brilliant.org/wiki/secure-hashing-algorithms// (дата звернення: 15.10.2023);
5. TOTP Algorithm Explained. URL – https://www.protectimus.com/blog/totp-algorithm-explained/ (дата звернення: 16.10.2023).

Відомості про авторів

Мордас Іван Сергійович, магістрант кафедри цифрових технологій в енергетиці, КПІ ім. І. Сікорського, ivanmordas49@gmail.com
Отрох Сергій Іванович, професор кафедри цифрових технологій в енергетиці, КПІ ім. І. Сікорського, д.т.н, професор, 2411197@ukr.net

Секція 1

ДОСЛІДЖЕННЯ ЗАСОБІВ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ІНТЕЛЕКТУАЛЬНИХ СИСТЕМ ВІДЕОСПОСТЕРЕЖЕННЯ

Набока С. А.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Пєвнєв В. Я.

Актуальність. Дослідження засобів забезпечення кібербезпеки інтелектуальних систем відеоспостереження є надзвичайно важливою у сучасному світі. Зростання використання відеоспостереження у різних сферах, таких як громадська безпека, бізнес, транспортна інфраструктура та інші, призводить до збільшення кількості цифрових відеоданих, які потребують захисту від кібератак [1]. Оскільки інтелектуальні системи відеоспостереження використовуються для розпізнавання облич, виявлення аномальної поведінки, відстеження об'єктів та інших функцій, вони стають привабливим мішенями для кіберзлочинців. Шахраї можуть намагатися зламати систему відеоспостереження для отримання незаконного доступу до відеоданих або зміни їх з метою вводу в оману, впливу на прийняття рішень або завдання шкоди [2].

Дослідження засобів забезпечення кібербезпеки інтелектуальних систем відеоспостереження спрямовані на виявлення потенційних вразливостей систем, розробку захисних механізмів, протоколів шифрування, аутентифікації та інших методів, що дозволяють забезпечити конфіденційність, цілісність і доступність відеоданих. Актуальність цих досліджень підвищується з поширенням нових технологій, таких як розподілені системи відеоспостереження, використання хмарних обчислень та штучного інтелекту [3].

Метою роботи є аналіз засобів забезпечення інтелектуальних систем відеоспостереження та відеоданих від кіберзагроз.

Основні положення дослідження засобів забезпечення кібербезпеки інтелектуальних систем відеоспостереження можуть включати наступні аспекти:

1. Аналіз загроз та вразливостей: Визначення потенційних загроз та вразливостей, яким піддаються інтелектуальні системи відеоспостереження. Це включає виявлення вразливих місць у системі, можливих шляхів атаки та потенційних кіберзагроз [4].
2. Розробка захисних механізмів: Розробка та впровадження захисних механізмів для запобігання кібератак та забезпечення безпеки інтелектуальних систем відеоспостереження. Це може включати розробку протоколів шифрування, систем аутентифікації, контролю доступу, систем виявлення вторгнень тощо.

3. Тестування та оцінка ефективності: Проведення тестування та оцінка ефективності розроблених захисних механізмів. Це включає проведення випробувань системи на наявність вразливостей, симуляцію кібератак та оцінку відповідності системи стандартам кібербезпеки.
4. Управління ризиками: Визначення та управління ризиками, пов'язаними з кібербезпекою інтелектуальних систем відеоспостереження. Це включає ідентифікацію потенційних загроз, оцінку ризиків, розробку стратегій запобігання і реагування на інциденти, а також розробку планів відновлення після кібератаки.
5. Свідомість та навчання: Залучення операторів систем відеоспостереження та користувачів до свідомого використання безпеки. Це включає проведення навчання, розробку освітніх матеріалів та розповсюдження кращих практик забезпечення кібербезпеки [5].
6. Розробка стандартів і рекомендацій: Внесення внеску у розробку стандартів і рекомендацій щодо кібербезпеки інтелектуальних систем відеоспостереження. Це допомагає створити загальноприйняті норми та вимоги до безпеки таких систем.

Ці основні положення спрямовані на створення надійних та безпечних інтелектуальних систем відеоспостереження, які забезпечують захист від кіберзагроз та збереження конфіденційності, цілісності та доступності відеоданих.

Висновки. Результатами досліджень засобів забезпечення кібербезпеки інтелектуальних систем відеоспостереження є методологія розробки ефективних механізмів захисту цих засобів від кіберзагроз, забезпечення конфіденційності та цілісності відеоданих, а також підвищення ефективності та надійності відеоспостереження.

Список літератури

1. Whitman, M. E., & Mattord, H. J. (2018). Management of Information Security. Cengage Learning.
2. Kizza, J. M. (2019). Guide to Computer Network Security. Springer.
3. Dargahi, V., & Mittal, S. (2019). Securing the Internet of Things: Concepts, Methodologies, Tools, and Applications. IGI Global.
4. Khalid, M. S., & Khan, M. K. (2018). Internet of Things Security: Fundamentals, Techniques, and Applications. CRC Press.
5. Chen, C., Leung, V. C. M., Shu, L., & Zhang, Y. (Eds.). (2016). Internet of Things and Big Data Analytics Toward Next-Generation Intelligence. Springer.

Відомості про авторів

Набока Сергій Андрійович, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», s.a.naboka@student.csn.khai.edu
Пєвнєв Володимир Яковлевич, професор кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», д.т.н, доцент, v.pevnev@csn.khai.edu

Секція 1

АНАЛІЗ ІСНУЮЧИХ МОДЕЛЕЙ ЗАГРОЗ І ПОРУШНИКІВ

Овчаренко Н. Д.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Пєвнєв В. Я.

Актуальність. Зростання кількості технологій та їх використання в різних сферах життя супроводжується також збільшенням кількості кіберзлочинів та інших порушень безпеки. Для забезпечення ефективного кіберзахисту необхідно розуміти, які методи та техніки використовують зловмисники.

Дослідження існуючих моделей порушників дозволяє виявити їхні мотивації, методи та стратегії. Це надає можливість створити більш ефективні заходи кіберзахисту та попередження кіберзлочинів. Також це допомагає виробникам програмного забезпечення та інших технологій покращувати свої продукти, зменшуючи їхню вразливість перед потенційними атаками.

Метою є вивчення та аналіз існуючих моделей поведінки кіберпорушників з метою розкриття їхніх мотивацій, використовуваних технік та стратегій.

Основні положення. В доповіді розглянуто мотивацію, кваліфікацію, технічну оснащеність, обмеження та припущення про характер можливих дій порушників, що дає змогу класифікувати їх за цими критеріями.

Розглядаючи мотивацію, можна виділити різні фактори, що підштовхують особу до порушення закону. Деякі з них можуть бути пов'язані з економічними труднощами, соціальною несправедливістю, амбіціями або навіть психологічними проблемами. У контексті кваліфікації та технічної оснащеності можна зрозуміти які інструменти можуть бути використані та визначити наскільки вірогідно і успішно може бути виконана атака.

Враховуючи обмеження та припущення про характер можливих дій порушника можливо зробити припущення щодо сценаріїв можливих атак. Класифікація порушників за цими критеріями дозволяє визначити спільні тенденції в їхній діяльності та розробляти ефективні стратегії протидії.

У доповіді було розглянуто моделі загроз, які дають нам систематичний підхід до аналізу потенційних небезпек і ризиків, які можуть виникнути у сфері інформаційних технологій або інших сферах. Цей термін може використовуватися в контексті кібербезпеки, фізичної безпеки, бізнес-аналізу та інших областей. Модель загроз допомагає ідентифікувати, класифікувати і аналізувати потенційні загрози для прийняття заходів з їх запобігання чи обмеження.

У доповіді було відзначено, що для кожної загрози потрібно визначити на порушення яких властивостей інформації вона спрямована, користуючись чотирма основними градаціями, а саме: порушення конфідеційності, цілісності, доступності інформації, а також порушення спостереженості та керованості системи. Також потрібно визначити які суб'єкти системи або суб'єкти зовнішні по відношенню до неї, можуть ініціювати загрозу. І наостанок треба визначити можливі способи здійснення загроз.

Висновки. Робота присвячена аналізу існуючих моделей загроз і порушників у кіберпросторі. Було проведено аналіз мотивацій, кваліфікацій, технічної оснащеності, обмежень та припущень про можливий характер дій порушників.

Список літератури

1. 6 Motivations of Cyber Criminals. *Coretech.* URL: https://www.coretech.us/blog/6-motivations-of-cyber-criminals (дата звернення: 10.10.2023);
2. Ramya Mohanakrishnan What Is Threat Modeling? Definition, Process, Examples, and Best Practices. *Spiceworks.* URL – https://www.spiceworks.com/it-security/network-security/articles/what-is-threat-modeling-definition-process-examples-and-best-practices/ (дата звернення: 12.10.2023);
3. Victoria Drake Threat Modeling. *Owasp.* URL – https://owasp.org/www-community/Threat_Modeling (дата звернення: 12.10.2023);
4. Комаров М.Ю. Ониськова А.В. Гончар С.Ф. Аналіз і дослідження моделі порушника безпеки інформації для захищеного вузла інтернет доступу. *Vernadskyjournals.* URL: http://www.tech.vernadskyjournals.in.ua/journals/2018/5_2018/part_1/26.pdf (дата звернення: 12.10.2023).

Відомості про авторів

Овчаренко Нікіта Дмитрович, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», n.ovcharenko@student.csn.khai.edu
Пєвнєв Володимир Яковлевич, професор кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», д.т.н, доцент, v.pevnev@csn.khai.edu

Секція 1

ЗАХИСТ ПРОМІЖНОГО ХОСТА ВІД АМПЛІФІКАЦІЇ ЧЕРЕЗ ВРАЗЛИВІСТЬ SSDP ПРОТОКОЛУ

Ориджук О. М.
Чернівецький національний університет імені Юрія Федьковича
Науковий керівник: Круліковський О. В.

Актуальність. Захист проміжного хоста від ампліфікації через вразливість SSDP протоколу визначається зростаючою загрозою кібербезпеки в сучасному світі. Запити Simple Service Discovery Protocol (SSDP), використовувані для виявлення мережевих пристроїв, можуть стати об'єктом ампліфікаційних атак. Захист від цих атак є критично важливим, оскільки вони можуть використовуватися для здійснення масштабних DDoS-атак та порушення безпеки мережевих систем. Дослідження та розробка ефективних методів захисту від ампліфікації через SSDP є актуальним завданням для кібербезпекових фахівців, оскільки це сприяє зміцненню стійкості мереж та зменшенню ризику кіберзагроз.

Метою роботи є створення методу захисту проміжного хоста від ампліфікації розподіленої атаки на відмову в обслуговуванні.

Основні положення. В рамках наукової роботи, в лабораторних умовах було проведено атаку на відмову в обслуговуванні проміжного хоста за допомогою спеціально написаного коду із використанням бібліотеки scapy на мові python. При цьому продемонстровані покрокові інструкції для перевірки на наявність вразливих пристроїв у власній мережі. В результаті наукового дослідження пропонується метод захисту від вразливості SSDP протоколу. В основі запропонованого методу лежить комбіноване використання системи уніфікованого управління міжмережними екранами Cisco Firepower Management Center що дозволяє здійснювати контроль над додатками, запобігати вторгненням, фільтрувати URL-адреси.

Запропонований метод захисту може використовуватись у системах з аналогічним функціоналом що лабораторне середовище та універсальним. Це в свою чергу дозволило сформувати список рекомендацій для розробників протоколів UPnP та описати основні проблеми, які стали наслідком виникнення описаної вразливості.

Висновки. Результатом Дослідження вразливості SSDP протоколу та пропозиція методу захисту проміжного хоста від ампліфікації розподіленої атаки на відмову в обслуговуванні – це крок у зміцненні кібербезпеки в сучасних мережах. Атаки через SSDP стають все більшою загрозою, і виявлення ефективних методів боротьби з цими атаками є критично важливим.

Дослідницька робота над цією темою виявила потенційні загрози для мережевих систем через вразливості протоколу UPnP, що може призвести до масштабних DDoS-атак та порушень безпеки. Пропонований метод захисту, який базується на комбінованому використанні Cisco Firepower Management Center, відображає практичний підхід до контролю над додатками, запобігання вторгненням та фільтрації URL-адрес.

Важливо відзначити, що розроблений метод захисту може бути застосований у різних системах з аналогічним функціоналом. Це відкриває можливості для впровадження схожих заходів безпеки у широкому спектрі мережних середовищ. Крім того, отримані результати дослідження дозволили сформулювати рекомендації для розробників протоколів UPnP та проілюструвати основні проблеми, що виникають внаслідок вразливостей, які були виявлені.

Список літератури

1. «DDoS, Machine Learning, Measures». // «Understanding Denial-of-Service Attacks». / , 2016. – (Taylor & Francis Group). – (ISBN:13: 978-1-4987-2965-9). – С. 12–34.;

2. The Crossfire Attack. // IEEE Symposium on Security and Privacy. – 2013. – С. 127– 142.;

3. D-FACE: An anomaly based distributed approach for early detection of DDoS attacks and flash events. // Journal of Network and Computer Applications. – 2018. – С. 49–63.;

4. UPnP Design by Example, 2003. – (Intel Press). – (ISBN 0-9717861).

Відомості про авторів

Ориджук Олександр Миколайович, магістрант кафедри радіотехніки та інформаційної безпеки, Чернівецький національний університет ім. Ю. Федьковича, orydzhuk.olesksandr@chnu.edu.ua

Круліковський Олег Валерійович, асистент кафедри радіотехніки та інформаційної безпеки, Чернівецький національний університет ім. Ю. Федьковича, o.krulikovskyi@chnu.edu.ua

Секція 1

МЕСЕНДЖЕРИ: ЗАГРОЗА КОНФІДЕНЦІЙНОСТІ ДЛЯ ДЕРЖАВНИХ СТРУКТУР

Подгорний Р. С.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Харченко В. С.

Актуальність. Сьогодні месенджери стали невід'ємною частиною повсякденного життя людей та використовуються у різних сферах, включаючи великий бізнес, банківський сектор та медицину. Також їх використання поширилося і на державні структури. Месенджери забезпечують швидке та зручне спілкування, але також можуть бути джерелом витоків конфіденційної та критичної інформації, що є значною загрозою безпеці країни.

Метою роботи є аналіз загроз, пов'язаних з використанням месенджерів у державних структурах, та запропонування рішення щодо використання месенджерів та серверів, які контролюються державою.

Основні положення. Месенджери, були створені з метою передачі інформації, і важливо враховувати, що державні службовці особисто можуть обмінюватися конфіденційною інформацією один з одним або залишати її в «нотатках» месенджерів. Необхідно враховувати, що в сучасних додатках часто присутні можливості використання різних датчиків смартфона.

Месенджери зазвичай збирають і зберігають такі дані: профіль користувача, список контактів користувача, історія листування, геолокацію користувача, дані пристроїв, дані активності.

Потенційні можливості негласного збору інформації. Сучасні месенджери часто отримують привілеї доступу до камери, мікрофона та різних датчиків пристроїв. Це означає, що потенційно вони мають можливість негласно збирати різні типи інформації [1], збереження фото та відео з галереї, фіксація місцеперебування, месенджер, потенційно, може збирати дані від датчиків телефону, інформацію про використання пристрою. У разі використання месенджерів в державних структурах, практично будь-які дані, які так чи інакше потрапляють до месенджера, можуть бути використані для компрометації безпеки держави.

У доповіді розглядаються додаткові ризики використання месенджерів держслужбовцями. До таких ризиків відносяться сервери, які розташовані в різних країнах світу, і відповідно підпорядковані законодавству цих країн, можливість зміни власників компаній, яким належать месенджери, достовірно не відомо, які дані збираються і як обробляються. У кого та який є фактичний доступ до зібраних даних, найбільш популярні месенджери мають повністю, або частково закритий код додатків та/або серверів.

Враховуючи обсяг інформації, яка збирається, або може збиратися месенджерами, зловмисники, або спецслужби іноземних держав, які отримають доступ до всієї цієї інформації, зможуть заволодіти таємною інформацією, скласти повні портрети держслужбовців та їх взаємозв'язки, з'ясувати маршрути пересування, графіки активності та підібрати експлойти для їх пристроїв. Що, своєю чергою, дасть можливість пошуку слабких місць для планування подальших атак.

У доповіді пропонується варіант розробки національного підконтрольного месенджера для використання держслужбовцями, та зберігання інформації на підконтрольних захищених серверах.. Одним із відповідних проєктів є «Matrix» - відкритий та вільний протокол для спілкування в реальному часі. Він може бути використаний для надсилання миттєвих повідомлень та файлів, аудіо- та відеозв'язку [2]. Сьогодні спілкування на базі протоколу «Matrix» вже випробувано у низці країн: у Франції для спілкування державних службовців [3], у збройних силах Німеччини [4].

Висновки. Найбільш безпечним та швидким варіантом розв'язання проблеми було б використання власних контрольованих месенджерів та серверів для зберігання даних, створених на базі чинних рішень з відкритим вихідним кодом. Одним із таких рішень, вже випробуваним у низці європейських країн, є «Matrix».

Список літератури

1. Твіт Фоад Дабірі. *Twitter.* URL – https://twitter.com/foaddabiri/status/1654856617723301888 (дата звернення: 7.10.23);
2. What is Matrix? *Matrix.* URL – https://matrix.org/ (дата звернення: 10.10.23);
3. «La messagerie instantanée des agents de l'État». *Modernisation.* URL – https://references.modernisation.gouv.fr/uploads/CP_TCHAP-699761.pdf (дата звернення: 10.10.23);
4. «Matrix» ist einheitlicher Messenger-Standard für die Bundeswehr. *Bwi.* https://www.bwi.de/magazin/artikel/open-source-matrix-ist-einheitlicher-messenger-standard-fuer-die-bundeswehr (дата звернення: 15.10.23).

Відомості про автора

Подгорний Руслан Сергійович, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», ruslanroool@gmail.com
Харченко Вячеслав Сергійович, завідуючий кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», д.т.н., професор, v.kharchenko@csn.khai.edu

Секція 1

ОЦІНКА МАТЕРІАЛЬНОСТІ КІБЕРРИЗИКУ

Поломошнова М. І.
Національний технічний університет «Харківський політехнічний інститут»
Науковий керівник: Мілевський С. В.

Актуальність. З розвитком інформаційних технологій, суттєво збільшилась кількість та вплив реалізованих інцидентів кіберризиків. Така ситуація підвищує актуальність досліджень питань щодо оцінки кіберризику, зокрема його основної складової – матеріальності. Майже всі міжнародні стандарти регламентують необхідність оцінки монетизованої складової ризику [1] для прийняття більш виважених управлінських ризиків на рівні управління, проте конкретні моделі щодо оцінки матеріальності ризику в цих документах відсутні. Аналізуючи best practices з питань оцінки матеріальності ризику можна визначити, що більшість результатів досліджень свідчить про необхідність прив'язки такої оцінки до фінансових показників компанії (такі, як чистий прибуток, активи, операційний прибуток тощо), деякі навіть встановлюють граничні межі такої матеріальності на рівні 1-5% від відповідного показника, опублікованого у фінансовій звітності компанії [2,3,4]. Ми натомість пропонуємо розглянути зазначену нижче модель оцінки матеріальності кіберризику, яка визначає кількісні рівні оцінки кіберризику та яка може бути інтегрована в IT-інфраструктуру компанії.

Метою даної роботи є дослідження питань оцінки матеріальності кіберризиків.

Основні положення. Запропонована модель ґрунтується на монетизованій оцінці показника чистого прибутку компанії, опублікованого у її фінансовій звітності. Для визначення мінімальної та максимальної межі розподілу рівня ризику, мінімальний рівень матеріальності ризику ($CRimin$) в моделі визначений на рівні «0» (можна також такий рівень прирівняти до мінімальної межі ризик-апетиту). Максимальний рівень матеріальності ризику ($CRimax$) в моделі визначений на рівні 1% чистого прибутку компанії за один фінансовий рік. Для розподілу рівнів оцінки матеріальності кіберризику використано трирівневу шкалу оцінки, для визначення яких діапазон значень показника розбито на 4 рівні частини (квартилі). У результаті отримаємо наступну трирівневу шкалу оцінки матеріальності кіберризику:

1. До низького рівня ризику відносяться рівні, значення яких знаходяться у проміжку $[CR_{imin};\ CR_{imin} + \frac{CR_{imax} - CR_{imin}}{4}$).

2. До середнього рівня ризику відносяться рівні, значення яких знаходяться у проміжках:
$[CR_{imin} + \frac{CR_{imax}-CR_{imin}}{4};\ CR_{imax} + 2 * \frac{CR_{imax}-CR_{imin}}{4})$;
$[CR_{imax} + 2 * \frac{CR_{imax}-CR_{imin}}{4};\ CR_{imax} + 3 * \frac{CR_{imax}-CR_{imin}}{4})$.
3. До високого рівня ризику відносяться рівні, значення яких знаходяться у проміжку $[CR_{imax} + 3 * \frac{CR_{imax}-CR_{imin}}{4};\ CR_{imax}]$.

Висновки. Суттєве збільшення інцидентів кіберризику підвищує актуальність розроблення моделей оцінки його матеріальності, особливо їх монетизованої складової. Запропонована для оцінки матеріальності кіберризику модель дає змогу установити конкретні межі рівнів ризику, може бути автоматизована та інтегрована в операційну діяльність компанії.

Список літератури

1. International Standard ISO 31000:2018, Risk management - Guidelines. ISO (International Organization for Standardization). URL – https://www.iso.org/obp/ui/en/#iso:std:iso:31000:ed-2:v1:en (дата звернення: 14.11.2023);
2. Materiality Threshold in Audits. *Corporate Finance Institute.* URL – https://corporatefinanceinstitute.com/resources/accounting/materiality-threshold-in-audits/ (дата звернення: 14.11.2023);
3. International standard on auditing (ISA) 320, Materiality in Planning and Performing an Audit. *The International Federation of Accountants (IFAC).* URL – https://www.ifac.org/_flysystem/azure-private/publications/files/A018%202020 13%20IAASB%20Handbook%20ISA%20320.pdf (дата звернення: 14.11.2023);
4. Danielle McWall.Materiality and its Practicalities. URL - https://www.cpaireland.ie/CPAIreland/media/Education-Training/Study%20Support%20Resources/P1%20Auditing/Relevant%20Articles/materiality-and-its-practicalities.pdf (дата звернення: 14.11.2023).

Відомості про авторів

Поломошнова Марія Ігорівна, магістрантка кафедри кібербезпеки, НТУ «ХПІ», mariia.polomoshnova@gmail.com
Мілевський Станіслав Валерійович, доцент кафедри кібербезпеки, НТУ «ХПІ», к.е.н, доцент, stanislav.milevskiy@hneu.net

Секція 1

АНАЛІЗ АЛГОРИТМІВ ЦИФРОВОГО ПІДПИСУ ДЛЯ РОЗРОБЛЕННЯ ЗАХИЩЕНОЇ СИСТЕМИ ПІДПИСАННЯ ФАЙЛІВ З МОЖЛИВІСТЮ ВИБОРУ АЛГОРИТМУ ЦИФРОВОГО ПІДПИСУ

Проценко Є. С.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Морозова О. І.

Актуальність. Сьогодні, в умовах зростаючого використання електронних документів та обміну інформацією в мережі, питання забезпечення безпеки та цілісності даних стають дедалі більш актуальними. Захищена система підписування файлів, яка надає можливість вибору алгоритму цифрового підпису, відіграє важливу роль у цьому контексті. Дані, що передаються та зберігаються в електронному форматі, повинні бути надійно захищеними від несанкціонованого доступу, змін та підробки. Тому аналіз алгоритмів цифрового підпису для розробки захищеної системи підписування файлів з можливістю вибору алгоритму цифрового підпису є надзвичайно актуальною та важливою темою для досліджень, що сприяє підвищенню рівня безпеки та довіри в інформаційному середовищі [1].

Мета роботи полягає в аналізі алгоритмів цифрового підпису для розроблення та впровадження захищеної системи підписування файлів, яка надає користувачам можливість вибору алгоритму цифрового підпису.

Основні положення. В роботі пропонується розглянути чотири основні алгоритми цифрового підпису [2-4]:

Rivest, Shamir и Adleman (RSA) – криптографічний алгоритм з відкритим ключем, що базується на обчислювальній складності завдання факторизації великих цілих чисел, що означає, що чим більша послідовність чисел у вас є, тим більше ви захищені. Алгоритм RSA був розроблений в Массачусетському технологічному інституті (MIT) у 1977 році Роном Рівестом, Аді Шаміром і Леонардом Адельманом.

Digital Signature Algorithm (DSA) – криптографічний алгоритм, який засновано на складності обчислення дискретних логарифмів у скінченному полі. Алгоритм запропоновано у 1991 та він створений лише для електронного підпису.

Elliptic Curve Digital Signature Algorithm (ECDSA) – це криптографічно захищена схема цифрового підпису, заснована на криптографії еліптичної кривої (ECC). Алгоритм підписання/перевірки ECDSA базується на математичний опис циклічних груп еліптичних кривих над кінцевими полями та на складність проблеми дискретного логарифмування еліптичної кривої (ECDLP).

Edwards-curve Digital Signature Algorithm – криптографічно захищена схема цифрового підпису, заснована на кривих Едвардса. EdDSA використовує стійкість відносно проблеми дискретного логарифмування на кривій Едвардса та надає високий рівень безпеки при невеликих розмірах ключів. Алгоритм детерміністичний, забезпечуючи ефективність та захист від різноманітних атак, і дозволяє підписувати повідомлення без попереднього обчислення хешу. EdDSA є ефективним і безпечним рішенням для цифрового підпису в різних сценаріях застосування.

Вибір чотирьох алгоритмів дозволяє представити ландшафт сучасного документообігу. Серед цих алгоритмів важливо звернути увагу на аспекти, такі як генерація ключів, процеси створення та перевірки підпису, а також ретельно розглянути математичну основу кожного алгоритму. Це дозволяє нам визначити їхню криптостійкість, що є ключовим параметром для повного та об'єктивного порівняння.

Висновки. Робота присвячена порівняльному аналізу алгоритмів цифрового підпису для подальшої розробки системи підписання файлів з можливістю вибору цифрового підпису. Було проведено аналіз кожного з чотирьох алгоритмів, які використовують метод відкритого ключа. Після проведення досліджень недоліків та переваг кожного з запропонованих алгоритмів було зроблено висновок, що алгоритм RSA є найбільш підходящим та надає гарантії цілісності даних та аутентифікацію власника, а також має невеликий розмір пари ключів.

Список літератури

1. Digital signatures. *Cryptobook*. URL – https://cryptobook.nakov.com/digital-signatures/ (дата звернення: 10.20.23);
2. What Are the Differences Between RSA, DSA, and ECC Encryption Algorithms? *Sectigo*. URL – https://sectigo.com/resource-library/rsa-vs-dsa-vs-ecc-encryption (дата звернення: 13.20.23);
3. Comparing SSH Keys – RSA, DSA, ECDSA, or EdDSA? *Goteleport*. URL – https://goteleport.com/blog/comparing-ssh-keys (дата звернення: 13.20.23);
4. What are the advantages and disadvantages of RSA, DSA, and ECDSA for SSH? *Linkedin*. URL – https://www.linkedin.com/advice/1/what-advantages-disadvantages-rsa-dsa-ecdsa-ssh (дата звернення: 15.20.23).

Відомості про авторів

Проценко Єгор Сергійович, студент кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», y.protsenko@student.csn.khai.edu
Морозова Ольга Ігорівна, професор кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», д.т.н., доцент, o.morozova@csn.khai.edu

Секція 1

АНАЛІЗ ЗАГРОЗ, СПРЯМОВАНИХ НА МЕДИЧНІ ЗАКЛАДИ ЗІ СПІЛЬНИМ СЕРВЕРОМ ТА ДОСТУПОМ ДО НЬОГО МЕДИЧНИХ ПРАЦІВНИКІВ

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

Актуальність. За останні роки стало очевидним, що кібербезпека в медичних установах є критично важливою проблемою. Зростаюча кількість витоків медичних даних та вразливість серверів у медичних закладах викликали серйозні обурення і підкреслили необхідність удосконалення заходів безпеки в цьому секторі [1, 2].

Метою нашої дослідницької роботи є ретельний аналіз угроз серверам медичних установ, що виникають через користувачів, а також розробка практичних рекомендацій для запобігання подібним загрозам. Ми прагнемо розкрити сутність ризиків та визначити стратегії для підвищення кібербезпеки в цій галузі [3].

Основні положення. Однією з ключових загроз є витоки медичних даних та ідентифікаційної інформації пацієнтів через недбалість або помилки користувачів [1]. Деякі із цих витоків можуть призвести до надзвичайно серйозних наслідків, таких як порушення конфіденційності та незаконний доступ до особистих медичних записів пацієнтів [2].

Розглянемо приклад фішинг-атаки на медичних працівників. Зловмисник створює підроблену електронну пошту, видаючи себе за офіційне джерело. Пошта може містити додатковий файл або посилання на веб-сторінку для введення облікових даних. Зловмисник розсилає листи медичним працівникам з медичної організації, видаючи себе за важливе повідомлення з безпеки, яке потребує входу в систему. Якщо медичний працівник не підозрює обману і натискає на посилання або відкриває доданий файл, зловмисник отримує доступ до його облікових даних. Після отримання доступу до облікових даних медичного працівника, зловмисник може проникнути в систему медичної організації, звертаючись до даних пацієнтів або порушуючи цілісність медичних записів. Зловмисник може отримати доступ до медичних даних пацієнтів, що може призвести до витоку чутливої інформації. Зловмисник може змінювати медичні записи, що може вплинути на якість медичної допомоги та безпеку пацієнтів. Атака може призвести до блокування доступу медичних працівників до даних, що може призупинити надання медичної допомоги. Витік даних і атаки можуть завдати серйозної шкоди репутації медичної організації.

Заходи безпеки, такі як встановлення потужних паролів, двофакторної аутентифікації та обмеження прав доступу, виявляються надзвичайно

важливими для захисту серверів медичних установ від недозволених дій користувачів [3]. Освіта та навчання медичного персоналу щодо кібербезпеки також можуть сприяти усвідомленню ризиків та зниженню ймовірності помилок, оскільки більшість атак відбуваються саме за допомогою фішингу електронних пошт працівників [4].

Висновки. У звязку із зростаючою загрозою витоків медичних даних через користувачів, медичні установи повинні приділити особливу увагу кібербезпеці. Комплексний підхід до цієї проблеми, включаючи технічні, організаційні та навчальні заходи, є надзвичайно важливим для захисту даних пацієнтів та забезпечення довіри до медичних установ. Забезпечення безпеки медичних даних на серверах вимагає постійної уваги і зусиль для запобігання потенційним загрозам.

Список літератури

1. Kim, D. S., Lee, S. M., & Koo, H. J. (2015). «Data breach and medical identity theft: The growing epidemics.» Healthcare Informatics Research, 21(1), 1-3.;
2. Raghavan, S., Peterson, R., Xiong, X., & Du, W. (2017). «Patient identity theft: Prevention and detection.» Health Informatics Journal, 23(3), 187-199.;
3. Reid, P., Fan, J., & Small, D. (2018). «Patient information breach threats: A healthcare provider perspective.» Healthcare Management Science, 21(4), 545-558.;
4. Nursing Informatics for the Advanced Practice Nurse: Patient Safety, Quality, Outcomes, and Interprofessionalism, Second Edition. (2016). Springer Publishing Company. (Chapter 10: Health Information Systems, p. 181-194);
5. Hoyt, R. E., & Yoshihashi, A. K. (2017). Health Informatics: Practical Guide for Healthcare and Information Technology Professionals. Lulu. (Chapter 9: Information Security and Confidentiality, p. 137-155).

Відомості про авторів

Рябко Іван Богданович, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», i.b.ryabko@student.csn.khai.edu
Желтухін Олександр Васильович, ст. викладач кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», a.zheltukhin@csn.khai.edu

Секція 1

МЕТОДИ ТА ЗАСОБИ ВИБОРУ ТА КОМПЛЕКСУВАННЯ СКАНЕРІВ ВРАЗЛИВОСТЕЙ ДЛЯ ОЦІНЮВАННЯ КІБЕРБЕЗПЕКИ ІНТЕРНЕТ-ТЕХНОЛОГІЙ

Семенець О. Ю.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Тецький А. Г.

Актуальність. Веб-додатки є фундаментальною частиною нашого життя та культури. Оскільки все більше і більше нашого життя та даних переміщується у кіберпростір, хакери зосередили свою увагу на веб-додатках. Веб-додатки - це складна суміш різних технологій. Ця складність, поєднана з інтенсивним тиском на розробників веб-програм, створює сприятливі умови для виникнення помилок і вразливостей. Відсутність вимог до кібербезпеки систем керування вмістом і використовуваних модулів, а також відсутність вимог до рівня знань у галузі інформаційної безпеки адміністраторів систем керування вмістом, є основними причинами успішності атак [1]. Тому спеціалісти з кібербезпеки повинні зосередитися на нових способах захисту веб-додатків від атак, розробити нові інструменти, щоб знайти вразливі місця раніше, ніж це зробить хакер. Існує багато різноманітних автоматизованих підходів до пошуку вразливостей у програмному забезпеченні. Інструменти аналізу вразливостей - автоматизовані, їх можна використовувати проти різноманітних програм. Крім того, вони значно дешевші, ніж наймання команди експертів. Інструменти аналізу вразливостей можна класифікувати залежно від того, яку інформацію веб-додатків вони використовують [2]. Веб-сканери вразливостей чорної скриньки можна використовувати для виявлення проблем безпеки у веб-додатках. Ці інструменти отримують доступ до веб-додатків так само, як і користувачі, і, отже, мають перевагу незалежно від конкретної технології, яка використовується для реалізації веб-додатку [3].

Метою даної роботи є аналіз якості виявлення вразливостей за допомогою доступних на ринку веб-сканерів чорного ящика.

Автори досліду у своїй статті [4], протестували 11 сканерів веб-додатків, запустивши їх на власному веб-сайті. Перевірені сканери включали 8 приватних інструментів і 3 програми з відкритим кодом. Автоматизовані сканери змогли виявити лише половину із доступних вразливостей.

Основні положення. Сканування веб-додатків може стати серйозною проблемою для сучасних сканерів веб-вразливостей. Результати оцінювання показали, що здатність сканувати веб-програму та проникати «вглиб» у ресурси програми є такою ж важливою, як і здатність виявляти

самі вразливості. Навіть якщо методи виявлення певних типів вразливостей добре опрацьовані та надійні, існують категорії вразливостей, які недостатньо вивчені та не можуть бути виявлені за допомогою сучасних сканерів. Помилки реалізації та відсутність підтримки поширених технологій, відсутність підтримки JavaScript (і Flash), потреба в більш складних алгоритмах для виконання «глибокого» сканування та відстеження стану програми, що тестується, ось лише малий перелік існуючих проблем.

Висновки. Немає сильного зв'язку між вартістю сканера та наданими функціями, оскільки деякі з безкоштовних або дуже рентабельних сканерів працюють так само, як і сканери, які коштують тисячі доларів. Сучасні сканери не в змозі виявити специфічні вразливості, а тому полягає питання у можливості комплексування їх роботи.

Список літератури

1. Тецький А. Г. Методи інформаційної технології забезпечення кібербезпеки систем керування вмістом при створенні web-застосунків : дис. канд. техн. наук : 05.13.06, Нац. аерокосм. ун-т ім. М. Є. Жуковського "Харків. авіац. ін-т". Харків, 2019. 187 с.;
2. Evaluation of Black-Box Web Application Security Scanners in Detecting Injection Vulnerabilities. *MDPI*. URL – https://www.mdpi.com/2079-9292/11/13/2049/ (дата звернення: 29.09.2023);
3. A Systematic Literature Review on Penetration Testing in Networks: Future Research Directions. *MDPI*. URL – https://www.mdpi.com/2076-3417/13/12/6986/ (дата звернення: 02.10.2023);
4. Why Johnny Can't Pentest: An Analysis of Black-Box Web Vulnerability Scanners. URL – https://www.researchgate.net/publication/221394405_Why_Johnny_Can't_Pentest_An_Analysis_of_Black-Box_Web_Vulnerability_Scanners/ (дата звернення: 09.10.2023).

Відомості про авторів

Семенець Олександр Юрійович, аспірант кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», o.y.semenets@csn.khai.edu
Тецький Артем Григорович, доцент кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», к.т.н., a.tetskiy@csn.khai.edu

Секція 1

АНАЛІЗ МЕТОДІВ ЗАХИСТУ ІГРОВИХ ЗАСТОСУНКІВ ВІД НЕСАНКЦІОНОВАНОГО ПОШИРЕННЯ

Федоренко В. О.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Певнєв В. Я.

Актуальність. Ігрові застосунки стають об’єктом зростаючого інтересу та популярності серед користувачів. Проте зі зростанням попиту зростає і загроза пов'язана з несанкціонованим поширенням ігрових застосунків, що призводить до серйозних проблем у сфері безпеки. Захист авторських прав та інтелектуальної власності в ігровій індустрії визначається як важливий елемент. Розробники повинні активно захищати свої творчі досягнення від незаконного використання та піратства. Боротьба з несанкціонованим поширенням ігор важлива для уникнення фінансових втрат. Вдосконалення систем ліцензування та технологій захисту від піратства є необхідними для забезпечення стабільних доходів. Репутація гравців на ринку гри — важливий ресурс. Захист від несанкціонованих варіантів гри, чатів, або шахрайських практик є ключовим для збереження довіри гравців. Дотримання законодавчих вимог та стандартів є критичним, зокрема, в контексті захисту персональних даних користувачів і відповідності до міжнародних нормативів. Все це доводить актуальність захисту ігрових застосунків від несанкціонованого поширення

Мета полягає в розгляді несанкціонованого поширення ігрових застосунків та розробці стратегій їх захисту.

Основні положення. Важливість захисту інтелектуальної власності: В контексті ігрової індустрії, захист інтелектуальної власності стає ключовим фактором для стимулювання творчості і забезпечення віддачі від інвестицій у розробку новаторських ігор. Авторські права, патенти та торгові марки відіграють важливу роль у збереженні унікальності та цінності гри. Розгляд технічних рішень, що використовуються для захисту ігрових застосунків від несанкціонованого поширення, включає оцінку систем DRM. Переглядання позитивних, негативних сторін та зручності під час використання. Аналіз сучасних тенденцій у сфері піратства та визначення найбільш актуальних викликів для ігрової індустрії. Розгляд впливу цих викликів на фінансову стабільність та репутацію компаній.

Вивчення взаємозв'язку між заходами безпеки та користувацьким досвідом, зокрема, уникнення негативного впливу заходів захисту на зручність та доступність ігор.

Перевірка, відповідності існуючих методів захисту до нормативів і вимогам законодавству в контексті захисту особистих даних та авторського

права. Дослідження впливу новітніх технологій, на зміну можливостей захисту ігрових застосунків від несанкціонованого використання, а також їхній внесок у забезпечення безпеки та відновлення довіри в ігровій галузі.

Висновки. Стійкість ігрової індустрії великою мірою залежить від ефективності заходів захисту, що визначається як технічними, так і правовими засобами. Захист інтелектуальної власності стає важливим каталізатором для стимулювання творчості та інновацій, важливих для динамічного розвитку галузі.

Технічні засоби, зокрема системи DRM, виявляються важливим елементом в запобіганні піратства та збереженні прибутковості ігрових компаній. Однак необхідно зберігати баланс між ефективністю заходів безпеки та зручністю для гравців, зокрема уникати негативного впливу на користувацький досвід.

Сучасні виклики в галузі боротьби з піратством вимагають постійного вдосконалення та адаптації заходів захисту до нових тенденцій у цифровому середовищі. стратегія повинна враховувати не лише технічні аспекти, а й економічні та репутаційні втрати від несанкціонованого використання.

Впровадження заходів безпеки повинно підкреслювати необхідність дотримання нормативів і законодавства, зокрема в галузі авторських прав і захисту особистих даних. Це сприяє створенню етичного та відповідального середовища в ігровій індустрії.

Список літератури

1. WTO Agreement on Trade-Related Aspects of Intellectual Property Rights. *Wto*. URL – https://www.wto.org/english/docs_e/legal_e/27-trips_01_e.htm (дата звернення: 10.11.2023);
2. How to Protect Your Game from Piracy. *Bytescare*. URL – https://bytescare.com/blog/how-to-protect-your-game-from-piracy/ (дата звернення: 12.11.2023);
3. How to stop software piracy. *Redpoints.* URL – https://www.redpoints.com/blog/how-to-stop-software-piracy/ (дата звернення: 12.11.2023);
4. General Data Protection Regulation. *GDPR*. URL – https://gdpr-info.eu/ (дата звернення: 17.11.2023).

Відомості про авторів

Федоренко Владислав Олександрович, студент кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», v.fedorenko@student.csn.khai.edu
Певнєв Володимир Яковлевич, професор кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», д.т.н, доцент, v.pevnev@csn.khai.edu

Секція 1

ДОСЛІДЖЕННЯ ПІДСИСТЕМ ЗАХИСТУ ОС ANDROID

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

Актуальність. На сьогоднішній день смартфони надійно закріпилися у повсякденному житті багатьох людей. Найпоширенішими сценаріями використання мобільних пристроїв є: переглядання пошти, обмін миттєвими повідомленнями або відеозйомка. Наразі існують різні мобільні операційні системи. Прикладом таких систем є: IOS, KaiOS, BlackBerry OS, Android. За даними сайту statcounter станом на квітень 2023, IOS займає 30,61% пристроїв, а Android – 68,61% [1]. З цього можна зробити висновки, що найпопулярнішою мобільною ОС є Android.

Наразі мобільні пристрої мають велику кількість датчиків, наприклад: мікрофон, динамік, камера, акселерометр, барометр, датчик освітлюваності, термометр, Wi-Fi модуль, сканер відбитку пальця. Це все перетворює смартфон в універсальний пристрій, який стає незамінним помічником у повсякденному житті. Однак всі ці можливості можуть бути використані не тільки власником, а й зловмисником.

Метою роботи є дослідження методів захисту, вбудованих в операційну систему Android.

Основні положення. Головною проблемою пристроїв на операційній системі Android є швидкість отримання виправлень безпеки. Ця проблема виникла через архітектурні особливості самої ОС, що призводить до сповільнення процесу створення оновлень системи. За даними офіційного інструмента для розробки додатків «Android Studio» станом на 01.06.23, версія операційної системи під назвою Tiramisu, яка вийшла у серпні 2022 року, встановлена лише на 5,2% пристроїв. В свою чергу найпоширенішою залишається версія Oreo, яка вийшла у серпні 2017 року [2]. З цього можна зробити висновки, що більшість користувачів не мають актуальної версії операційної системи. Наразі безпеку мобільних пристроїв можна поділити на 3 рівні: ядро, система Android та прикладний рівень. Розглянемо їх детальніше.

На рівні ядра реалізовані базові системи захисту: розмежування доступу, SeLinux та IPC. Система розмежування доступу у системі Android перейшла від базового ядра Linux. Також у ядрі ОС реалізована підсистема SeLinux. Дана технологія є частиною Linux Security Module (LSM), та розпізнає різні об’єкти ядра і конфіденційні дії, що виконуються над ними. Ще однією системою у складі ядра системи є IPC. Дана технологія контролює обмін даними між різними процесами в ОС [3].

Рівень ОС постійно модифікується та отримує нові методи підвищення рівня захищеності з кожною версією системи. Розглянемо найважливіші зміни

в ОС: обов'язкове попередження користувача під час додавання нового сертифікату до системи, журнал дій для всіх додатків у системі, шифрування повного диску, технологія Treble, яка розділила Android на 2 складові: рівень ОС та рівень вендору. Завдяки цьому, розробники могли оновлювати драйвери та версію системи незалежно один від одного. Це дозволило прискорити створення швидких оновлень безпеки. З появою версії Android 11, до системи було додано можливість видати одноразове дозволення додатку на використання модулю системи.

Прикладний рівень захисту є найменш захищеним. Незважаючи на наявність великої кількості стороннього ПЗ для захисту мобільних пристроїв, залишається проблема каналу отримання додатків. Це зумовлено наявністю можливості встановлювати додатки з невідомих джерел та слабкої модерації фірмового магазину від Google.

Починаючи з 2015 року, Google випускає щомісячні «патчі безпеки Android» з метою екстреного виправлення проблем безпеки у ОС. Дані патчі виправляють проблемі на всіх трьох розглянутих рівнях безпеки.

Висновки. Проаналізувавши найпопулярніші мобільні операційні системи було виявлено, що найпоширенішою є система Android. Головною причиною популярності даної ОС є її відкритість. Але одночасно це є її найбільшим недоліком, так як система розроблюється без прив'язки до апаратної платформи. Це призводить до того, що кожний виробник пристроїв вимушений самостійно адаптувати систему до кожного з своїх пристроїв. Нажаль, під час адаптації безпека не є пріорітетною.

Проаналізувавши 3 рівні безпеки операційної системи Android було виявлено, що найбільш вразливим є рівень програмного забезпечення. Це зумовлено тим, що він є найменш контрольованим. Наявність вбудовані системи «Play захист» не покращує ситуацію, так як вона носить лише рекомендаційний характер, тому більшість користувачів ігнорують повідомлення про можливу небезпеку.

Список літератури

1. Mobile Operating System Market Share Worldwide. *Statcounter*. URL – https://gs.statcounter.com/os-market-share/mobile (дата звернення: 30.05.2023);
2. Android Studio. *Android*. URL – https://developer.android.com/studio (дата звернення: 31.05.2023);
3. Linux з підвищеною безпекою в Android. *Android*. URL: https://source.android.com/docs/security/features/selinux?hl (дата звернення: 01.06.2023).

Відомості про авторів

Шипунов Микита Юрійович, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», m.shypunov@student.csn.khai.edu
Цуранов Михайло Віталійович, старший викладач кафедри кібербезпеки та DATA-технологій факультету № 6 Харківського національного університету внутрішніх справ (ХНУВС), ukrear2006@gmail.com

Секція 1

ДОСЛІДЖЕННЯ ПИТАНЬ КОНФІДЕНЦІЙНОСТІ ТА БЕЗПЕКИ В СИСТЕМАХ РОЗПІЗНАВАННЯ ТЕКСТУ

Щеглов А. О.
Національний аерокосмічний університет ім. М.Є. Жуковського «ХАІ»
Науковий керівник: Шостак А. В.

Актуальність. Інтенсивний розвиток комп'ютерних систем логічно призвів до широкого впровадження інноваційних методів обробки даних, які базуються на використанні штучного інтелекту. Ця тенденція особливо помітна у сфері оптичного розпізнавання тексту. Оптичне розпізнавання тексту (англ. optical character recognition, OCR) — це механічне або електронне переведення зображень рукописного, машинописного або друкованого тексту в послідовність кодів, що використовуються для представлення в текстовому редакторі [1]. Однак із збільшенням використання OCR також зростає занепокоєність щодо конфіденційності та безпеки.

Мета. Дослідження та аналіз питань безпеки в системах оптичного розпізнавання тексту.

Основні положення. Технологія оптичного розпізнавання символів (OCR) має можливість сканувати та аналізувати інформацію зображень документів, яка часто містить конфіденційну інформацію. Ці документи можуть включати медичні файли, фінансові звіти, юридичні договори та інші конфіденційні дані. Це породжує занепокоєння щодо можливого ризику витоку конфіденційної інформації, яка може потрапити до несанкціонованих осіб. Технологія OCR також може неочікувано отримувати особисті дані, такі як ім'я, адреса чи номери соціального страхування, що може викликати загрозу крадіжки особистої інформації. Відтак, важливо, бути уважним до цих конфіденційних питань та приймати заходи для захисту конфіденційної інформації під час використання технології OCR. Технологія оптичного розпізнавання символів викликає занепокоєння через потенційні проблеми не лише з конфіденційністю, але й з безпекою даних. Ця технологія передбачає зберігання та передачу даних, що створює ризики, які можуть використовувати кіберзлочинці. Якщо дані, отримані через OCR, не захищені належним чином в базі даних, несанкціоновані особи можуть мати до них доступ. Це може призвести до витоку даних, що, в свою чергу, може призвести до фінансових збитків, шкоди репутації або юридичних відповідальності. Отже, важливо вирішити ці проблеми безпеки та гарантувати захист конфіденційних даних під час усього процесу використання OCR.

Висновки. Роботу з OCR необхідно розпочати з проведення оцінки ризиків для виявлення потенційних загроз та вразливостей, пов'язаних із

використанням технології. Одним із ключових аспектів є обробка конфіденційних даних під час процесу розпізнавання тексту. Слід передбачити вразливість даних при передачі їх відкритими каналами зв'язку. Важливо встановити протоколи обробки даних, що захищають конфіденційну інформацію від несанкціонованого доступу, використання або розголошення. Це може включати універсальні методи кодування повідомлень, контроль доступу та процедури резервного копіювання, відновлення даних та їх безпечне знищення у разі припинення використання.

Список літератури

1. Оптичне розпізнавання символів. *Wikipedia*. URL: https://uk.wikipedia.org/wiki/Оптичне_розпізнавання_символів (дата звернення: 22.11.2023);
2. Konstantin Dergachov. Development of tools for information protection of optical text recognition systems. URL: https://www.researchgate.net/publication/361828225_Development_of_tools_for_information_protection_of_optical_text_recognition_systems (дата звернення: 22.11.2023).

Відомості про авторів

Щеглов Антон Олександрович, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», a.shchehlov@student.csn.khai.edu
Шостак Анатолій Васильович, доцент кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», к.т.н., доцент, a.shostak@csn.khai.edu

Section 1

ANALYZING ALGORITHMS FOR VERIFYING PRIMALITY OF LARGE NUMBERS

Oles Yudin
National Aerospace University «Kharkiv Aviation Institute»
Scientific advisor: Vladimir Pevnev

Relevance. In the modern world, an information and communication system without cryptographic protection is inconceivable. The Entrust report «Global Encryption Trends» highlights that client data stands as the primary encryption priority among surveyed enterprises. However, only 42% of respondents are projected to utilize encryption to safeguard their clients' data in 2021 [1]. It is worth noting that prime numbers play a pivotal role in the field of cryptography and are considered a fundamental element in many cryptographic systems. One of the primary reasons for their relevance is their unique mathematical property: they have only two divisors – 1 and themselves. This property makes them a suitable tool for generating cryptographic keys. For instance, in asymmetric encryption systems like RSA, the security of keys relies on the complexity of factoring large composite numbers into their prime factors. Due to this complexity, it becomes challenging for attackers to break cryptographic messages encrypted using such keys.

The importance of analyzing algorithms for checking the primality of large numbers lies in the fact that with the increase in computational power of modern electronic computing machines, it becomes possible to factorize increasingly larger composite numbers, thereby posing a risk to the security of cryptographic systems [2]. In 1991, the «RSA Factoring Challenge» was introduced with the aim of stimulating research in the field of computational number theory. The latest achievement in the challenge was the factorization of a number of length 829 bits into prime factors. As of 2023, the optimal key length in the RSA cryptosystem is considered to be a 2048-bit key. Considering the current pace of development in information technologies and computational systems, questions arise regarding the security of existing encryption algorithms in the near future.

The purpose of this work is to analyze existing algorithms used for primality testing of large numbers.

Principal provisions. The report examined the fundamental and most popular algorithms for determining the primality of numbers, such as: sieve of Eratosthenes; Miller-Rabin primality test; sieve of Atkin; AKS primality test.

A significant breakthrough occurred in 2004 when researchers from the Indian Institute of Technology in Kanpur proposed a primality testing method named AKS (Agrawal-Kayal-Saxena) [3]. The test was simultaneously general, polynomial, deterministic, and unconditional.

The report investigates the possibility of transforming the prime number determination problem by integrating it with the task of number factorization. It asserts that when determining two factors, which can be either prime or composite, it is possible to conclude that a number is composite. Additionally, the report provides evidence that such tasks do not belong to the class of NP-complete problems. The evidence in the report is illustrated by an example showing that these algorithms have polynomial complexity.

Conclusions. The protection of information through cryptography continues to evolve, especially during data transmission over unsecured communication channels. However, public key encryption algorithms quickly exhaust the supply of known prime numbers. Additionally, the capability of modern computing systems is growing, potentially enabling the factorization of larger prime numbers in the future. Due to these reasons, it's necessary to optimize existing and develop new primality testing algorithms to cover a broader range of potential prime numbers within a given range.

List of references

1. Ponemon Institute. Global Encryption Trends Study, 2021. – Page 5. URL: https://www.entrust.com/lp/en/global-encryption-trends-study (date of access: 05.10.2023).
2. Pevnev V. Pseudoprime Numbers: Basic Concepts and the Problem of Security. ICT in Education, Research and Industrial Applications: Integration, Harmonization and Knowledge Transfer : Proc. of 13th Int. Conf. Kyiv, Ukraine, May 15 18. 2017. Kyiv. 2017. P. 583–593.
3. Agrawal M., Kayal N., Saxena N. Primes is in P. Annals of Mathematics. 2004. Volume 160. Page 781–793. DOI: https://doi.org/10.4007/annals.2004.160.781.

Information about the authors

Oles Yudin, a PhD student from the Department of Computer Systems, Networks and Cybersecurity, o.yudin@csn.khai.edu
Vladimir Pevnev, Dr. Sc., professor from the Department of Computer Systems, Networks and Cybersecurity, v.pevnev@csn.khai.edu

ТЕЗИ ДОПОВІДЕЙ

Секція 2. Функційна безпека

Секція 2

ДОСЛІДЖЕННЯ МЕТОДІВ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ ОСОБИ ВОДІЯ

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

Актуальність. У сучасному світі збільшується кількість автомобілів в користуванні людей. Станом на 2021 рік кількість автомобілів наприклад в Сан-Марино становить 1263 на 1000 чоловік населення, а в Україні 212 на 1000 осіб, тобто практично в кожній сім'ї є свій персональний автомобіль. При цьому кількість автомобілів зростає і до 2050 року як мінімум подвоїться [1].

У зв'язку зі зміною ставлення до автомобіля почастішали випадки несанкціонованого користування автотранспортом неповнолітніми, які не мають право керування автотранспортною технікою. У світі зафіксовано випадки викрадення батьківської машини дітьми у віці 9 років. Управління автомобілем дітьми дуже часто призводить до аварій в яких не тільки знищується майно, а й юні водії отримують серйозні травми, такі ДТП найчастіше бувають зі смертельними наслідками.

У правилах дорожнього руху багатьох країн водії з малим стажем водіння мають додаткові обмеження як по швидкісному режиму (наприклад обмеження максимальної швидкості руху 70 км/год), так і додаткові обмеження (заборона на управління в темний час доби) [2]. За дотриманням цих правил повинна стежити дорожня поліція, але як на око вона може визначити водійський стаж людини, що керує автомобілем. Так всі сучасні автомобілі мають бортовий комп'ютер і можна програмно обмежити максимальну швидкість руху, але дуже часто одним і тим же автомобілем можуть керувати різні люди, які не перенастроюють кожен раз бортовий комп'ютер перед поїздкою.

При нинішньому автомобільному бумі випадки "підліткових" ДТП зустрічаються все частіше. Таке ДТП набагато страшніше, ніж звичайно, тому що аварія, спровокована дитиною, зазвичай абсолютно непередбачувана і супроводжується тяжкими тілесними ушкодженнями.

Тому забезпечення надійної і зручної системи ідентифікації особи водія є актуальним [3].

Метою даної роботи є дослідження сучасних біометричних методів ідентифікації особи водія транспортного засобу. Проаналізувавши статистику ДТП в Україні, та сучасні тенденції в автомобільній

промисловості ми можемо сформулювати завдання для нашої розробки, яка направлена на поліпшення безпеки руху, та запобіганню несанкціонованого використання транспортного засобу (угон, або викрадення).

Серед основних вимог до розроблювальної системи відноситься функція ідентифікації власника транспортного засобу, або особи яка має право керувати цим транспортним засобом. Після успішної ідентифікації особи завдяки додатковим функціям ми можемо встановлювати певні обмеження до осіб яким дозволено керувати транспортним засобом.

Основні положення. Дослідження використання сучасних контактних та безконтактних способів ідентифікації особи, та вплив засобів контролю на зручність та безпечність керування транспортним засобом.

Висновки. Метою представленої роботи є підвищення безпеки шляхом ідентифікації водія для захисту від угону, а також перешкоду недозволеному водінню. Для досягнення поставленої мети визначено організацію та архітектуру мобільної апаратно-програмної системи для реєстрації та обробки біометричних даних водія.

Список літератури

1. Розповсюдженість автомобілів у світі. *Investory News*. URL: https://investory.news/doslidzhennya-skilki-zagalom-avtomobiliv-u-sviti (дата звернення 15.09.2023);
2. Постанова Кабінету Міністрів України «Про правила дорожнього руху» від 10 жовтня 2001 року № 1306. URL: https://document.vobu.ua/wp-content/uploads/2023/05/pdr.pdf (дата звернення 15.09.2023);
3. Біометрія в автомобілях. *Dnepr security*. URL: https://dneprsecurity.com/statji/biometrija-v-avtomobiljah.html (дата звернення 15.09.2023).

Відомості про авторів

Ванін Іван Юрійович, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», i.vanin@student.csn.khai.edu
Желтухін Олександр Васильович, ст. викладач кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», a.zheltukhin@csn.khai.edu

Секція 2

СИСТЕМА АВТОМАТИЗАЦІЇ АДРЕСНОГО РОЗСИЛАННЯ ЛИСТІВ

Власенко О. В.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Перепелицин А. Є.

Актуальність. В умовах цифрової епохи зростає важливість ефективного управління онлайн-подіями та засіданнями. Завдяки розвитку хмарних технологій та популярності віртуальних зустрічей, виникає потреба в автоматизації процесів організації та управління цими заходами. Особливо це стосується автоматизації розсилки листів та управління запрошеннями на відеоконференції.

Інтеграція Google сервісів для автоматизації створення та розсилки запрошень на відеоконференції є відповіддю на потребу ефективнішого управління часом та ресурсами. Поєднання таких сервісів, як Google Forms, Google Sheets, Google Calendar та скриптової платформі Google Apps Script [1], дозволяє спростити підготовку до конференцій, мінімізувати помилки у ручному введенні даних та забезпечити більш гнучке управління запрошеннями.

Автоматизація процесів також сприяє більш ефективному використанню часу як організаторами, так і учасниками. Оптимізація процедур запрошення та реєстрації дозволяє зосередитись на змісті події, а не на технічних деталях її організації.

Розробка системи автоматизації адресного розсилання листів для відеоконференцій на базі Google сервісів є актуальною та перспективною задачею, що відповідає сучасним вимогам цифрової ери.

Метою даної роботи є зниження трудовитрат під час виконання обробки запитів з інформуванням за допомогою поштових сервісів.

Для досягнення поставленої мети необхідно вирішити завдання аналізу можливості автоматизації процесів розподілу прав доступу до заходів та завдання розробки практичної реалізації.

Основні положення. Розроблювана система базується на інтеграції декількох Google сервісів, що дозволяє автоматизувати та оптимізувати процес організації відеоконференцій. Одним із основних сервісів є Google Forms, який використовується для збору заявок від учасників. Ці заявки обробляються через Google Apps Script, який дозволяє автоматизувати створення подій у Google Calendar [2].

На основі даних з форм, система створює індивідуальні події в календарі, в яких визначається час, дата та інші важливі параметри відеоконференції. Після створення події, автоматизована система генерує

та відправляє електронні листи з інформацією про подію та посиланням на Google Meet конференцію ініціатору та учасникам, які зареєструвалися.[3]

Така комплексна система спрощує та автоматизує процес організації відеоконференцій.

Висновки. Сервіси Google надають широкі можливості в створенні систем автоматичної розсилки листів, мають широкий спектр інструментів, що дозволяє створити системи під конкретні вимоги користувачів. Проведене дослідження можливостей автоматизації сервісів Google для створення системи адресного розсилання листів показало, що така автоматизація може бути частково реалізована з використанням мови JavaScript на скриптовій платформі Apps Script.

Розроблена система автоматизації покращує управління онлайн-заходами і створює безпроблемний досвід для організаторів та учасників. Її впровадження може суттєво спростити планування та проведення віртуальних зустрічей, що є важливим кроком у напрямку автоматизації процесів.

Список літератури

1. Automate & extend Google Workspace with simple code. *Google.* URL – https://developers.google.com/apps-script (дата звернення: 10.11.2023);
2. Create a sign-up for sessions at a conference. *Google*. URL – https://developers.google.com/apps-script/samples/automations/event-session-signup (дата звернення: 11.11.2023);
3. How to Schedule a Meeting in Google Meet with Apps Script. *Amit Agarwal*. URL – https://www.labnol.org/schedule-google-meeting-calendar-210529 (дата звернення: 11.11.2023).

Відомості про авторів

Власенко Олександр Вікторович, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», o.v.vlasenko@student.csn.khai.edu

Перепелицин Артем Євгенович, доцент кафедри комп'ютерних систем, мереж і кібербезпеки, к.т.н., доцент, a.perepelitsyn@csn.khai.edu

Section 2

IMPLEMENTATION OF SMART GRID TECHNOLOGIES IN THE POWER SYSTEM OF UKRAINE

Heorhii Zemlianko
National Aerospace University «Kharkiv Aviation Institute»
Scientific advisor: Vyacheslav Kharchenko

Relevance. Over the past 30 years, energy consumption has increased by 45% and is expected to increase by 70% in the next 15-20 years. This is accompanied by rising energy prices due to limited mineral reserves. Therefore, it is necessary to pay immediate attention to reducing energy consumption. Many developed countries are developing energy-efficient solutions to improve the competitiveness of their products.

Ukraine is particularly interested in developing energy efficient solutions as the country's electricity consumption efficiency is very low. The fastest and most cost-effective way to reduce energy consumption is to improve the production, distribution and use of electricity by building an intelligent power system. This system includes smart generation, flexible distribution, consumer-side management, smart facilities, and electric transportation. The power supply systems of the future (so-called «smart grids») are already being actively developed by the world's technological leaders (primarily the United States and China, Japan and South Korea). The Smart Grid concept [3] is designed to solve such global energy problems: power supply reliability, power system management, and the development of alternative energy sources.

Purpose. Optimization of power consumption, improvement of quality and reliability of power supply based on information technology.

Principal provisions. The implementation of smart grids requires the equipment of industrial controllers that, in addition to their primary purpose, can transmit data and have access to the Internet, use renewable energy, and act as a consumer regulator.

The Smart Grid concept emerged after the accidents in the US and Fukushima power grids and aims to transform the outdated power supply system. The smart grid will allow power companies to manage the entire grid, consumers to use power efficiently, and the government to create a smart energy infrastructure. This reform will also improve energy security and confidence in electricity supply, and improve the environmental situation.

In the conditions of Ukraine, the construction of intelligent power supply system's faces many obstacles, namely: contradictions in the requirements of the for Electrical Installations (PUE) and the International Electrotechnical Commission (IEC), the lack of measurement and monitoring systems (quality of electrical energy, reactive load compensation, etc.), Manufacturing Execution Systems (MES) and Building Management Systems (BMS), and regular

electricity audits. At present, electricity consumption is constantly increasing due to the construction of powerful shopping and entertainment centers, the expansion of industrial infrastructure, the development of urban electric transportation, and the proliferation of electric vehicles. the proliferation of electric vehicles.

To successfully implement a smart grid, Ukrainian authorities should adopt legislation, promote standardization of SCADA systems, consider bi-directional power transmission, and implement building management systems. It is also important to adopt international standards in the design and manufacture of electrical equipment.

Conclusions. It is crucial to promptly enhance the regulatory framework to align with European and global standards. This involves revising energy-related laws and regulations, especially establishing a legal structure for integrating smart electricity transmission systems.

Simultaneously, fostering an environment conducive to smart electricity transmission infrastructure development is essential. This encompasses encouraging investments in new technologies that promote a flexible electricity distribution system. Additionally, facilitating active consumer participation in electricity management and utilization is paramount.

Furthermore, exploring the integration of various energy facilities and consumers into a unified smart grid is vital. This network should facilitate data exchange and programmatic management across all levels, ensuring a more efficient and resilient energy supply in response to increasing demand and energy fluctuations.

List of references

1. Technical publications Schneider Electric. *Forum for designers of electrical and low-voltage circuits*. *Eom.* URL: http://eom.com.ua/index.php?topic=5637.0 (date of access: 01.10.2023).
2. Gellings C. W. The smart grid: Enabling energy efficiency and demand response. Lilburn, GA : Fairmont Press, 2009.
3. Smart Grids: inteligentne sieci elektroenergetyczne. Cz. 2 / Krzysztof Billewicz. *Szukaj*. URL: https://szukaj.bu.umk.pl/discovery/fulldisplay/alma9910452256405606/48OMNIS_UMKWT:UMK (date of access: 01.10.2023).

Information about the authors

Heorhii Zemlianko, a PhD student from the Department of Computer Systems, Networks and Cybersecurity, National Aerospace University «Kharkiv Aviation Institute», g.zemlynko@student.csn.khai.edu
Vyacheslav Kharchenko, Dr. Sc., professor, Head of the Department of Computer Systems, Networks and Cybersecurity, National Aerospace University «Kharkiv Aviation Institute», v.kharchenko@csn.khai.edu

Секція 2

ПОРІВНЯЛЬНИЙ АНАЛІЗ ЛЕГКОВАГОВОГО АЛГОРИТМУ ASCON З ІНШИМИ ЛЕГКОВАГОВИМИ АЛГОРИТМАМИ

Зуб А. М.
Харківський національній університет радіоелектроніки
Науковий керівник: Руженцев В. І.

Актуальність. Порівняльний аналіз алгоритмів є ключовим етапом при розробці різноманітних систем програмного забезпечення та обробки даних. Ця робота допомагає визначити, який алгоритм або підхід найкраще підходить для конкретних завдань та потреб системи або користувачів. Правильний вибір алгоритму може вплинути на ефективність, швидкість обробки, масштабованість, а також її вартість та можливість розвитку.

Метою роботи є дослідження та порівняльний аналіз легковаговагових алгоритмів та визначення їхньої відмінності в продуктивності та ефективності на avr-архітектурі. В ході порівняльного аналізу легковагового алгоритму Ascon буде обрано три алгоритми: Ascon, Speck, Acron.

Основні положення. Аналіз буде складатись з декількох кроків. Першою порівняльною характеристикою шифрів є середній час необхідний для встановлення ключа. Цей етап необхідний при ініціалізації шифру перед початком шифрування або дешифрування. Другою та третьою порівняльною характеристикою є швидкість шифрування та дешифрування шифрів при однаковому розмірі даних. Четвертою порівняльною характеристикою є додавання даних автентифікації. Ця характеристика є важливим кроком для забезпечення цілісності та автентифікації даних. Останньою порівняльною характеристикою буде обчислення тегу автентифікації. Операція вимагає виконання хешування внутрішніх станів алгоритму для забезпечення цілісності та автентичності даних.

Аналіз легковаговагових алгоритмів буде відбуватись у середовищі Arduino [1] та на мікроконтролері Arduino Uno [2]. Цей мікроконтролер має чіп Atmega328p, що чудово підходить для тестування, оскільки чіп Atmega328p базується на avr-архітектурі [3], який використовується у мікроконтролері Arduino Uno, має достатньо обмежені обчислювальні ресурси і пам’ять, що дозволяє перевірити ефективність алгоритмів у ресурсних обмеженнях, що характерні для багатьох систем. Результати аналізу нададуть розуміння, який з легковагових алгоритмів може бути кращим варіантом для тієї чи іншої системи.

Висновки. Результати порівняльного аналізу легковагових алгоритмів Ascon, Speck, Acron на avr-архітектурі підтверджують, що оптимальний вибір алгоритму залежить від конкретних завдань та обмежень ресурсів

системи. Кожен алгоритм має свої переваги та обмеження, які слід враховувати при розробці системи забезпечення безпеки даних.

Швидкість встановлення ключа, шифрування та дешифрування є ключовими факторами при виборі алгоритму для ресурсно-обмежених систем. Робота демонструє, що розглядувані алгоритми мають відмінні характеристики у цих аспектах, і вибір має бути здійснений з урахуванням конкретних вимог проекту.

Додавання даних автентифікації виявляється значущим етапом для забезпечення цілісності та автентифікації даних. Результати вказують на різниці в ефективності алгоритмів у виконанні цього завдання, що може впливати на вибір залежно від конкретних вимог до безпеки.

Список літератури

1. Arduino Integrated Development Environment (IDE) v1. *Arduino*. URL – https://docs.arduino.cc/software/ide-v1/tutorials/arduino-ide-v1-basics (дата звернення: 15.10.2023);
2. Arduino UNO R3. *Arduino*. URL – https://docs.arduino.cc/hardware/uno-rev3 (дата звернення: 16.10.2023);
3. What is AVR Microcontroller. *Arduino*. URL – https://www.javatpoint.com/what-is-avr-microcontroller (дата звернення: 16.10.2023).

Відомості про авторів

Зуб Анастасія Миколаївна, магістрантка кафедри безпеки інформаційних технологій, Харківський національній університет радіоелектроніки, anastasiia.zub@nure.ua

Руженцев Віктор Ігорович, професор кафедри безпеки інформаційних технологій, Харківський національній університет радіоелектроніки, д.т.н., доцент, viktor.ruzhentsev@nure.ua

Секція 2

ДОСЛІДЖЕННЯ ВИКОРИСТАННЯ МОВИ PYTHON ДЛЯ ВИРІШЕННЯ ЗАВДАНЬ ІНДУСТРІАЛЬНИХ СИСТЕМ

Калантай О. В.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Бабешко Є. В.

Актуальність. Індустріальні системи становлять основний стовп нашої сучасної цивілізації, обслуговуючи різноманітні галузі, від виробництва до транспорту та енергетики. Зростаюча складність та кількість вимог до ефективності цих систем вимагають впровадження нових технологій, які допоможуть оптимізувати їх функціонування та забезпечити надійність та безпеку.

Один з ключових аспектів, які заслуговують на увагу, це потреба в зборі та обробці даних. Пристрої в індустріальних системах постійно збирають великі обсяги інформації. Python може бути використаний для створення програм, які допомагають збирати, аналізувати та візуалізувати ці дані, що сприяє прийняттю обґрунтованих рішень.

Важливою областю є автоматизація виробництва та контроль над індустріальним обладнанням. Python дозволяє створювати програми для автоматизації процесів, моніторингу стану обладнання та вчасної реакції на відхилення в роботі. Крім того, Python забезпечує інтеграцію з різноманітними системами та пристроями, що є важливим аспектом в індустріальних застосуваннях.

Метою даної роботи є аналіз та дослідження використання мови Python для вирішення завтра в індустріальних системах.

Основні положення. Зі зростанням складності та потреб в оптимізації, управлінні та моніторингу індустріальних систем з’являється підвищене зацікавлення в використанні мови програмування Python для розв'язання викликів цієї галузі.

Можна виділити наступні переваги мови Python. Універсальність та простота використання Python: Python славиться своєю простотою вивчення та читабельністю коду. Обробка та аналіз даних: Python пропонує розширений спектр бібліотек, таких як NumPy, Pandas та Matplotlib, які дозволяють легко обробляти та аналізувати великі обсяги даних, що генеруються сенсорами індустріальних систем.

Висновки. У цьому контексті дослідження ролі та можливостей Python для розв'язання завдань в індустріальних системах стає актуальним і важливим завданням. Це дослідження спрямоване на аналіз і дослідження можливостей використання мови Python, визначення її переваг та

недоліків, а також розробку практичних рішень для поліпшення функціонування індустріальних систем.

Результати дослідження можуть допомогти покращити управління та контроль в індустрії, а також сприяти подальшому розвитку цієї області.

Список літератури

1. Samuel Greengard Website: Amazon “The Internet of Things”. Covers how IoT works in our current world, as well as the impact it will have in the long run on society;
2. Klaus Schwab The Fourth Industrial Revolution Kindle Edition. *Amazon Web Services*. URL – https://www.amazon.com/Fourth-Industrial-Revolution-Klaus-Schwab-ebook/dp/B01JEMROIU (дата звернення: 12.11.2023);
3. Python for IoT: Connecting and Controlling Devices. *Media*. URL – https://medium.com/@VAISHAK_CP/python-for-iot-connecting-and-controlling-devices-3f1c7f7e9423 (дата звернення: 12.11.2023).

Відомості про авторів

Калантай Ольга Вадимівна, магістрантка кафедри комп’ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», o.kalantai@student.csn.khai.edu
Бабешко Євген Васильович, доцент кафедри комп’ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», к.т.н, доцент, e.babeshko@csn.khai.edu

Секція 2

ДОСЛІДЖЕННЯ СИСТЕМИ ІДЕНТИФІКАЦІЇ ОСОБИ ВОДІЯ ЗА ТЕРМОГРАМОЮ ДОЛОНІ

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

Актуальність. Біометрія в автомобільній промисловості явище не нове – відомі виробники авто давно впроваджують її у свої автомобілі з метою підвищення їхньої безпеки, зменшення кількості крадіжок.

Біометрична система доступу в автомобілях може бути реалізована як сканування відбитків пальців, розпізнавання особи або голосу, тобто. заснована на фізіологічних та поведінкових характеристиках, які відрізняють одну людину від іншої. В даний час також доступні такі варіанти контролю доступу до автомобіля, як ідентифікація водія – спеціальні біометричні датчики сидіння та керма, автоматичний стартер двигуна. Їх почали впроваджувати в автомобілях високого класу, таких виробників як Ford, BMW, Mercedes-Benz і Volkswagen.

У найближчому майбутньому такі способи доступу до біометричних транспортних засобів, ймовірно, зростатимуть у зв'язку з останніми технологічними досягненнями та підвищеними вимогами до безпеки [1].

Ще одна цікава опція – це моніторинг показників здоров'я водія. Спостерігаючи за кількістю нещасних випадків, в яких виявляються люди з будь-якими захворюваннями, виробники авто почали приділяти більше уваги впровадженню спеціальних біометричних датчиків, здатних визначати артеріальний тиск водія, його частоту серцевих скорочень та інші важливі параметри з метою попередження та запобігання ДТП [2].

Традиційні методи персональної ідентифікації, засновані на застосуванні паролів або матеріальних носіїв (паспорт, водійське посвідчення, електронний ключ), не завжди відповідають сучасним вимогам безпеки. Пароль можна забути або перехопити, матеріальний носій - скопіювати, втратити або передати іншій особі. Вирішенням даних проблем є вдосконалення методів ідентифікації і аутентифікації користувачів за рахунок застосування біометричних технологій, які дозволяють забезпечити доступ до фізичного керування автомобілем.

Тому забезпечення точної ідентифікації особи водія транспортного засобу є актуальним.

Метою даної роботи є дослідження сучасних безпечних і точних методів ідентифікації особи водія транспортного засобу. Особливо актуально ця задача стоїть для систем безпеки керування транспортними. Задача ідентифікації особи водія і контролю психофізичного стану водія транспортного засобу стоїть дуже давно і люди можуть вирішити цю

задачу різними способами. Використання того чи іншого способу дає можливість вирішити цю задачу і додатково контролювати неадекватні стани водія транспортного засобу.

Основні положення. Дослідження використання сучасних методик біометричної ідентифікації особи водія, та вплив природних та штучних факторів на точність ідентифікації і можливого визначення стану водія транспортного засобу.

Висновки. Метою представленої роботи є підвищення безпеки руху транспортних засобів на дорогах загального користування шляхом автоматизації процесу визначення особи водія з використанням контактних засобів контролю. Для досягнення поставленої мети визначено організацію та архітектуру апаратно-програмної системи для ідентифікації особи водія транспортного засобу.

Список літератури

1. Біометрія в автомобілях. *Dnepr Security*. URL: https://dneprsecurity.com/statji/biometrija-v-avtomobiljah.html (дата звернення 15.09.2023);

2. Статистика ДТП в Україні та основні причини аварій на догорах у 2020 році. *ForinsUser*. URL: https://www.forinsurer.com/news/21/01/19/39063 (дата звернення 15.10.2023).

Відомості про авторів

Мільохін Максим Ігорович, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», m.i.milokhin@student.csn.khai.edu

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

Секція 2

ОСОБЛИВОСТІ ЗАБЕЗПЕЧЕННЯ НАДІЙНОСТІ АРХІТЕКТУРИ AWS

Немов М. Р.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Узун Д. Д.

Актуальність. В сучасному світі, де обчислення в хмарі визначають нові стандарти ефективності та масштабованості, Amazon Web Services стали важливим інструментом для багатьох компаній та організацій. Забезпечення надійності архітектури в AWS є ключовим аспектом в розробці та управлінні інфраструктурою, наприклад для реалізації веб-сайтів, обчислювальних потужностей для навчання нейромереж або Big Data, серверів для різноманітних додатків. У зв'язку з цим виникає необхідність дослідження особливостей та стратегій забезпечення надійності в середовищі AWS.

Метою даної роботи є розгляд основних аспектів та особливостей, що визначають надійність архітектури AWS. Доступність і запит до сайтів або серверів не завжди може бути задоволена, оскільки зміни для інфраструктури не завжди можуть бути гнучкими й швидкими при ручному налаштуванні. А при виході з ладу сервера архітектура може повністю стати цілком непрацездатною. Дослідження спрямоване на визначення тих технічних аспектів, які дозволяють AWS забезпечити доступність, цілісність даних.

Основні положення. При проєктуванні інфраструктури важливо уникати єдиних точок відмови, де відмова одного елемента може призвести до повної недоступності системи. AWS надає різноманітні інструменти для забезпечення надійності. Сервіси, такі як Amazon EC2 Auto Scaling та Amazon Load Balancer, забезпечують доступність та надійність інфраструктури. Amazon EC2 Auto Scaling являє собою автоматизований процес регулювання розміру інфраструктури, який дозволяє автоматично збільшувати або зменшувати обсяг ресурсів в залежності від поточного навантаження системи для оптимізації продуктивності й витрат. Тут використовується загальний підхід до обчислювальних потужностей у хмарних провайдерах «Design services, not servers», де сервер – це одноразовий, витратний, ресурс. Найкраща практика це, коли сервери не повинні зберігати в собі важливі дані. Для них важливо налаштувати розгортку програми або утиліти для нового віртуального сервера і відновлення функціонала. Балансувальник навантаження Amazon Load Balancer дозволяє з'єднати між собою дві різні групи серверів через себе. Load balancing є технікою розподілу навантаження між різними компонентами системи, щоб забезпечити оптимальний розподіл ресурсів і

покращити ефективність роботи системи, уникнути перевантажень та забезпечити надійність. Для забезпечення доступності баз даних RDS використовується snapshot – це знімок бази даних, який фіксує стан даних в конкретний момент часу, що дозволяє вам відновлювати базу даних до певного стану в разі втрати даних чи виникнення інших проблем. Amazon RDS надає можливість використовувати репліки читання для забезпечення доступності. Read replica копіює оновлення з основного екземпляра бази даних, і при відмові основного сервера, запити автоматично переадресовуються до репліки, забезпечуючи безперервну роботу системи. У разі повної відмови інфраструктури її можна відновити у спосіб «IaC». Тобто описати інфраструктуру, щоб її компоненти автоматично і швидко були перестворені чи навпаки – бути вивільненими для оптимізації коштів. Для цього використовується сервіс Amazon CloudFormation, який дозволяє описувати інфраструктуру у вигляді коду та автоматично створювати та управляти ресурсами AWS.

Висновки. Ці практики дозволяють бути інфраструктурі не тільки надійною та гнучкою, а й більш оптимальною у витратах. Ці особливості включені й для інших хмарних провайдерів як Azure або GoogleCloud, використовуючи їх аналоги AWS. Доступність і надійність відіграють ключову роль, оскільки можуть вплинути на досвід користувача використання вашого додатка в бізнес цілях.

Список літератури.

1. *Rajesh Daswani* AWS Certified Cloud Practitioner Exam Guide: Build your cloud computing knowledge and build your skills as an AWS Certified Cloud Practitioner. // Packt Publishing;
2. AWS Well-Architected Framework. *Amazon Web Services*. URL – https://wa.aws.amazon.com/wellarchitected/2020-07-02T19-33-23/index.en.html (дата звернення: 12.11.2023).

Відомості про авторів

Немов Микита Русланович, студент кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», m.r.nemov@student.csn.khai.edu
Узун Дмитро Дмитрович, доцент кафедри комп'ютерних систем, мереж і кібербезпеки, к.т.н., доцент, d.uzun@csn.khai.edu

Секція 2

ПРИНЦИПИ «БЕЗПЕЧНОГО» КОДУВАННЯ

Павленко К. Є.
Національний університет «Запорізька політехніка» «НУЗП»
Науковий керівник: Зайко Т. А.

Актуальність. Сучасний світ нерозривно пов'язаний із використанням програмного забезпечення. Однак цей зростаючий попит на програми також призводить до збільшення кількості потенційних загроз для інформаційної безпеки та конфіденційності даних користувачів. За даними щорічного звіту центру скарг на злочини у всесвітній мережі Інтернет загальні збитки в 2022 році внаслідок кіберзлочинів склали 10,3 млрд. доларів [1]. Відповідно до офіційної статистики Офісу Генерального прокурора України, лише за останні 8 років в Україні кількість виявлених кіберзлочинів збільшилась майже в 7,5 разів [2].

У цьому контексті принципи «безпечного» кодування набувають надзвичайної важливості.

Метою даної роботи є дослідження принципів «безпечного» кодування.

Основні положення. Безпечне програмування — одна з форм безпечного проектування програм, мета якої забезпечити тривале функціонування певної частини коду програми під впливом непередбачуваних обставин [3].

Основні принципи безпечного кодування в програмуванні спрямовані на мінімізацію ризику вразливостей і атак на програмне забезпечення. Ось декілька основних принципів безпечного кодування:

– мінімізація атакувальної поверхні. Зменшення можливостей для атак шляхом обмеження функцій та можливостей, які доступні користувачам із зовнішнього середовища. Провести аналіз і визначити, які частини програми можуть бути доступні для потенційних атак і обмежити їх;

– валідація введення. Перевірка і фільтрація всіх введених даних, щоб уникнути атак на введення, такі як SQL-ін'єкції, XSS-атаки і інші. Ніколи не довіряйте даним, які надходять від користувачів або з зовнішніх джерел;

– безпечність аутентифікації та авторизації. Забезпечення надійних методів аутентифікації користувачів і контролю над їх доступом до ресурсів. Важливо визначити, хто має доступ до яких функцій і даних із суворим дотриманням прав доступу;

– захист даних. Використання механізмів шифрування та інших методів захисту для збереження конфіденційності та цілісності даних. Ніколи не зберігайте конфіденційну інформацію в явному вигляді;

– управління помилками та винятками. Обробка помилок та винятків повинна бути належним чином налаштованою, щоб уникнути розкриття чутливої інформації та запобігти втраті даних;

– оновлення та патчі. Забезпечення своєчасного виправлення виявлених уразливостей та надання оновлень для програмного забезпечення з метою підтримки його безпеки в актуальному стані;

– перевірка вразливостей. Регулярне тестування і аудит безпеки програмного забезпечення для виявлення можливих уразливостей і вирішення їх;

– безпека сторонніх компонентів. Перевірка безпеки сторонніх бібліотек і компонентів, які використовуються в програмі, і вчасне оновлення їх для виправлення вразливостей;

– документація. Збереження докладної документації щодо безпечних практик, архітектури програми та інших аспектів безпеки для спрощення спільної роботи та аудиту.

Висновки. Важливість та необхідність безпечного кодування не можна недооцінювати в сучасному світі. Забезпечення безпеки програмного забезпечення має вирішальне значення для захисту користувачів, конфіденційності даних і запобігання фінансовим втратам та репутаційним ризикам. Принципи безпечного кодування є необхідними для запобігання вразливостям і атакам, що можуть нанести серйозну шкоду як користувачам, так і організаціям. Дотримання цих принципів створює надійне та стійке програмне забезпечення, яке може витримати випробування часом і забезпечити безпеку від сучасних кіберзагроз.

Список літератури

1. Internet Crime Complaint Center (IC3). *Federal Bureau of Investigation*. URL – https://www.ic3.gov (дата звернення: 13.10.2023);

2. Про зареєстровані кримінальні правопорушення та результати їх досудового розслідування. *Офіс Генерального прокурора*. URL: https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2 (дата звернення: 14.10.2023);

3. 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.

Відомості про авторів

Павленко Кирило Євгенійович, студент кафедри програмних засобів, Національний університет «Запорізька політехніка», pavlenkokirya02@gmail.com

Зайко Тетяна Анатоліївна, доцент кафедри програмних засобів, Національний університет «Запорізька політехніка», к.т.н., доцент, nika270202@gmail.com

Секція 2

РОЗРОБКА ПІДХОДУ ЩОДО ПОРІВНЯЛЬНОГО АНАЛІЗУ AI ІНСТРУМЕНТІВ В СФЕРІ ДИЗАЙНУ ЦИФРОВИХ ДОДАТКІВ

Поліщук К. В.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Брежнєв Є. В.

Актуальність. На даний момент існує багато рішень на основі AI, що покликані спростити роботу дизайнерів та розробників за рахунок автоматизації їх роботи чи навіть для генерування цілих частин додатків.

Зважаючи на швидкий розвиток AI-технологій, дизайнерам важливо слідкувати за новими розробками і вивчати, як вони можуть застосовувати ці інструменти в проекті [1]. Аналіз і використання AI-інструментів може покращити якість дизайну, зменшити час, витрачений на технічні завдання, і зробити програмні продукти більш конкурентоспроможними на ринку. AI-інструменти можуть автоматизувати рутинні завдання, такі як розробка логотипів, підбір кольорової палітри, створення шаблонів інтерфейсів, що дозволяє дизайнерам витратити менше часу на технічні аспекти і більше - на креативну роботу [2]. Такі інструменти дозволяють створювати інтерфейси, які пристосовані до потреб кожного користувача, роблячи взаємодію з програмами більш зручною та ефективною. Також невід'ємною частиною таких інструментів є можливість автоматизувати процеси тестування і оптимізації інтерфейсу користувача, допомагаючи виявляти проблеми та змінювати дизайн для покращення користувацького досвіду [3]. Штучний інтелект стає необхідним інструментом для дизайнерів у світі, де швидкість та точність відіграють важливу роль. Основні цілі включають визначення специфічних завдань, пошук оптимальних інструментів, які відповідають цим потребам, та їх інтеграцію в дизайнерський процес. Головна мета полягає в покращенні якості роботи, оптимізації часу та ефективності процесу дизайну.

Як результат швидкого зростання кількості та комплексності рішень на основі AI, виникає проблема підбору таких застосунків. Ця задача не є тривіальною та потребує ретельного аналізу самих рішень та результатів генерації.

Метою роботи є обґрунтування підходу щодо вибору інструментарію для вдосконалення дизайну, оптимізації робочих процесів та покращення взаємодії користувачів з продуктами.

Основні положення. Вибір AI рішень можливо на основі визначення потреб, розуміння конкретних завдань, які дизайнер хоче вирішити за допомогою AI. Це може включати автоматизацію певних процесів, створення елементів дизайну, редагування зображень тощо.

Після визначення задач можливо звернутися до вибору підходящого рішення за характеристиками. До прикладу можливо звернути увагу на характеристики такого типу як Функціональність, Користувацький Досвід Якість результату та Деталізація та Якість, Гладкість та Натуральність. Необхідно також порівняти результат з очікуваннями та стандартами рішеннями. Також необхідно звернути увагу на швидкість, можливості інтеграції, вартість. Після представлення цих характеристик в кількісному вигляді потрібно провести порівняння та вибрати максимально наближений до поставлених цілей

В роботі проведено приклад порівняльного аналізу декількох інструментів, функціональність яких може бути використана у розробці дизайну додатків. Такими сервісами є – RunwayML призначений для видалення фону з зображення, може бути корисним для виокремлення компонентів інтерфейсу. Sketch2React – це інструмент, який допомагає спеціалістам конвертувати свій дизайн у прототипи.

Висновки. Наявні AI рішення дуже різноманітні та покликані вирішувати різноманітні задачі, поєднання таких інструментів один з одним та з розповсюдженими інструментами розробки можуть суттєво спростити та пришвидшити виконання поставлених перед дизайнерами та розробниками задач. Тому для підбору AI інструменту потрібно провести дуже ретельний аналіз, ґрунтуючись на різноманітні характеристики та метрики цих систем. Ґрунтуючись на характеристиках, їх кількісних та якісних показниках, викладений вище підхід підходить для різних типів задач та створений для загального вектору розвитку додатків та рішень на основі AI, що відкриває великий спектр можливостей в автоматизації процесів та генерації проміжних та кінцевих результатів.

Список літератури

1. Andra Irbite, Aina Strode. Artificial intelligence vs designer: the impact of artificial intelligence on design practice. Rezekne, Latvia. Conference: society. Integration. Education 2021;

2. Rezk, Sara Mohammed Mamdouh. The Role of Artificial Intelligence in Graphic Design. 2023. *Journal of Art, Design and Music*. Ч.2. Видання 1, Стаття 1. DOI: 2785-9649.1005;

3. AI in Graphic Design: Revolutionizing Creativity. *Linkedin*. URL – https://www.linkedin.com/pulse/ai-graphic-design-revolutionizing (дата звернення: 28.07.2023).

Відомості про авторів

Поліщук Кирило Володимирович, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», k.polishchuk@student.csn.khai.edu

Брежнєв Євген Віталійович, професор кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», д.т.н., старший науковий співробітник, e.brezhnev@csn.khai.edu

Секція 2

ДОСЛІДЖЕННЯ МЕТОДІВ ВИМІРЮВАННЯ РІВНЯ НАФТОПРОДУКТІВ У РЕЗЕРВУАРАХ НАФТОБАЗИ

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

Актуальність. З метою регулювання обігу моторного палива та етилового спирту в Україні були прийняті нормативні акти які регулюють дану сферу господарської діяльності. Так згідно до Закону України від 18.12.2019 №391-IX Законодавець оновив систему державного контролю за обігом пального та спирту етилового [1].

Реформа спрямована на ліквідацію підпільніх виробництв нафтопродуктів и їх реалізацію. З фальсіфікаторамі паливо, особливо скрапленого газу для автомобільних установок, боролися різнімі методами, но всі зусилля виявило Марні. "Достовірно оцініті Частка нелегального паливо Неможливо, но Це не менше 50% від всього об'єму реалізованого моторного палива [2].

Торгівля неякісним товаром - шлях до втрати ліцензії. Реформа повинна підштовхнути власників АЗС до посилення контролю якості та підвищення безпеки на об'єктах. Безпека в даному випадку дійсно грає важливу роль. Чого тільки варто згадати техногенну екологічну катастрофу на нафтобазі мережі АЗК «БРСМ-Нафта» біля смт. Глеваха в червні 2015 року, де в результаті аварії шестеро людей загинули і 15 постраждали.

Нові форми контролю обороту палива значно знизять і можливості виробників фальсифікованих паливних сумішей [3].

Після ведення нової системи обліку на ринку ПММ очікується скорочення частки фальсифікату приблизно на третину. Однак повністю вивести нелегальних виробників з гри не вийде. В результаті боротьби на «чорному ринку» дрібні представники зійдуть з дистанції.

Тому забезпечення точного вимірювання рівня нафтопродуктів в резервуарах нафтобази є актуальним.

Метою даної роботи є дослідження сучасних безпечних і точних методів вимірювання рівня нафтопродуктів у резервуарах нафтобази. Задача вимірювати рівень пального в ємності стоїть дуже давно і люди можуть вирішити цю задачу різними способами. Використання того чи іншого способу залежить від конкретної задачі.

На нафтобазах та АЗС треба вимірювати рівень пального з великою точністю яка повинна складати +/- 1 літр при об'ємі резервуару пального 20 – 200м^3 і більше, для запобігання крадіжок пального, а також витоку пального у оточуюче середовище.

Основні положення. Дослідження використання сучасних автоматичних, пожежобезпечних та вибухобезпечних точних способів вимірювання рівня на продуктів у сховищах нафтобаз та АЗС, та вплив природних та штучних факторів на точність вимірювання.

Висновки. Метою представленої роботи є підвищення безпеки вимірювання рівня нафтопродуктів у резервуарах сховища шляхом автоматизації процесу вимірювання і використання безконтактних засобів для вимірювання рівня. Для досягнення поставленої мети визначено організацію та архітектуру апаратно-програмної системи для вимірювання та забезпечення ведення автоматичного обліку обігу нафтопродуктів на нафтобазі, або АЗС.

Список літератури

1. Про внесення змін до Податкового кодексу України та деяких інших законодавчих актів України щодо покращення адміністрування акцизного податку: Закон України від 18.12.2019 р. № 391-IX. С. 4.
2. Рівень фальсифікації моторного палива в Україні. *Regulation Gov*. URL: https://cdn.regulation.gov.ua/2c/e5/e3/9f/regulation.gov.ua_GREEN%20BOOK_Motor%20Fuels%20Market%20Regulation.pdf (дата звернення 15.10.2023);
3. Безпека обігу моторного пального в Україні. *Ukrinform*. URL: https://www.ukrinform.ua/rubric-regions/1921211-komisiya-vstanovila-prichini-pojeji-na-naftobazi-brsm.html (дата звернення 18.10.2023).

Відомості про авторів

Рудов Олексій Вікторович, магістрант кафедри комп’ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», o.rudov@student.csn.khai.edu
Желтухін Олександр Васильович, ст. викладач кафедри комп’ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», a.zheltukhin@csn.khai.edu

Секція 2

ДОСЛІДЖЕННЯ ТА ВПРОВАДЖЕННЯ ДОДАТКОВОЇ ПАНЕЛІ КЕРУВАННЯ ПРОМИСЛОВИМ ОБЛАДНАННЯМ

Томілов Д. В.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Желтухін О. В.

Актуальність. Нині у всіх галузях виробництва йде повальне використання промислової електроніки. З'являється нове більш досконале обладнання призначене для автоматизації технологічних процесів у різних галузях промисловості. У процесі виробництва дедалі менше бере участь людина як робоча сила. На нинішньому етапі розвитку виробництва людині приділяється місце або спостерігача, який стежить за процесом виробництва, або місце, на якому людина обслуговує це обладнання при його експлуатації або несправності. Головне завдання, що стоїть перед інженерами, у тому, щоб максимально зменшити роль людського чинника з виробництва. Це веде до зниження собівартості виготовлення товарів з одного боку, і до поліпшення якості своєї продукції, з іншого [1].

В даний час виникає необхідність відображати інформацію про стан технологічного процесу в системах управління у наочному, зручному для сприйняття вигляді. Це пов'язано з удосконаленням технологій, що призвело до створення складніших та універсальних верстатів, гнучких автоматизованих ліній, автомобілів, медичного обладнання. Це обладнання містить велику кількість датчиків, які видають різну інформацію як про саму систему, так і про навколишнє середовище. При контролі за даним обладнанням виникає завдання зручного виведення інформації для сприйняття людиною. Відображення великої кількості різних даних посимвольно незручно, оскільки людині важко стежити за змінами даних як виведення інформації як символів. Інша річ, відображення цих змінних даних графічно як графіків [2].

Основним принципом роботи є зміна інтенсивності світлового потоку, що поступає від підсвітки дисплею. В залежності від рівня електричного поля який створюється між двома пластинами молекули рідких кристалів займають різні положення в просторі, таким чином регулюючи рівень освітлення що поступає від підсвітки дисплею. Особливістю цієї технології є те, що молекули повертаються в одній площині, тому глядач має можливість бачити якісне зображення під широкими кутами огляду [3].

Тому забезпечення зручної індикації і керування промисловим обладнанням є актуальним.

Метою даної роботи є дослідження сучасних пристроїв відображення графічної інформації і забезпечення зручного наочного процесу керування промисловим обладнанням у зручному і безпечному для цього місті

оператором з виростанням однієї, або декількох додаткових панелей керування. Особливо актуально ця задача стоїть для систем безпечного керування великогабаритним промисловим обладнанням, або у небезпечному оточуючому середовищі при виникненні техногенної аварії.

Основні положення. Дослідження використання сучасних засобів відображення інформації з використанням технологій дистанційного контролю, та вплив природних та штучних факторів на достовірність інформації, що відображається, та передачу керуючих сигналів на промислове.

Висновки. Метою представленої роботи є підвищення безпеки керування промисловим обладнанням шляхом використання додаткових мобільних панелей керування обладнанням у зручних, та безпечних місцях для обслуговуючого.

Список літератури

1. Підвищення технологічності виробництва. *Економіка та організація інноваційної діяльності*. URL: https://elib.tsatu.edu.ua/dep/feb/ptbd_1/page7.html (дата звернення 18.10.2023);
2. Пристої виведення графічної інформації. URL: https://ua.izzi.digital/DOS/193559/196755.html: (дата звернення 19.10.2023);
3. Принцип дії РКІ матриці. *LG*. URL: https://lg-b2b.com.ua/ips (дата звернення 20.10.2023).

Відомості про авторів

Томілов Дмитро Владиславович, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», d.tomilov@student.csn.khai.edu
Желтухін Олександр Васильович, ст. викладач кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», a.zheltukhin@csn.khai.edu

Секція 2

ДОСЛІДЖЕННЯ СИСТЕМИ КОНТРОЛЮ СТАНУ ВОДІЯ ТРАНСПОРТНОГО ЗАСОБУ

Тягленко В. Р.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Желтухін О. В.

Актуальність. Щорічно у світі, за даними ООН, внаслідок дорожньо-транспортних пригод гине понад 1,2 мільйона осіб, від 20 – 50 мільйонів зазнають травм, а сумарні економічні втрати перевищують 500 млрд. доларів. Величезний збиток, який завдає державам дорожньо-транспортного травмування, дозволяє віднести його до основних загроз сучасності. Як показує практика, понад 80 відсотків усіх ДТП трапляється з вини самих водіїв. Дослідження показують, що водії, які перебувають за кермом без відпочинку протягом чотирьох годин, час реакції погіршується відразу на 50%. А якщо керувати машиною без перерви на шість годин, то ризик потрапляння в аварію подвоюється [1].

Поки вводяться окремі заходи щодо безпеки автолюбителів, у країнах Євросоюзу планується запуск загальної системи eCall, яка в ручному або автоматичному режимі зможе сповіщати рятувальні служби про аварійну ситуацію [2].

Система обробляє отримані дані та у разі виявлення будь-яких відхилень від норми видає попередження.

Дослідники пояснюють, що аритмія та прихована ішемія міокарда найчастіше призводять до найважчих наслідків: раптової смерті водія чи серйозної дорожньо-транспортної пригоди. Тим часом аналіз електрокардіограми та серцевого ритму дозволяє виявити негативні зміни у стані людини за дві години до настання можливого критичного стану.

Компанія NeuroSky, розробила датчики, що вбудовуються в підголівники крісла водія.

Датчики NeuroSky здатні відстежувати мозкову активність водія навіть через тканину підголівника. Нова система компанії по сигналах з датчиків здатна відрізнити мозкові хвилі дрімаючого або засинаючого водія від хвиль при нормальній активності головного мозку [3].

Не виключено, що в перспективі ці системи увійдуть в оснащення сучасних автомобілів. Вони дозволять знизити ризик раптової смерті водія та зменшити кількість ДТП, пов'язаних із погіршенням його фізичного стану.

Тому забезпечення точної ідентифікації психофізичного стану водія транспортного засобу є актуальним.

Метою даної роботи є дослідження сучасних безпечних і точних методів вимірювання психофізичного стану водія транспортного засобу.

Особливо актуально ця задача стоїть для систем безпеки керування великовантажними транспортними засобами і пасажирськими автобусами тому, що ДТП з участю вище зазначених транспортних засобів мають як правило важкі наслідки з великою кількістю постраждалих. Задача контролю психофізичного стану водія транспортного засобу стоїть дуже давно і люди можуть вирішити цю задачу різними способами. Використання того чи іншого способу дає можливість вирішити цю задачу і додатково контролювати неадекватні стани водія транспортного засобу.

Основні положення. Дослідження використання сучасних методик визначення психофізичного стану водія, та вплив природних та штучних факторів на точність визначення стану водія транспортного засобу.

Висновки. Метою представленої роботи є підвищення безпеки руху транспортних засобів на дорогах загального користування шляхом автоматизації процесу визначення стану водія з використанням безконтактних засобів контролю. Для досягнення поставленої мети визначено організацію та архітектуру апаратно-програмної системи для контролю стану водія транспортного засобу.

Список літератури

1. Статистика причин ДТП. *Судово-юридична газета в Україні*. URL: https://sud.ua/uk/news/ukraine/270012-glavnye-prichiny-dtp-s-postradavshimi-v-ukraine-v-2023-godu-statistika (дата звернення 5.10.2023);
2. Реакція водія та її вплив на аварійність. *Avarii*. URL: http://avarii.com/info_5 (дата звернення 12.10.2023);
3. Система контролю за станом водія. *Автотачки*. https://uk.avtotachki.com/opisanie-i-princip-raboty-sistemy-kontrolya-ustalosti-voditelya. (дата звернення 18.10.2023).

Відомості про авторів

Тягленко Владислав Русланович, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», v.tyaglenko@student.csn.khai.edu
Желтухін Олександр Васильович, ст. викладач кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», a.zheltukhin@csn.khai.edu

Секція 2

ДОСЛІДЖЕННЯ МЕТОДІВ РЕАЛІЗАЦІЇ БЛОКЧЕЙН ПРОТОКОЛІВ З ДОКАЗОМ НУЛЬОВОГО ЗНАННЯ

Тяпко М. В.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Харченко В. С.

Актуальність. Зі зростанням використання технології блокчейну приватність стала значущою проблемою у фінансових транзакціях [1]. Традиційні системи блокчейну є прозорими, що означає, що всі транзакції є публічно доступними. Прозорість блокчейну - це функція, яка забезпечує відповідальність та усуває потребу в посередниках. Однак ця прозорість може стати проблемою для користувачів, які хочуть зберегти конфіденційність своїх транзакцій. Тому існує потреба у більш безпечному та ефективному методі проведення приватних транзакцій на блокчейні. Для можливості приватних транзакцій на блокчейні були розроблені докази нульового знання [2].

Метою цього дослідження є вивчення використання ZK-доказів для транзакцій з підвищеною приватністю в блокчейн протоколах.

Основні положення. Нинішні методи здійснення приватних транзакцій на блокчейні є обмеженими та часто ґрунтуються на довірі до третіх сторін. Наприклад, використання міксерів [3] може бути скомпрометовано зловмисниками, які можуть відстежувати рух коштів [4]. Крім того, рішення, що працюють поза ланцюжком, такі як Lightning Network [5], потребують використання довірених посередників, що суперечить децентралізованій природі блокчейну. Дослідження включає огляд літератури щодо існуючих методів здійснення приватних транзакцій на блокчейні та аналіз обмежень цих методів. Дослідження також включає оцінку використання доказів знань для підвищення приватності транзакцій.

Висновки. Використання доказів нульового знання (ZK-докази) для транзакцій з підвищеною приватністю на блокчейні є перспективним напрямом дослідження. Дослідження може допомогти в розробці більш безпечних та ефективних систем блокчейну, досліджуючи існуючі методи проведення приватних транзакцій на блокчейні з використанням ZK-доказів. Результати дослідження можуть допомогти виявити обмеження існуючих методів та дати висновки щодо оптимізації їх продуктивності. Крім того, дослідження може оцінити ефективність та продуктивність існуючих методів та надати рекомендації щодо їх удосконалення. Знання, отримані в результаті дослідження, можуть сприяти розвитку кращого розуміння використання ZK-доказів для транзакцій з підвищеною приватністю на блокчейні та можуть бути корисними для розвитку майбутніх досліджень в цій галузі.

Список літератури

1. Blockchain Technology: Data Privacy Issues and Potential Mitigation Strategies. URL: https://www.davispolk.com/sites/default/files/blockchain_technology_data_privacy_issues_and_potential_mitigation_strategies_w-021-8235.pdf (дата звернення 11.04.2023);
2. *Justin Thaler*. Proofs, Arguments, and Zero-Knowledge – с. 171. *Georgtown University*. URL: https://people.cs.georgetown.edu/jthaler/ProofsArgsAndZK.pdf (дата звернення: 13.04.2023);
3. On How Zero-Knowledge Proof Blockchain Mixers Improve, and Worsen User Privacy – с. 11. *ARXIV*. URL: https://arxiv.org/pdf/2201.09035.pdf (дата звернення 11.04.2023);
4. Analyzing the Bitcoin Transaction Graph: A Look at Mixers and Traceability – с. 11. *MIT* URL: http://www.css.csail.mit.edu/6.858/2013/projects/jeffchan-exue-tanyaliu.pdf (дата звернення: 11.04.2023);
5. *Joseph Poon, Traddeus Dryja.* The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments. URL: https://lightning.network/lightning-network-paper.pdf (дата звернення: 11.04.2023).

Відомості про авторів

Тяпко Михайло Вікторович, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», m.tiapko@student.csn.khai.edu
Харченко В'ячеслав Сергійович, завідувач кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», д.т.н, професор, v.kharchenko@csn.khai.edu

АЛФАВІТНИЙ ВКАЗІВНИК

АЛФАВІТНИЙ ВКАЗІВНИК

ЗМІСТ

СТУДЕНТСЬКА КОНФЕРЕНЦІЯ ІНФОРМАЦІЙНА, ФУНКЦІЙНА і КІБЕРБЕЗПЕКА СКІФіК

Відповідальний за випуск Г.А. Землянко

Видавець ФОП Бровін О.В.
Свідоцтво про внесення субєкта до Державного реєстру видавців та виготовників видавничої продукції серія ДК 3587 від 23.09.09 р.
Формат 60х86/16. Ум. друк. арк. 7.56. Тир. 100 прим. Зам. 754.

Надруковано з макету замовника ФОП Бровіна І.П.
61022, м. Харків, вул. Трінклера, 2, корп.1, к.19. Т. (066) 822-71-30

СТИЛЬ-ИЗДАТ
ТИПОГРАФИЯ