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 другої науково-технічної конференції

30 листопада, 1 грудня 2022 року

ХАРКІВ - 2022

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 другої науково-технічної конференції

30 листопада, 1 грудня 2022 року

Харків 2022

УДК 004.056

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

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ КОНФЕРЕНЦІЇ

ISBN 978-617-8009-90-8

ПЛАН ПЕРШОГО ДНЯ КОНФЕРЕНЦІЇ

<table>
<tr><td colspan="3">30 листопада 2022 року, Час: 15:00 – 18:45, онлайн</td></tr>
<tr><td>15:00
–
15:10</td><td colspan="2">Вітальне слово</td></tr>
<tr><td>15:10
–
15:20</td><td colspan="2">Вітальне слово спонсора конференції «Distributed Lab».</td></tr>
<tr><td>15:20
–
15:45</td><td colspan="2">Виступ аспіранта кафедри 503, НАУ «ХАІ»; QA-інженера, WebSpellChecker LLC, Абакумова Артема Ігоровича
Тема: Тестування на проникнення для оцінки кібербезпеки промислових роботизованих систем: виклики та рішення</td></tr>
<tr><td>15:45
–
15:50</td><td colspan="2">Перерва</td></tr>
<tr><td rowspan="3">15:50
–
18:30</td><td>Секція 1</td><td>Секція 2</td></tr>
<tr><td>Інформаційна безпека</td><td>Функційна безпека</td></tr>
<tr><td>https://meet.google.com/skn-nvtp-vrb</td><td>https://meet.google.com/edu-saim-gft</td></tr>
<tr><td>18:30
–
18:45</td><td colspan="2">Обговорення результатів роботи секцій</td></tr>
</table>

ПЛАН ДРУГОГО ДНЯ КОНФЕРЕНЦІЇ

<table>
<tr><td colspan="3">1 грудня 2022 року, Час: 15:00 – 18:30, онлайн</td></tr>
<tr><td>15:00
–
15:05</td><td colspan="2">Оголошення Оргкомітету</td></tr>
<tr><td>15:05
–
15:30</td><td colspan="2">Виступ аспіранта кафедри 503, НАУ «ХАІ»; Software Developer, WebSpellChecker LLC, Неретіна Олексія Сергійовича
Тема: Кібератаки на системи штучного інтелекту: аналіз вразливостей з використання Big Data засобів</td></tr>
<tr><td>15:30
–
15:35</td><td colspan="2">Перерва</td></tr>
<tr><td rowspan="3">15:35
–
18:00</td><td>Секція 1</td><td>Секція 2</td></tr>
<tr><td>Інформаційна безпека</td><td>Функційна безпека</td></tr>
<tr><td>https://meet.google.com/skn-nvtp-vrb</td><td>https://meet.google.com/edu-saim-gft</td></tr>
<tr><td>18:00
–
18:15</td><td colspan="2">Перерва</td></tr>
<tr><td>18:15
–
18:30</td><td colspan="2">Підсумкове пленарне засідання</td></tr>
</table>

ПРОГРАМА КОНФЕРЕНЦІЇ

30 листопада, 1 грудня 2022 року, Онлайн формат

Відкриття конференції, привітання учасників організаторами конференції та запрошеними гостями

Пленарні доповіді:

Аспірант кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», **Абакумов Артем Ігорович**. Тема доповіді: «Комбіновані методи тестування на проникнення робототехнічних систем»

Аспірант кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», **Неретін Олексій Сергійович**. Тема доповіді: «Кібератаки на системи штучного інтелекту: аналіз вразливостей з використання Big Data засобів»

Секція 1. Інформаційна безпека
Посилання: https://meet.google.com/skn-nvtp-vrb
Модератор: Шипунов Микита Сергійович
Спів модератори: Селіванова Марія Олександрівна, Стацишина Ірина Павлівна

Секція 2. Функційна безпека
Посилання: https://meet.google.com/edu-saim-gft
Модератор: Юдін Олесь Вікторович
Спів модератор: Землянко Георгій Андрійович

ТЕЗИ ДОПОВІДЕЙ

Секція 1. Інформаційна безпека

Секція 1

ЗЛОВМИСНІ АТАКИ БОТІВ, ЩО СПРЯМОВАНІ НА ОТРИМАННЯ МАТЕРІАЛЬНОЇ ВИГОДИ

Гайдук П. В.
Національний авіаційний університет, м. Київ
Науковий керівник Петренко А.Б.

Актуальність. Шахрайство з ботами стає дедалі поширенішим, оскільки все більше кіберзлочинців використовують ботів для здійснення різних форм кібератак: шахрайство з ботами з використанням шахрайських ботів, сканування зловмисних вразливостей, захоплення облікових записів, впровадження SQL, витоку даних тощо.

Мета. Виявлення інтернет-шахрайств, що застосовують ботів, використовуючи перевірку браузерів на наявність постійних юзер-агентів.

Основні положення. Найбільш поширеним типом інтернет шахрайства в інтернеті можна привести два наступних типи:

1) Шахрайство з кредитними картками [1]. Техніка шахрайства з кредитними картками за допомогою ботів, яку найчастіше використовують хакери, — це злом карток. Злом базується на ідеї про те, що легко отримати номер кредитної картки, відомий як номер приватного рахунку, разом із ім'ям, надрукованим на картці. Зловмисники використовують ботів, щоб вгадати та підтвердити додаткову інформацію, необхідну для «злому» та незаконного використання кредитної картки [2].

2) Атаки на захоплення облікового запису [3]. Атаки, також відомі як надсилання облікових даних - це метод, за якого зловмисники використовують списки скомпрометованих облікових даних користувача, щоб зламати систему. Атака використовує ботів для автоматизації та масштабування та базується на припущенні, що багато людей повторно використовують імена користувачів і паролі в кількох службах. Надсилання облікових даних є вектором загрози, що зростає, з двох основних причин:

– Широка доступність масивних баз даних облікових даних про зловмисники, наприклад, «Колекція №1-5», яка зробила 22 мільярди комбінацій імен користувачів і паролів відкрито доступними для спільноти хакерів у вигляді звичайного тексту.

– Більш складні боти, які одночасно намагаються ввійти з кількох користувачів і походять з різних IP-адрес.

Виходом може бути лише концентрація на найбільш пріоритетних напрямам, до яких слід віднести розвиток системи захисту у напрямі створення:

– Перевірка браузера. Деякі зловмисні боти вдають, що запускають певний браузер, а потім перемикаються між агентами користувача, щоб їх не виявили. Перевірка веб-переглядача гарантує, що кожен веб-переглядач користувача є тим, за що він себе представляє – що він має очікуваний агент JavaScript, здійснює виклики у спосіб, який очікується від цього веб-переглядача, і працює у спосіб, який очікується від користувачів.

Висновок. У зв'язку з тим, що більшість інтернет-ресурсів нехтують захистом своїх сайтів, випускаючи з поля зору захист за допомогою перевірки браузерів користувачів на наявність постійних та незмінних юзер-агентів, так як звичайна людина ніколи не буду навмисно змінювати юзер-агент, запропонований метод є досить доречним та слід звернути на нього увагу.

Список літератури

1. Клімов С. В. Система виявлення шахрайських операцій з банківськими картками. (м. Суми, 22–23 листопада 2018 р). Суми, 2018. С. 303-307.;
2. Usman A., Shah M. Critical Success Factors for Preventing eBanking. Journal of Internet Banking and Commerce. 2013. Issue 18(2). Pp. 1 –13.;
3. Що таке веб-боти. *Antoinevastel*. URL: https://antoinevastel.com/crawler/2019/12/29/families-web-bots.html (дата звернення: 15.11.22).

Відомості про авторів

Гайдук Павло Вікторович, магістрант кафедри комп'ютеризованих систем захисту інформації, м.т. 0638210059, 5254757@stud.nau.edu.ua
Петренко Андрій Борисович, доцент кафедри комп'ютеризованих систем захисту інформації, к.т.н., доцент, andrii.petrenko@npp.nau.edu.ua

Секція 1

ДОСЛІДЖЕННЯ БЕЗПЕКИ САЙТІВ УНІВЕРСИТЕТІВ НА ПРИКЛАДІ ХАІ

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

Актуальність. З розвитком сучасних технологій уся необхідна інформація для студента знаходиться в мережі Інтернет. Є два типи сайтів: інформаційного характеру та сайти для дистанційного навчання, де знаходиться необхідна користувачеві інформація. Як правило, у кожного університету є обидва типи цих сайтів. Наприклад, як є інформаційний сайт ХАІ, та навчальні сайти moodle, mentor, elearn. Тобто, можна сказати, що якість навчання та успішність студента – цілком залежить від доступності подібних ресурсів. З чого можна зробити висновок, що інформаційні та навчальні ресурси мають бути стійкими до навантаження та захищеними від несанкціонованого проникнення.

Метою даної роботи є дослідження сайту університету з метою покращення доступу та надійності роботи сайту, в умовах великого навантаження.

Основні положення. Для того, щоб зрозуміти та перевірити безпеку сайтів – проводять тести на проникнення. Тест на проникнення (penetration test) — метод оцінювання захищеності комп'ютерної системи чи мережі шляхом часткового моделювання дій зовнішніх зловмисників з проникнення у неї (які не мають авторизованих засобів доступу до системи) і внутрішніх зловмисників (які мають певний рівень санкціонованого доступу) [1]. Цей процес включає активний аналіз системи з виявлення основних потенційних вразливостей для сайту. Які можуть виникати внаслідок неправильної конфігурації веб-сервісу, непередбачених дефектів апаратних засобів при створенні сайту, або програмного забезпечення, чи оперативне відставання в процедурних чи технічних контрзаходах. Цей аналіз проводиться з позиції потенційного нападника і може включати активне використання вразливостей.

Основні шляхи взаємодії сайту та користувача – це пошук інформації. Для ідеального сайту, є правило, що уся необхідна інформація, та функціонал сайту повинні знаходитись максимально на 3 рівні вкладеності починаючи з початкової сторінки [2]. Адже, зручніше та краще буде сайт для користувача, коли він зможе робити менше помилок. Якщо, ця умова дотримується – то для користувача немає проблеми щось знайти на сайті без витрати часу на пошук.

Ця умова використовується для усіх сайтів, але основна ціль – це сайти, основною метою яких є надання інформації

Для сайтів, що використовуються для навчання – поряд з цим правилом, стоїть ще одне. Це навантаження великою кількістю користувачів, та при завантаженні великих за обсягом файлів. Навантаження великою кількістю користувачів, в цьому контексті означає тестування продуктивності. Тестування продуктивності - це тестування, яке проводиться з ціллю визначення, як швидко працює програма або її частина під деяким навантаженням [3]. Для тестування будуть обрані більш схожі на реальні цифри навантаження, ніж при тестування критичної відмови. Адже сайт повинен бути готовим до цього, бо в період вступу – кількість користувачів сайту зростає в рази. Для цього використовувався додаток JMeter. Було проведено перевірку навантаженням сайту кафедри – elearn (у середньому 800-1000 людей), та сайтів університету – ХАІ, moodle, mentor (6-7 тис. людей).

Висновки. У результаті, були перевірені такі сайти університету ХАІ: Головний сайт, elearn, moodle, mentor. Усі вони використовуються кожного дня. Але критичні дні для таких сайтів – це тижні модульного контролю, тижні підсумкового контролю, та декілька тижнів до цього моменту, літні дні, коли є температурне навантаження на сервери, та несумлінні студенти, які з метою не навчатись можуть зробити DoS-атаку. Як результат, вони пройшли два види тестування, що були наведені вище. Сьогодні сайти перейшли на хмарну платформу CloudFlare. В безкоштовній версії є базовий захист від невеликих DoS-атак. Окрім цього, вони також витримують середні навантаження, які є на серверах ХАІ. Але, при поточних відключеннях електроенергії, ці сайти стають недоступними, коли в ХАІ немає світла, чи інтернету. Для вирішення цієї проблеми слід перемістити сайти в захищену хмару, щоб вони були доступні студентам 24/7.

Список літератури

1. Тест на проникнення. *Wikipedia*. URL: http://surl.li/dndyh (дата звернення: 30.10.2022);

2. Правила для ідеального сайту. URL: https://sdmne.com/9-pravil-idealnogo-dizayna-sayta/ (дата звернення: 30.10.2022);

3. Тестування продуктивності. *Wikipedia*. URL: http://surl.li/dndyu (дата звернення: 30.10.2022).

Відомості про авторів

Бохан Кирило Андрійович. Студент кафедри комп'ютерних систем, мереж і кібербезпеки, м.т. 050-600-86-03, k.a.bokhan@student.csn.khai.edu.

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

Секція 1

МЕТОД ЗАХИСТУ ПЛАТІЖНИХ ДАНИХ У ВЕБ-ЗАСТОСУНКУ ДЛЯ ОСББ

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

Актуальність. Сьогодні у світі є велика кількість різноманітних платіжних систем, завдяки чому все менше людей користуються готівковими розрахунками. Онлайн розрахунки спрощують життя людям за рахунок швидкості транзакцій, доступності з будь-якої точки світу за умови наявності інтернету, можливості проведення їх у будь-який час доби тощо. Вони використовуються у багатьох сферах, наприклад, таких як інтернет-покупки, оплата таксі тощо. Сфера ОСББ не стала виключенням. Для зручної оплати комунальних та житлових платежів через застосунки для ОСББ, необхідно використовувати платіжні системи.

Метою роботи є дослідження методів захисту платіжних даних.

Основні положення. Для початку необхідно визначити що є платіжною системою.

Платіжна система - платіжна організація, учасники платіжної системи та сукупність відносин, що виникають між ними при проведенні переказу коштів. Проведення переказу коштів є обов'язковою функцією, що має виконувати платіжна система [1]. До складу платіжної системи як екосистеми в цілому входить ціла низка учасників: платіжні провайдери, банки, центральний координуючий орган (як правило, центробанк країни), процесингові центри та провайдери технічної інфраструктури, що забезпечують обчислювально-комунікаційну базу для проведення платежів[2]. Усі учасники системи взаємодіють між собою за певними правилами та домовленостями, спираючись на чітко виписану законодавчу основу[2].

Існує основні два методи захисту інформації, що використовуються для захисту платіжної інформації найчастіше. Це токенізація та шифрування.

Шифрування – це засіб захисту цифрових даних за допомогою одного або декількох математичних прийомів, разом із паролем або «ключем», що використовується для дешифрування інформації. [3]. Існує два основних типи шифрування – це симетричне та асиметричне. При симетричному шифруванні використовується один ключ, як для шифрування, так і для дешифрування, що і є головною перевагою цього типу шифрування. За рахунок його простоти він є швидшим за асиметричний тип алгоритмів та потребує менше обчислювальних потужностей. При асиметричному шифруванні використовується два різних ключа. Одним з ключів може користатися хто завгодно, бо він є загальнодоступним і називається

«відкритим ключем». Другий ключ є приватним і називається «закритим ключем». Відкритий ключ використовується для шифрування даних, а закритий для дешифрування, що гарантує, що дані будуть розшифровані тільки особою, що має закритий ключ. Основною перевагою цього типу шифрування є підтримка роботи з неструктурованими базами даними.

Токенізація — це процес обміну конфіденційних даних на неконфіденційні дані, які називаються «токенами», які можна використовувати в базі даних або внутрішній системі, не зачіпаючи їх [4]. На відміну від шифрування, токенізація не використовує математичний процес для перетворення інформації. В процесі токенізації інформація замінюється на дані, які не мають цінності і їх неможливо використати у корисливих цілях. На відміну від зашифрованих даних, токенізовані нерозшифровуються і є незворотними.

Надійний захист платіжних даних також залежить від самих користувачів, тож окремо потрібно займатися освітою користувачів за допомогою інструктажів безпеки.

Висновки. В останні роки платіжні системи набули чималої популярності, через що, багато застосунків почали їх використовувати для зручного отримання оплати послуг. У сфері ОСББ онлайн платежі не стали виключенням. Додавання платіжної системи до застосунка дозволяє користувачам зручно сплачувати за комунальні та житлові послуги одразу з особового кабінету. Звісно постало питання захисту платіжних даних. Для зберігання платіжних даних найчастіше використовується токенізація та шифрування. Основним мінусом токенізації є складне масштабування для великих обсягів даних. Якщо хакери дізнаються ключ дешифрування, то дані будуть дешифровані, це і є основним мінусом шифрування. Для захисту даних найкраще використовувати токенізацію та шифрування разом.

Список літератури

1. Закон України Про платіжні системи та переказ коштів в Україні [ст. 1, п. 1.29]. URL: https://zakon.rada.gov.ua/laws/show/2346-14#Text (дата звернення: 07.11.22);
2. Що таке платіжна система та які з них працюють в Україні. *Fondy*. URL: https://fondy.ua/uk/knowledge/payment-system/ (дата звернення: 15.11.22);
3. Шифрування. *Nesrakonk*. URL: https://ua.nesrakonk.ru/encryption/ (дата звернення: 16.11.22);
4. What is Tokenization? *Tokenex*. URL: https://www.tokenex.com/blog/what-is-tokenization/ (дата звернення: 15.11.22);

Відомості про авторів

Волобуєва Дар'я Михайлівна, студент кафедри комп'ютерних систем, мереж і кібербезпеки, м.т. 0999707472 d.volobueva@student.csn.khai.edu
Землянко Георгій Андрійович, асистент кафедри комп'ютерних систем, мереж і кібербезпеки. g.zemlynko@csn.khai.edu

Секція 1

КЛІЄНТ-СЕРВЕРНИЙ ЗАСТОСУНОК ЗАХИЩЕНОГО ЗБЕРІГАННЯ ОБЛІКОВИХ ДАНИХ КОРИСТУВАЧІВ

Гірич О. С.
Національний авіаційний університет, м. Київ
Науковий курівник Казмірчук С. В.

Актуальність. У наш час стрімко зростає кількість послуг, пропонованих мережею Інтернет, тому і пропорційно зростає кількість паролів, які повинен запам'ятати користувач. Рано чи пізно виникає проблема, що користувачі вже не в змозі запам'ятати новий надійний пароль для нового облікового запису. Користувачі зазвичай вирішують цю проблему одним із двох способів. Загальним рішенням є повторне використання одного пароля на багатьох різних веб-сайтах. Іншим способом є використання спеціалізованих програмних застосунків і сервісів для безпечного зберігання паролів та інших облікових даних, їх ще називають менеджерами паролів.

Мета. Розробка програмного застосунку для захищеного зберігання облікових даних користувачів із використанням клієнт-серверної архітектури.

Основні положення. Менеджер паролів — вид програмного забезпечення, який вимагає від користувача запам'ятати єдиний надійний головний пароль, який використовується для доступу до збережених облікових даних. Ці програмні застосунки мають широкий функціонал від генерації випадкового паролю по певних критеріях (довжини, наявність літер обох регістрів, цифр, знаків) до вибору алгоритму шифрування сховища з обліковими даними, тому користувачам варто детальніше ознайомитись з ними [1].

Даний програмний додаток було розроблено із використання клієнт-серверної архітектури з вибором концепції «Сильний клієнт». Це означає, що клієнт відповідає за обробку інформації, а сервер виконує функції сховища даних або надсилання до сховища даних [2].

Розробку даного програмного пристрою можна розділити на два основних етапи – розробку серверної частини та розробку клієнтської частини. Під час розробки серверної частини відбувається створення вебсерверу, який відповідно до запитів клієнта відсилає свої запити до БД для модифікації даних відповідно до запиту клієнта. Розробка клієнтської частини полягає в розробці зручного користувацького інтерфейсу, методів

відображення, шифрування, розшифрування та надсилання інформації, введеної користувачем на сервер.

При реєстрації користувач зберігає свої реєстраційні дані на сервері в зашифрованому вигляді. Шифрування даних користувача відбувається на боці клієнта за допомогою алгоритму Argon2. Хеш парою також створюється на боці клієнта за допомогою алгоритму SHA256. Хеш використовується при авторизації, коли користувач повторно хоче отримати доступ до бази даних (сховища) своїх облікових записів. Щодо сховища, то воно теж шифрується на стороні клієнта. Шифрування вмісту сховища виконується за допомогою ключа від сховища, який створюється функцією стандарту PBKDF2 з вхідними даними хешу пароля, електронної адреси. Таким чином всі важливі дані зберігаються в зашифрованому вигляді і навіть, якщо зловмисник матиме доступ до бази даних, то бачитиме тільки криптограми.

Висновки. Отже, було розроблено клієнт-серверний застосунок захищеного зберігання облікових даних користувачів. Даний застосунок забезпечує конфіденційність інформації користувача шляхом шифрування. Вибір клієнт-серверної архітектури мотивується кращим розподіленням навантаження при обробці даних, особливо коли клієнтів багато, а сервер один.

Список літератури

1. S. Oesch, A. Gautam, S. Ruoti. “It Basically Started Using Me:” An Observational Study of Password Manager Usage// CHI '22: Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems:C. 1-23.

2. Войтко В., Денисюк П. Особливості розробки серверних додатків клієнт-серверної архітектури/ В. Войтко, П. Денисюк // Електронні інформаційні ресурси: створення, використання, доступ. – 2014. – С. 96-100.

Відомості про авторів

Гірич Олександр Сергійович, магістрант кафедри комп’ютеризованих систем захисту інформації, 5234357@stud.nau.edu.ua

Казмірчук Світлана Володимирівна, завідувач кафедри комп’ютеризованих систем захисту інформації, д.т.н., професор, svitlana.kazmirchuk@npp.nau.edu.ua

Секція 1

ПРОБЛЕМИ ІДЕНТИФІКАЦІЇ ТА АУТЕНТЕФІКАЦІЇ В КІБЕРБЕЗПЕЦІ

Городничий А. С.
Національний аерокосмічний університет ім. М. Є. Жуковського
«Харківський авіаційний інститут»
Науковий керівник Морозова О. І.

Актуальність. У сучасному світі майже кожна людина має власні сторінки в соціальних мережах, аккаунт в Google та багато інших різних облікових записів на веб-сайтах, у мобільних додатках, всередині корпорацій, тощо. Через нехтування стандартами та сучасними методами аутентифікації, кіберзлочинцям вдається викрасти паролі, а з ними і доступ до конфеденційної інформації, банківських рахунків, доступ до приміщень із секретною інформацією, а також викрасти Вашу цифрову ідентичность. Наприклад, у 2021 році на одному хакерському форумі було опубліковано файл RockYou2021 з більш як 8 мільярдами паролів, а оскільки користувачі часто використовують один і той самий пароль для декількох облікових записів, кількість постраждалих у майбутньому може сягати мільйонів, якщо не мільярдів [1].

Мета роботи – дослідження існуючих проблем аутентифікації, шляхи їх виправлення та сучасних методів аутентифікації.

Основні положення. Сьогодні розроблено багато методів ідентифікації/аутентифікації, які включають як загальні методи аутентифікації (паролі, двофакторна аутентифікація (2FA), токени, біометрія, аутентифікація транзакцій, розпізнавання власника комп'ютера, CAPTCHA та single sign-on (SSO)), так і спеціальні протоколи аутентифікації (включаючи Kerberos і SSL/TLS) [2]. Кожен з них має свої сильні та слабкі сторони.

Вразливості ідентифікації/аутентифікації які використовують зловмисники для викрадення – стандартні, слабкі або добре відомі паролі, наприклад «Password1» або «admin/admin», облікові дані користувача для аутентифікації, які не захищені під час зберігання, ідентифікатори сеансу, які розкриваються в URL-адресі (наприклад, перезапис URL-адреси), значення сеансу, яке не закінчується або стає недійсним після виходу, ідентифікатори сеансу, які не змінюються після успішного входу, дані, надіслані через незашифровані з’єднання, слабкі або неефективні процеси відновлення облікових даних і забутих паролів, відсутня або неефективна багатофакторна аутентифікація, сеанси користувача або маркери

аутентифікації (переважно маркери єдиного входу (SSO)) не анулюються належним чином під час виходу з системи або періоду бездіяльності.

На підставі аналізу існуючих вразливостей були сформульовано поради, яких потрібно дотримуватись аби уникнути витоку даних: застосовувати багатофакторну аутентифікацію, узгодити політику щодо довжини, складності та ротації пароля за інструкціями Національного інституту стандартів і технологій (NIST), та перевіряти нові або змінені паролі, переконатись, що реєстрація, відновлення облікових даних і шляхи програмного інтерфейсу захищені від атак нумерації облікових записів за допомогою однакових повідомлень для всіх результатів, обмежуйте або частіше відкладайте невдалі спроби входу, використовувати захищений вбудований менеджер сеансів на стороні сервера, який генерує новий випадковий ідентифікатор сеансу з високою ентропією після входу, ідентифікатор сеансу не має бути в URL-адресі, а повинен надійно зберігатися та вважатися недійсним після виходу з системи, простою та абсолютних тайм-аутів [3].

Висновки. Завдяки використанню сучасних методів ідентифікації/аутентифікації та дотримання сучасних стандартів, які допомогають закривати найбільш поширені вразливості, можна зменшити ризик отримання даних зловмисниками.

Список літератури

1. Edvardas Mikalauskas, Cybernews – RockYou2021: largest password compilation of all time leaked online with 8.4 billion entries. *Cyber news*. URL – https://cybernews.com/security/rockyou2021-alltime-largest-password-compilation-leaked/ (дата звернення: 27.07.2022);

2. Common Network Authentication Methods. *N-able*. URL – https://www.n-able.com/blog/network-authentication-methods (дата звернення: 27.07.2022);

3. OWASP Top 10 2021. *OWASP*. URL – https://owasp.org/Top10/A07_2021-Identification_and_Authentication_Failures/ (дата звернення: 27.07.2022).

Відомості про авторів

Городничий Анатолій Сергійович, студент кафедри комп'ютерних систем, мереж і кібербезпеки, м.т. 066-32-44-338, a.horodnychyi@student.csn.khai.edu

Морозова Ольга Ігорівна, професор кафедри комп'ютерних систем, мереж і кібербезпеки, м.т. 050-300-17-58, o.morozova@csn.khai.edu

Секція 1

ОРГАНІЗАЦІЯ ЗАХИСТУ ХМАРНОГО СЕРЕДОВИЩА

Даценко В. А.
Національний аерокосмічний університет ім. М. Є. Жуковського
«Харківський авіаційний інститут»
Науковий керівник Землянко Г. А.

Актуальність. Хмарні середовища – це зручний сервіс для зберігання та обробки будь-якої інформації користувачів, що тісно інтегровані в сучасні пристрої, це забезпечує доступ до даних і передових обчислювальних ресурсів де завгодно [1]. Проте захист інформації від несанкціонованого доступу, безпека використання хмарних технологій та передбачення ймовірних ризиків, що виникають у процесі їх використання, є пріоритетним напрямком у повсякденні.

Мета. Аналіз технологій захисту інформаційних ресурсів при використанні хмарних технологій.

Основні положення. Хмарна безпека, також відома як безпека хмарних обчислень, складається з набору політик, засобів керування, процедур і технологій, які працюють разом для захисту хмарних систем, даних та інфраструктури від загроз та кібератак.

Компанії хмарних послуг забезпечують комплексний багаторівневий захист, що включає: системи керування доступом, постійний моніторинг загроз, шифрування даних під час передачі та зберігання, захист фізичних центрів обробки даних; захист мережі, захист програм, резервне копіювання даних, постійні перевірки, захист від масового видалення файлів та моніторинг підозрілих дій під час входу [2].

Найбільш ефективні способи захисту у сфері безпеки хмар опублікувала організація Cloud Security Alliance (CSA) [3]. Проаналізувавши матеріли, було виявлено такі рішення:

1. Збереження даних. Шифрування – один із найефективніших способів захисту даних. Провайдер, що надає доступ до даних, повинен шифрувати інформацію клієнта, що зберігається в ЦОД, а також у разі відсутності необхідності безповоротно видаляти.
2. Захист даних під час передачі. Зашифровані дані під час передачі повинні бути доступні лише після аутентифікації. Дані не вдасться прочитати або зробити зміни, навіть у разі доступу через ненадійні вузли. Для цього використовуються провайдерами такі технології: протоколи AES, TLS, IPsec та інші.

3. Аутентифікація – захист паролем. Для забезпечення більш високої надійності використовують такі засоби, як токени та сертифікати. Для прозорої взаємодії провайдера з системою ідентифікації при авторизації також рекомендується використовувати протоколи LDAP та SAML.
4. Ізоляція користувачів. Використання індивідуальної віртуальної машини та віртуальну мережу. Віртуальні мережі повинні бути розгорнуті із застосуванням таких технологій, як VPN, VLAN та VPLS. Часто провайдери ізолюють дані користувачів один від одного за рахунок зміни даних коду в єдиному програмному середовищі [4].

Висновки. Найдієвішими технологіями захисту інформаційних ресурсів при використанні хмарних середовищ на сьогодні є: шифрування, захист даних при передаванні, аутентифікація та ізоляція користувачів. Засоби безпеки потребують постійного вдосконалення і передбачання ризиків, що виникають у процесі користування. Хмарні технології постійно розвиваються, витісняють інші та закорінюються в IT-індустрії, а отже питання безпеки у цьому середовищі завжди актуальне, тому на часі є розробка та впровадження нових методів захисту інформації у хмарі.

Список літератури

1. Безпека хмарних сховищ і технологій: Основні правила. *Datami*. URL: https://datami.ua/bezpeka-hmarnih-shovishh-i-tehnologij-osnovni-pravila/ (дата звернення: 17.11.2022).
2. Paul Diamond. Хмарне сховище чи локальні сервери: 9 критеріїв, які слід врахувати під час вибору. *Microsoft*. URL: https://www.microsoft.com/uk-ua/microsoft-365/business-insights-ideas/resources/cloud-storage-vs-on-premises-servers (дата звернення: 18.11.2022).
3. Guideline on Effectively Managing Security Service in the Cloud. *Cloud Security Alliance*. URL – https://cloudsecurityalliance.org/artifacts/guideline-on-effectively-managing-security-service-in-the-cloud/ (дата звернення: 20.11.2022).
4. Загрози хмарних обчислень та їх методи захисту. *Habr*. URL: https://habr.com/ru/post/183168/ (дата звернення: 26.11.2022).

Відомості про авторів

Даценко Владислав Анатолійович, бакалавр кафедри комп'ютерних систем, мереж і кібербезпеки, v.datsenko@student.csn.khai.edu
Землянко Георгій Андрійович, асистент кафедри комп'ютерних систем, мереж і кібербезпеки, g.zemlianko@csn.khai.edu

Секція 1

ЗАХИСТ ЦІЛІСНОСТІ ДАНИХ У БАЗАХ ДАНИХ

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

Актуальність. В умовах розвитку інформаційних технологій, збільшення кількості інформації, права на зберігання якої передані користувачем третій особі, значно підвищується попит на якісні інструменти захисту цілісності, конфіденційності та доступності даних. Також віртуалізація юридичних та економічних процесів у локальних і глобальних системах додає актуальності завданню побудови системи захисту інформації (ЗІ), яка здатна якісно блокувати широкий спектр атак. Наразі об’єми інформації для зберігання та обробки збільшуються щодня, і потужним інструментом управління даними є бази даних (БД).

Цілісність є однією із основних характеристик інформаційної безпеки, а отже дослідження методів захисту цілісності інформації у БД є актуальним і необхідним для подальшого розвитку інформаційних технологій.

Метою даної роботи є аналіз методів забезпечення захисту цілісності даних у БД.

Основні положення. База даних (БД) являє собою упорядкований набір даних, які логічно взаємопов'язані. Головним завданням БД є збереження значних обсягів інформації. Дані в БД повинні зберігатися з гарантуванням безпеки та конфіденційності. Інформація не повинна бути загубленою або викраденою [1].

Якщо в системі захисту є недоліки, то даним може бути завдано шкоди, наприклад такої, як: порушення цілісності даних, викрадення (витік) даних, розсекречення даних з обмеженим доступом.

Система управління БД (СУБД) – це сукупність програм і мовних засобів, призначених для створення, ведення і використання БД [2].

Нижче наведено аналіз основних методів захисту інформації, що забезпечать надійний захист інформації від несанкціонованого втручання:

- захист паролем. Пароль має бути складною комбінацією літер, цифр та символів, зберігатися в СУБД у зашифрованому вигляді. Проте він має вразливість людського фактору;
- шифрування даних – це надійний метод, що забезпечує

неможливість прочитати інформацію, не знаючи ключа для дешифрування;

- права доступу дають контроль над спектром можливостей редагування даних у БД кожного з авторизованих користувачів;
- резервне копіювання – інструмент запобігання втрати цілісності всієї БД, або її частини. Копії зазвичай зберігають останній коректний образ БД, але можуть використовуватись для пошуку причини деякого інциденту безпеки БД [3];
- захист полів та записів – особливості БД, а саме як вона реалізована програмно та які модифікатори доступу мають її складові;
- аудит – це допоміжна процедура, яка призначена для перевірки повноти залучення передбачених засобів керування й відповідності рівня захищеності БД встановленим вимогам [3];
- забезпечення цілісності зв'язків таблиць БД;
- організація спільного використання об'єктів БД в мережі.

Висновки. Якість впровадження розглянутих методів захисту цілісності даних у БД та самої БД у цілому буде пропорційною стійкості системи. Однак, неможливо створити ідеально захищену систему, зловмисники все одно і надалі шукатимуть і використовуватимуть програмні і фізичні вразливості СУБД. Однак, при використанні методів захисту інформації, можливо створити систему, якій можна буде довіряти дані БД.

Список літератури

1. Захист інформації в базах даних. *IRlib*. URL: https://ir.lib.vntu.edu.ua/bitstream/handle/123456789/24448/Касянчук%20Н.1.pdf?sequence=1&isAllowed=y (дата звернення 23.11.2022);
2. Системи управління базами даних. *Rodak*. URL: http://rodak.if.ua/komptech/lection4.htm (дата звернення 23.11.2022);
3. Захист БД від несанкціонованого доступу. *RDP*. URL: https://rdb.dp.ua/uk/chapter_11 (дата звернення 23.11.2022).

Відомості про авторів

Жарий Іван Ігорович, студент кафедри комп'ютерних систем, мереж і кібербезпеки, м.т. 0937232779, i.zharyi@student.csn.khai.edu
Морозова Ольга Ігорівна, професор кафедри комп'ютерних систем, мереж і кібербезпеки. д.т.н., професор, м.т. 0503001758, o.morozova@khai.edu

Секція 1

АНАЛІЗ ТА ФОРМУВАННЯ ОСНОВНИХ РИЗИКІВ ДЛЯ БЕЗПЕКИ ДАНИХ КОРИСТУВАЧІВ ДЕРЖАВНОГО ЗАСТОСУНКУ «ДІЯ»

Зміївський В.С
Національний аерокосмічний університет ім. М.Є. Жуковського «ХАІ»
Науковий керівник Шевченко І.В.

Актуальність. Безумовним є те, що сучасний світ ІТ невпинно розвивається, роблячи наше повсякденне життя максимально комфортним. Наша держава на сьогодні є однією з найбільш прогресивних та сучасних країн Європейського контингенту з точки зору діджалізації життя суспільства. Український уряд спрямовує значні ресурси на розвиток цільової галузі та процесу діджалізації, розуміючи, що саме за цим буде майбутнє. Одним з доказів цього є створення державного застосунку «ДІЯ» [1], який був впроваджений у користування українських громадян. Але, чи є цей застосунок безпечним з точки зору зберігання даних?

Мета роботи: полягає у аналізі та виділенні основних ризиків, які можуть призвести до порушення безпечності зберігання, а отже до «витікання» даних користувачів.

Основні положення. Дія (скорочення від «Держава і я») – мобільний застосунок і офіційний веб-сервіс для отримання державних онлайн-послуг, розроблений Міністерством цифрової трансформації України, який дозволяє працювати з цифровими документами та публічними послугами.

Встановивши Дію користувач отримує можливість отримати електронні документи в смартфоні, а також передавати їхні копії при отриманні державних послуг. Також користувач може скористатися послугами отримання різних за типом і призначенням довідок. Станом на травень 2022 року застосунком і веб-сервісом користується вже понад 17 млн людей, у веб-сервісі доступно вже 72 послуги, а у застосунку – 9 послуг та 15 цифрових документів, в планах уряду до 2024 року перевести 100 % державних послуг у Дію [2].

Аналізуючи проблему безпечності даних в Дії було виділено ряд ризиків, які можуть нести інформаційну небезпеку для зберігання даних користувачів:

Ризик 1. Порушення розмежування інструментів ідентифікації за рівнями довіри. Потрібно розуміти, що можливість ідентифікації особи через програмний інструмент BankID, яку надає Дія, є сумнівною для такого рівня важливості документів, які зберігаються у Дії.

Ризик 2. Дія збирає, опрацьовує та зберігає дані користувача. Як і будь-який програмний застосунок, Дія збирає, опрацьовує та зберігає дані, про що прямо написано на офіційному сайті «Дії» та у розділі

«Меню/Повідомлення про обробку персональних даних» мобільного додатка.

Ризик 3.Вхідна аутентифікація за допомогою пароля-кода. Звичайно, що код – це найпростіший у запам'ятовуванні та введені вид аутентифікації, але також і найпростіший у підборі та взламуванні. До речі пароль-код у Дії складається всього з 4 цифр.

Ризик 4. Дані зберігаються на смартфоні чи гаджеті, на якому встановлено застосунок. Згідно з заявами розробників програми «Дія», програма не зберігає електронні документи громадян, при цьому зображення з даними документа зберігаються у смартфоні. При втраті смартфона даними з застосунку можна неправомірно користуватися.

Ризик 5. Незрозумілість порядку використання та «підтягування» даних сторонніми організаціями. Немає чіткого роз'ясненого порядку використання електронної версії паперів у державних організаціях. Є ризики, що електронна версія може бути використана без дозволу власника [3].

Висновки. В результаті проведеного аналізу було виділені основні ризики, які можуть нести інформаційну небезпеку для зберігання даних користувачів Дії. На основі відгуків користувачів був проаналізований їх практичний досвід використання Дії, а також він був порівняний з власним досвідом автора. Отримані результати будуть використані для вирішення проблеми підвищення рівня довіри до державної цифрової програми на прикладі Дії.

Список літератури

1. Дія. *Wikipedia*. URL: https://ru.wikipedia.org/wiki/Дія (дата звернення: 27.10.2022);

2. Оформлення субсидій у Дії та перепис населення з Apple - Михайло Федоров про цифрові плани України. *Surl*. URL: http://surl.li/dsdmj (дата звернення: 27.10.2022);

3. Як працює «Дія» та звідки беруться данні. *Surl*. URL: http://surl.li/dsdlm (дата звернення: 29.10.2022).

Відомості про авторів

Зміївський Володимир Сергійович, студент кафедри інженерії програмного забезпечення, м.т. 0971718829, vovazmievskoy2003@gmail.com

Шевченко Ілона Володимирівна, доцент кафедри інженерії програмного забезпечення, к.т.н., доцент, i.shevchenko@khai.edu

Секція 1

ДОСЛІДЖЕННЯ МЕТОДІВ БЕЗПЕКИ ВЕБ-ЗАСТОСУНКІВ

Зуєв Д. М.
Харківський національний університет імені В.Н. Каразіна
Науковий керівник Родінко М.Ю.

Актуальність. Web-додатки щодня піддаються різним атакам. При наявності великої кількості інструментів для атак, статей з докладним описом і відео демонстрацій проведення атак, багато людей намагаються спробувати свої сили.

Існують люди, які перетворюють злом web-сайтів в так званий бізнес. Через їх дії багато власників web-додатків терплять фінансові збитки, а їх користувачі втрачають конфіденційність власних даних.

Мета. Теоретичний аналіз та дослідження механізмів атак на веб-додатки; теоретичний аналіз технологій захисту від можливих атак на додатки; теоретичний аналіз технологій ідентифікації й автентифікації користувачів, веб-додатків;

Злом веб-додатків є найбільш, або хоча б одним з найчастіше використовуваних методів кібератак як на організації, так і на приватних осіб. Зламані сайти використовуються в різних цілях - для поширення шкідливого ПЗ, крадіжки інформації, розміщення несанкціонованої реклами або забороненої інформації, шахрайства, проникнення у внутрішню мережу компанії. Через цю проблему забезпечення інформаційної безпеки веб-застосунків є актуальним завданням. І лише маючи представлення про найбільш поширені атаки на веб-застосунки, слабкі місця цих самих додатків та варіанти реалізації захисту, одним з яких являється вдала реалізація доступу до сайту шляхом автентифікації, можливо створити безпечніший для користувачів сервіс [1].

Перелік найбільш поширених атак на веб-застосунки: SQL ін'єкція; обхід шляху (Path Traversal); XSS атаки; включення локального файлу; витік інформації (Information Leakage); атака грубою силою (Brute Force); віддалене виконання коду; відмова в обслуговуванні (Denial of Service); template ін'єкція з боку сервера.

Висновки. На основі аналізу загроз інформаційній безпеці, що стосуються веб-додатків, було проведено аналіз методів їх захисту від вразливостей інформації і принципів побудови сайтів з урахуванням можливостей різних атак. Також було досліджено декілька з існуючих засобів ідентифікації та аутентифікації користувачів інформаційних систем.

Парольний захист на сьогодні є одним з найпоширеніших способів захисту інформації від несанкціонованого доступу як в окремих

комп'ютерах і системах, так і в мережах світового масштабу [2]. Проте без використовування інших механізмів захисту парольний захист, сам по собі, не є надійним, оскільки не може забезпечити потрібного захисту. Досить розповсюдженими в якості ідентифікаторів є також різноманітні електронні ключі, наприклад, токени.

Список літератури

1. Fu K. et al. The dos and don'ts of client authentication on the web //10th USENIX Security Symposium (USENIX Security 01). – 2001;
2. Smith R. E. Authentication: from passwords to public keys. – Addison-Wesley Longman Publishing Co., Inc., 2001.

Відомості про авторів

Зуєв Денис Михайлович, магістрант кафедри моделювання систем і технологій, факультет комп'ютерних наук, м.т. 0668395288, xa11867678@student.karazin.ua
Родінко Марія Юріївна, старший викладач каф. моделювання систем і технологій, д-р. філософії з комп'ютерних наук, mariia.rodinko@karazin.ua

Секція 1

АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ РЕСУРСІВ ЯКІ ЗНАХОДЯТЬСЯ У ХМАРНОМУ СЕРЕДОВИЩІ

Кобиляшний Д. В.
Ліцей № 33 Полтавської міської ради
Науковий керівник Юдіна Н. В.

Актуальність. З кожним роком збільшується відсоток користувачів мережею Інтернет, згідно з результатами опитування USAID-Interwiews, популярність IT-технологій, рівно як і використання веб-ресурсів зросла більш ніж на 25% за останні 5 років [1]. Так відбулося завдяки стрімкому переходу бізнес інфраструктури в онлайн середовище, у зв'язку з адаптацією до нових умов через COVID-19. Однак, через стрімкий ріст використання веб-додатків, розробнику майже не можливо передбачити робоче навантаження на сервер у дата-центрі, що призводить до надлишкового використання ресурсів або створення небажаного досвіду для користувача через повільне завантаження додатку. Також, при розміщені інфраструктури у дата-центрі адміністратору веб-додатка майже не можливо впровадити вертикальне масштабування для оптимізації навантаження на сервер у пікові часи. Вертикальне масштабування починає розгортати додаткові сервера під час пікового навантаження, щоб основний сервер не був перенавантажений. Після того як навантаження на сервер зменшилося, за допомогою спеціалізованих сервісів хмарного провайдера кількість серверів зменшується до оптимальної. Модель типового дата-центру передбачає передоплату за виділені ресурси, що унеможливлює отримання бажаного ресурсу в будь-який час та на короткий термін. Саме тому, все більше компаній переходять на використання хмарних технології та обчислень. Аналізуючи статистику Українського IT-ринку, у 2021 році використання хмарних сервісів та технологій мало зріст більше ніж на 50% [2].

Однак, слід зазначити, що хоча більшість компаній обирають для себе обчислення за допомогою хмарних провайдерів, більшість з них не приділяють належної уваги до кібербезпеки. З проаналізованих компаній, 73% починають приділяти значну увагу до безпеки хмарних провайдерів. Тому що, з усіх компаній, які мають свої дані в хмарній інфраструктурі – 34% потерпають від втрата та витіків різних даних, в тому числі персональних [3]. Витік конфіденційної інформації може відбуватися за різних причин та умов: не коректна політика безпеки, витік за допомогою інсайдера, використання вразливих компонентів у системі, тощо.

Метою роботи є аналіз засобів та методів покращення безпеки ресурсів, які знаходяться під керуванням хмарного провайдера.

Основні положення. Існує чи мало загроз та ще більше вразливостей, які стосуються ресурсів, які створюються розробником або адміністратором у хмарному середовищі. Не зважаючи на це, достатньо велика кількість загроз є зоною відповідальності хмарного провайдера. Так відбувається тому, що більшість хмарних провайдерів надають модель спільної відповідальності за безпеку інфраструктури [4]. Однак, більшість клієнтів хмарних провайдерів приділяють недостатньо уваги кібербезпеці та вважають, що засоби, які вже були впроваджені хмарним провайдером є прийнятними для їх потреб [3]. Наприклад, користувач може некоректно налаштувати сховище даних, в наслідок чого зловмисник зможе за допомогою автоматизованих засобів просканувати вміст сховища та за потребою отримати привілейований доступ. Одним з лідерів автоматизованого збору інформації про хмарну інфраструктуру є Paku, який виконує розвідку на основі відкритих джерел.

Висновки. З точки зору користувача, не завжди можна розібратися, що саме потрібно для протидії кібератакам. В наслідок чого інтерес зловмисників до хмари з кожним роком тільки збільшується. Важливо пам'ятати про політку найменших привілеїв при проектуванні системи, а також вчасно проводити зовнішній та внутрішній аудит безпеки інфраструктури, наприклад за допомогою програмного засобу Paku.

Список літератури

1. Опитування USAID-internews щодо споживання медіа. *Укрінформ*. URL: https://www.ukrinform.ua/rubric-presshall/3349746-opituvanna-usaidinternews-sodo-spozivanna-media.html (дата звернення: 06.09.2022).
2. Український ринок хмарних сервісів зріс на 50% за рік. *InternetUA*. URL: https://internetua.com/ukrainskii-rynok-oblacsnyh-servisov-vyros-za-god-na-50- (дата звернення: 06.09.2022).
3. Cybersecurity Insiders, 2021 Cloud Security Report. – Fortinet. – 2021.
4. Shared responsibility and shared fate on Google Cloud. *Google Cloud*. URL – https://cloud.google.com/architecture/framework/security/shared-responsibility-shared-fate (дата звернення: 12.09.2022).

Відомості про авторів

Кобиляшний Дмитро Володимирович, учень 10-В класу ліцею № 33 Полтавської міської ради

Юдіна Наталія Вікторівна, вчитель-методист ліцею № 33 Полтавської міської ради, yudina.karantin@gmail.com

Секція 1

ПЕРЕПОВНЕННЯ БУФЕРА

Корінчук В.І.
Національний аерокосмічний університет ім. М.Є Жуковського
«Харківський авіаційний інститут»
Науковий керівник Пєвнєв В.Я

Актуальність. Переповнення буфера був і залишається дуже важливою проблемою в аспекті безпеки програмного забезпечення. Саме з можливістю використання нападів на переповнення буфера для видалення шкідливого коду, який пов'язаний з постійними дискусіями, та галасуванням навколо нападів цього класу. Проблема переповнення буфера протягом багатьох років лише стала складнішою, з'явилися інші типи атак, і, як наслідок, були розроблені принципово нові напади на переповнення буфера.

Мета. Запобігти переповнення буфери, ознайомитися з причинами переповнення та їх уникнення

Основні положення. Переповнення буфера – це, мабуть, одна з найцікавіших і найпоширеніших вразливостей програмного забезпечення. Це може призвести до пошкодження даних, збоїв у програмі та навіть до шкідливого коду. Здається, це невелика помилка програміста (за особливих обставин), щоб дозволити розлюченому хакеру зробити майже все на комп'ютері невинного користувача програми [2].

Помилка полягає в тому, що в будь-якому місці програми дані копіюють з одного розділу пам'яті в інший, не перевіряючи, чи є для них достатньо місця, де вони копіюються. Область пам'яті, де дані копіюються, зазвичай називають буфером. Таким чином, якщо є занадто багато даних, то частина їх виходить за межі буфера – існує «переповнення буфера» [1]. Відомі такі типи атак, які здійснюються за рахунок переповнення буфера: напади на стек, напади на формат лінії та напади на хіп.

Цікавим фактом є те, що переповнення буфера є однією з найпоширеніших причин, чому атака можливі за допомогою довільного коду через вразливості [3]. Крім того, багато програм, розроблених класичними мовами, такими як C та C ++, вважаються дуже чутливими до цього типу проблем.

Серед найефективніших заходів протидії цим типам нападів необхідно розрізнити наступні: своєчасна перевірка даних, введення «точок попередження» та використання сучасних мережевих екранів.

Висновок. Наприкінці розгляду основних методів боротьби з атаками переповнення буфера слід зазначити, що, звичайно, компетентне програмування залишається найбільш ефективним і в той же час найважче

реалізованим способом. Саме якісно складений код зможе найбільш ефективно витримати всілякі спроби зовнішніх злому.

Список літератури

1. Захист від переповнення буфера. *Wiki*. URL: https://uk.zahn-info-portal.de/wiki/Buffer_overflow_protection (дата звернення: 20.11.2022);
2. Способи реалізації атак переповнення буфера. *Blocklist.net*. URL: http://um.co.ua/10/10-6/10-6472.html (дата звернення: 20.11.2022);
3. Фэрроу, Р. Атаки на сеть через переполнение буфера: технологии и способы борьбы // Защита информации. INSIDE. – 2006. – № 4.

Відомості про авторів

Корінчук Валентина Ігорівна, студент кафедри комп'ютерних систем, мереж і кібербезпеки, м.т. 095-691-07-75, Valyakorinchuk@gmail.com
Пєвнєв Володимир Яковлевич, професор кафедри комп'ютерних систем, мереж і кібербезпеки, д.т.н., доцент, v.pevnev@csn.khai.edu

Секція 1

РЕАЛІЗАЦІЯ СТЕГАНОГРАФІЧНИХ МЕТОДІВ НА ОСНОВІ МІКРОСЕРВІСНОЇ АРХІТЕКТУРИ

Кравченко Є.М
Харківський Національний економічний університет імені Семена Кузнеця
Науковий керівник Алексієв Володимир Олегович

Актуальність. Говорячи про актуальність стеганографії у сучасному світі на думку приходять два напрямки. Перший – спеціального призначення, з огляду на події у світі, можна стверджувати, що, іноді, недостатньо приховати інформацію, що передається, а й приховати той факт, що така інформація існує. Такий підхід зменшує ризики виявлення дружніх агентів у ворожому тилу. Другий – економічний, найімовірніший сценарій використання – це впровадження водяних знаків у мультимедійні файли. Це корисно, коли критичним є визначення справжнього власника інтелектуальної власності.

При реалізації стеганографічних сервісів іноді застосовують підхід мікросервісів. Такий підхід є логічним. Мікросервіс легкий, відносно надійний, його легко розгорнути і протестувати. Але в доступних реалізаціях найчастіше зустрічається недолік універсальності. З таким підходом даний сервіс не має можливості подальшого покращення, або ж покращення відбудеться шляхом повного переписування застосунку[1][2][3].

Мета. Метою даної роботи служить аргументація доцільності застосування мікросервісної архітектури у поєднанні з стеганографічними методами.

Основні положення. Мікросервіс – як зрозуміло з назви, це не великий за розміром, інтернет застосунок. Це і є його перевагою. Такі сервіси відносно легко розробити, бо вони, як правило, мають обмежену функціональність, більше того їх легко розгортати у проектному середовищі. Така архітектура дозволяє розділити обов'язки розробників. Кожен реалізує певну функціональність у своєму сервісі і далі всі вони об'єднуються в один великий застосунок. Важливим уточненням є те, що сервіси між собою спілкуються за допомогою мережі [3][4].

Стосовно стеганографічних функцій у сервісі, вони можуть бути будь-які: приховування повідомлень, приховування водяних знаків, вбудовування менших файлів у більші. Також не має значення формат медіа файлу, бо як правило різні методи працюють з різними форматами

файлів, тому сервіс може працювати з масивом бітів, і в залежності від методу, розуміти цей масив, чи як зображення, чи як аудіо файл, чи відео. Така універсальність добре впливає на гнучкість застосунку. Стеганографічні методи мають певну кількість недоліків. Найкритичніший з них – це швидкодія, в найпростіших методах, як мінімум необхідно обробити кожен піксель зображення, а в оптимізованих на ємність варіантах, ще й декілька разів. Сучасні технології дозволяють розробляти реактивні інтернет застосунки. Це означає, що їх швидкодія у багатопоточному середовищі на дуже високому рівні. Завдяки таким технологіям і оптимізації алгоритмів для багатопоточності, можливо досягти мінімальних часових затримок. Але, що якщо кількість контенту, що проходить через сервіс збільшиться? Для цього існують середовища розгортання і супроводу, наприклад, Kubernetes. Завдяки таким технологіям і правильному підходу до розробки застосунку, кількість робочих сервісів можна збільшити автоматично під час роботи системи, при необхідності, що дасть приріст у швидкодії інфраструктури [5].

Висновки. Отже, поєднання мікросервісної архітектури та стеганографії представляє собою перспективний напрям розробки, для впровадження нових методів приховування факту передачі інформації, впровадження водяних знаків, чи оптимізації місця зберігання даних.

Список літератури

1. Data hiding and its applications: digital watermarking and steganography. MDPI, 2022. URL: https://doi.org/10.3390/books978-3-0365-2937-0 (дата звернення: 12.11.2022);
2. Newman S. Building microservices: designing fine-grained systems. O'Reilly Media, Incorporated, 2020. 250 с.;
3. Steganography and watermarking. Nova Science Pub Inc, 2013. 412 с.;
4. Wolff E. Practical microservices. Apress, 2017. 310 с.;
5. Малець І. О., Андрушко О. А., Панасюк М. А. Docker-технології в побудові мікросервісів: Thesis. 2017. URL: http://hdl.handle.net/123456789/4286 (дата звернення: 12.11.2022).

Відомості про авторів

Кравченко Євгеній Миколайович, магістрант кафедри кібербезпеки та інформаційних технологій, м.т. +380956334094, yevhenii.kravchenko@hneu.net.
Алексієв Володимир Олегович, професор кафедри кібербезпеки та інформаційних технологій, vlax@hneu.edu.ua

Секція 1

МЕТОДИ ЗАХИСТУ ДАНИХ МЕДИЧНИХ КАРТОК ПАЦІЄНТІВ У BIG DATA. МЕДИЧНІ ТА ПЕРСОНАЛЬНІ ДАНІ

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

Актуальність. З кожним днем цифровізація все більше впроваджується в медичній сфері, де одна електронна база даних одразу інтегрує державну базу даних охорони здоров'я із приватними компаніями, через які люди, лікарі, аптеки та клініки мають онлайн-доступ до бази і можуть керувати записами, рецептами тощо. Проте слід пам'ятати, що збереження даних в електронному форматі завжди несе великі ризики оприлюднення даних завдяки кібератакам, навмисного розкриття лікарями/медичними сестрами чи випадкової помилки самого медичного сервісу.

Метою даної роботи є дослідження методів захисту даних медичних карток пацієнтів задля виявлення найбільш якісних та ефективних для медичних баз даних.

Основні положення. Дані, внесені до медичних карток, умовно можна поділити на: персональні дані та медичні дані. До першої категорії даних відносяться такі відомості: прізвище, ім'я, по-батькові, реєстраційний номер облікової картки платника податків, етнічне походження особи, тощо. Тому виявлені методів захисту даних медичних карток пацієнтів акцент робиться саме на захисті персональних даних.

Захист баз даних повинен бути багаторівневим.[1]. Починатися багаторівнева система безпеки повинна з контролю на рівні користувача. Захист бази даних на первинному етапі полягає в умінні розподіляти процеси, привілеї та права доступу. Загроза інформації може бути не тільки зовнішньою, але й внутрішньою [1].

Першим рівнем захисту є фізичний захист. Він включає в себе обмежене надання доступу до серверів з персональними даними, встановлення програм, які забороняють робити копії даних.[2]

Другим рівнем захисту є шифрування. Алгоритм шифрування перетворює інформацію в незрозумілі символи за допомогою математичного процесу, що навіть у разі злому системи інформація буде доступна для читання тільки авторизованим користувачам, які мають ключі шифрування [3].

Дієвим методом захисту може бути ізолювання особливо конфіденційної інформації. Особливо це може стосуватися безпосередньо персональних

даних, не включаючи медичної інформації, такий метод буде проти атак нульового дня. Навіть наявність і використання уразливості не дасть хакеру уявлення про всю структуру бази даних завдяки ізольованості, особливо цінної інформації.[1]

Третім рівнем захисту є захист IT-ресурсів. До нього належить метод управління змінами, передбачає управління внесенням змін до самої системи бази даних: злиття, редагування, тощо. Необхідно задокументувати, які зміни відбулися і чи не пошкодять вони безпечний доступ до бази даних та її додатків.

Висновки. Ведення медичних карток пацієнтів в електронному варіанті гарантують більшу надійність збереження інформації та її цілісність, але в той же час несе великі ризики опилення персональних даних у відкритому доступі. Результати дослідження показали, що захист медичних карток, в яких зберігаються персональні дані пацієнтів, має бути на трьох рівнях. Це дає контролювати: доступ до роботи із медичними картками; контроль ПЗ на комп'ютері; дозволяє підвищити захист так відокремити персональні дані від медичної інформації, контролювати потік даних та дій у базі даних.

Список літератури

1. Шифрування та захист баз даних. *iIT Distribution*. URL: https://iitd.com.ua/shifruvannja-ta-zahist-baz-danih/ (дата звернення: 15.11.2022);

2. Conceptual Model of Information Security. *Springer*. URL – https://link.springer .com/chapter/10.1007/978-3-030-66717-7_14 (дата звернення: 17.11.2022);

3. “Smart City” Technology: Conception, Security Issues and Cases. *Springer*. URL – https://link.springer.com/chapter/10.1007/978-3-030-94259-5_19 (дата звернення: 20.11.2022);

Відомості про авторів

Луханін Богдан Юрійович. Студент кафедри комп’ютерних систем, мереж і кібербезпеки, м.т. 096-875-81-12. b.lukhanin@student.csn.khai.edu

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

Секція 1

АНАЛІЗ ЗАГРОЗ СПРЯМОВАНИХ НА МОБІЛЬНІ ПРИСТРОЇ

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

Актуальність. На даний момент у світі прогресує кількість смартфонів у світі, люди все більше взаємодіють саме з смартфонами та планшетами на ОС IOS та android. Кількість можливостей, що надаються мобільними пристроями, набагато більша, ніж у традиційних мобільних телефонів: вони мають встановлену мобільну операційну систему (iOS, Android) і можуть працювати як з мережами мобільного зв'язку, так і з бездротовими технологіями Wi-Fi та Bluetooth, завдяки чому користувачі можуть завантажувати та запускати сторонні програми використовуючи мережу Інтернет. Серед інших особливостей мобільних пристроїв відзначається підтримка сервісу мультимедіа повідомлень (MMS) та наявність вбудованих датчиків: гіроскоп, приймач сигналів GPS, акселерометр, а також мікрофон, камера з великою роздільною здатністю та динамік. Через це все більше критично важливих застосунків з’являються на цих пристроях, такі як, мобільний банкінг, або «Дія» у якій знаходяться персональні дані користувача пристрою. Як наслідок, зацікавлені в розробці шкідливого ПО та подальшого зараження ним мобільного пристрою. А розробники антивірусів навпаки зацікавлені в запобіганні подібних інцидентів. Саме для цього треба спочатку проаналізувати можливі загрози спрямовані на мобільні пристрої.

Мета. Переглянути статистику за перші квартали 2021 року та 2022 року та проаналізувати зростання чи спадання популярності тих чи інших загроз та можливість залежності популярності тих чи інших зловмисних ПО від навколишніх обставин.

Основні положення. Шкідливе програмне забезпечення – це будь-який код, що може поставити під загрозу користувача, його дані чи пристрій. До шкідливого ПО належать, зокрема, потенційно шкідливі додатки, двійкові коди та модифікації фреймворків, серед яких можна виділити категорії троянських програм, фішингових і шпигунських додатків.[1] Ці типи зловмисного програмного забезпечення покладаються на використання конкретних мобільних операційних систем і технологій мобільних телефонів. Розробники шкідливого ПО для мобільних пристроїв, яких також називають кіберзлочинцями, можуть мати одну або кілька цілей,

зокрема викрадення даних, підписання користувачів на послуги та стягнення з них плати за послуги, на які вони не погоджувалися, або блокування пристрою чи даних і вимагання грошей за їх не оприлюднення. Додаток, двійковий код чи модифікація фреймворку можуть бути потенційно шкідливі, навіть якщо їх не розроблено як зловмисні програми. Причина полягає в тому, що функції додатків, двійкових кодів і модифікацій фреймворків відрізняються залежно від багатьох змінних параметрів. Тому поведінка, шкідлива для одного пристрою Android, може не становити загрози для іншого. Згідно зі звітом про глобальні ризики Всесвітнього економічного форуму за 2022 рік, 95% проблем кібербезпеки пов'язані з людською помилкою [2]. Це є тривожним сигналом для всіх організацій, особливо з переходом на віддалену та гібридну роботу, коли співробітники частіше використовують мобільні пристрої. Тепер ці пристрої мають доступ до конфіденційних даних компанії та пряме підключення до корпоративної мережі.

Висновки. Отже після аналізу статистики зараження мобільних пристроїв можна зробити висновок. Найпопулярніші типи зловмисних програм це RiskTool, AdWare, Trojan, та Trojan-Banker. Всі вони направлені на масового користувача, на якому можливо заробити, або показуючи йому рекламу, або скриваючи/погрожуючи видалити файли, але випадок с файлами все ж ситуативний не у всіх користувачів є щось дійсно важливе на телефоні що не можна відновити. Але наприклад майже у всіх користувачів є мобільний банкінг, що як раз є цілю Trojan-Banker. Тому на мою думку, в сегменті масового користувача, антивіруси повинні дуже сильно розвиватись у направленні цих чотирьох направленнях шкідливих програм.

Список літератури

1. Malware - Play Console Help. *Google Help.* URL: https://support.google.com/googleplay/android/developer/answer/9888380 (дата звернення: 23.11.2022);
2. Зловмисне ПЗ для мобільних пристроїв у 2022 році. *KO IT для бізнесу.* URL: https://ko.com.ua/zlovmisne_pz_dlya_mobilnih_pristroyiv_u_2022_roci_142676 (дата звернення: 23.11.2022).

Відомості про авторів

Литвинов Олександр Андрійович, студент кафедри комп'ютерних систем, мереж і кібербезпеки, м.т. 095-304-66-95, a.lytvynov@student.csn.khai.edu
Пєвнєв Володимир Яковлевич, професор кафедри комп'ютерних систем, мереж і кібербезпеки, д.т.н., доцент, v.pevnev@csn.khai.edu

Секція 1

АНАЛІЗ АЛГОРИТМІВ ЦИФРОВОГО ПІДПИСУ

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

Актуальність. Сьогодні криптографія має велике значення для більшості сучасних технологій, наприклад, електронної комерції або цифрового документообігу. Дані, які передаються з однієї системи в іншу через загальнодоступну мережу, повинні бути захищеними за допомогою методів шифрування, а саме алгоритмів цифрового підпису. Довести те, що певний документ не був змінений або підроблений, має значну роль, бо весь світ пов'язаний з документообігом. Отже, можна зробити висновок, що важливо використовувати алгоритм, який дає гарантію цілісності даних та аутентифікації власника [1-2].

Мета роботи полягає в аналізі основних чотирьох алгоритмів цифрового підпису та визначити, який саме з алгоритмів має наразі переваги в порівнянні з іншими.

Основні положення. Розглянемо основні чотири алгоритми цифрового підпису [3-5]. Ця вибірка алгоритмів має змогу описати картину сучасного документообігу на дуже високому рівні. Серед них представлено алгоритми, які набирають суттєвих оборотів серед розробників та використовуються в сервісах. В цих алгоритмах необхідно звернути основну увагу на генерацію ключів, генерацію та перевірку підпису, а також розглянути математичне обґрунтування кожного алгоритму, щоб дізнатися про їх крипостійкість, що є одним з потрібних параметрів для повного порівняння.

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.

ElGamal – криптосистема, яку засновано на складності обчислення дискретних логарифмів у скінченному полі. Криптосистема включає у себе алгоритм шифрування та алгоритм цифрового підпису. Схема підпису ElGamal дозволяє верифікатору підтвердити автентичність повідомлення, надісланого підписувачем через незахищений канал. Цей алгоритм описав Тахер Ель-Гамал у 1984 році.

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.

В тому ж році було запропоновано алгоритм 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).

Висновки. Робота присвячена порівняльному аналізу алгоритмів цифрового підпису. Було проведено аналіз кожного з чотирьох алгоритмів, які використовують метод відкритого ключа, та було досліджено недоліки та переваги кожного з запропонованих алгоритмів Виявлено, що алгоритм RSA має переваги у порівнянні з іншими алгоритмами, а саме надає гарантії цілісності даних та аутентифікацію власника, має невеликий розмір пари ключів, досить непогану швидкодійність та велику криптостійкість.

Список літератури

1. Information Security Stack Exchange. *Stackexchange*. URL – https://security.stackexchange.com (дата звернення: 23.10.2022);

2. Digital signatures. *Cryptobook*. URL – https://cryptobook.nakov.com/digital-signatures/ (дата звернення: 27.10.2022);

3. What Are the Differences Between RSA, DSA, and ECC Encryption Algorithms? *Sectio*. URL – https://sectigo.com/resource-library/rsa-vs-dsa-vs-ecc-encryption (дата звернення: 25.10.2022);

4. Comparing SSH Keys – RSA, DSA, ECDSA, or EdDSA? *Goteleport*. URL – https://goteleport.com/blog/comparing-ssh-keys/ (дата звернення: 29.10.2022);

5. Xianmeng Meng, Xuexin Zheng, Cryptanalysis of RSA with a small parameter revisited. Information Processing Letters, Elsevier, p. 858–862.

Відомості про авторів

Лісних Олександр Ігорович, студент кафедри комп'ютерних систем, мереж і кібербезпеки, м.т. 0638118220, o.lisnykh@student.csn.khai.edu

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

Секція 1

АНАЛІЗ МЕТОДІВ ЗМЕНШЕННЯ ЦИФРОВИХ СЛІДІВ ДЛЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ КОРИСТУВАЧІВ

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

Актуальність. Згідно зі щорічним звітом про витік даних за 2021 рік, опублікованим ITRC, загальна кількість скомпрометованих даних зросла більш ніж на 68% порівняно з 2020 роком [1]. Одним із аспектів захисту від крадіжки цифрових даних є розуміння концепції цифрових слідів. Цей автоматичний слід реєструє звички, інтереси, події, спілкування в мережі Інтернет, і саме через цю інформацію можна провести паралель між віртуальним аватаром та реальною особою. Особисті дані про користувачів, які доступні в мережі Інтернет також містяться в таких джерелах, як: судові та майнові записи, реєстрації гарантій, сайти соціальних мереж і дані перепису населення. Отже, погано керований цифровий слід може розкрити конфіденційну інформацію особи.

Мета роботи полягає у аналізі методів зменшення цифрових слідів для захисту даних користувачів.

Основні положення. Серед багатьох визначень цифрового сліду найбільш влучним є, що це інформація про конкретну особу, яка існує в мережі Інтернет в результаті її онлайн активності, а саме: листування через сервіси електронної пошти, покупка в Інтернеті, поширення контенту (фото, відео, дописи, коментарі), відвідування веб-сайтів [2].

Дані про користувачів залишені в мережі Інтернет зберігаються у величезній кількості місць, тому зовсім видалити свій цифровий слід не вдасться. Але необхідно обережно поширювати інформацію про особу в мережі, бо[2]: поширення опублікованої інформації в мережі Інтернет неможливо повністю контролювати; цифрові сліди складно зробити знеособленими, за ними можливо виявити соціальні зв’язки, звички людей, знайти особисті дані.

Існують два основні типи цифрових слідів: пасивні та активні. Активний цифровий слід з'являється, коли користувач передає свої персональні дані самостійно, наприклад, майже для кожного створюваного онлайн-облікового запису потрібні особисті ідентифікатори, такі як ім'я, дата народження, адреса, тощо. Також таким слідом є електронні листи, пости, лайки, коментарі, які залишають користувачі.

Пасивний цифровий слід з'являється у мережі без відома користувача. Програми на смартфоні, сайти, розумний годинник та інші пристрої постійно збирають та передають на сервери компаній дані про користувачів, а саме: IP-адреси, історію пошуку, файли cookie та ін. Ця

інформація зберігається на серверах відповідних компаній та може бути використана комерційними організаціями, правоохоронними органами або злочинцями.

Активний цифровий слід користувач може мінімізувати самостійно. Для цього потрібно: регулярно перевіряти яка інформація доступна у відкритому доступі; налаштувати конфіденційність в соціальних мережах, що дозволить контролювати список користувачів, що «стежать» за профілем; обмежувати дані, що викладаються в мережу Інтернет; видалити старі акаунти; видаляти метадані та приховувати геолокацію; не під'єднуватись до загальнодоступної мережі Wi-Fi; не реєструватися на веб-сайтах за допомогою соціальних мереж; підтримувати програмне забезпечення у актуальному стані; скасувати підписку на сервіси розсилки; очищати файли cookie.

Пасивний цифровий слід скоротити досить складно, але "розмити" його можна різними методами. До базових відносять наступні: використання пошукових систем, які не зберігають інформацію про пошук, наприклад, DuckDuckGo, використання платних сервісів для видалення цифрового сліду, але вони можуть бути не досить ефективними; використовувати режиму «інкогніто» у браузері; користуватись розширеннями браузера для запобігання несанкціонованого стеження.

Висновки. Усе, що потрапляє в Інтернет зберігається, аналізується та використовується, тому методу повного видалення цифрових слідів не існує. Різні сервіси та платформи можуть бути корисні для пошуку та видалення інформації про людину, але вони не дають стовідсотковий результат. Проте, загалом, користувач може сам контролювати інформацію, яка доступна про нього в мережі та впроваджувати організаційні методи для зменшення свого цифрового сліду.

Список літератури

1. Identity Theft Resource Center's 2021 Annual Data Breach Report Sets New Record for Number of Compromises. *ITRC*. URL: https://www.idtheftcenter.org/post/identity-theft-resource-center-2021-annual-data-breach-report-sets-new-record-for-number-of-compromises/ (дата звернення 28.10.2022);
2. Цуранов М.В. Методи та засоби боротьби з правопорушеннями в інформаційній сфері: навчальний посібник / М.В. Цуранов, В.М. Струков, В.Я. Пєвнєв. – Харків: ХНУВС, 2015. – 256 с.

Відомості про авторів

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

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

Секція 1

ДОСЛІДЖЕННЯ АВТОМАТИЗОВАНИХ ЗАСОБІВ ДЛЯ УПРАВЛІННЯ ВРАЗЛИВОСТЯМИ

Медведєва Ю. В.
Національний аерокосмічний університет ім. М. Е. Жуковського «ХАІ»
Науковий керівник: Брежнєв Є. В.

Актуальність. Згідно зі статистикою [1], 60% організацій, які зазнали кібератак за останні два роки, заявляють, що вони були атаковані через невиправлену відому вразливість, де патч не було застосовано. 62% опитаних зазначають, що вони не мали інформації щодо вразливостей, які були використані під час кібератаки. В той же час 52% респондентів впевнені, що їх організації мають невигідну позицію у реагуванні на вразливості, оскільки вони використовують лише ручні процеси пошуку, аналізу та виправлення вразливостей [1]. Отже, процес управління вразливостями IT-систем є важливою та невід'ємною частиною забезпечення кібербезпеки організації, який практикується разом з управлінням ризиками та іншими практиками безпеки. Управління вразливостями включає в себе ідентифікацію, класифікацію, усунення та пом'якшення різних вразливостей у системі [2]. Для зменшення кількості ручної роботи та збільшення обсягів оброблюваної інформації під час управління вразливостями існують автоматизовані засоби, які повністю чи частково виконують задачі спеціаліста з управління вразливостями.

Метою даної роботи є дослідження автоматизованих засобів для управління вразливостями IT-систем організації .

Сучасний ринок надає широкий вибір засобів, призначених для виявлення слабких місць у системі організації щоб пом'якшити потенційні порушення безпеки в майбутньому. Кожний засіб володіє своїми функціями, перевагами та недоліками, тому основна задача лежить у порівнянні роботи і особливостей обраних засобів. Для цього використовується документація, література, демонстраційні матеріали та тестовий період використання. Результатом дослідження є виведена порівняльна таблиця обраних засобів.

Основні положення. Об'єктами дослідження були обрані три автоматизованих засоби для управління вразливостями на основі публічно-доступних рейтингів, документації та відповідності тестовій середі: Tenable.io (Tenable) [3], InsightVM (Rapid7) [4] та Qualys Vulnerability Management, Detection and Response (VMDR) (Qualys) [5]. Основними

категоріями для порівняння виступають набір можливостей, простота використання, рекомендації щодо пріоритезації, підтримка користувача, цінова політика, API та розширюваність, сторонні інтеграції.

Кожен критерій оцінюється експертом по десятибальній шкалі, де 1 відповідає найнижчій оцінці, 10 – найвищій. 0 відповідає відсутності інформації чи функціоналу. Для кожної категорії виведено вагу згідно з важливістю категорії – коефіцієнт, який враховується при виведенні підсумкової оцінки для кожного засобу. За результатами оцінювання визначається найбільш придатна система для конкретного кейсу тестового середовища.

Висновки. Автоматизовані засоби для управління вразливостями є невід'ємною частиною процесу управління вразливостями для забезпечення кібербезпеки організації. Для ефективного побудування процесу управління вразливостями важливим є вибір найбільш відповідного засобу для конкретної системи. В роботі було розглянуто три варіанту програмного забезпечення, проведено їх порівняльну характеристику та виведена найбільш придатна система для конкретного кейсу тестового середовища.

Список літератури

1. Ponemon study on gaps in vulnerability response. *Servicenow*. URL – https://www.servicenow.com/lpayr/ponemon-vulnerability-survey.html (дата звернення: 15.06.2022);

2. Що таке управління вразливістю?. *Технопедія.* URL – https://uk.theastrologypage.com/vulnerability-management (дата звернення: 15.06.2022);

3. Tenable.io. *Tenable.* URL – https://www.tenable.com/products/ tenable-io (дата звернення: 15.06.2022);

4. InsightVM. *Rapid7.* URL: https://www.rapid7.com/products/insightvm/ (дата звернення: 15.06.2022);

5. Vulnerability management. *Qualys*. URL: https://www.qualys.com/apps/vulnerability-management/ (дата звернення: 15.06.2022).

Відомості про авторів

Медведєва Юлія Віталіївна, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, м.т. 050-193-77-79, y.medvedieva@student.csn.khai.edu

Брежнєв Євген Віталійович, професор кафедри комп'ютерних систем, мереж і кібербезпеки, д. т. н., професор, e.brezhniev@csn.khai.edu

Секція 1

ПРОГРАМНЕ РІШЕННЯ ІЗ ЗАСТОСУВАННЯМ AI/ML ДЛЯ ПОШУКУ ВРАЗЛИВОСТЕЙ У ВЕБДОДАТКАХ

Мілінчук А.А.
Національний авіаційний університет, м. Київ
Науковий керівник Петренко А.Б.

Актуальність. Вебдодатки стали невід'ємною частиною повсякденного життя, але багато з них пов'язані з вразливостями. Для виявлення даних проблем у безпеці часто застосовуються спеціалізовані сканери, які побудовані на чіткозаданому пошуку, однак не враховують людської логіки.

Мета. Розробка програмного рішення для виявлення вразливостей у вебдодатках із застосуванням алгоритмів машинного навчання.

Основні положення. Потрібно наголосити на важливості розумного сканування та підкреслити той факт, що багато вразливостей виявляються лише після того, коли користувач повністю завершує шлях до шуканої сторінки. Це те, чого не вистачає звичайним сканерам, які не враховують людську логіку. Коритсувачі можуть розуміти, яка інформація, ймовірно, буде дійсною для певної форми введення та що потрібно виконати, щоб перейти до наступного кроку. Крім того, користувачі можуть швидко зрозуміти повідомлення про помилки та виправити недолік. Повідомлення на сторінці «Електронна адреса недійсна» означає, що адресу електронної пошти введено неправильно.

Сканер на основі машинного навчання розроблено з урахуванням певних важливих умов, це: розпізнавання типу сторінки, визначення успішного та неуспішного переходу сторінки, використання оптимальних значень в параметрах. Для перших двох вимог було використано наївний баєсовий класифікатор, а для третьої — багатошаровий персептрон (MLP) [1] та Q-навчання. Для розпізнавання типів сторінок застосовано класифікатор із заздалегідь визначеними категоріями та ймовірністю появи ключового слова. Функції були реалізовані так, щоб класифікувати представлену сторінку на основі ключових слів, знайдених на сторінці, і ймовірності існування цих ключових слів в одній із попередньо визначених категорій. Для створення такої таблиці ключових слів у заздалегідь визначених категоріях з нуля, було проаналізовано приблизно 25 вибраних вебдодатків. Для переходу між сторінками реалізовано функціональну таблицю слів успіху та слів невдачі та знову використано класифікатор.

Вхідними даними для MLP були поточна сторінка вебсайту та майбутня наступна сторінка. Вихідні дані були вхідними значеннями для переходу до наступної сторінки. Потім Q-навчання використовувалося для контролю за навчанням MLP та оптимізації результатів. Але після проведення аналізу

та після приблизно 100 раундів оптимізації ефективність створеного MLP все ще була низькою. Щоб покращити результати обробки, в код було вирішено підключити бібліотеку word2vec із косинусною подібністю для обчислення подібності слів, які вже бачило ПЗ. Word2vec представляє слово як вектор, а косинус-подібність вимірює кут між двома векторами, щоб дати оцінку подібності. Кожному вектору задано значення косинуса, і подібні вектори матимуть однакові кути. Для пошуку вразливостей було використано алгоритм довгострокової пам'яті (LSTM) [2]. Даний алгоритм може генерувати вихід із початкового числа. Після аналізу близько 20 000 сторінок синтаксису HTML і 10 000 сторінок JavaScript для навчання, ПЗ змогло генерувати дійсний синтаксис. Для уникнення вибраної системи захисту вебсайту – механізмів фільтрації вхідних даних, було використано MLP з Q-навчанням для нагляду за введенням коректної інформації. Для підвищення ефективності обходу фільтрів використано попереднє навчання.

Висновки. Таким чином, представлено методику та програмну реалізацію, яка використовує декілька комбінованих алгоритмів машинного навчання та імітує шаблони людського мислення, що допомагає з виявленням існуючих вразливостей.

Список літератури

1. Staudemeyer R. C. Understanding LSTM -- a tutorial into Long Short-Term Memory Recurrent Neural Networks / R. C. Staudemeyer, E. R. Morris. – 2019. Expert Systems with Applications, 42(7), 3508–3516.

Відомості про авторів

Мілінчук Аліна Анатоліївна, магістрант кафедри комп'ютеризованих систем захисту інформації,м.т. 0997648187, 5154578@stud.nau.edu.ua
Петренко Андрій Борисович, к.т.н., доцент кафедри комп'ютеризованих систем захисту інформації, andrii.petrenko@npp.nau.edu.ua

Секція 1

ДОСЛІДЖЕННЯ ТЕХНОЛОГІЙ ТА МЕТОДІВ ЗАХИСТУ ВЕБ-ЗАСТОСУНКУ У ІНФРАСТРУКТУРІ ЗВО

Муржа Д. Ю.
Харківський національний економічний університет ім. С. Кузнеця «ХНЕУ»
Науковий керівник Алексієв В. О.

Актуальність. Ми живемо у час змін та трансформації суспільства, коли в усьому світі відбувається процес діджиталізації. На наших очах відбувається перехід від аналогових джерел інформації до цифрових. Поява різноманітних сервісів у мережі інтернет робить життя людей більш зручним та комфортним. Поруч з цим, сфера освіти також не стоїть на місці і впевнено крокує в ногу з часом. Поява різноманітних платформ для онлайн навчання, робить процес отримання нових знань ефективним та доступним для кожної людини у будь-який час, у будь-якому місці.

Однак, разом із стрімкою цифровізацією нашого навколишнього середовища зростають також і кількість кіберзагроз. В процесі створення сервісів для потреб навчальних закладів потрібно приділяти неабияку увагу захисту персональних даних та інтелектуальної власності.

Основні положення. Різноманітна архітектура, висока ступінь поширення та інтеграція веб-застосунків в мережеву інфраструктуру робить їх привабливою мішенню для кіберзлочинців. Методи зловмисників залишаються незмінними на протязі багатьох років, ось основні з них[1]:

- SQL ін’єкції;
- DDoS-атаки;
- міжсайтовий скриптінг (XSS);
- міжстайтова підробка запитів;
- автоматизований перебір паролів (brute-force атаки);
- неперевірений перехід і редирект;
- відсутність функції контролю доступу.

Також не варто забувати технологію «соціальної інженерії» якою активно користуються кіберзлочинці. Цей метод атаки використовує необізнаність та неуважність користувачів. Але, спеціалісти з інформаційної безпеки роблять усе можливе щоб протидіяти зазначеним вразливостям, і на сьогоднішній день нам вже доступні ефективні інструменти захисту веб-додатків [2].

Один з основних інструментів захисту – WAF (Web Application Firewall). Суть роботи якого полягає в захисті веб-ресурсів, що виставлені назовні, тобто доступні кожному в мережі інтернет.

WAF дозволяє захиститися від багатьох видів атак. Серед них SQL і PHP-ін'єкції, міжсайтовий скриптінг (XSS), підбір пароля, експлуатація вразливостей нульового дня, DDoS-атаки, тощо. Перш за все потрібно розуміти, що WAF – це вузькоспеціалізований пристрій і він активно контролює тільки HTTP / HTTPS протоколи, і завдяки своїй архітектурі може розібрати весь сеанс зв'язку користувача. Завдяки цьому WAF здатний виявляти атаки з використанням автоматичних засобів (сканування, підбір паролів, DDoS, фрод, залучення в ботнети) [3].

Також незайвим буде, регулярне створення резервних копій системи, своєчасне оновлення модулів системи та ПЗ на сервері. Обов'язково потрібно використовувати зашифроване з'єднання HTTPS, поширювати інформаційну обізнаність користувачів та адміністраторів, регулярно проводити аудит системи [4].

Висновки. Комплексний та ефективний захист системи завжди починається з її проектування. Розуміння слабкостей ПЗ, яке необхідно захистити, робить простішим процес ідентифікації вразливостей та боротьби з ними. Такий підхід дозволяє зосередиться на актуальних методах атак і захиститися від них ще до початку використання системи.

Список літератури

1. OWASP Top 10. *OWASP*. URL: https://owasp.org/www-project-top-ten/ (дата звернення: 22.10.2022);
2. Кращі рішення для захисту сайтів та web-додатків. *Softkb*. URL: http://softkb.com.ua/krashhi-rishennya-dlya-zahystu-sajtiv-ta-web-dodatkiv/ (дата звернення: 23.10.2022);
3. Захист WEB-додатків. Чому це актуально? *Liga.NET*. URL: https://blog.liga.net/user/vberegovoy/article/33552 (дата звернення: 25.10.2022);
4. 5 ефективних способів захисту вашого веб-додатка. *Alltechbuzz*. URL: https://www.alltechbuzz.net/uk/5-efficient-ways-to-secure-your-web-app/ (дата звернення: 25.10.2022).

Відомості про авторів

Муржа Дмитро Юрійович, магістрант кафедри кібербезпеки та інформаційних технологій, м.т. 0685113292, dmytro.murzha@hneu.net
Алексієв Володимир Олегович, професор кафедри кібербезпеки та інформаційних технологій, д.т.н., vlax@hneu.edu.ua

Секція 1

ВИЯВЛЕННЯ АНОМАЛЬНОГО ТРАФІКУ У ЗАГАЛЬНОДОСТУПНИХ КОМП'ЮТЕРНИХ МЕРЕЖАХ

Петляк Н.С.
Хмельницький національний університет
Наукові керівники Кльоц Ю.П., Хохлачова Ю.Є.

Актуальність. Збільшення користувачів Інтернет-послуг та цифровізація суспільства призводить до стрімкого збільшення об'ємів трафіку, а комп'ютерні мережі все частіше стають об'єктами кібератак.

Ідентифікація зловмисного трафіку та аномалій відіграє важливу роль для безпеки. Тому потрібно використовувати системи виявлення вторгнень (СВВ, Intrusion Detection System, IDS), які можуть захистити мережу від існуючих та майбутніх загроз. IDS забезпечують вчасне оповіщення адміністраторів системи.

Мета. Наявні системи виявлення вторгнень орієнтовані на захист власної мережі та не розраховані на виявлення аномального трафіку, що орієнтований на атаку по відношенню до третіх осіб із власної мережі. Така система дозволить зменшити загальну кількість атак у мережах та зменшити трафік у власній мережі.

Основні положення. З приходом цифровізації та діджиталізації збільшується кількість загальнодоступних мереж (в тому числі Wi-Fi), де можна отримати анонімний доступ. З ростом покриття та кількості користувачів пропорційно зростає кількість атак, що проводяться користувачами-зловмисниками на об'єкти, що знаходяться за межами загальнодоступних комп'ютерних мереж (ЗКМ). Серед відомих атак на сторонні ресурси, що може призвести до компрометації ЗКМ, до якої підключився зловмисник є:

- віддалене проникнення (remote penetration);
- атака на відмову в обслуговуванні (denial of service);
- зламувачі паролів (password crackers);
- фішинг;
- тощо.

У порівнянні з аналогічним періодом 2021 року кількість DoS-атак (та DDoS-атак) зросла в 4,5 рази [1]. Із статистикою стрімкого розвитку фішингових атак можна ознайомитись у джерелі [2].

До популярних систем виявлення вторгнень можна віднести Snort, Wireshark, Microsoft Network Monitor, Security Onion. Усі вони орієнтовані на захист поточної мережі від атаки. І не пристосовані для недопущення атак, що виходять за межі цієї мережі.

Відомі системи виявлення вторгнень на основі машинного навчання [3-5] орієнтовані на виявлення атак на корпоративні мережі, та не націлені на

виявлення атак, що виходять із ЗКМ та використовують її потужності для атак на третіх осіб.

Варто враховувати, що задоволення потреби клієнта в анонімному доступі до загальнодоступної комп'ютерні мережі дозволяє зловмиснику підвищити рівень анонімності при проведенні атак на сторонні ресурси.

Відомі системи IDS орієнтовані на виявлення атак, що надходять в мережу, або вражають об'єкти в поточній мережі. Зазвичай аналізу вихідного трафіку приділяється недостатня увага.

Загальнодоступні сегменти мереж – зазвичай найменш контрольовані сегменти мереж, що забезпечують потреби гостьових, анонімних клієнтів. Використання для таких сегментів комерційних IDS на думку багатьох адміністраторів є недоцільним, тому такі мережі залишаються не захищеними від дій зловмисників.

Висновки. Оскільки відомі методи та засоби захисту мереж не забезпечують вирішення таких задач безпеки доцільним є розробка нових методів та засобів, що одночасно можуть забезпечити безпеку ЗКМ та, з відповідним рівнем достовірності, не допускатимуть зловмисних дій користувачів цієї мережі по відношенню до третіх осіб.

Список літератури

1. У першому кварталі 2022 року DDoS-атаки б'ють рекорди. *10Guards*. URL: https://10guards.com/ua/articles/ddos-attacks-at-an-all-time-high-in-q1-2022/ (дата звернення: 15.06.2022);
2. State of Phishing & Online Fraud. *Bostler*. URL – https://boost.bolster.ai/rs/540-RFH-299/images/2021_PhishingandFraudReport-109.pdf (дата звернення: 17.06.2022);
3. Real-Time DDoS Attack Detection System Using Big Data Approach. *DOI*. URL – https://doi.org/10.3390/su131910743 (дата звернення: 25.06.2022);
4. CorrAUC: A Malicious Bot-IoT Traffic Detection Method in IoT Network Using Machine-Learning Techniques. *IEEE*. URL – https://ieeexplore.ieee.org/document/9116932 (дата звернення: 26.06.2022);
5. Variational LSTM Enhanced Anomaly Detection for Industrial Big Data. *IEEE*. URL – https://ieeexplore.ieee.org/document/9195000 (дата звернення: 28.06.2022).

Відомості про авторів

Петляк Наталія Сергіївна, асистент кафедри кібербезпеки ХНУ, аспірант кафедри безпеки інформаційних технологій НАУ, м.т. 068-291-98-73, npetlyak@khmni.edu.ua
Кльоц Юрій Павлович, завідувач кафедри кібербезпеки, к.т.н. доцент, klots@khmnu.edu.ua
Хохлачова Юлія Євгеніївна, доцент кафедри безпеки інформаційних технологій, к.т.н. доцент, hohlachova@gmail.com

Section 1

SUBSTANTIVE CHARACTERISTICS OF THE "CYBER RISK"

Polomoshnova Mariia
National Technical University «Kharkiv Polytechnic Institute»

Relevance. Modern sustainable economic development requires effective implementation of the full potential of information technology and the latest IT developments. However, this path is closely related to the threats of misuse of information technology, which is a significant threat to the effective development of the public and private sectors. Therefore, building and ensuring the effective functioning of the cyber risk management system under the latest innovations is becoming increasingly important.

Objective. Developing theoretical approaches and further improving the concept of «cyber risks».

Main provisions. The development of each company co-occurs with the introduction of innovative services that often radically change business processes, with the expansion of the ecosystem of interaction with customers, partners, and counterparties, including the use of remote online channels, remote systems, and automated procedures. This development is associated with threats in information and cyberspace, which raises the task of timely detection, analysis of the probability of their implementation, the severity of possible consequences, and taking preventive measures.

In order to analyze the theoretical and essential characteristics of the concept of "cyber risks," the author analyzed the main definitions of this term contained in scientific publications and best practices [1-5]. Based on the analysis results, the main features of this term are formulated, which can be grouped into three classifiers:

1. By financial component: financial and non-financial.
2. By the vector of implementation of the consequences: direct and indirect.
3. By source of origin: internal and external.

After the classification into three groups according to certain standard features of the above disparate definitions, it should be recognized that most authors believe that cyber risks are, first of all, the risk of any losses resulting from the failure of information technology systems. However, this interpretation is somewhat narrow, as it does not consider the risk realization vectors and all possible sources of their origin.

In this regard, it seems advisable to apply the author's definition of "cyber risks" as any risk of financial and/or non-financial losses caused by internal

and/or external illegal actions of employees of the organization or other stakeholders (including intruders) on the operation of information technology systems.

The proposed definition more accurately reveals this phenomenon's essence and features and makes it possible to determine this term's theoretical and essential characteristics.

Conclusions. The author analyzed the most important definitions of "cyber risk." The analysis results revealed some generalizations regarding approaches to the definition of this phenomenon. For a more thorough assessment of the essence of this term, the author classified the approaches to defining the definition of "cyber risk" and supplemented the classifier for a more accurate assessment of this term. As a result of these actions, the author formulated and proposed a new definition of the concept of "cyber risk," which more accurately reveals this term's theoretical and essential characteristics.

References

1. Cyber Risk – Enlightenment through information risk management. PricewaterhouseCoopers. *PWC*. URL – https://www.pwc.com.au/consulting/assets/cyber-risk-paper-july2017.pdf (дата звернення: 14.08.2022).;
2. Віннікова І.І., Марчук С.В. Кібер-ризики як один із видів сучасних ризиків у діяльності малого та середнього бізнесу та управління ними. Східна Європа: економіка, бізнес та управління. 2018. №5(16). С.110-114.
3. Волосович С., Клапків Л. Детермінанти виникнення та реалізації кіберизиків. Зовнішня торгівля: економіка, фінанси, право. 2018. № 3. С.101-115;
4. Official site of the Institute of Risk Management. *Theirm*. URL – https://www.theirm.org/what-we-say/thought-leadership/cyber-risk/ (дата звернення: 18.08.2022);
5. Chartered Institute of Internal Auditors. *Cyber risk*. URL – https://www.iia.org.uk/resources/it-auditing-and-cyber-security/cyber-risk/?downloadPdf=true (дата звернення: 21.08.2022).

Information about the authors

Polomoshnova Mariia, a master`s student from the Department of cybersecurity, phone number 067-417-99-53, mariia.polomoshnova@gmail.com

Секція 1

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ У СОЦІАЛЬНИХ МЕРЕЖАХ

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

Актуальність. З ростом популярності соціальних мереж зростає і питання захисту персональних даних. Коли користувачі реєструються в соціальних мережах, вони, як правило, надають особисту інформацію, таку як ім'я, адреса та дата народження. Ця інформація потім зберігається на серверах соціальної мережі.

Відомо, що хакери націлені на соціальні мережі, щоб отримати доступ до цієї особистої інформації. Отримавши доступ до облікового запису користувача, вони можуть переглядати його особисті дані, такі як список контактів і приватні повідомлення[1]. Виходячи з цієї інформації, було виділено необхідність розглянути та застосувати методи захисту особистої інформації у розробці соціальної мережі.

Мета роботи: полягає у дослідженні методів захисту персональних даних в соціальних мережах.

Основні положення. Існує багато методів захисту особистих даних у веб-додатках. Деякі поширені методи включають в себе: використання SSL/TLS для шифрування даних під час передачі, зберігання даних у зашифрованому форматі, використання механізмів контролю доступу для обмеження доступу до даних.

Для захисту під час передачі даних між браузером користувача та сервером в соціальній мережі використовується протокол HTTPS, який являє собою звичайний HTTP, що працює через шифровані транспортні механізми SSL/TLS[2]. Це важливо, оскільки дані часто передаються через мережі, які не є повністю захищеними. Коли дані зашифровані, навіть якщо хакери зможуть перехопити дані, наприклад при використанні користувачем скомпрометованої мережі, вони не зможуть розшифрувати та переглянути їх без відповідних ключів.

Не менш важливим є захист даних, що зберігаються на сервері. Для цього використовуються кілька методів. База даних і веб-сервер знаходяться на різних серверах, при чому тільки веб-сервер має доступ до мережі інтернет, база даних пов'язана з ним тільки по приватній мережі. Це дозволяє обмежити несанкціонований доступ до бази даних і захистити дані при передачі між БД і сервером. Дані у базі даних зберігаються у зашифрованому форматі. Коли дані потрібні, вони розшифровуються за допомогою відповідних ключів. Це гарантує, що навіть якщо хакери зможуть отримати доступ до бази даних, вони все одно не зможуть переглянути дані.

Іншим поширеним методом є використання механізмів контролю доступу для обмеження доступу до даних. Наприклад, доступ до конфіденційних даних користувачів є тільки у адміністраторів, у чиї обов'язки входить робота з даними користувачів.

У самій соціальній мережі користувач може отримати доступ лише до своїх даних та даних якими явно поділилися інші користувачі. Також користувач може запросити надання архіву з усіма даними, що зберігаються про нього, а також запросити видалення свого облікового запису та всіх даних пов'язаних з ним, як зазначено в GDPR[3].

Висновки. Розглянуті в цій роботі способи захисту персональних даних у соціальних мережах - це лише деякі з багатьох способів захисту даних користувачів. Важливо пам'ятати, що за безпеку даних користувачів відповідає як соціальна мережа, так і сам користувач. Користувачі повинні усвідомлювати ризики обміну особистими даними в Інтернеті та вживати заходів для захисту власних даних, наприклад, використовувати надійні паролі та не ділитися конфіденційною інформацією з іншими особами. Соціальні мережі ж повинні надавати користувачам можливості контролювати свої дані та забезпечувати наявність адекватних заходів безпеки для захисту даних користувачів.

Список літератури

1. 5 Of the Biggest Hacks in Cybersecurity History. *Discover Magazine*. URL – https://www.discovermagazine.com/technology/5-of-the-biggest-hacks-in-cybersecurity-history (дата звернення: 10.11.2022);
2. HTTPS. *Wikipedia*. URL: https://uk.wikipedia.org/wiki/HTTPS (дата звернення: 15.11.2022);
3. Регламент (ЄС) 2016/679 Європейського парламенту та Ради від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних).

Відомості про авторів

Резніков Андрій Олександрович, студент кафедри комп’ютерних систем, мереж і кібербезпеки, м.т. 0975418608, a.reznikov@student.csn.khai.edu
Землянко Георгій Андрійович, асистент кафедри комп’ютерних систем, мереж і кібербезпеки. g.zemlynko@csn.khai.edu

Секція 1

АНАЛІЗ ІСНУЮЧИХ ЗАСОБІВ ЗАХИСТУ ПІД ЧАС ВИКОРИСТАННЯ ХМАРНИХ ТЕХНОЛОГІЙ

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

Актуальність. На сьогодні поширеними є хмарні технології або хмарні обчислення. В них зацікавлені як звичайні користувачі, так і великі компанії. Усім потрібно зберігання даних, інформації, як конфіденційної, так і секретної, і для цього використовуються хмарні технології. Але паралельно з цим є потреба в чинному захисті таких технологій, бо з розвитком комп'ютерних технологій все більше є можливість крадіжки, злому та використання конфіденційних або секретних даних у хмарі.

Метою даної роботи є: вивчення та аналіз існуючих засобів та методів захисту хмарних технологій.

Основні положення. Хмарні обчислення охоплюють технології, які дозволяють окремим особам або компаніям отримувати доступ до певних даних або послуг без потреби у фізичній інфраструктурі.

Інтерфейс включає в себе все, що стикається з користувачем, те, що клієнти бачать безпосередньо. Наприклад, те, що ви бачите в цій роботі та/або на веб-сайті, все завдяки інтерфейсній веб-розробці на задній частині. Однак, є всі процеси та дані, які забезпечують безперебійну роботу цієї сторінки. Бекенд-розробка контролює сервери, бази даних і все, що допомагає підтримувати стабільність цієї веб-сторінки. Коли хмарні обчислення з'являються в картині, вони займають стійку позицію як накладання для всього, що відбувається на сервері. Іншими словами, все, що відбувається на сервері, тепер відбувається в хмарі.[1]

Зі збільшенням кількості віддалених працівників зростає потреба у захисті доступу та переміщенні даних компанії в різних відомих і невідомих мережах. Для того, щоб зробити безпечну та надійну хмарну систему, треба користуватись або одним з даних методів, або для кращої надійності всіма [2]:

- методи автентифікації та ідентифікації;
- методи контролю доступу;
- методи шифрування;
- методи безпечного видалення;
- методи відновлення даних.

Хмарні рішення безпеки поділяються на шість основних категорій, які виконують певну роль у захисті хмарних баз даних, програм і контейнерів:

- CASB – брокери безпеки доступу до хмари
- SAST – статичне тестування безпеки додатків

- SASE – Secure Access Service Edge
- CSPM – Cloud Security Posture Management
- CWPP – хмарні платформи захисту робочого процесу
- CIEM – Cloud Infrastructure Entitlement Management[4]

Плюсом захисту даних у хмарі є систематичне визначення уніфікованих політик, які застосовуються на всіх рівнях. Політики щодо зберігання даних, словника даних, правил доступу та дозволів на основі ролей запобігають будь-якій формі вторгнення, захищаючи конфіденційні дані. Сучасні хмарні рішення для захисту даних також завчасно виявляють ризики та аномалії даних, дозволяючи командам безпеки зупиняти будь-які спроби кібератак або впровадження шкідливого програмного забезпечення.[3]

Висновки. Захист даних є однією з головних проблем безпеки для багатьох організацій у хмарі. Без нього передача особистих даних на віддалені машини була б просто неможливою. Підбиваючи підсумки, методи захисту даних можна використати як окремо, так і всі разом. Щодо оглянутих інструментів безпеки, кожен з них має своє направлення захисту хмарної системи.

Список літератури

1. Cloud Technology: What Is Cloud Computing and How Does It Work? | Trio Developers. *Trio Developers - Stop searching. Start building.* URL – https://www.trio.dev/blog/cloud-technology (дата звернення: 28.10.2022);
2. Proven Security Techniques for Data Protection in Cloud. *LightEdge Solutions*. URL – https://www.lightedge.com/blog/proven-security-techniques-for-data-protection-in-cloud/ (дата звернення: 30.10.2022);
3. What Is Cloud Data Protection? Definition, Importance, and Best Practices |. *Business and Industry News, Analysis and Expert Insights | Spiceworks*. URL – https://www.spiceworks.com/tech/cloud/articles/what-is-cloud-data-protection/#_001 (дата звернення: 03.11.2022);
4. Top 12 Cloud Security Tools for 2022 - Spectral. *Spectral*. URL – https://spectralops.io/blog/top-12-cloud-security-tools/ (дата звернення: 06.11.2022).

Відомості про авторів

Селіванова Марія Олександрівна, студент кафедри комп'ютерних систем, мереж і кібербезпеки, т. 099-230-48-13, m.selivanova@student.csn.khai.edu
Пєвнєв Володимир Яковлевич, професор кафедри комп'ютерних систем, мереж і кібербезпеки, д.т.н., доцент, v.pevnev@csn.khai.edu

Секція 1

АНАЛІЗ АТАК НА СИСТЕМИ ШТУЧНОГО ІНТЕЛЕКТУ

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

Актуальність. В сучасному світі аналіз атак на системи штучного інтелекту це доволі актуальне питання. Можливо це стверджувати через те, що у наші дні штучний інтелект стає більш популярним і його використання зустрічається у все більшої кількості програмних продуктів. Тому передчасне виявлення вразливостей систем захисту, аналіз та використання засобів протидії атакам є дуже важливим крок, від якого іноді може залежати робота компанії, безпека майна або навіть власне життя.

Метою даної роботи є аналіз існуючих загроз щодо систем штучного інтелекту та методів їх реалізації.

Основні положення. Штучний інтелект — це здатність машин симулювати розум та імітувати людські когнітивні здібності. Тобто збирати й адаптувати зовнішні дані, а на їх основі навчатися ухвалювати рішення та робити висновки, як могла би людина.

Технології штучного інтелекту міцно увійшли у життя людей на всіх рівнях — від голосових помічників до керованого алгоритмами синтезу стовбурових клітин. І це далеко не межа того, як вони можуть змінити розвиток людської цивілізації [1].

В рамках проведеної роботи було проаналізовано такі загрози:

- змагальні атаки;
- системні маніпуляції;
- пошкодження та отруєння даних;
- передача атак навчання;
- онлайн маніпуляції системою;
- конфіденційності даних.

В доповіді представлено наступні результати: механізми проведення атак, можливі варіанти відбиття цих атак, наслідки втручання в систему штучного інтелекту.

Висновки. В ході аналізу було виявлено, що кожен випадок і набір даних можуть вимагати розгортання іншої стратегії захисту, щоб зберегти базову модель. Різні змагальні підходи можна вирішити за допомогою різних засобів захисту, але немає чітких ознак того, що існує стратегія

захисту, яка може належним чином охопити широкий спектр методів нападу. А високі показники успіху змагальних атак проти справжнього випадку з використанням фактичних даних, отриманих із реального виробничого середовища, вказують на те, що сучасна виробнича система з підтримкою штучного інтелекту може стати плодом розумних зловмисників. Тобто дослідження та інновації необхідно заохочувати, щоб розробити надійні архітектури для очищення конвеєрів даних у виробничих середовищах, фільтрації зловмисних екземплярів і виявлення ін'єкції ворожих прикладів у процесі [2].

Щоб організації могли захистити свої програми штучного інтелекту та моделі машинного навчання, вони повинні використовувати рішення безпеки, які забезпечують дуже безпечне конфіденційне обчислювальне середовище. Коли конфіденційне обчислення поєднується з правильними рішеннями кібербезпеки, такими як стійкий апаратний модуль безпеки (HSM), це може забезпечити надійний наскрізний захист даних у хмарі для додатків штучного інтелекту – великих і малих [3].

Список літератури

1. Даниленко Ю. Від Ш до І: що таке штучний інтелект та як він трансформує світ. *Speka*. URL – https://speka.media/ai/vid-s-do-i-shho-take-stucnii-intelekt-ta-yak-vin-transformuje-svit-xv7039#shho-take-stucnii-intelekt (дата звернення: 01.11.2022);

2. Security threats for AI and machine learning. *Hubsecurity*. URL – https://hubsecurity.com/blog/cyber-security/security-threats-for-ШІ-and-machine-learning/ (дата звернення: 03.11.2022);

3. Towards Robustifying Image Classifiers against the Perils of Adversarial Attacks on Artificial Intelligence Systems. *MDPI*. URL – https://www.mdpi.com/1424-8220/22/18/6905/htm (дата звернення: 06.11.2022).

Відомості про авторів

Стацишина Ірина Павлівна, студент кафедри комп'ютерних систем, мереж і кібербезпеки, м.т. 067-649-59-21, i.statcyshyna@student.csn.khai.edu

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

Секція 1

АНАЛІЗ ВРАЗЛИВОСТЕЙ ВЕБ-ДОДАТКІВ

Сухіненко С.Є.
Відокремлений структурний підрозділ « Краматорський фаховий коледж Донбаської державної машинобудівної академії»
Науковий керівник Сагай О.В.

Актуальність. Популярність Інтернету стала повсюдною і важливою для повсякденного життя людей та бізнесу. Кількість веб-додатків в Інтернеті швидко зростає, але, на жаль, багато з них мають дірки у безпеці. Ці вразливості можуть варіюватися від дрібних проблем до катастрофи для хост-системи та її власників.

Мета. Провести це аналіз існуючих вразливостей веб – додатків та класифікацій вразливостей.

Основні положення. В Інтернеті існує безліч веб-додатків, які обробляють дані і запити від користувачів, які пройшли перевірку автентичності, і від тих, хто цього не зробив. Додаток також має бути стабільним щоб користувачі могли завжди мати до нього доступ [1].

Ін'єкції даних SQL-injection це один з найбільш небезпечних і поширених способів зламу сайтів і програм, що працюють з базами даних, заснований на впровадженні в запит довільного SQL коду. Запобігання ін'єкції вимагає збереження даних окремо від команд та запитів.

Незахищеність критичних даних Багато веб-додатків не захищають конфіденційні дані. Зловмисники можуть вкрасти або модифікувати слабо захищені дані для використання в своїх корисливих цілях. Як ий приклад - передача даних по протоколу HTTP ніяк не зашифровано, а при проходженні даних від користувача до Web-сервера, дані пройдуть багато різних вузлів. На кожному з цих вузлів може знаходитися програма, яка зчитує весь трафік і передає зловмисникам [2].

Експлуатація вразливостей XXE Атака зовнішніх об'єктів XML - це тип атаки на додаток, що аналізує вхід XML. Ця атака може призвести до розголошення конфіденційних даних, відмови в обслуговуванні, підробки запиту на стороні сервера, сканування портів з точки зору машини, де розташований аналізатор, та інших системних впливів [3].

Контроль доступу полягає в тому, як веб-додаток надає доступ до вмісту та функцій деяким користувачам, а не іншим. Ці перевірки виконуються після автентифікації та регулюють те, що дозволено користувачам. Модель контролю доступу веб-програми тісно пов'язана з вмістом та функціями, які надає сайт.

Безпека Web-додатків вимагає наявності безпечної конфігурації всіх компонентів інфраструктури: компонентів програми (таких як фреймворки - frameworks), веб-сервера, сервера баз даних і самої платформи. Налаштування компонентів сервера за замовчуванням найчастіше небезпечні і відкривають можливості до атак [4].

Міжсайтовий скриптинг передбачає введення шкідливого коду на сервер з входом користувача. Тим часом коли атаки в один клік зосереджуються на довірі, яку сервер має до автентифікованого користувача, міжсайтовий скриптинг націлений на те, що користувач довіряє певному веб-сайту.

Неперевірені переадресації та пересилання Web-додатки часто переадресовують користувача з однієї сторінки на іншу. В процесі можуть неналежним чином перевіряються параметри із зазначенням сторінки кінцевого призначення переадресації. Цей вид вразливостей є різновидом помилок перевірки вхідних даних (input validation).

Небезпечні прямі посилання на об'єкти є наслідком недостатньої перевірки призначених для користувача даних. Суть її полягає в тому, що для доступу до об'єкта використовується ідентифікатор, який передається у відкритому вигляді в адресному рядку браузера.

Висновки. Захищеність веб – додатків від атак зловмисників залежить від технологій та компонентів, які використовуються при побудові веб – додатків, а також від можливих вразливостей у цих компонентах. Існують різні класифікації вразливостей, кожна атака через вразливість має свої особливості, але причина виникнення вразливостей – помилки при проєктуванні, реалізації та застосуванні компонентів веб – додатків, отже виникає необхідність пошуку вразливостей та реагування на інформацію про випадки їх знайдення.

Список літератури

1. Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу НД ТЗІ 1.1-003-99. URL: http://iszzi.kpi.ua/images/Info_bezpeka/ND_TZI/4_НД_ТЗІ_1.1-003-99.pdf (дата звернення: 03.11.2022);
2. External Entity Attack. *OWASP*. URL – https://www.owasp.org/images/5/ 5d/XML_Exteral_Entity_Attack.pdf (дата звернення: 06.11.2022);
3. OWASP Mobile Application Security. *OWASP*. URL – https://www.owasp.org/index.php/Category:Access_Control (дата звернення: 15.11.2022);
4. Вразливості веб – додатків. *PTsecurity.* URL: https://www.ptsecurity.com/upload/corporate/ruru/analytics/Web-Vulnerabilities-2019-rus.pdf (дата звернення: 17.11.2022).

Відомості про авторів

Сухіненко Софія Євгенівна, студентка спеціальності «Інженерія програмного забезпечення» м.т.0665255546, suhinenko.sonya@gmail.com
Сагай Ольга Володимирівна, методист, викладач вищої категорії спеціальних дисциплін з програмування, olya.sagay@gmail.com

Секція 1

ЗАХИСТ АВТОРСЬКОГО ПРАВА З ВИКОРИСТАННЯМ СТЕГАНОГРАФІЧНОГО МЕТОДУ ФАЗОВОГО КОДУВАННЯ

Телющенко В.А.
Національний авіаційний університет, м. Київ
Науковий керівник Петренко А.Б.

Актуальність. Зростання можливостей сучасних комунікацій потребує спеціальних засобів захисту, особливо у комп'ютерних мережах. Безпека мережі стає все більш важливою у міру збільшення кількості даних, якими обмінюються користувачі через Інтернет. Доступність аудіо, відео та інших джерел в цифровій формі у відкритому доступі приводить до масштабного несанкціанованого їх копіювання, при чому цифрові формати дозволяють забезпечити високу якість зображення навіть при багаторазовому копіюванні Це потребує альтернативних рішень в області захисту авторських прав.

Мета роботи: полягає у розгляданні можливості вбудовування цифрових водяних знаків із використанням стеганографічного методу фазового кодування для захисту авторських прав медіа об’єктів.

Основні положення. Основними методами захисту секретної інформації є: криптографічний метод, який полягає у зміні інформації таким чином, щоб вона стала незрозумілою для сторонніх людей та стеганографічний, що не змінює зміст повідомлення, а приховує сам факт передачі інформації, чи факту реальності існування секретного повідомлення в об’єкті [1].

Однак передача зашифрованої інформації спричиняє певні підозри. Щоб уникнути цього використовується разом дві науки: насамперед шифрування – криптографія, та стеганографія, щоб приховати факт передачі зашифрованих даних.

Проте стеганографія не лише передає певну інформацію, а й служить захистом від зловмисників. Наприклад, при захисті авторських прав у документі можуть бути приховані певні теги, які вказують, кому саме належить нелегальна копія, якщо її вкрадено або розміщено в іншому джерелі [2].

Цифрові методи стеганографії широко застосовуються в аудіосередовищі. Вони здатні забезпечити пересилку повідомлень великого обсягу у медіа файлах, які розповсюджуються в Інтернеті. Звукові файли можуть бути змінені таким чином, щоб вони містили приховану інформацію, наприклад, інформацію про авторські права Але ці модифікації повинні бути зроблені так, щоб зловмисник не міг усунути їх, принаймні, не знищивши вихідний сигнал. Методи вбудовування даних до звукових файлів використовують властивості слухової системи людини. Слуховий апарат людини чутливий до адитивних перешкод, але не

чутливий до зміни абсолютної фази. Ці властивості людини дають змогу використовувати аудіосередовища для передачі інформації, яка не буде помітна.

Цифрові водяні знаки (ЦВЗ) були запропоновані як вирішення проблеми захисту авторських прав володіння мультимедійними даними (зображення, аудіо, відео).

Одним із стеганографічних методів вбудовування ЦВЗ в медіа об'єкти є метод фазового кодування, що використовує слухову здатність людини не відчувати зміни фази сигналу. В даному методі фаза початкового сегмента аудіо сигналу модифікується в залежності від даних, що вбудовуються, а фаза наступних сегментів узгоджується, щоб зберегти різницю фаз. Це необхідно тому, що до різниці фаз людське вухо чутливе. Потрібно перевести значення вбудовуваного повідомлення у значення фаз $\frac{\pi}{2}$ і $\left(-\frac{\pi}{2}\right)$, які представляють одиниці і нулі відповідно. Схема водяних знаків на основі методу фазового кодування передбачає внесення змін в область високих частот, завдяки чому досягається стійкість до різних типів атак. Також, у порівнянні з іншими стеганографічними методами, метод фазового кодування є одним із методів, який стійкий до стиснення і впливу шумів. Недоліком даного методу являється низька пропускна здатність, яка складає від 8 до 32 біт/с в залежності від звукового контексту [1].

Висновки. Вбудовані ЦВЗ методом фазового кодування вносять незначні зміни в параметри аудіофайла, які не відчутні для слухової системи людини. Дана інформація вбудовується таким чином, щоб зловмиснику було неможливо її вилучити, значно не пошкодивши при цьому сам контейнер. Фазове кодування є одним із найбільш ефективних методів по критерію відношення сигнал/шум. Враховуючи вищевикладене, метод фазового кодування є одним із стеганографічних методів, який можливо і доцільно використовувати для захисту авторських прав медіа об'єктів.

Список літератури

1. Конахович Г.Ф. Компьютерная стеганография. Теория и практика // Конахович Г.Ф., Пузыренко А.Ю – К: «МК-Пресс», 2006. – 288с.;
2. Методи підвищення стійкості та пропускної здатності систем прихованої передачі інформації. *Nure*. URL: https://nure.ua/wp-content/uploads/2018/Dissertation/dis_Vovk.pdf (дата звернення: 24.06.2022);
3. Хорошко В.О., Яремчук Ю.Є., Карпінець В.В. Комп'ютерна стеганографія : навчальний посібник– В. : Вид. ВНТУ, 2017. – 86 с.

Відомості про авторів

Телющенко Валентина Анатоліївна, студент кафедри комп'ютеризованих систем захисту інформації, м.т. 097-276-42-89, telyushchenko@bigmir.net
Петренко Андрій Борисович, доцент кафедри комп'ютеризованих систем захисту інформації, к.т.н., доцент, pab.05@ukr.net

Секція 1

МЕТОДИ ЗАХИСТУ САЙТУ «ІНТЕРНЕТ-МАГАЗИНУ» ВІД КІБЕРАТАК

Фещук Д.Ю.
Національний аерокосмічний університет ім. М.Є Жуковського
«Харківський авіаційний інститут»
Науковий керівник Землянко Г.А.

Актуальність. Комп'ютерні та інформаційні технології сьогодні охопили багато галузей економіки, а саме торгівлю, і в них є дуже багато факторів небезпеки. Однією із небезпек являється безпека їх торгівельних майданчиків в мережі інтернет. Мова йдеться не лише про безпеку самої компанії а й про її клієнтів. Для будь-якої сучасної компанії інформація стає одним із головних ресурсів, тому актуальною проблемою для підприємства стає забезпечення інформаційної безпеки.
Тому дуже важливо захистити свій сайт від можливих кібератак та іншого.

Мета. Метою доповіді буде проаналізувати методи які зможуть захистити сайт «інтернет-магазин» від кібератак

Основні положення. Інформаційна безпека – властивість системи протягом заданого часу протистояти несанкціонованому зняттю та модифікації інформації.

Розглянемо основні способи того, як можна вберегти свій сайт «інтернет магазин» від кібератак:
1. Захист корпоративної пошти. Половина всіх кібератак відбувається з боку корпоративної пошти, адже це критично важливий інструмент для компанії. Якщо безліч рекламних листів одразу не фільтрувати та не видаляти, то вони швидко заповнять всі ресурси сервера. Щоб убезпечитися від таких базових кібератак, поштовий сервіс варто розмістити у хмарі. Наприклад, хмарна платформа Microsoft Azure вже передбачає базовий захист від спаму, антифішинг тощо [1].
2. Аналіз поведінки внутрішніх користувачів. Система для аналізу поведінки користувачів допомагає виявити нетипові дії співробітників.
User behavior analytics (UBA) та User and Entity Behavior Analytics (UEBA) дозволяють за допомогою штучного інтелекту створити матрицю поведінки користувача або пристрою. Наприклад, співробітник щодня для робочих задач використовує Outlook, Microsoft Teams та завантажує 10 Мб файлів з пошти. Система запам’ятовує такий перелік дій, а тому помічає, коли раптом користувач починає завантажувати великий об’єм даних з

внутрішнього сервера компанії на зовнішній ресурс. Це суттєве відхилення від матриці, а тому UBA одразу реагує. Вона може просто повідомити службу безпеки про нетипову поведінку або ж тимчасово заблокувати дії користувача [1].

3. Турбота про безпеку клієнтів [2]:

– підвищуйте обізнаність клієнтів у питаннях ІБ;

– регулярно нагадуйте клієнтам про правила безпечної роботи в інтернеті, роз'яснюйте методи атак та способи захисту;

– застерігайте клієнтів від введення облікових даних на підозрілих веб-ресурсах і тим більше від повідомлення такої інформації будь-кому

– електронною поштою або під час телефонної розмови;

– роз'яснюйте клієнтам порядок дій у разі підозри про шахрайство;

– повідомляйте клієнтів про події, пов'язані з інформаційною безпекою.

Висновки. Проаналізувавши статистику з сайту компанії techexpert.ua [3], можна побачити , що кількість втрачених записів даних з кожним роком дуже стрімко збільшується – в 2005 році приблизно 15 мільйонів, в 2017 році – приблизно 63 мільйони, а в 2020 вже 101 мільйон втрачених записів даних. Зі звіту також видно, що інвестиції на захист даних за 2020 рік збільшилися на 10% з попереднього року і становлять близько 53 мільярдів доларів. Отже, можемо зробити висновок. З розвитком інформаційних технологій виростає ймовірність бути жертвою кібератаки.Тому варто серйозно віднестися до складової кібербезпеки в вашій компанії, а в нашому випадку сайту «інтернет-магазину».

Список літератури

1. 7 способів вас зламати або як захиститися від кібератак. *Kyivstar*. URL: https://hub.kyivstar.ua/news/7-sposobiv-vas-zlamaty-abo-yak-zahystyty-kompaniyu-vid-kiberatak/ (дата звернення: 23.06.2022).

2. Як захиститися від кібератак. *Positive Technologies*. URL: https://www.ptsecurity.com/ru-ru/research/knowledge-base/kak-zashchititsya-ot-kiberatak/ (дата звернення: 23.06.2022);

3. Кількість кібератак збільшується: що з цим робити. *Techexpert*. URL: https://techexpert.ua/ru/cyberattacks-number-research/ (дата звернення: 24.06.2022).

Відомості про авторів

Фещук Дмитро Юрійович, студент кафедри комп'ютерних систем, мереж і кібербезпеки,м.т. 0665868122, d.y.feshchuk@student.csn.khai.edu

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

Секція 1

АНАЛІЗ АТАК НА СИСТЕМУ eHealth МОЗ УКРАЇНИ

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

Актуальність. Цифровізація охорони здоров'я почалася 2016 року з Концепції реформи фінансування, яка вбачає якісний доступ до медичної допомоги. Медичні дані вважаються чутливими. Електронна система охорони здоров'я eHealth – це інструмент для забезпечення прозорості процесів в охороні здоров'я [1]. І найголовніше – це система, якій люди довіряють дані про своє здоров'я.

В Україні в цілях забезпечення захисту персональних даних, до яких стосуються і дані про стан здоров'я, біометричні або генетичні дані, діє Закони України «Основи законодавства України про охорону здоров'я» [2] та «Про захист персональних даних». Саме вони регулюють питання забезпечення захисту персональних даних у сфері охорони здоров'я.

Мета. Провести аналіз можливих загроз щодо захисту персональних даних, які використовуються в системі охорони здоров'я eHealth.

Основні положення. Персональні дані пацієнтів у електронну систему eHealth можуть вводити лише визначені медичним закладом уповноважені особи. В електронній системі працює етап підтвердження входу - CAPTCHA - автоматизований комп'ютерний тест, який аналізує «поведінку» користувача при вході та може відрізнити людину від бота. На програмному рівні безпечний доступ ґрунтується на технології двофакторної авторизації протоколу Oauth.2 [3]. Саме цей протокол забезпечує верифікацію входу та розгалуження прав доступу до даних.

Передача інформації здійснюється у зашифрованому вигляді згідно з вимогами законодавства. Додатково в системі реалізовано принцип відокремленого зберігання персональних та медичних даних пацієнта. Однак ризики щодо стороннього втручання у дану платформу досі існує. Одними із можливих атак на систему eHealth може бути [4]:

– denial of service (DoS attack) — мережева атака, завданням якої є перенавантаження компонентів комп'ютерних систем;

– malware — запуск усередину комп'ютера шкідливого програмного забезпечення (віруси, трояни);

– phishing — атака з використанням технічних засобів і засобів соціальної інженерії з метою введення в оману авторизованих користувачів;

– ransomware — запуск всередину комп'ютера шкідливого програмного забезпечення, що шифрує дані або робить їх копію;

– man-in-the-middle — мережева атака, завданням якої є додавання стороннього користувача до вже наявного каналу зв'язку між двома системами;

– zero-day exploit — атака на вразливі місця ліцензованого програмного забезпечення, задля втручання в нього та виконання потрібних хакеру задач;

– cross-site scripting (XSS) — атака на користувачів безпечного сайту внаслідок додавання до нього небезпечного коду;

– logic bombs — атака за допомогою легальних програм через додавання до них шкідливого коду, що виконується за певних умов.

Висновки. Електронні реєстри не дають можливості так легко отримати інформацію, але особи, які мають спеціальні знання та навички роботи в комп'ютерних системах, здатні на це.

Незважаючи на безліч плюсів електронної медицини вона має низку недоліків. І основний з них — ризик, що персональні дані пацієнта з легкої руки кіберзлочинців можуть опинитися в руках шахраїв.

Список літератури

4. Кожне робоче місце підключено до електронної системи охорони здоров'я. URL: https://nszu.gov.ua/academy/osnovni-kroki-2020/pidkluch-mic (дата звернення: 18.06.2022);

5. Закон України «Основи законодавства України про охорону здоров'я». URL: https://zakon.rada.gov.ua/laws/show/2801-12#Text (дата звернення: 20.06.2022);

6. Як захищений вхід до системи eHealth. *Ezdorovya*. URL: https://www.facebook.com/ezdorovya/posts/ (дата звернення: 22.06.2022);

7. What is a Cyber Attack? *IBM*. URL – https://www.ibm.com/topics/cyber-attack (дата звернення: 24.06.2022).

Відомості про авторів

Храмцов Микола Юрійович, студент кафедри комп'ютерних систем, мереж і кібербезпеки, м.т. 095-304-66-95, nickthomson769@gmail.com

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

Секція 1

АНАЛІЗ СПОСОБІВ ЗАПОБІГАННЯ XSS-АТАК РЕАЛІЗОВАНИХ В ASP.NET CORE

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

Актуальність. Однією з найрозповсюдженіших атак, яка застосовувалася останнім часом для веб-застосунків є Cross-Site Scripting (XSS). Міжсайтові сценарії (XSS) — це вразливість безпеки, яка дає змогу зловмиснику розміщувати на веб-сторінках клієнтські скрипти (зазвичай JavaScript). Коли користувач завантажує уражені сторінки, запускаються сценарії зловмисника, що дозволяє зловмиснику вкрасти файли cookie та маркери сеансу, змінити вміст веб-сторінки за допомогою маніпуляції DOM або перенаправити браузер на іншу сторінку. Уразливості XSS зазвичай виникають, коли програма приймає дані користувача та виводить їх на сторінку без перевірки, кодування чи екранування. Недоліки, які дозволяють цим атакам досягати успіху, є досить поширеними і виникають скрізь, де веб-додаток використовує вхідні дані від користувача в межах результату, який він генерує, не перевіряючи чи не кодуючи його [1].

Мета. Провести аналіз можливих сценаріїв запобіганню XSS-атак.

Основні положення. Щоб можна було вважати успішною, зловмиснику необхідно вставити та виконати шкідливий вміст на веб-сторінці. Тому Для захисту від XSS атаки необхідно щоб кожна змінна у веб-додатку проходила перевірку, а потім була вилучені або очищена. Фреймворки дозволяють легко переконатися, що змінні правильно перевірені, екрановані або очищені. Вихідне кодування та очищення HTML допомагають усунути ці прогалини [2].

Движок Razor, що використовується в ASP.NET Core MVC, автоматично кодує весь вихід. Він використовує правила кодування атрибутів HTML щоразу, коли використовується директива @. Оскільки кодування атрибутів HTML є наднабором кодування HTML, це означає, що при розробці не потрібно турбуватися про те, яке саме кодування необхідно використовувати. Іноді користувачам потрібно створити свою власну HTML-розмітку, що в тому числі передбачає написання скриптів, і одним із способів задовільнити цю потреби є використання візуального редактору WYSIWYG. Цей спосіб допоможе запобігти появі XSS вразливостей, але

порушить передбачувану функціональність програми. У цих випадках слід використовувати HTML Sanitization [3]. За замовчуванням ASP.NET Core не має бібліотеки для роботи з HTML Sanitization, але існує декілька HTML-парсерів, таких як HtmlSanitizer та HtmlAgilityPack, написаних на мові програмування C#, які можна використовувати для очищення HTML від потенційно шкідливих конструкцій.

Окрім вставки скриптів у розмітку веб-сторінки, XSS атака може також бути реалізована шляхом вставки шкідливих скриптів у URL. Перевірка HTTP-запитів додає захист від розмітки або коду в рядку запиту URL-адреси, файли cookie або опубліковані значення форми, які могли бути додані зі зловмисними цілями. Ця перевірка допомагає запобігти XSS-атаці, викликаючи в браузері помилку «потенційно небезпечне значення виявлено» та зупиняючи обробку сторінки, якщо вона виявляє введення, яке може бути зловмисним, як-от розмітка або код у запиті. Але варто зазначити, що ASP.NET Web API не використовує функцію перевірки запитів для очищення введених користувачами даних за замовчуванням, як це є в ASP.NET MVC, тому розробник має додати цю перевірку самостійно [4].

Висновки. У доповіді наведені можливі підходи щодо протидії XSS атакам при використанні технології ASP.NET.

Список літератури

1. Prevent Cross-Site Scripting (XSS) in ASP.NET Core. *Microsoft*. URL – https://docs.microsoft.com/en-us/aspnet/core/security/cross-site-scripting?view=aspnetcore-6.0 (дата звернення: 24.06.2022);
2. Cross Site Scripting Prevention Cheat Sheet. *OWASP*. URL – https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html (дата звернення: 24.06.2022);
3. Cross Site Scripting Prevention Cheat Sheet. *OWASP*. URL – https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html (дата звернення: 24.06.2022);
4. ASP.NET Request Validation. *OWASP*. URL – https://owasp.org/www-community/ASP-NET_Request_Validation (дата звернення: 24.06.2022).

Відомості про авторів

Чучин Віталій Вадимович, студент кафедри комп'ютерних систем, мереж і кібербезпеки, м.т. 099-093-55-43, v.chuchin@student.csn.khai.edu
Пєвнєв Володимир Яковлевич, професор кафедри комп'ютерних систем, мереж і кібербезпеки, д.т.н., доцент, v.pevnev@csn.khai.edu

Секція 1

АНАЛІЗ МЕТОДІВ ПРОТИДІЇ АВТОМАТИЗОВАНОМУ СКАНУВАННЮ ВЕБ-САЙТІВ

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

Актуальність. З кожним роком кількість відвідувачів Інтернет ресурсів невпинно зростає. Однією з причин є доступність інформаційних технологій звичайним користувачам та зниження плати за доступ до мережі Інтернет. Згідно даних аналітичної компанії Similarweb, у вересні 2022 року найпопулярнішими сайтами серед українців є Google, YouTube, Facebook, Ukr.net, Sinoptik, OLX, Deepstatemap та Wikipedia [1]. Згідно цих даних видно, що серед користувачів популярністю користується розважальний контент, портали новин, електрона пошта, соціальні мережі та торгівельні майданчики. Збільшення кількості користувачів сайту призводить до появи автоматизованих систем, які мають на меті злочинні наміри. Такі боти можуть мати різні цілі, а саме: збирання інформації про товари (для перепродажу їх по більшій ціні), сканування вразливостей сайту (не завжди з метою нанесення збитків, також для перевірки захищеності) або генерація спам повідомлень (поширення рекламної інформації у коментарях сайту). Виходячи з цього стає зрозумілим, що сайти повинні мати не тільки потужні сервери для безперервної роботи, а також механізми, які здатні протидіяти системам автоматизованого сканування.

Мета роботи полягає у аналізі методів протидії автоматизованому скануванню веб-сайтів.

Основні положення. Автоматизовані системи аналізу сайтів поділяються на 2 категорії: ті, які допомагають власнику сайту та ті, які наносять шкоду. До корисних відносяться індексатори пошукових систем, які аналізують веб-ресурси з метою додавання їх до результатів пошуку користувачів [2]. До шкідливих відносяться боти, метою яких можуть бути: поширення реклами у коментарях, сканування товарів з метою продажу їх по вищій ціні або сканування вразливостей сайту. Важливо зазначити, що не існує чітких меж між корисними та шкідливими ботами. Таким чином пентестингові боти можуть одночасно відноситися до обидвох категорій, в залежності від того, хто їх використовує (власник сайту для перевірки рівня захищеності або зловмисник з метою нанесення шкоди). Окрім прямого нанесення збитків веб-ресурсу, боти також створюють зайве навантаження на сервери. Це може призвести як до уповільнення завантаження сайту, так і до повної відсутності доступу до нього реальними користувачами.

Згідно даних компанії Imperva, яка займається розробкою корпоративного програмного забезпечення у сфері інформаційної безпеки,

кількість мережевого трафіку у 2021 році, який припадає на мережевих ботів складає 42,6%, що на 1,5% більше порівняно з 2020 роком [3]. Окрім цього, найпопулярнішими сферами застосування Інтернет ботів є спортивні сайти, сайти з азартними іграми та ресурси туристичних агенств.

На сьогоднішній день, для захисту веб-сайту від мережевих ботів існує багато методів та готових рішень. Серед них варто виділити: чорні списки (містять в собі IP адреси хостів, які треба заблокувати), сигнатурне блокування (блокування ботів на основі сигнатур у HTTP запитах), використання WAF (сукупність моніторів та фільтрів, призначених для виявлення та блокування мережевих атак на прикладному рівні) та використання технології Captcha (автоматизований тест Тюрінга, який має на меті розрізнення комп'ютерів та людей) [4].

Висновки. Під час аналізу даних компанії Imperva було виявлено, що найчастіше системи автоматизованого сканування мають на меті заробіток для їх власників. Таким чином, наприклад, автоматичне сканування облікових записів сайту онлайн казино дозволяє викрасти гроші користувачів шляхом перехоплення даних акаунту. Окрім цього, виходячи з розглянутої статистики, з кожним роком кількість трафіку, який генерується шкідливими мережевими ботами лише збільшується. Але, нажаль не існує єдиного та універсального рішення для боротьби з автоматизованими системами. Це зумовлено тим, що під час вибору методів захисту треба враховувати тип мережевих ботів, яким треба протидіяти. Таким чином для боротьби з ботами, які маскуються під користувачів треба використовувати Captcha, проти спамерів – чорні списки IP адрес, а для боротьби з сканерами вразливостей доцільніше використовувати WAF.

Список літератури

1. Рейтинг топ-сайтів. URL: https://www.similarweb.com/ru/top-websites/ukraine/ (дата звернення: 19.10.2022);
2. Google Indexing API. URL: https://developers.google.com/search/apis/indexing-api/v3/quickstart (дата звернення: 20.10.2022);
3. Bad Bot Report 2021: The Pandemic of the Internet. URL – https://www.imperva.com/blog/bad-bot-report-2021-the-pandemic-of-the-internet/ (дата звернення: 20.10.2022);
4. V. Pevnev, O. Popovichenko, and Y. Tsokota, "WEB APPLICATION PROTECTION TECHNOLOGIES", A.I.S., vol. 4, no. 1, pp. 119–123, Mar. 2020.

Відомості про авторів

Шипунов Микита Юрійович, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, м.т. 0980344388, m.shypunov@student.csn.khai.edu
Цуранов Михайло Віталійович, дослідник у сфері ІБ

Секція 1

АНАЛІЗ СТАНУ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ НА ДЕРЖАВНИХ САЙТАХ

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

Актуальність. На сьогодні Україна продовжує впроваджувати цифровізацію держави. Все більш громадян отримують змогу звертатися до різних державних установ за допомогою мережі інтернет. Чисельність цих установ збільшується. Через ріст онлайн послуг, виникає питання захисту персональних даних громадян, їх ідентифікація та зберігання даних. Захист персональних даних у державних реєстрах є вимогою законів і нормативно-правових документів [1,2]. Витік персональних даних громадян підриває їх довіру до можливостей використання цих сервісів і має негативні наслідки щодо захисту конфіденційної інформації.

Мета. Провести аналіз можливих загроз щодо захисту персональних даних, які використовуються в додатку «Дія».

Основні положення. Дія (скорочення від «Держава і я») — мобільний застосунок, вебпортал і бренд цифрової держави в Україні, розроблений Міністерством цифрової трансформації України. Дію було вперше презентовано у 2019 році й офіційно запущено у 2020 році [3].

Застосунок «Дія» дає змогу зберігати водійське посвідчення, внутрішній і закордонний паспорти й інші документи в смартфоні, а також передавати їхні копії при отриманні банківських чи поштових послуг, заселенні в готель і в інших життєвих ситуаціях.

Також через «Дію» (застосунок і/або портал) можна отримати такі державні послуги як єМалятко (комплексна послуга при народженні дитини), зареєструвати бізнес і ФОП онлайн, сплачувати податки й подавати декларації, підписувати будь-які документи, змінювати місце реєстрації тощо. До 2024 року планується перевести 100 % державних послуг у Дію [3].

Аналіз стану захисту персональних даних на державних сайтах напряму має зв'язок до Дії. Для реалізації плану переведення 100% державних послуг у Дію до 2024 року необхідно чітко визначити дії щодо захисту інформації, а саме забезпечення цілісності, доступності, конфіденційності та спостережності.

В доповіді наведено аналіз існуючих порушень в функціонуванні державних послуг «Дія». Ці порушення виникають під час роботи сервісу та призводять до відтоку конфіденційної інформації. Наслідком чого можуть бути незаконне отримання фінансової допомоги, кредитів, які

оформляються на сторонніх осіб. Має «Дія» проблеми з програмним забезпеченням. Наприклад програмне забезпечення не підтримує старих версій ОС Android і не встановлюється на смартфони з відкритими для користувача root-правами. Проаналізувавши існуючі рішення, можна дати оцінку Дії з точки зору безпеки та, за потреби, визначити кращі рішення для усунення можливих загроз у безпеці.

Висновки. Персональні дані на державних сайтах – це будь-які дані з державних реєстрів. Додаток «Дія» має за мету надати зручний доступ до всіх персональних даних користувачеві. Захист таких даних повинен включати: цілісність, щоб дані не можна було б змінити сторонніми особами; доступність, щоб тільки володілець або передбачені законодавством особи мали доступ до даних; конфіденційність, щоб ніхто сторонній не мав доступу до даних.

С точки зору фахівців з кібербезпеки [4] у додатку «Дія » існує можливість перехоплення та накопичення персональних даних під час перевірки е-документів, можливість необмеженого клонування документів, можливість слідкувати за користувачами, непрозорість порядку використовування іншими організаціями, ризики дистанційного несанкціонованого проникнення до смартфону («зламу») зі встановленим додатком. неможливість самостійно заблокувати свій акаунт в «Дії».

Список літератури

1. Закон України «Про інформацію» // Відомості Верховної Ради України (ВВР), 1992, № 48, ст.650;
2. Закон України «Про електронні документи та електронний документообіг» // Відомості Верховної Ради України (ВВР), 2003, № 36, ст.275;
3. Міністерство та Комітет цифрової трансформації України. *TheDidital*. URL: https://thedigital.gov.ua/projects (дата звернення 20.11.2022);
4. Що не так з додатком Дія? *Spilno*. URL https://spilno.org/article/scho-ne-tak-z-diyeyu (дата звернення 20.11.2022).

Відомості про авторів

Шумара Лев Романович, студент кафедри комп'ютерних систем, мереж і кібербезпеки, м.т. 0990935543, l.shumara@student.csn.khai.edu
Пєвнєв Володимир Яковлевич, професор кафедри комп'ютерних систем, мереж і кібербезпеки, д.т.н., доцент, v.pevnev@csn.khai.edu

Section 1

RESEARCH OF SECURITY OF INFRASTRUCTURE AS A CODE TECHNOLOGIES

Yudin O.V.
National Aerospace University «Kharkiv Aviation Institute»
Scientific adviser Tsuranov M.V.

Relevance. With the **growth** of companies providing cloud computing services, tools for definition Infrastructure as a Code (IaC) are gaining popularity rapidly. Modern business is trying to reduce the amount of time spent on deploying applications. After describing the desired project infrastructure, the developer is given the possibility to quickly deploy the environment without performing unnecessary operations with the New IaC approach.

According to statistics, 63% of IT companies partially use the approach of describing infrastructure with code, and 7% of all IT companies completely use this approach in their projects [1]. It is given significant advantages in convenience, speed, reliability, and standardization of the project.

However, not all specialists working with this technology check the security of the described architecture in practice. According to Snyk estimates, 38% of companies do not check the security of their infrastructure during the process of code delivery from the remote repository to the server that is responsible for the health CI/CD of applications, and also do not think about checking static vulnerability scanners [1].

The purpose of this work is to investigate the mechanisms of protection confidentiality of cloud infrastructure, in case of vulnerabilities that arise from an incorrect description of the infrastructure code.

There are a plurality number of threats aimed at revealing the confidential information of a project described using IaC, such as architecture data, passwords, keys, etc.

According to OWASP, the threat disclosure of confidential information occurs in 19.84% of projects [2]. In the OWASP list, the aforementioned threat is called differently but is directly related to it, namely A05:2021 - Security Misconfiguration. This is on account of the fact that in a test project it is much more convenient to immediately place the credentials in the code.

The problem is that the developer may not remember to delete sensitive data after performing certain tasks when changes need to be submitted to the version control system. Such inattention is observed by 24% of cloud infrastructure developers and can completely compromise the customer's company, because

initially, before the targeted attack, the attacker will conduct an OSINT investigation of the victim [1].

Principal provisions. To timely validation the code for the presence of sensitive information, as well as validation for vulnerabilities inside the software libraries used, it is possible to use special static scanners that will detect vulnerabilities accidentally or intentionally embedded in the source code [3]. There are many vulnerability scanners in the community for different tasks. In most cases, the customer uses scanners such as Snyk, Clair, and Trivy.

It is also worth noting that many version control systems already have mechanisms for checking the code being loaded into the repository for the presence of authorization keys. However, such solutions can only detect and exclude those keys that are created directly by the version control system, which is not enough to ensure the security of the project infrastructure.

Conclusions. The Infrastructure as a Code technology helps flexibly configure and administrate the required project architecture. However, there are abundant threats, part of which are not obvious and need exploring. One of the non-obvious threats is exposing sensitive information from the variable by intercepting network traffic over an unsecured network. The thesis considers the main threats and vulnerabilities in describing IaC technology, which could be profitable and exploited to attack privacy.

List of references

1. Snyk research report, Infrastructure as Code Security Insights. – Snyk. – February 2021.
2. A05:2021 – Security Misconfiguration. OWASP Top 10:2021. URL – https://owasp.org/Top10/A05_2021-Security_Misconfiguration/ (дата звернення: 21.06.2022).
3. Савчук В. О., Цуранов М. В. Аналіз засобів безпеки хмарних платформ. У кн.: Проблеми інформатизації: тези доп. 8-ї міжнар. наук.-техн. конф., 26-27 листопада 2020 р., м. Черкаси, м. Харків, м. Баку, м. Бельсько-Бяла : [у 3 т.]. Т. 1 / Черк. держ. технолог. ун-т [та ін.]. – Харків : Петров В. В., 2020. – 83 с.

Information about the authors

Yudin Oles Viktorovich, a master`s student from the Department of Computer Systems, Networks and Cybersecurity, phone number 066-554-94-07, o.yudin@student.csn.khai.edu
Tsuranov Mikhail Vitalievich, information security researcher and advisor

ТЕЗИ ДОПОВІДЕЙ

Секція 2. Функційна безпека

Секція 2

МЕТОД ЗАХИСТУ КАНАЛУ ЗВ'ЯЗКУ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ ВІД АТАК ТИПУ GPS-СПУФІНГ

Аністратенко В. В.
Національний авіаційний університет, м. Київ
Науковий керівник Петренко А. Б.

Актуальність. В умовах сьогодення глобальна система позиціонування (GPS) використовується для навігації пристроїв по всьому світу, зокрема, безпілотних літальних апаратів. Пристрої, які працюють за допомогою GPS, незважаючи на великі можливості, вразливі до навмисних і ненавмисних атак, в тому числі, атак з підміною та викраденням даних. Зокрема, набирають популярності атаки типу GPS-спуфінгу на БПЛА, через що відбувається втрата інформації і навіть непомітне для користувачів БПЛА викрадення пристрою [1]. На основі цього, актуальності набуває проблема захисту БПЛА від спуфінг-атак в умовах мирного та воєнного стану.

Мета. Метою роботи є вдосконалення методу захисту від атак на синхронізацію часу через GPS-спуфінг за допомогою оцінки прогнозованого положення, швидкості і часу.

Основні положення. Типові GPS-приймачі використовують метод найменших квадратів (МНК) для розв'язання рівняння вимірювання псевдодальності ρ_n і оцінки значення псевдодальностей, які пов'язані з відносною швидкістю супутника v_n і швидкістю БПЛА v_u, на основі яких надається оцінка місцезнаходження, швидкості, зсуву та дрейфу годинника БПЛА. Для додаткового вивчення послідовного характеру оцінок використовується динамічна модель випадкових величин [2]. Динамічна система та вимірювання рівнянь є основою для оцінювання положення, швидкості і часу БПЛА.

Хоча атаки на синхронізацію часу мають різні фізичні механізми, вони проявляються як атаки на псевдодальності і значення псевдодальностей.

Важливо виділити також типи спуфінг-атак, які розглядаються далі в роботі:

– Атака типу I: Зловмисник маніпулює автентичним сигналом таким чином, що зсув відбуваються різко, за дуже короткий час.

– Атака типу II: Підробник поступово маніпулює автентичними сигналами і змінює зсув годинника в часі.

Ці атаки не змінюють положення або швидкості БПЛА, а лише зміщують тактовий зсув і дрейф тактової частоти годинника. Коли зсув та дрейф коригуються за допомогою оціненої атаки, розрідженість щодо загальної варіації з'являється для наступних часових моментів. У ці моменти часу вплив виявляється більш помітним, і, по суті, низька динамічна поведінка впливу посилюється, що полегшує виявлення атаки і також буде перевірено чисельно. У вікні спостереження довжиною L оцінка атаки $\hat{s}$ використовується для компенсації впливу атаки на зсув тактового генератора та дрейф тактового генератора. Після того, як БПЛА зібрав L вимірювань, розв'язується рівняння підсумування вимірювань та оцінки станів сигналу. На основі оціненої атаки, зсув та дрейф тактового генератора очищується за допомогою модифікації зсуву та дрейфу шляхом віднімання кумулятивного результату атак.

Висновки. Вдосконалений метод захисту зводиться до розв'язання простого квадратичного рівняння з невеликою кількістю змінних і, таким чином, запропоноване рішення може бути впроваджене в приймач БПЛА з можливістю виконання в реальному часі, що є істотною перевагою при захисті БПЛА від високоінтелектуальних атак спуферів.

Список літератури

1. Д. Г. Волошин, С. С. Бульба. Інтелектуальний метод визначення спуфінгу БПЛА.: Advanced Information Systems. 2022. Vol. 6, No. 1. Національний технічний університет “Харківський політехнічний інститут”, Харків, Україна, 2022;
2. B. W. Parkinson, J. J. Spilker, P. Axelrad, and P. Enge, Global Positioning System: Theory and Applications, vol. I. Washington, DC, USA: Amer. Inst. Aeronaut. Astronaut., 1996.

Відомості про авторів

Аністратенко Вікторія Віталіївна, магістрант кафедри комп’ютеризованих систем захисту інформації, м.т. 099-775-63-61, 5265181@stud.nau.edu.ua
Петренко Андрій Борисович, доцент кафедри комп’ютеризованих систем захисту інформації, к.т.н., доцент, andrii.petrenko@npp.nau.edu.ua

Секція 2

ТЕСТУВАННЯ НА ПРОНИКНЕННЯ ДЛЯ ОЦІНКИ КІБЕРБЕЗПЕКИ ПРОМИСЛОВИХ РОБОТИЗОВАНИХ СИСТЕМ: ВИКЛИКИ ТА РІШЕННЯ

Абакумов А.І.
Національний аерокосмічний університет ім. М.Є Жуковського «Харківський авіаційний інститут»
Науковий керівник Харченко В.С.

Актуальність. Інциденти, спричинені атаками на промислові роботизовані системи (РС) впровдовж останніх років [1,2], свідчать про зростання кіберзагроз і відповідних відмов компонентів РС. Затримки в розробленні та впровадженні стандартів і інструментів для оцінювання та пом'якшення загроз, а також забезпечення кібербезпеки (КБ) РС в цілому, посилюють їх вразливість до кібератак, особливо з огляду на інтеграції з інтернетом речей і хмарними сервісами [3] через великі ризики вторгнення. Брак методів та інструментів оцінювання КБ РС обумовлює наступне [1]:

- відмовлення від впровадження тестування на проникнення (ТнП) може призвести до порушення кібербезпеки розгорнутих програм, включаючи різні компоненти РС;
- відсутність патчів безпеки збільшує ймовірність зловмисних атак, зокрема, викрадення конфіденційних даних, віддалений доступ і руткіт.

Таким чином, для забезпечення ринкової конкурентоспроможності впроваджуваних послуг з урахуванням принципу «нульового інжинірингу» та мінімізації ризиків безпеки, які є невід'ємною частиною впровадження «нульового бізнес-ризику», необхідно надати надійні та зрозумілі гарантії безпеки під час експлуатації систем. Це вимагає поєднання аналітичних та формальних методів, зокрема, IMECA-аналізу (Intrusion Modes and Criticality Analysis) та ТнП з урахуванням специфіки архітектури РС.

Аналіз інформаційних джерел. Автори [1-3] аналізують загрози, вразливості та атаки РС, але не формулють системні вимоги щодо впровадження ТнП спільно з іншими методами. У [4] розроблено метод ТнП, адаптований для інтернету речей шляхом поєднання методоів ТнП та IMECA-аналізу. З огляду на аналіз публікацій, об'єктивними є висновки: по-перше, про відсутність методу ТнП з урахуванням специфікі промислових РС і його недосконаліть для індустріального інтеренту речей; по-друге, необхідності більш системного погляду на задачі ТнП у поєднанні з іншими методами задля обєктивного оцінювання кібербезпеки і функційної безпечності РС.

Метою досліджень є підвищення достовірної оцінки ризиків і надання надійних гарантій функційної та кібербезпеки впродовж експлуатації РС шляхом поєднання методів IMECA та ТнП.

Задачі, які розвязуються задля досягненя мети досліджень**,** полягають у проведенні аналізу інформації про вразливості РС та напрями атак, описі процесу ТнП та IMECA за допомогою функціональної моделі IDEF, наданні прикладу використання IMECA для аналізу вразливостей РС та оцінки ризику атак, а також обґрунтуванні напрямів майбутніх досліджень.

Висновки. У даній роботі зроблений перший крок вирішення проблеми відсутності методів ТнП, адаптованих до специфіки РС, а саме розроблена дворівнева IDEF модель процесу проведення ТнП та детально розглянуто етап впровадження IMECA для аналізу вразливостей РС та оцінювання ризиків успішних кібератак. Подальші дослідження необхідно проводити за напрямом практичного підтвердження дієвості запропонованого методу за допомогою використання реальної РС або її емулятора. Цей процес пропонується розділити на етапи, які дозволяють розглянути окремі компоненти РС, її інфраструктурну частину та зробити наступний крок щодо аналізу КБ і функційної безпечності коботів.

Список літератури

1. *Yaacoub P.A., Noura H.N., Salman O.* Robotics cyber security: vulnerabilities, attacks, countermeasures, and recommendations // International Journal of Information Security, Vol. 21, PP. 115–158, Режим доступу: https://doi.org/10.1007/s10207-021-00545-8

2. *Pu H., He L., Cheng P., Sun M., Chen J.* Security of Industrial Robots: Vulnerabilities, Attacks, and Mitigations // IEEE Network, Режим доступу: https://doi.org/10.1109/MNET.116.2200034

3. *Bhardwaj A., Avasthi V., Goundar S.* Cyber security attacks on robotic platforms // Network Security, Vol. 2019, No. 10, PP. 13–19, Режим доступу: https://doi.org/10.1016/S1353-4858(19)30122-9

4. *Абакумов А.І., Харченко В.С.* Тестування на проникнення систем Інтернету речей: кіберзагрози, методи та етапи // Electronic Modeling, Vol. 44, No. 4, PP. 79–104, Режим доступу: https://doi.org/10.15407/emodel.44.04.079

Відомості про авторів

Абакумов Артем Ігорович, аспірант кафедри комп'ютерних систем, мереж і кібербезпеки, м.т. 095-024-79-98, a.i.abakumov@csn.khai.edu

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

Секція 2

БЕЗПЕКА API ІНТЕРФЕЙСУ

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

Актуальність. API працюють як backend частина багатьох сучасних веб-додатків, утому числі додатків у банківській сфері, сфері інтернет-платежів та у медичній сфері. Тому дуже важливо захистити конфіденційні дані, які вони передають завдяки API інтерфейсу.

API-системи стрімко розвиваються, так каталог API, сервісу ProgrammableWeb, у період з 2016 року по 2018 рік виріс на 35% в цілому, і на 98% у фінансовій сфері [1]. Все більше компаній роблять сої API публічно відкритими, ріст трафіку клієнтських запитів до API виріс на 168% у порівнянні з минулим 2021 роком [2]. Але з зі зростанням кількості API викликів зростає і інтерес зловмисників до цього вектору атаки, так зловмисний трафік виріс на 117% за аналогічний період, і наразі становить 2,1% від загальної кількості трафіку API запитів [2].

З сучасних загроз можна відмітити вразливості в Tesla Backup Gateway APIs(які відповідають за електросистему господарства з сонячними панелями), через які у публічному доступі опинилися дані про споживання та виробництво енергії (ім'я, країна та штат, назва комунальної компанії тощо). Також можна відмітити атаку на API сайту findadoctor.com, через яку зловмисники отримали особисті дані 1,41 млн американських лікарів [3].

Метою даної роботи є підвищення ефективності методів боротьби з загрозами API інтерфейсу.

Основні положення. Серед найбільш актуальних вразливостей API можна виділити [4]:

− некоректна автентифікація користувачів - механізми автентифікації часто функціонують некоректно, дозволяючи зловмисникам компрометувати дані автентифікації або експлуатувати недосконалості в реалізації механізму з метою тимчасового чи постійного присвоєння облікового запису користувача;

− відсутність обмежень на кількість запитів та споживання ресурсів - це може вплинути на продуктивність API, що призводить до відмови в обслуговуванні (DoS);

− масове перепризначення параметрів - присвоєння даних, що надійшли від користувача, наприклад у форматі JSON, моделі даних без належної фільтрації параметрів на базі білого списку зазвичай призводить до масового перепризначення параметрів. Зловмисник може змінити властивості об'єктів, до яких не повинен мати доступ.

Для вирішення цих проблем ми можемо використовувати наступні рекомендації [5]: автентифікація та авторизацію варто використовувати на основі токенів, а не прямих логінів/паролів; варто використовувати https протокол з шифруванням TLS, замість htttp протоколу; використовувати обмеження швидкості та регулювання кількості запитів від одного користувача за одиницю часу.

Висновки. API інтерфейс дуже швидко розвивається за останні роки, тому він все частіше стає ціллю атак зловмисників. Для запобігання вразливостей інтерфейсу варто їх визначити та знати, також треба враховувати і додатково до них вхідних вразливостей форматів даних, таких найбільш розповсюджених форматів передачі даних в API як JSON та XML. Тож для боротьби з вразливостями API інтерфейсу варто використовувати ряд рекомендацій, таких як додатково встановлювати на веб-сервер автоматичні системи захисту з фільтрами запитів, а також розвивати захист на рівні архітектури і функціонуванні системи в цілому.

Список літератури

1. Financial APIs continue to see big growth. ProgrammableWeb. URL – www.programmableweb.com/news/financial-apis-continue-to-see-big-growth/research/2020/08/26 (дата звернення: 09.11.2022);
2. API Security Trends. *Salt*. URL – salt.security/api-security-trends (дата звернення: 09.11.2022);
3. Data at Risk: API Vulnerabilities. *10Guards*. URL – https://10guards.com/en/articles/data-at-risk-api-vulnerabilities/ (дата звернення: 09.11.2022);
4. OWASP API Security Project. *OWASP*. URL – https://owasp.org/www-project-api-security (дата звернення: 10.11.2022);
5. API Security: The Complete Guide to Threats, Methods & Tools. *Bright*. URL – brightsec.com/blog/api-security/#rest-api-vs-soap-security (дата звернення: 10.11.2022).

Відомості про авторів

Єлюхін Роман Валерійович, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, м.т. 068-756-69-94, r.yeliukhin@student.csn.khai.edu
Землянко Георгій Андрійович, асистент кафедри комп'ютерних систем, мереж і кібербезпеки, g.zemlynko@csn.khai.edu

Секція 2

ПРАВОВІ ТА ТЕХНІЧНІ АСПЕКТИ КІБЕРБЕЗПЕКИ В СИСТЕМАХ «ІНДУСТРІЇ 4.0»

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

Актуальність. Із збільшенням кількості виробників і різноманітності продукції, що виходить на світовий ринок, ростуть витрати на товарообіг між компаніями з метою створення кінцевого продукту. Тому виникає потреба у спрощенні комунікацій, мінімізації витрат і збільшення кількості виробництв. Це тягне за собою виникнення нових технологій і підходів до їх застосування. Четверта індустріальна революція (Індустрія 4.0) - перехід на повністю автоматизоване цифрове виробництво, яке керується інтелектуальними системами в режимі реального часу в постійній взаємодії із зовнішнім середовищем, що виходить за межі одного підприємства, з перспективою об'єднання в глобальну промислову мережу «Речей і послуг».

Метою даної роботи є дослідження правових та технічних аспектів кібербезпеки в системах «ІНДУСТРІЇ 4.0».

Основні положення. Початок «Індустрія 4.0» взяла в концепції розумної промисловості, яка була описана німецьким урядом для переходу на новий рівень у виробництві і підтримці конкурентної спроможності продукції.

Висновки. Як підсумок, варто перерахувати велику кількість переваг від інновацій, що вводяться разом з «Індустрія 4.0». Такі як підйом економіки, використання роботизованої техніки в місцях небезпечних для життя людини, зменшення людського фактора у вирішенні виробничих завдань за рахунок штучного інтелекту і системи аналізу великих даних. Але на жаль, всі вони супроводжуються критичними для всієї ідеї четвертої революції недоліками. Такими як недбалість при розробці алгоритму, можливі помилки при розробці та відсутність юридичного покарання за критичні збої в процесі використання. Також сучасні методи кібербезпеки не пристосовані до захисту ділянок виробництва з відкритим зв'язком із зовнішнім світом. Відсутність загальних стандартів і правил з налаштування та адміністрування подібного роду інфраструктури, може уповільнити удосконалення методів захисту підприємств в рамках «Індустрії 4.0». Основні принципи четвертої революції можуть привести до витоку конфіденційних даних і розголошення виробничої таємниці. Можливий крах четвертої промислової революції змусить світ повернутися до системи, заснованої на результатах третьої революції. Інакше, дії, вжиті з метою зміцнення економіки і підняття рівня життя, приведуть до її критичних пошкоджень або знищать повністю.

Список літератури

1. Лоцман Є. Р. Методи деанонимізації як засіб виявлення правопорушників. Протидія кіберзагрозам та торгівлі людьми: тези доп., м. Харків, 26 листоп. 2019 р. ХНУВС, 2019. С. 259 – 261;
2. Лоцман Є. Р. Аналіз методів побудови приватної хмари. Проблеми інформатизації: тези доп., м. Харків, 26-27 листопада. 2020 р. ХПІ, 2020. С. 59;
3. Лоцман Є. Р. Аналіз механізмів забезпечення кібербезпеки методології DevOps. Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління: тези доп., м. Харків, 9-10 квітня. 2020 р. ХПІ, 2020. С. 59.

Відомості про авторів

Лоцман Євгеній Романовіч, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, м.т. 097-546-49-43, e.lotsman@student.csn.khai.edu
Цуранов Михайло Віталійович, дослідник у сфері ІБ

Секція 2

ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ АВТОНОМНОГО ЕЛЕКТРОГЕНЕРУЮЧОГО ОБ'ЄКТУ

Моїсеєнко Д.Д.
Національний аерокосмічний університет ім. М.Є Жуковського
«Харківський авіаційний інститут»
Науковий керівник Желтухін О.В.

Актуальність. Існуючі системи охоронної сигналізації мають недостатні функціональні можливості або ж, надмірно велику вартість.

Метою є потреба в розробці недорогої та ефективної системи охоронної сигналізації, яка в той же час матиме достатню функціональну насиченість, надійність щоб без шкоди виконувати свої функції – запобігти псуванню майна

Основні положення. У світі вчені завдання розпізнавання типу живих істот намагаються здійснити у різний спосіб. Так, наприклад, Доктор Серж Віч розробив систему моніторингу за допомогою інфрачервоних камер, встановлених на безпілотниках. Випробування у Честерському зоопарку та сафарі-парку Ноуслі показали, що система може розпізнавати тварин навіть через зарості.

Виходячи з досліджень проведених Вагнером Торндайком, Гаггерті, Уатсоном, можна зробити висновок, що можлива організація атак на проникнення на підконтрольну територію з використанням спеціально дресованих тварин для присипання пильності охоронної системи та організації маси хибних спрацьовувань, для залучення на їх відпрацювання персоналу. Мета цих атак - відвернути увагу від реального проникнення на підконтрольний об'єкт зі злими намірами.

Центральне місце посідає завдання розпізнавання образів. Рішення її технічними засобами може бути здійснено шляхом моделювання операцій, що виконуються живими організмами у процесі комунікації та сприйняття навколишнього світу. Ці здібності досить добре вивчені на різних тваринах (кажани, деякі примати). Однак найбільш природно покласти в основу моделі розпізнавання здатності людини та її реакції на навколишню дійсність.

Розпізнавання образів є сукупність методів та засобів, що дозволяють, щонайменше, досягти, а якщо можливо, то й перевершити природні засоби сприйняття та аналізу навколишнього світу живими істотами..[2]

Висновок. На жаль, не існує загальноприйнятого набору візуальних символів, які необхідні та достатні для опису зображення. Відсутність набору єдиних візуальних символів створює певні труднощі під час аналізу зображень. По-перше, є проблема відбору, суть якої у тому, щоб визначити, які символи необхідно сформувати з ознак зображення на вирішення конкретних завдань аналізу зображень. Крім того, є проблема визначення необхідної точності при формуванні символів [3].

Список літератури

1. За рідкісними тваринами спостерігають за допомогою методів астрономії . Naked Science. URL – https://naked-science.ru/article/sci/za-redkimi-vidami-zhivotny (дата звернення 22.11.2022);
2. Тропченко А.Ю. Методы вторичной обработки и распознавания зображений. Учебное пособие. – СПб: СПбГУ ИТМО, 2012. – 52 с.;
3. Ветров Д. П., Кропотов Д. А. Алгоритм множественного трекинга лабораторных животных. Москва, ВМиК МГУ, Вычислительный Центр РАН.

Відомості про авторів

Моїсеєнко Денис Дмитрович, студент кафедри комп'ютерних систем, мереж ікібербезпеки, м.т. 0677179894, d.moiseienko@student.csn.khai.edu
Желтухін Олександр Васильович, старший викладач кафедри комп'ютерних систем, мереж і кібербезпеки, м.т. 097-715-26-42 A.Zheltukhin@csn.khai.edu

Секція 2

ЗБИРАННЯ ТА АНАЛІЗ ІНФОРМАЦІЇ ПРО ВРАЗЛИВОСТІ КОМПОНЕНТІВ І СИСТЕМ ШТУЧНОГО ІНТЕЛЕКТУ З ВИКОРИСТАННЯМ ЗАСОБІВ BIG DATA

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

Актуальність. Зростання використання систем штучного інтелекту (СШІ) в різних сферах індустрії транспорту, оборони, медицини супроводжується із збільшенням загроз, зростанням кількості і видів кібератак [1]. Враховуючи поширення цих систем в критичних доменах, важливим є забезпечення їх захищеності, що в свою чергу, обумовлює актуальність удосконалення науково обгрунтованих методів і засобів об'єктивного оцінювання кіберзахисту цих систем. Беручи до уваги те, що якість цього процесу залежить від повноти і достовірності інформації про вразливості і загрози системам, перш за все, важливо проаналізувати існуючі методи і засоби збирання і оброблення такої інформації. Слід підкреслити, що інформація про вразлвості СШІ не є достатньо систематизованою і міститься в джерелах різного типу, а саме базах даних вразливостей, наукових статтях, технічних звітах, що потребує використання сучасних технологій Big Data. Тому актуальними є дослідження і розробки науково-технологічного інструментарію для збору, аналізу і представлення в зручному вигляді даних про вразливості СШІ.

Аналіз інформаційних джерел. У роботі [2] розроблена метамодель, яка складається з компонентів атак, методів та інструментів пом’якшення наслідків. Модель наочно описує зв’язки понять за напрямом кібербезпеки СШІ, але не є повною. Дослідження оцінки загроз у машинному навчанні [3] є певним енциклопедичним документом, але йому не вистачає деталізації щодо СШІ, зокрема, використання ШІ як сервісу. Отже, з огляду на аналіз [1-3] та інших публікацій і розробок об’єктивним є висновок про відсутність досконалих концептуальних моделей і методів збору інформації про вразливості для оцінювання кібербезпеки СШІ.

Метою досліджень є розроблення методу опису процесів збору і аналізу вразливостей СШІ на базі відомої моделі IDEF (Integrated Definition).

Задачі роботи полягають у проведенні критичного аналізу існуючих методів та засобів збору інформації про вразливості для оцінювання кібербезпеки СШІ, формуванні підходу до аналізу, розробленні опису процесу збору та аналізу вразливостей СШІ за допомогою моделі IDEF, ілюстрації особливостей цієї моделі для системи NLP як сервісу та обґрунтуванню напрямів майбтніх досліджень.

Підхід. Пропоновний підхід базується на систематизованому зборі, обробці, нормалізації та поєднанні розрізненої інформації з різних сховищ даних, різних за джерелами наповнення, змістом і форматом, для отримання актуальної, структурированої інформації про вразливості СШІ. Функційний модель цих процесів базується на IDEF нотації.

Для реалізації будемо використовувати програмні засоби: Apache Spark, NumPy, Pandas, SciPy, Matplotlib, Scikit-learn, spaCy та BeautifulSoup.

Висновки. В даній роботі зроблений перший крок до подолання проблеми пошуку та представлення інформації про вразливості СШІ, а саме розроблена трирівнева IDEF модель процесу збору та аналізу інформації про вразливості СШІ для оцінювання кібербезпеки з використанням інструментів великих даних. Визначено показники якості, які оцінюють повноту, узгодженість і достовірність інформації. Подальші дослідження будуть присвячені розробленню методів аналізу і оновлення інформації про вразливості компонентів і СШІ як сервісу та визначення їх критичності, а а також оцінювання та забезпечення кібербезпеки СШІ шляхом аналізу наслідків атак на вразливості та вибору контрзаходів.

Список літератури

1. Неретін, О., Харченко, В. (2022). Забезпечення кібербезпеки систем штучного інтелекту: аналіз вразливостей, атак і контрзаходів. Вісник Національного університету «Львівська політехніка». Інформаційні системи та мережі. Випуск 12, 2022.

2. Fazelnia, M., Khokhlov, I., Mirakhorli, M. (2022). Attacks, Defenses, And Tools: A Framework To Facilitate Robust AI/ML Systems [Online]. Available at: https://arxiv.org/abs/2202.09465.

3. Tidjon, L.N., Khomh, F. (2022). Threat Assessment in Machine Learning based Systems [Online]. Available at: https://arxiv.org/abs/2207.00091.

Відомості про авторів

Неретін Олексій Сергійович, аспірант кафедри комп'ютерних систем, мереж і кібербезпеки, м.т. 099-367-00-71, o.s.neretin@csn.khai.edu

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

Секція 2

РОЗРОБКА МЕТОДУ КЛАСИФІКАЦІЇ РІВНЯ НЕБЕЗПЕКИ ВРАЗЛИВОСТЕЙ СУЧАСНИХ РОЗПОДІЛЕНИХ СИСТЕМ

Пономаренко В. В.
Харківський національний університет імені В. Н. Каразіна
Науковий керівник Олійников Р. В.

Актуальність. Забезпечення належної безпеки інформаційних ресурсів є актуальним завданням у кіберпросторі. Згідно зі звітом Cisco Annual Internet Report (AIR), до 2023 року користувачами Інтернету стануть 66% населення Землі. До глобальної мережі будуть підключені більше 28 мільярдів пристроїв [1]. Зазначимо той факт, що на фоні росту кількості інтернет користувачів і підключених пристроїв буде спостерігатися зростання кібератак. Щодня інформаційні ресурси піддаються зазіханням сторонніми особами. Тому, критично важливим є ефективна протидія та мінімізація можливих збитків від потенційних загроз. Одним із способів протидії загрозам є своєчасне виявлення існуючих вразливостей системи. Виникає потреба в обґрунтованому наданні пріоритету виправлення знайденим недолікам, для того щоб першочергово усунути найбільш критичні вразливості. Отже актуальною є розробка методу класифікації рівня небезпеки вразливостей.

Метою досліджень є підвищення безпеки сучасних розподілених систем. Підвищення безпеки системи вимагає використання обґрунтованих засобів та методів пошуку недоліків. Від оперативної ідентифікації загроз суттєво залежить надійність системи.

Основні положення. В роботі запропоновано метод класифікації вразливостей в межах сучасних розподілених систем. Запропонована модель задачі класифікації рівня небезпеки вразливостей та спосіб її реалізації на основі вирішення задачі дискретної оптимізації. Модель задачі вибору оптимального плану усунення найкритичніших серед виявлених вразливостей, яка зведена до формулювання задачі про покриття множини. Задача про покриття множини широко відома в дискретній оптимізації і має численні додатки. Дана задача узагальнює NP-повну задачу про вершинне покриття і тому також є NP-складною. До задачі про покриття можна звести багато завдань дискретної оптимізації: стандартизації, упаковки і розбиття множини, побудови розкладів. Відома також і зворотна зводимість задачі до цих завдань. Постановка задачі полягає в наступному. Для скінченної множини $M = \{m_1, m_2, \dots, m_m\}$ і

деякого скінченного сімейства її підмножин S_j , $j = 1, 2, \dots, n$ потрібно знайти підсімейство $S_j^{`} \subseteq S_j$ з мінімальним набором підмножин $S_j$ таке, що кожен елемент вихідної множини M належить, принаймні, одній із цих підмножин. Знайдені підмножини $S_j^{`}$ зазвичай називають покривними, а сімейство $S_j^{`}$ – найменшим покриттям M. У тому випадку, коли покривним елементам приписана деяка вага, розглядають зважену задачу про покриття, яка передбачає пошук найменшого зваженого покриття M . Коли ж покривні підмножини попарно не перетинаються, задача про найменше покриття трактується як задача про розбиття множини M на найменшу кількість класів [2]. Таким чином, коректне визначення ваги покривних елементів і найменшого покриття визначає оптимальне вирішення завдання забезпечення безпеки інформаційної системи.

Висновки. Запропонований метод дозволяє визначити оптимальний шлях мінімізації ризиків і потенційних збитків за рахунок попередження найбільш критичних вразливостей при використанні обмежених ресурсів, що виділені для цих задач.

Список літератури

1. Cisco Annual Internet Report (2018–2023) White Paper: веб-сайт. URL: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html;

2. Рощин В. О., Боярчук Д. О., Ляшко В. І., Шило П. В. Алгоритм глобального рівноважного пошуку розв'язання задачі про покриття. Наукові записки. Том 163. Комп'ютерні науки. 2014.

Відомості про авторів

Пономаренко Віталій Віталійович, магістрант кафедри безпеки інформаційних систем і технологій, м.т. 095-559-14-04, vponomarenko1712@gmail.com

Олійников Роман Васильович, професор кафедри безпеки інформаційних систем і технологій, д.т.н., доцент, roliynykov@gmail.com

Секція 2

ЗАБЕЗПЕЧЕННЯ КОНТОЛЮ БЕЗПЕЧНОЇ ШВИДКОСТІ АВТОМОБІЛЯ ПІД КЕРУВАННЯМ АВТОПІЛОТОМ

Руднєв М.А.
Національний аерокосмічний університет ім. М.Є Жуковського
«Харківський авіаційний інститут»
Науковий керівник Желтухін О.В.

Актуальність. У світі збільшується кількість автомобілів у користуванні людей. Ще якісь 50 - 60 років тому автомобіль на території України був можна сказати на диво. Міськими вулицями машини проїжджали в кількості одиниць на день. Кількість власних автомобілів у громадян було менше 1 на 1,0тис. населення. Нині ж станом на 2019 рік кількість автомобілів, наприклад, у Сан-Марино становить 1273 на 1000 осіб населення, а в Україні 232 на 1000 осіб, тобто практично в кожній родині є свій персональний автомобіль. У цьому кількість автомобілів зростає і до 2050 року щонайменше подвоїться [1].

Метою представленої роботи є підвищення безпеки шляхом ідентифікації водія для захисту від потрапляння у ДТП, а також перешкода недозволеному водінню. Для досягнення поставленої мети визначено організацію та архітектуру мобільної апаратно-програмної системи для реєстрації та обробки даних водія передачі даних для обмеження максимальної швидкості руху транспортного засобу.

Основні положення. З метою безпеки та комфорту багато автовиробників розробляють системи розпізнавання обличчя водія.

Технологія ідентифікації, розроблена BMW, потрібна, перш за все, для автоматичного підстроювання особистих уподобань автомобіліста.

Розпізнавши свого водія, автомобіль автоматично регулює дзеркала, сидіння та кермо під початкові налаштування, і навіть може увімкнути улюблену радіостанцію. Після випробувань система також зможе регулювати підвіску та інші механічні частини.

Якщо автомобілем користуються кілька людей, наприклад, сімейні пари, їм не доведеться заново підлаштовувати під себе дзеркала, сидіння та різні бортові системи [2].

Компанії Ford та Intel вивчають можливість, при якій автомобілі зможуть впізнавати своїх власників.

Висновки. Факт передачі керування транспортним засобом сторонній особі, яка має право керувати цим типом транспортних засобів, фіксується у фіскальній пам'яті іммобілайзера для можливого вирішення всіх конфліктних ситуацій, що виникли в момент керування автомобілем сторонньою особою, а саме: можливі ДТП та порушення правил дорожнього руху [3].

Список літератури

1. List of countries by vehicles per capita. *Wikipedia*. URL – https://en.wikipedia.org/wiki/List_of_countries_by_vehicles_per_capita (дата звернення 25.11.2022);
2. Деталі налаштування авто при декількох власниках. *Autonews*. URL: https://www.autonews.ru/news/ (дата звернення 25.11.2022);
3. Алгоритм роботи іммобілайзеру автомобілів. *BladeMSP*. URL: Електронний ресурс: http://pr.ua/news.php?new=966 (дата звернення 26.11.2022).

Відомості про авторів

Руднєв Микита Андрійович, магістрант науковець кафедри комп'ютерних систем, мереж і кібербезпеки, м.т. 0675724888, m.rudniev@student.csn.khai.edu
Желтухін Олександр Васильович, старший викладач кафедри комп'ютерних систем, мереж і кібербезпеки, м.т. 097-715-26-42 A.Zheltukhin@csn.khai.edu

Секція 2

ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ РУХУ ТРАНСПОРТНОГО ЗАСОБУ ПІД КЕРУВАННЯМ АВТОПІЛОТУ

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

Актуальність. У світі в даний час здійснюється активний перехід до керування транспортними засобами за допомогою автопілота що виключає повністю, або частково керування людиною. Перехід до автоматичного управління повинен забезпечити комфортніші та безпечніші умови пересування для всіх учасників дорожнього руху. Сьогодні автовиробники та різні незалежні експерти намагаються знайти правильні рішення та зібрати загальну інформацію щодо потреб людей, зацікавлених у купівлі авто. Примітно, що результати опитування, проведеного онлайн-порталом Autoscout24, показали, що з 800 осіб Європи лише 160 віддали перевагу безпеці будь-що інше. Інші всі, як один, заявили, що найважливішим для них в автомобілі є його безпечна функціональна можливість. На друге місце після безпеки 800 європейців з різних соціальних верств суспільства поставили різні мережеві технології, які брали на себе керування автомобілем, даючи одночасно людині комфорт і безпеку. До таких технологічних систем, наприклад, європейці віднесли автоматичне гальмування, яке підключалося тоді, коли попереду розпізнавалася небезпека чи перешкода.[1]

У самій Tesla вже неодноразово підкреслювали, що автопілот є допоміжною функцією і вимагає від водія тримати руки на кермі. Автомобіль постійно нагадує про це і автоматично сповільнюється, доки водій не покладе руки на кермо. Функція повноцінного автопілота, як і раніше, знаходиться в стадії бета-тестування, повідомили в компанії.

Це не перший дорожній інцидент за участю автомобілів Tesla. Найбільш гучний випадок трапився 7 травня у місті Віллістон, штат Флорида. Тоді внаслідок аварії загинув водій Tesla Model S. ДТП сталося, коли вантажна фура повернула ліворуч перед автомобілем на перехресті.

Розслідування торкнулося 25 тис. моделей Model S. [3].

Як видно з усього вищепереліченого сучасні автопілоти автомобілів мають величезну кількість недоліків, непомічають низькі перешкоди, високі просвіти причепів автомобілів, малорозмірні перешкоди, нерухомі припарковані автомобілі з порушенням правил дорожнього руху, автомобілі порушують при русі правила дорожнього руху , не враховують складну траєкторію руху на звивистих ділянках доріг та дорожніх розв'язках довгомірного транспорту, автопоїздів (не враховують можливе винесення причепа, напівпричепа при маневруванні).

У зв'язку з наведеними вище недоліками існуючих систем автопілотів автомобілів. Для парування їх необхідно будувати 3-D модель довколишньої ділянки автомагістралі з розташованими на ній учасниками дорожнього руху.

Список літератури

1. Сучасні системи автопілота для авто, види, принцип та особливості роботи. *Avtopulss*. URL: http://www.avto-pulss.ru/vse-pro-avtomobili/735-city-safety-pedestrian-detection.html (дата звернення: 20.09.2022);
2. Аварія спровокована автопілотом автомобіля Tesla model-S. *Autonews*. URL: https://www.autonews.ru/news/5a67497b9a79471fb87ac6b8 (дата звернення: 21.11.2022).

Відомості про авторів

Русін Данило Олександрович, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, м.т. 066-465-69-31, d.o.rusin@student.csn.khai.edu
Желтухін Олександр Васильович, старший викладач кафедри комп'ютерних систем, мереж і кібербезпеки, a.zheltukhin@csn.khai.edu

Секція 2

ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ДЗЕРКАЛ ГЕЛІОЦЕНТРИЧНОЇ СОНЯЧНОЇ ЕЛЕКТРОУСТАНОВКИ

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

Актуальність. У місцевості, де можливі сильні вітри, тропічні урагани, курячі бурі, торнадо, досить високий сонячний енергетичний потенціал. На жаль великі за площею сонячні дзеркала мають і велику парусність. Відповідно на них діятиме велика сила, здатна пошкодити як саму дзеркало, так і механізм орієнтації. Другий чинник - забруднення самого дзеркала, яке знижує його ефективність, а чищення дзеркал ускладнена тим, що їх встановлюють у малозаселеній місцевості, і виникає потреба у періодичній доставці персоналу обслуговування поля сонячних дзеркал.[1]

Метою є розробка методу захисту дзеркал геліоцентричної сонячної електроустановки.

Основні положення. Правильна орієнтація параболічного дзеркала щодо сонця дозволяє використовувати сонячну енергію з максимальною ефективністю.

Вчені Національної лабораторії Лоуренса Берклі запропонували за допомогою нанотехнологій перетворити на видиме світло інфрачервоне випромінювання сонця, щоб підвищити продуктивність електроустановки.

Слабке місце відкриття полягає в тому, що барвник, як і раніше, дуже нестабільний, і в ході експериментів доводилося використовувати штучне азотне середовище. Завдання вчених полягає в тому, щоб створити захисне покриття для апконвертуючих наночастинок, і тоді можна буде досягти суттєвого підвищення продуктивності сонячних електроустановок.[2]

Як бачимо сучасні розробки, спрямовані на підвищення ефективності сонячних електростанцій. Нові розробки спрямовані на створення електроустановок, здатних утилізувати широкий спектр сонячного випромінювання і втрачати до 50% і більше потужності за рахунок неправильної орієнтації дзеркала та його забрудненості вкрай безглуздо.

Висновок. Тому створення системи управління полем параболічних дзеркал, які дозволять автоматизувати процеси правильної орієнтації поля параболічних дзеркал щодо концентратора сонячної енергії, а також захистити саме дзеркало від зовнішніх природних факторів які можуть

призвести як дзеркало, що само відображає, так і систему орієнтації дзеркала в непридатність.

Жодна з перерахованих вище систем орієнтації не дозволяє захистити дзеркало від впливу зовнішніх природних факторів: дії вітру, абразивів, сильних потоків води, налипання великої маси мокрого снігу та зледеніння. Тому створення цієї системи дуже актуально.

Список літератури

1. В Каліфорнії зобов'яжуть усіх встановити сонячні батареї. *Електротехніка*. URL: https://ecotechnica.com.ua/energy/solntse/3365-v-kalifornii-vse-doma-obyazhut-oborudovat-solnechnymi-batareyami.htm (дата звернення 20.11.2022);

2. Забарвлення ІЧ-випромінювання підвищило продуктивність сонячних батарей. *Електротехніка*. URL: https://ecotechnica.com.ua/energy/solntse/3345-okrashivanie-ik-izlucheniya-povysilo-proizvoditelnost-solnechnykh-batarej.html (дата звернення 21.11.2022).

Відомості про авторів

Слива Віталій Віталійович, студент кафедри комп'ютерних систем, мереж і кібербезпеки, м.т. 099-968-99-62, v.slyva@student.csn.khai.edu

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

Секція 2

ЗАБЕЗПЕЧЕННЯ СТЯГНЕННЯ ПЛАТНІ ЗА КОРИСТУВАННЯ ПЛАТНИМИ АВТОШЛЯХАМИ

Чічіло А.С.
Національний аерокосмічний університет ім. М.Є Жуковського
«Харківський авіаційний інститут»
Науковий керівник Желтухін О.В.

Актуальність. Роль транспорту в усьому світі досить велика. Платні дороги насамперед призначені для розвантаження приміських доріг, а також прискорення руху потоку транспорту, оскільки максимальна швидкість на них досить часто більша, ніж на приміських дорогах, хоча майже завжди є альтернативні безкоштовні дороги. Досить часто дороги включають проїзд тунелями і переправу через міст. Іноді для об'їзду необхідно подолати у рази більший відрізок шляху [1].

Метою роботи є аналіз методів стягнення платні за користування платними дорогами.

Основні положення. У більшості країн є кілька способів оплати, існують такі як: безконтактна (за допомогою спеціального бортового пристрою прикріпленого до автомобіля, зі зниженням швидкості, без зупинки ТЗ), безготівково (за допомогою банківської картки, або спеціальної безконтактної картки, за умови зупинки ТЗ), готівковим розрахунком (за допомогою готівки, за умови зупинки ТЗ), а також купівлею проїзного на певний період [3] (в Австрії це віньєтка, в Румунії це звичайний чек). Під час подорожі європейськими країнами для великої частини водіїв постає проблема здійснення швидкої оплати за проїзд. У зв'язку з тим, що у багатьох країнах національна валюта відрізняється одна від одної, що завдає водієві певного дискомфорту пересування між країнами. Також досить часто водіям необхідна інформація про тип дороги, на якій вони знаходяться (платна або безкоштовна). Для вирішення цієї проблеми необхідно створити єдину систему, яка спрощуватиме процедуру стягнення плати (он-лайн конвертація валюти, згідно з виставленим рахунком) за проїзд з усіма можливими знижками на тариф та контроль безпечної експлуатації певних ділянок доріг.

Висновки. На платних відрізках доріг використовують спеціальні бортові пристрої які встановлені в автомобілі та зчитувачі на в'їздах і виїздах з платних ділянок доріг. Передача даних виконується наступним методом: - при під'їзді до відрізку платної дороги встановлені портали

контролю проїзду, на яких розміщені сканери габариту авто, автоматичне зважування авто, фотофіксація його міжнародного номера, зчитування даних з бортового пристрою автомобіля та в деяких країнах ідентифікація справжності номерного знака з використанням інфрачервоного прожектора для підсвічування державного номерного знака.

У певних країнах існують також екологічні збори, які запроваджуються лише для вантажних автомобілів.

Список літератури

1. Автомобільні дороги в Іспанії. *Autotrevel*. URL: http://autotraveler.ru/esp/#.WMjlkm-LQdU (дата звернення 19.11.2022);
2. Evans A. W. Ціни за проїзд в пробках: коли це хороша політика? Journal of Transport Economics and Policy 1992 №26, 213 243;
3. Віньєтка - де купити і скільки вона коштує. *Autotrevel*. URL: http://autotraveler.ru/spravka/vignette-in-europe.html#.WMjipG-LQdU (дата звернення 19.11.2022).

Відомості про авторів

Чічіло Артур Сергійович, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, м.т. 066-449-53-24, a.chichilo@student.csn.khai.edu
Желтухін Олександр Васильович, старший викладач кафедри комп'ютерних систем, мереж і кібербезпеки, a.zheltukhin@csn.khai.edu

АЛФАВІТНИЙ ВКАЗІВНИК

АЛФАВІТНИЙ ВКАЗІВНИК

ЗМІСТ

СТУДЕНТСЬКА КОНФЕРЕНЦІЯ
ІНФОРМАЦІЙНА, ФУНКЦІЙНА і КІБЕРБЕЗПЕКА
СКІФіК

Відповідальний за випуск Г.А. Землянко