



МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ
УНІВЕРСИТЕТ ІМЕНІ СЕМЕНА КУЗНЕЦЯ

КАФЕДРА КІБЕРБЕЗПЕКИ
ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

МАТЕРІАЛИ

XVI-ої МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ
«FREE AND OPEN SOURCE SOFTWARE»



Дякуємо за підтримку



IDCMP
PROJECT
IDEA DEVELOPMENT CONSULTING MANAGEMENT



13-14 лютого 2025 р.
м. Харків

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ СЕМЕНА КУЗНЕЦЯ

КАФЕДРА КІБЕРБЕЗПЕКИ
ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

МАТЕРІАЛИ

XVI-ої МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

«FREE AND OPEN SOURCE SOFTWARE»

13-14 лютого 2025 р.

ХАРКІВ 2025

УДК 004
БК 32.973.202

Матеріали XVI-ої Міжнародної науково-практичної конференції «Free and Open Source Software», Харків, 13-14 лютого 2025 р. – Харків: Харківський національний економічний університет імені Семена Кузнеця, 2025. – 188 с.

Представлено матеріали пленарних та секційних засідань XVI-ої Міжнародної науково-практичної конференції «Free and Open Source Software». Обговорено основні проблеми, науково-технічні досягнення, впровадження і досвід використання сучасних технологій в області безкоштовних програмних продуктів, а також з відкритим вихідним кодом. Висвітлено основні питання безкоштовного прикладного, серверного програмного забезпечення та прикладного програмного забезпечення з відкритим вихідним кодом, безкоштовних сервісів, в тому числі в контексті кібербезпеки, ліцензування та правові аспекти використання безкоштовного програмного забезпечення. Для фахівців науково-дослідних, комерційних організацій, аспірантів та студентів.

Редакційна колегія:
Старкова О.В. – голова, д.т.н.;
Міхєєв І.А. – к.т.н.;

Відповідальний за випуск:
Старкова О.В.

Роботи надруковані з авторських оригіналів, що надані оргкомітету, за авторської редакції.

Електронний варіант матеріалів конференції доступний на сайті конференції:

<https://foss.kn-it.info/>

ЗМІСТ

СЕКЦІЯ 1

INTEGRATING CRYPTOGRAPHY, IPFS, AND BLOCKCHAIN FOR DATA PROTECTION <i>Dolgova N.G., Pochanskiy O.M.</i>	15
ARTIFICIAL INTELLIGENCE IN CYBERSECURITY AND COMPUTER SCIENCE <i>Shapovalova O.O., Pochanskiy O.M.</i>	16
DOCKER IMAGES LISTING LIMITATIONS <i>Suprun M.V., Mikheev I.A.</i>	18
THE USE OF FREE AND OPEN SOURCE SOFTWARE IN CRYPTOLOGY: A FOCUS ON VERACRYPT <i>Zhuravka A., Ostapenko I.</i>	19
ENHANCING CYBERSECURITY WITH OPEN SOURCE CRYPTOGRAPHIC LIBRARIES <i>Zhuravka A., Mishchuk I.</i>	20
THE ROLE OF OPEN-SOURCE SOFTWARE IN ADVANCING CRYPTOGRAPHIC RESEARCH <i>Zhuravka A., Stupak D.</i>	21
ЗАСОБИ ГЕНЕРАЦІЇ ТА ПЕРЕВІРКИ ЦИФРОВОГО ПІДПИСУ <i>Азаров А.В., Солодовник Г.В.</i>	23
АВТОМАТИЗОВАНІ СИСТЕМИ ПЕРЕВІРКИ БЕЗПЕКИ САЙТІВ <i>Акуленко А.Є., Старкова О.В.</i>	24
КРОСПЛАТФОРМНІ ФАЄРВОЛИ ДЛЯ КІБЕРБЕЗПЕКИ: АНАЛІЗ, ПОРІВНЯННЯ ТА ВИБІР ОПТИМАЛЬНОГО РІШЕННЯ <i>Балим Г.В.</i>	25
АЛГОРИТМИ ШИФРУВАННЯ В СУЧАСНИХ МЕТОДАХ ПЕРЕВІРКИ АВТЕНТИЧНОСТІ ЦИФРОВИХ ПІДПИСІВ <i>Білошанка А.С., Долгова Н.Г.</i>	27
РОЗРОБКА ВЕБ-ЗАСТОСУНКУ КЕРУВАННЯ ФАЄРВОЛОМ <i>Бойко В.В., Леуненко О.В.</i>	28

РОЗРОБКА ІНТЕРАКТИВНОЇ СИСТЕМИ ВІЗУАЛІЗАЦІЇ ЦИФРОВОГО СЛІДУ ДЛЯ ОЦІНКИ РИЗИКІВ КОНФІДЕНЦІЙНОСТІ ТА ПІДВИЩЕННЯ КІБЕРОБІЗНАНОСТІ <i>Ваталінський Д.А., Муржа Д.Ю.</i>	30
ОГЛЯД ІСНУЮЧИХ СИСТЕМ ПЕРЕВІРКИ НАДІЙНОСТІ ПАРОЛЯ <i>Войтенко С.Р., Почанський О.М.</i>	31
РОЗРОБКА МОДЕЛІ УПРАВЛІННЯ ІНЦИДЕНТАМИ БЕЗПЕКИ З ВИКОРИСТАННЯМ XDR СИСТЕМ <i>Гребельний Р.С., Долгова Н.Г.</i>	32
КОНТЕКСТНО-ОРІЄНТОВАНІ СИСТЕМИ БАГАТОФАКТОРНОЇ АУНТИФІКАЦІЇ ДЛЯ ГЕТЕРОГЕННИХ ІНФОРМАЦІЙНИХ <i>Гришко М.С., Розломій І.О.</i>	33
ВИКОРИСТАННЯ SNORT ДЛЯ ЗАХИСТУ ІОТ-ПРИСТРОЇВ: ІНТЕГРАЦІЯ З ДОМАШНІМИ МАРШРУТИЗАТОРАМИ ТА ВИЯВЛЕННЯ БОТНЕТ-АТАК <i>Довбня М.В., Леуненко О.В.</i>	34
ДОСЛІДЖЕННЯ ПОТЕНЦІЙНИХ КІБЕРЗАГРОЗ ТА МЕТОДІВ ЗАХИСТУ ЗАГАЛЬНИХ ПЛОЩАДОК ЕЛЕКТРОННОЇ ТОРГІВЛІ <i>Донченко А.О., Семенов С.Г.</i>	35
ПРОГРАМНА РЕАЛІЗАЦІЯ ЗДІЙСНЕННЯ БАГАТОЕТАПНОГО ВИБОРУ В УМОВАХ РИЗИКУ <i>Єфімов М.Ю., Солодовник Г.В.</i>	36
КРИТИЧНА РОЛЬ ТЕСТУВАННЯ РІВНЯ ЗАХИЩЕНОСТІ ВЕБ-РЕСУРСІВ <i>Єфременков К.О., Лимаренко В.В.</i>	38
БЕЗКОШТОВНІ СЕРВІСИ ДЛЯ ОЦІНКИ СКЛАДНОСТІ ТА ГЕНЕРАЦІЇ ПАРОЛІВ <i>Загнібеда А.О., Міхєєв І.А.</i>	39
РОЗРОБКА МОДЕЛІ ДЛЯ ПРОТИДІЇ СПАМУ НА ІНФОРМАЦІЙНО- КОМУНІКАЦІЙНІ СИСТЕМИ <i>Іванько А.С., Старкова О.В.</i>	42
ЗАСТОСУВАННЯ ДИФЕРЕНЦІАЛЬНОЇ ПРИВАТНОСТІ ДЛЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В ІНФОРМАЦІЙНИХ СИСТЕМАХ <i>Клюєв В.О., Розломій І.О.</i>	43

ОГЛЯД СУЧАСНИХ КРИПТОГРАФІЧНИХ АЛГОРИТМІВ <i>Ключко О.О., Венгіна О.С.</i>	44
РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ВИЯВЛЕННЯ КІБЕРЗАГРОЗ З ВИКОРИСТАННЯМ АЛГОРИТМУ RANDOM FOREST <i>Костерний В.О., Шаповалова О.О.</i>	45
ПЛАТФОРМА КЕРУВАННЯ ОНЛАЙН-ОГОЛОШЕННЯМИ <i>Линник Я.І., Науменко С.В.</i>	47
QUAD9 ЯК ПРОГРАМА ДЛЯ ЗАПОБІГАННЯ ФІШИНГУ В Е-МАІЛ <i>Літвінов В.Д., Лимаренко В.В.</i>	48
ЙМОВІРНІСНИЙ ПІДХІД ДО ВИЗНАЧЕННЯ ПРАЦЕЗДАТНОСТІ ІС <i>Мазена І.В., Солодовник Г.В.</i>	49
ІНТЕГРАЦІЯ EDGE ТА FOG ОБЧИСЛЕНЬ ДЛЯ РОЗПОДІЛЕНОГО ЗАХИСТУ ДАНИХ У РЕАЛЬНОМУ ЧАСІ <i>Малига З.П., Розломій І.О.</i>	50
БЛОКЧЕЙН ТА РОЗПОДІЛЕНІ РЕЄСТРИ ДЛЯ ЗАБЕЗПЕЧЕННЯ НЕЗМІННОСТІ ТА АУДИТУ ДАНИХ У ГІБРИДНИХ ХМАРНИХ СИСТЕМАХ <i>Маліщук А.Р., Розломій І.О.</i>	51
РОЗРОБКА ІНСТРУМЕНТІВ ЗАПОБІГАННЯ АТАКАМ, ЗАСНОВАНА НА МАНІПУЛЯЦІЇ ЛЮДЬМИ <i>Мамон К.Д., Муржа Д.Ю.</i>	52
ОГЛЯД СИСТЕМ ВИЯВЛЕННЯ ТА БЛОКУВАННЯ ПРИХОВАНИХ КІБЕРАТАК У РЕАЛЬНОМУ ЧАСІ <i>Матюшечко М.В., Солодовник Г.В.</i>	53
АНАЛІЗ СУЧАСНИХ СИСТЕМ ВИЯВЛЕННЯ ТА ЗАПОБІГАННЯ КІБЕРЗАГРОЗАМ НА ОСНОВІ АНАЛІЗУ ПОВЕДІНКИ КОРИСТУВАЧІВ <i>Ментяник Д.О., Солодовник Г.В.</i>	55
RIPЕ ATLAS – НЕЗАМІННИЙ ІНСТРУМЕНТ ДЛЯ МОНІТОРИНГУ ІНТЕРНЕТ-МЕРЕЖ <i>Мерлак О.В., Литвиненко Є.М.</i>	56
ІНСТРУМЕНТИ КІБЕРБЕЗПЕКИ НА ОСНОВІ LINUX- ДИСТРИБУТИВІВ: KALI, OPENVAS, WIRESHARK <i>Мінаєв А.І., Латанська Л.О.</i>	58

АНАЛІЗ БЕЗПЕКИ СМАРТ-КОНТРАКТІВ ДЛЯ ДЕЦЕНТРАЛІЗОВАНИХ ФІНАНСОВИХ ОПЕРАЦІЙ (DEFI) <i>Налігацьких М.М., Долгова Н.Г.</i>	59
ІННОВАЦІЙНИЙ МЕТОД ПОБУДОВИ S-ВОХ ДЛЯ ПОЛЕГШЕНИХ БЛОКОВИХ ШИФРІВ У ВБУДОВАНИХ ПРИСТРОЯХ <i>Науменко С.В., Розломій І.О.</i>	61
СУЧАСНІ ТЕХНОЛОГІЇ ЗАХИСТУ ДАНИХ У ВБУДОВАНИХ ПРИСТРОЯХ З ОБМЕЖЕНИМИ РЕСУРСАМИ <i>Науменко С.В., Михайловський Є.В., Стабецька Т.А.</i>	63
АДАПТИВНІ КРИПТОГРАФІЧНІ ПРОТОКОЛИ З ДИНАМІЧНОЮ ГЕНЕРАЦІЄЮ КЛЮЧІВ ДЛЯ ГІБРИДНИХ БАЗ ДАНИХ <i>Норенко М.С., Розломій І.О.</i>	65
РОЗРОБКА ФІЛЬТРА КОНТЕНТУ ДЛЯ ЗАХИСТУ ВІД ФІШИНГУ <i>Підмурняк М.В., Шаповалова О.О.</i>	66
РОЗРОБКА ПРОГРАМНОЇ МОДЕЛІ СИСТЕМИ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ В МЕРЕЖАХ ЗВ'ЯЗКУ СТАНДАРТУ GSM <i>Попов В.Ю., Семенов С.Г.</i>	67
РОЗРОБКА ЗАХИЩЕНОЇ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ СИСТЕМИ ДЛЯ МОНІТОРИНГУ СТАНУ БУДІВЕЛЬНИХ КОНСТРУКЦІЙ НА ОСНОВІ ІОТ <i>Пугач Т.А.</i>	68
ВИЗНАЧЕННЯ ПОГОДЖЕНОСТІ ДУМОК ЕКСПЕРТІВ ЗАСОБАМИ ВІЛЬНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ <i>Пчолка В.Е., Солодовник Г.В.</i>	69
БЕЗКОШТОВНІ СИСТЕМИ ВИЯВЛЕННЯ ВТОРГНЕНЬ У КОМП'ЮТЕРНИХ МЕРЕЖАХ <i>Рихва В.І., Солодовник Г.В.</i>	70
ЕФЕКТИВНИЙ АРХ ПІДХІД ДО ЗАХИСТУ ІНФОРМАЦІЇ В СЕРЕДОВИЩІ З ОБМЕЖЕНИМИ РЕСУРСАМИ <i>Розломій І.О., Науменко С.В.</i>	72
РОЗРОБКА ВЕБ-ЗАСТОСУНКУ ДЛЯ ЗАХИСТУ ВІД DDOS-АТАК У РЕЖИМІ РЕАЛЬНОГО ЧАСУ <i>Романов І.Р., Борисенко Д.В.</i>	74

РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ ВИЯВЛЕННЯ АТАК ТИПУ DOS/DDOS <i>Россол О.С., Лимаренко В.В.</i>	75
БАГАТОРІВНЕВИЙ АНАЛІЗ ПОВЕДІНКОВИХ ПАТЕРНІВ КОРИСТУВАЧІВ ЯК ІНСТРУМЕНТ ПОПЕРЕДЖЕННЯ КІБЕРАТАК <i>Ротань К.В., Розломій І.О.</i>	76
ОГЛЯД СПЕЦІАЛІЗОВАНОГО ПЗ ДЛЯ АНАЛІЗУ ВРАЗЛИВОСТЕЙ СМАРТ-КОНТРАКТІВ <i>Селегей О.Є., Долгова Н.Г.</i>	77
ПЕРЕВАГИ ТА НЕДОЛІКИ ІНСТРУМЕНТІВ ДЛЯ ВИЯВЛЕННЯ ЗАГРОЗ У МЕРЕЖЕВИХ ТА ХОСТОВИХ СЕРЕДОВИЩАХ <i>Сивуха А.Л., Венгріна О.С.</i>	79
РОЗРОБКА СИСТЕМИ МОНІТОРИНГУ ТА ПРОТИДІЇ АТАКАМ НА БЕЗДРОТОВІ МЕРЕЖІ З ВИЯВЛЕННЯМ ШКІДЛИВИХ ТОЧОК ДОСТУПУ <i>Синявський К.Є., Муржа Д.Ю.</i>	80
РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ АНАЛІЗУ УРАЗЛИВОСТЕЙ КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ СИСТЕМ <i>Скрипніков Є.М., Муржа Д.Ю.</i>	80
ПРОГРАМНА РЕАЛІЗАЦІЯ ВИБОРУ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ ЗА КРИТЕРІЄМ РИЗИКОВАНОСТІ <i>Супрун М.В., Солодовник Г.В.</i>	81
СТАТИСТИЧНИЙ АНАЛІЗ ТА ОПТИМІЗАЦІЯ МЕТОДІВ ВИЯВЛЕННЯ ТА ЗАХИСТУ ВІД СОЦІАЛЬНО-ІНЖЕНЕРНИХ АТАК У СУЧАСНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ <i>Таласкаєв Д.І., Лимаренко В.В.</i>	82
ІНТЕГРАЦІЯ КВАНТОВИХ КРИПТОГРАФІЧНИХ ПРОТОКОЛІВ З ГЛИБОКИМ НАВЧАННЯМ ДЛЯ ПРОГНОЗУВАННЯ КІБЕРЗАГРОЗ <i>Ткаченко Д.В., Розломій І.О.</i>	83
ГІБРИДНІ АЛГОРИТМИ НЕЙРОННИХ МЕРЕЖ ТА СТАТИСТИЧНОГО АНАЛІЗУ ДЛЯ ВИЯВЛЕННЯ АНОМАЛІЙ У ВЕЛИКИХ ДАНИХ. <i>Троян К.С., Розломій І.О.</i>	84
ДЕЦЕНТРАЛІЗОВАНЕ ЗБЕРІГАННЯ ДАНИХ У ЗАХИЩЕНИХ МЕСЕНДЖЕРАХ <i>Харитонов Г.Д., Лимаренко В.В.</i>	85

ГОМОМОРФНЕ ШИФРУВАННЯ В РОЗПОДІЛЕНИХ БАЗАХ ДАНИХ ДЛЯ КОНФІДЕНЦІЙНИХ ОБЧИСЛЕНЬ. <i>Чікін Д.М, Розломій І.О.</i>	86
ПАРОЛІ ЯК КРИТИЧНИЙ ФАКТОР УРАЗЛИВОСТІ В КІБЕРБЕЗПЕЦІ <i>Чуєва А.О., Долгова Н.Г.</i>	87
ВИКОРИСТАННЯ ОПЕРАЦІЙНОЇ СИСТЕМИ TAILS ДЛЯ ЗАБЕЗПЕЧЕННЯ АНОНІМНОСТІ РОБОТИ В ІНТЕРНЕТ ТА ПЕРЕДАВАННЯ ДАНИХ <i>Шапо В.Ф., Воловщиков В.Ю.</i>	89
ОГЛЯД ІНТЕРАКТИВНИХ ЗАСОБІВ НАВЧАННЯ ОСНОВАМ КІБЕРБЕЗПЕКИ <i>Шарун П.В., Солодовник Г.В.</i>	92
ВИКОРИСТАННЯ БЕЗКОШТОВНИХ ПЛАТФОРМ АНАЛІЗУ КІБЕРЗАГРОЗ ДЛЯ ПІДВИЩЕННЯ ЗАХИСТУ ОРГАНІЗАЦІЙ <i>Шелестова А.М., Лубенець С.В.</i>	94
ФУНКЦІОНАЛ MONGODB ДЛЯ ВИЯВЛЕННЯ ФІШИНГУ <i>Шерстнюк А.В., Шаповалова О.О.</i>	96
ВИКОРИСТАННЯ ОПЕРАЦІЙНОЇ СИСТЕМИ PARROT ДЛЯ ПІДВИЩЕННЯ КВАЛІФІКАЦІЇ З КІБЕРГІГІЄНИ ТА КІБЕРБЕЗПЕКИ <i>Шестопалов М.А., Шапо В.Ф., Воловщиков В.Ю.</i>	98
ЗАСОБИ ПРОТИДІЇ SQL-ІН'ЄКЦІЯМ ТА XSS-АТАКАМ <i>Шишлов А.С., Солодовник Г.В.</i>	101

СЕКЦІЯ 2

BANDIT: AUTOMATED STATIC SECURITY ANALYZER FOR PYTHON CODE <i>Kolotii M.O., Leunenko O.V.</i>	104
COMPARATIVE ANALYSIS OF OPEN SOURCE INFRASTRUCTURE AS CODE (IAC) TOOLS FOR MANAGING HETEROGENEOUS CLOUD RESOURCES <i>Yenhalychev S.O., Leunenko O.V.</i>	105

DEVELOPMENT OF METHODS FOR DYNAMIC LOAD BALANCING DURING THE TRANSFER OF LARGE VOLUMES OF DATA: A COMPARATIVE STUDY OF APACHE KAFKA AND RABBITMQ <i>Yenhalychev S.O., Leunenko O.V.</i>	108
ОСОБЛИВОСТІ ПОБУДОВИ ПРИВАТНОЇ ХМАРИ НА ОСНОВІ ТЕХНОЛОГІЇ KUBERNETES <i>Алексієв В.О.</i>	110
ВЕБЗАСТОСУНОК ДЛЯ КООРДИНАЦІЇ СПІВПРАЦІ МІЖ ФРІЛАНСЕРАМИ ТА ЗАМОВНИКАМИ <i>Антонюк О.А., Науменко С.В.</i>	112
РОЗРОБКА ОСВІТНЬОГО ВЕБ-ЗАСТОСУНКУ ДЛЯ ВИВЧЕННЯ ОСНОВНИХ АЛГОРИТМІВ ШИФРУВАННЯ <i>Бойко С.О., Лимаренко В.В.</i>	113
GIT – СИСТЕМА КЕРУВАННЯ ВЕРСІЯМИ: GITHUB, GITLAB <i>Бондаренко В.В., Голуб Д.А., Єгоян В.Б.</i>	114
ОГЛЯД ФРЕЙМВОРКІВ ТА БІБЛІОТЕК ДЛЯ РОЗРОБКИ ВЕБ-ДОДАТКУ ОНЛАЙН-КІНОТЕАТРУ <i>Булатов О.С., Гайдаєнко О.В.</i>	116
NEO4J – ГРАФОВА БАЗА ДАНИХ <i>Венгіна О.С., Почанський О.М.</i>	117
ПРОБЛЕМИ ЕФЕКТИВНОГО РОЗПОДІЛЕННЯ РЕСУРСІВ В СИСТЕМАХ ОРКЕСТРУВАННЯ ВІРТУАЛЬНИХ КОНТЕЙНЕРІВ <i>Воєводін Є.В., Стабецька Т.А., Розломій І.О.</i>	119
IFOGSIM: СИМУЛЯЦІЯ РЕСУРСНОГО УПРАВЛІННЯ В СЕРЕДОВИЩАХ IOT, EDGE ТА FOG ОБЧИСЛЕНЬ <i>Волощук С.І.</i>	120
ПОРІВНЯННЯ СПОЖИВАННЯ ОПЕРАТИВНОЇ ПАМ'ЯТІ У WEB IDE <i>Гюльмамедов Н.М., Бурлаченко І.С.</i>	121
САКЕРНР – ФРЕЙМВОРК ДЛЯ ВЕБ-РОЗРОБКИ <i>Давидов Д.В., Латанська Л.О.</i>	123
НАВАНТАЖУВАЛЬНЕ ТЕСТУВАННЯ АГРЕГАТОРУ ДАНИХ З ВИКОРИСТАННЯМ APACHE JMETER <i>Зеленський О.Д., Воловщиків В.Ю., Шапо В.Ф.</i>	124

РОЗРОБКА ВЕБ-ЗАСТОСУНКУ ДЛЯ УПРАВЛІННЯ РЕЗЕРВНИМИ КОПІЯМИ ТА ВІДНОВЛЕННЯМ ДАНИХ У ХМАРІ <i>Іванюк В.Р., Борисенко Д.В.</i>	126
СЕРВІСИ ГЕНЕРАЦІЇ 3D-МОДЕЛЕЙ <i>Иценко Н.Ю., Обухова К.О.</i>	127
ОГЛЯД ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ ОЦІНКИ ТА ТЕСТУВАННЯ РІВНЯ ЗАХИЩЕНОСТІ ВЕБ-ЗАСТОСУНКІВ <i>Кваша М.В., Мерлак О.В.</i>	129
ЕФЕКТИВНА РОБОТА З ASYNC/AWAIT У UNITY ЗА ДОПОМОГОЮ UNITASK <i>Клецов А.А., Гусєва-Божаткіна В.А.</i>	130
БЕЗКОШТОВНІ СЕРВІСИ ТА УТИЛІТИ ДЛЯ РЕАЛІЗАЦІЇ СИСТЕМ БАГАТОФАКТОРНОЇ АВТЕНТИФІКАЦІЇ <i>Кравченко А.В., Леуненко О.В.</i>	132
ОГЛЯД ІСНУЮЧИХ ЧАТ-БОТІВ ДЛЯ БРОНЮВАННЯ У ТУРИСТИЧНІЙ СФЕРІ <i>Кудін Д.О., Венгріна О.С.</i>	133
ІНСТРУМЕНТИ ДЛЯ АНАЛІЗУ ВІДЕО: ОГЛЯД ТА ПОРІВНЯННЯ <i>Макаров Д.С., Кобилін О.А.</i>	135
ВИКОРИСТАННЯ ВІДКРИТОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ РОЗРОБКИ БАГАТОФАКТОРНОЇ АВТЕНТИФІКАЦІЇ У ВЕБ-ДОДАТКАХ <i>Овсянніков М.О., Венгріна О.С.</i>	136
РОЗРОБКА МОДУЛЯ ДЛЯ АНАЛІЗУ МЕРЕЖЕВОГО ТРАФІКУ НА КЛЮЧОВІ СЛОВА <i>Орлов В.Є., Почанський О.М.</i>	137
ВРАЗЛИВОСТІ МОДЕЛІ DEEPSEEK-R1 ЯК ВИКЛИК ДЛЯ OPEN-SOURCE AI <i>Пасюк Б.Б., Божаткін С.М.</i>	138
ROUTEROS ЯК ПРОГРАМНО-ТЕХНІЧНИЙ ЗАСІБ ДЛЯ ЗАХИСТУ МЕРЕЖІ <i>Проскурнін Ф.М., Мерлак О.В.</i>	140
BLACKBOX AI – AI-ЗАСТОСУНОК ДЛЯ ПРОГРАМУВАННЯ <i>Сівіцкий В.В., Сажко Г.І.</i>	142

СТВОРЕННЯ ЗАХИЩЕНОГО ЧАТ-БОТА ДЛЯ АВТОМАТИЗАЦІЇ ОБСЛУГОВУВАННЯ КЛІЄНТІВ <i>Слабоспицький Д.О., Борисенко Д.В.</i>	143
РОЗРОБЛЕННЯ ВЕБ-ДОДАТКА ДЛЯ ЗБЕРІГАННЯ ТА ШИФРУВАННЯ ПАРОЛІВ НА БАЗІ OPEN-SOURCE БІБЛІОТЕК ТА СЕРВІСІВ <i>Степаненко Є.О., Леуненко О.В.</i>	144
AMD UPROF: КОМПЛЕКСНИЙ ІНСТРУМЕНТ ПРОФІЛЮВАННЯ ПРОДУКТИВНОСТІ <i>Трибрат А.С., Латанська Л.О.</i>	145
МАТЕМАТИЧНЕ ТА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ДЛЯ ОПТИМІЗАЦІЇ РОЗМІЩЕННЯ ІМПЛАНТІВ У БРАХІТЕРАПІЇ <i>Чугай А.М., Яськова Є.Г., Яськов Г.М.</i>	147
АНАЛІЗ ЯКОСТІ ПРОГРАМНОГО КОДУ PHP ЗА ДОПОМОГОЮ PHRMETRICS <i>Шутко І.С</i>	148
РОЗРОБКА ТА ВИКОРИСТАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ ВИЯВЛЕННЯ АНОМАЛІЙ У МЕРЕЖЕВОМУ ТРАФІКУ ЗА ДОПОМОГОЮ CNN <i>Ярмоленко В.С., Шаповалова О.О.</i>	149
 СЕКЦІЯ 3	
COMPARISON OF RANDOM FOREST REGRESSION AND POLYNOMIAL REGRESSION ANALYSIS FOR CODE METRICS <i>Bryzghalov M.V., Kaminsky S.S., Makarova L.M.</i>	152
CLOUDCOMPARE – FREE SOFTWARE FOR POINT CLOUD PROCESSING <i>Toots R.</i>	154
ІШТУЧНИЙ ІНТЕЛЕКТУАЛЬНИЙ КАПІТАЛ ЯК НОВИЙ ВИД РЕСУРСІВ НЕМАТЕРІАЛЬНОГО ПОХОДЖЕННЯ <i>Андрейчиков О.О., Старкова О.В.</i>	155

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ПІДТРИМКИ ПРОСУВАННЯ ПОДАЛЬШИХ ПОКУПОК	157
<i>Артамошин Є.В., Льовкін В.М.</i>	
ПРИСТРІЙ ДЛЯ ВИМІРЮВАННЯ ТЕМПЕРАТУРИ ПОВІТРЯ СКЛАДСЬКОГО ПРИМІЩЕННЯ ТА КОНТРОЛЮ УМОВ ДЛЯ ЗБЕРІГАННЯ ПРОДУКЦІЇ НА БАЗІ ARDUINO	158
<i>Барда М.О., Крайник Я.М.</i>	
ВИКОРИСТАННЯ LORAWAN ТА МАШИННОГО НАВЧАННЯ ДЛЯ АВТОМАТИЗАЦІЇ РОБОТИ РОЮ ДРОНІВ	160
<i>Басов Д.Є., Пузирьов С.В.</i>	
ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ДЛЯ АНАЛІЗУ ВІДГУКІВ ПРО МУЗИЧНИЙ КОЛЕКТИВ	162
<i>Гордієнко А.В., Льовкін В.М.</i>	
ІІІ-МЕНЕДЖМЕНТ ЯК НОВА ПАРАДИГМА УПРАВЛІННЯ НА ОСНОВІ ШТУЧНОГО ІНТЕЛЕКТУ	163
<i>Єль Мутахід А.Р., Щербина Н.В.</i>	
ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ОПТИМІЗАЦІЇ СКЛАДУ ФУТБОЛЬНОЇ КОМАНДИ НА ОСНОВІ ПРОГНОЗУВАННЯ РЕЗУЛЬТАТИВНОСТІ ГРАВЦІВ	165
<i>Коваленко В.П., Льовкін В.М.</i>	
ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ РЕКОМЕНДУВАННЯ МУЗИЧНИХ КОМПОЗИЦІЙ НА ОСНОВІ ІНТЕРЕСІВ КОРИСТУВАЧА	166
<i>Коганті К.К., Льовкін В.М.</i>	
АНАЛІЗ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ УПРАВЛІННЯ ІТ-ПРОЄКТАМИ	167
<i>Назаров Д.Л., Слісаренко М.В.</i>	
СТВОРЕННЯ ГЕОІНФОРМАЦІЙНОЇ СИСТЕМИ ДЛЯ ПРОЄКТІВ ВІДНОВЛЕННЯ	170
<i>Осауленко І.А.</i>	
ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ АВТОМАТИЗОВАНОГО ВИЗНАЧЕННЯ АКОРДІВ У АУДІОФАЙЛАХ	171
<i>Панченко Є.О., Льовкін В.М.</i>	

СИСТЕМА ВИЗНАЧЕННЯ НОТ НА ОСНОВІ ЧАСТОТИ ЗВУКОВИХ КОЛИВАНЬ	173
<i>Петров А.Р., Обухова К.О.</i>	
ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ПРИ ВИВЧЕННІ ДИСЦИПЛІНИ «ПРОТИПОЖЕЖНЕ ВОДОПОСТАЧАННЯ»	175
<i>Петухова О.А., Білаш Є.А., Швед А.В.</i>	
ПРОГРАМНІ ЗАСОБИ ДЛЯ СТАТИЧНОГО АНАЛІЗУ КОДУ НА KOTLIN	177
<i>Приходько С.Б., Кольцов А.В.</i>	
РОЗРОБКА СИСТЕМИ АУНТЕТИФІКАЦІЇ З ВИКОРИСТАННЯМ БІОМЕТРІЇ ЗА ДОПОМОГОЮ ARDUINO	178
<i>Пудла М.С., Лимаренко В.В.</i>	
BLENDER – ПОТУЖНИЙ ІНСТРУМЕНТ ДЛЯ АРХІТЕКТУРНОЇ ВІЗУАЛІЗАЦІЇ	179
<i>Свинаренко М.С.</i>	
РОЗРОБКА ПОШУКОВОЇ СИСТЕМИ ДЛЯ РІЗНИХ ГАЛУЗЕЙ ЗНАНЬ	181
<i>Сімак А.В., Льовкін В.М.</i>	
ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ АНАЛІЗУ ІНФОРМАЦІЙНОГО ВМІСТУ НА ВИЯВЛЕННЯ РЕКЛАМНОГО КОНТЕНТУ	182
<i>Степанов І.А., Льовкін В.М.</i>	
ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ДЛЯ АВТОМАТИЗОВАНОГО ВИЗНАЧЕННЯ ЖАНРІВ КІНОСТРІЧОК	183
<i>Федишен С.В., Льовкін В.М.</i>	
3D MODELING APP – БЕЗКОШТОВНІ ІНСТРУМЕНТИ ДЛЯ МОДЕЛЮВАННЯ НА ТЕЛЕФОНІ	184
<i>Чайка А.В., Сажко Г.І.</i>	
ОГЛЯД ФРЕЙМВОРКУ KIVU З ТОЧКИ ЗОРУ РОЗРОБКИ МОБІЛЬНИХ ЗАСТОСУНКІВ	187
<i>Штаба В.Г., Макарова Л.М.</i>	

Секція 1

INTEGRATING CRYPTOGRAPHY, IPFS, AND BLOCKCHAIN FOR DATA PROTECTION

Dolgova N.G., Pochanskiy O.M.
E-mail: natalya.dolgova@hneu.net

Kharkiv, Simon Kuznets Kharkiv National University of Economics

The internet was built on trust – trust in centralized authorities to store, manage, and protect our data. But trust is a fragile thing. With each passing year, high-profile breaches and mass data leaks remind us that traditional storage solutions are vulnerable by design. What if we could eliminate trust from the equation entirely? Enter blockchain and decentralized storage systems, where security is enforced not by corporations, but by cryptographic algorithms and distributed networks.

Applications leveraging blockchain and the InterPlanetary File System (IPFS) offer innovative approaches to data protection, ensuring security, transparency, and accessibility. Integrating these technologies mitigates vulnerabilities inherent in traditional storage systems and enhances user trust. As noted in recent analyses, blockchain plays a pivotal role in collaborative cybersecurity by eliminating single points of failure and promoting a decentralized data management method [1].

The market offers numerous data storage solutions, each with distinct limitations. Popular cloud services such as Google Drive and Dropbox are convenient, but their centralized nature makes them vulnerable to data breaches. Users often do not have complete control over data encryption, which increases the risk of unauthorized access. In 2024, data breaches exposed more than 422 million records worldwide [2].

While modern solutions such as Tresorit emphasize privacy through end-to-end encryption, their high costs can be prohibitive for small and medium-sized enterprises. Decentralized storage platforms such as Storj and Sia represent advances in security, but the lack of integration with blockchain limits their ability to provide data transparency and verifiability. Digital signature services, including DocuSign, offer robust document management tools but do not provide decentralized storage, which can be a drawback when handling highly confidential information.

Statistically, over 80% of organizations are concerned about the risks inherent in centralized storage, and 60% are seeking hybrid solutions that include distributed storage. This underscores the critical need for innovative approaches to data storage and protection.

Applications that combine key technologies can achieve optimal security and convenience.

The blockchain creates records for each document, ensuring immutability and transparency. Consensus algorithms prevent attempts to manipulate data, and the SHA-256 hashing algorithm provides strong collision protection [3].

IPFS assigns a unique content identifier (CID) to each file, which facilitates fast and efficient data retrieval in a decentralized network. The P2P protocol eliminates the need for centralized servers, increasing the system's fault tolerance.

Cryptographic techniques are fundamental to security. Data is encrypted before being transmitted to the IPFS network, and digital signatures are implemented using algorithms such as RSA and ECDSA to verify the authenticity of documents. RSA offers high security through asymmetric encryption with public and private keys, while ECDSA, based on elliptic curves, is optimal for distributed systems due to its efficiency.

For backend development, frameworks like Django are often selected for flexibility and rapid development capabilities. PostgreSQL is commonly used as a database to store metadata and integrate with other services.

Integrating IPFS for decentralized storage, employing blockchain for change auditing, and implementing digital signatures to protect document authenticity make applications in this category highly desirable. An intuitive interface allows users to adapt and utilize all system features quickly.

Implementing such solutions opens up a wide range of opportunities in various fields. These applications can be used in the financial sector to store and audit contracts and transactions securely. Legal firms can use them to protect confidential documents and ensure their authenticity. In the education sector, such systems are suitable for storing diplomas and certificates, preventing them from being tampered with. Future developments of these solutions include integration with existing document management systems, advanced support for smart contracts, and the application of machine learning techniques to analyze stored data. These applications demonstrate a unique approach to solving today's security challenges and have the potential to change the way data is stored and processed in the digital world.

Companies employing similar technologies, such as Google, Dropbox, DocuSign, Tresorit, Storj, and Sia, confirm the demand and success of approaches based on modern cryptographic methods and decentralized technologies. However, combining the best aspects of these technologies offers a comprehensive approach to security and user convenience.

References

[1] Loïc Miller and Marc-Oliver Pahl. 2024. Collaborative Cybersecurity Using Blockchain: A Survey. 1, 1 (March 2024), 35 pages.

[2] Global Data Breach Statistics 2024 [Electronic resource] – Resource access mode: <https://www.statista.com/markets/424/topic/1065/cyber-crime-security/#overview>

[3] Muhammad Haroon, Zaheer Alam, Rukhsana Kousar, Jawad Ahmad, Fawad Nasim, "Sentiment Analysis of Customer Reviews on E-commerce Platforms: A Machine Learning Approach", Bulletin of Business and Economics (BBE), vol.13, no.3, pp.230, 2024.

ARTIFICIAL INTELLIGENCE IN CYBERSECURITY AND COMPUTER SCIENCE

Shapovalova O.O., Pochanskiy O.M.

E-mail: olena.shapovalova@hneu.net

Kharkiv, Simon Kuznets Kharkiv National University of Economics

Artificial intelligence is increasingly being utilized for cyber threat analysis, attack prediction, and the development of more effective security systems. AI applications in computer science encompass areas such as automated vulnerability detection, AI integration into cryptographic algorithms, machine learning for malware analysis, and autonomous threat response systems.

Despite its vast potential, integrating AI into computer science and cybersecurity poses challenges related to model explainability, data security, and the need for open-source approaches in development. Key areas where AI is applied in cybersecurity and computer science include AI for cyberattack detection and cryptography, automated vulnerability analysis in source code, and autonomous security management systems.

At the initial stage of cyberattack detection, machine learning algorithms have proven effective for both network traffic analysis and anomaly recognition. Automated detection of DDoS attacks, unauthorized access attempts, and real-time identification of phishing and fraudulent activities using neural networks have significantly enhanced communication security.

Another critical application of AI is automated vulnerability analysis in software code. Deep learning models have demonstrated high accuracy in detecting security flaws in source code, while intelligent systems have been effectively employed for static and dynamic code analysis. Transformer-based models, such as GPT, are widely used for automated patch generation and code correction.

The use of AI in cryptography can be aimed at solving the following tasks: creating reliable cryptographic keys using random number generators combined with neural networks, developing AI systems for testing encryption resilience against hacking, automating vulnerability detection in

cryptographic code and developing fundamentally new approaches to information protection using quantum computers and neural networks.

A promising direction is the development of autonomous security management systems based on AI. The key aspects include: automation of monitoring and incident response processes using AI, intelligent access control and user authentication systems and combining blockchain methodology with AI to prevent data integrity breaches.

Open-source AI platforms and libraries allow researchers and engineers not to start from scratch each time but to leverage the latest developments to advance progress and security. Among the libraries, frameworks, and machine learning tools developed by different companies yet aimed at continuous innovation, the following stand out: TensorFlow, PyTorch, Scikit-learn, SonarQube, Bandit, and Sempreg. The latter, in particular, is worth highlighting as it helps identify potential vulnerabilities in various programming languages.

Among FOSS solutions that can be useful in cybersecurity, the following are noteworthy: a network traffic analyzer Zeek that enables real-time threat detection and alerts, an intrusion detection system Suricata that notifies users of unauthorized access attempts and a platform for automated incident analysis TheHive, allowing classification of suspicious activities based on multiple criteria.

When developing cryptographic algorithms, it is advisable to use two powerful open-source libraries: OpenSSL, which contains materials on implemented cryptographic algorithms for securing data transmission and LibSodium, which provides encryption algorithms and tools for digital signatures and PyCryptodome, a Python library for cryptographic algorithm implementation.

To better understand the practical implementation of AI in cybersecurity, we present a series of real-world case studies and initiatives (Tables 1-2).

Table 1. AI Applications in Cybersecurity – Examples and Use Cases

Direction	Example Description
Using GPT Models for Cyber Threat Analysis	OpenAI and Microsoft have explored the potential of large language models (LLMs) for cyber threat analysis. GPT-4 is used for deobfuscating malicious code, automating threat intelligence, and analyzing cybercriminal communications.
Machine Learning for Mitigating DDoS Attacks	Cloudflare employs machine learning algorithms to analyze network traffic in real time, allowing it to automatically distinguish legitimate traffic from botnet attacks and effectively prevent DDoS incidents.
Automated Vulnerability Detection in Source Code	Facebook (Meta) has developed CodeQL, an AI-powered tool that scans source code for vulnerabilities and detects potential exploits during the development phase.
Blockchain + AI for Secure Digital Transactions	IBM Watson, combined with blockchain technologies, analyzes financial transactions for anomalous activity, helping to prevent potential fraud.
Deep Neural Networks for Malware Analysis	Google DeepMind is developing deep learning-based systems that can recognize new types of malware, even before they are added to antivirus databases.

Table 2. Open Research Initiatives and Collaborations

Initiative	Description
OpenAI Cybersecurity Grant Program	Funding research in AI and cybersecurity to develop innovative security solutions.
AI for Cyber Defense (DARPA)	A U.S. government initiative aimed at creating autonomous AI systems for cybersecurity protection.
MITRE ATT&CK + AI	An analytical cyber threat framework that actively integrates machine learning models for threat detection and response.

Despite significant advancements, AI-driven cybersecurity still faces several challenges. Threats to neural networks and algorithm compromise pose risks; if the security of AI models themselves is breached, their reliability in protecting other resources becomes questionable. Ethical concerns and resource limitations arise due to AI-driven decision-making responsibility and the high computational complexity of deep learning models.

Looking ahead, the continued development of FOSS in AI will contribute to creating more secure and accessible technologies for a wider range of researchers. AI is transforming cyber threat analysis, risk management, and digital infrastructure protection. Open-source security and computer science solutions foster transparency and trust in AI models, thereby enhancing overall digital security.

DOCKER IMAGES LINTING LIMITATIONS

Suprun M.V.

Supervisor: Mikheev I.A.

E-mail: i.a.mikheev@gmail.com

Kharkiv, Semyon Kuznets Kharkiv National University of Economics

With the rapid growth of containerized applications, especially with the involvement of the open-source solution Docker, the number of vulnerabilities in such applications has increased due to the wrong configuration of Docker images. To detect these vulnerabilities and threats, it is necessary to use specialized tools.

They can be used at different levels and stages of the design and operation of a Docker container to identify security smells and vulnerabilities. For example, 2 groups of tools can be distinguished. Those that work with Docker files, and those that work with Docker images.

One of the effective solutions for working with Docker files is my own solution DocSecLint [2], which is ahead of its competitors in the context of detecting some security smells. The main problems of the DocSecLint tool are its unoptimized speed, as well as limitations in the ability to see a complete picture of vulnerabilities and misconfigurations. Working with only a single artifact – a Dockerfile – we encounter some conceptual limitations, including:

- Less visibility of security vulnerabilities in dependencies. While tools can track installed libraries via RUN apt-get install, pip install, npm install, etc. Dockerfiles do not track all dependencies they may pull.
- Vulnerability detection in base image. Dockerfile only contains a reference to the base image (FROM ubuntu:20.04), but does not analyze its contents.
- Difficulty in detecting poorly configured file or user permissions

According to the [1] more than 50% of the 4 million images have packages or app dependencies with at least one critical vulnerability and 13% had high-severity security flaws.

This highlights the importance of scanning all libraries loaded into the container, as well as in-depth scanning of the dependencies that these libraries entail. This task for a Docker linter that works exclusively with Dockerfiles is possible if you integrate an SBOM generation tool into the tool, as well as connect a vulnerability scanning tool that will scan all dependencies. However, solving this task will be more efficient if you work with another artifact, namely a Docker image.

Another important limitation we encounter when working exclusively with Dockerfiles is the difficulty of checking file permission settings inside the container.

Docker image scans are the sole way to detect specific types of threats, such as incorrect container permission settings. These hazards do not exist until container images exist, thus analyzing images after they are built is the only way to detect problems before deploying containers into production. [3]

That is why the further evolution of the linter is to explore ways to overcome these limitations, or to expand the functionality to scan Docker images, and even containers themselves, in addition to the Dockerfile itself.

References

[1] Analysis of 4 Million Docker Images Shows Half Have Critical Vulnerabilities [Electronic resource] – Resource access mode: <https://www.securityweek.com/analysis-4-million-docker-images-shows-half-have-critical-vulnerabilities/>

[2] LAKPI, Розробка автоматизованого рішення по виявленню безпекових міskonфігурацій в докерфайлах [Electronic resource] – Resource access mode: <https://ela.kpi.ua/items/e31ff908-8dde-47c2-a33c-4a44e30501ce>

[3] Aqua, Securing Containers with Docker Scanning [Electronic resource] – Resource access mode: <https://www.aquasec.com/cloud-native-academy/docker-container/docker-scanning/>

THE USE OF FREE AND OPEN SOURCE SOFTWARE IN CRYPTOLOGY: A FOCUS ON VERACRYPT

Andrii Zhuravka, Irina Ostapenko

E-mail: andrii.v.zhuravka@lpnu.ua

Lviv, Lviv Polytechnic National University

In the digital age, cybersecurity is paramount. This paper explores the importance of applying open-source cryptographic libraries to enhance security across different applications. This article explores these libraries' benefits, challenges, and real-world applications.

Benefits of Open-Source Cryptographic Libraries.

Transparency and trust. Open-source code is peer-reviewed, which leads to verifying cryptographic algorithms for reliability and security. Due to the ability to quickly identify and solve problems, transparency becomes a huge advantage. Since no one can seal open-source code, its flaws will likely be spotted and fixed early. This control level builds trust among users and developers [1].

Key Features of VeraCrypt.

On-the-Fly Encryption. VeraCrypt automatically encrypts data as saved and decrypts it as it is read, provided the user mounts the encrypted drive. This allows for data always to be stored securely without compromising usability.

Multiple Encryption Algorithms.

Supports various algorithms, such as AES, Serpent, Twofish, Camellia, and Kuznyechik. Users may use combinations of cascaded algorithms, including AES-Twofish-Serpent, for extra security.

Plausible deniability.

VeraCrypt has plausible deniability functionality, allowing users to create hidden volumes and operating systems. Thus, if the authorities compel a user to disclose a password, the user may give a false password that reveals a different data set and keep the sensitive data hidden.

Pre-Boot Authentication.

VeraCrypt is also using pre-boot authentication for full disk encryption. In this case, the user has to input a password before the operating system starts up, allowing the entire system to be encrypted and protected from unauthorised access.

VeraCrypt can run on Windows, macOS, and Linux platforms. This makes it a valuable tool for people who work with data across different platforms—some Further Details [2]. The software uses the XTS mode of operation for block cyphers to enhance disk encryption security. It produces header keys using PBKDF2 with 512-bit salt and has many iterations to prevent brute-force attacks.

The cryptographic hash functions available in VeraCrypt are BLAKE2s-256, SHA-256, SHA-512, Streebog, and Whirlpool. They are used to guarantee the integrity and security of the encrypted data.

Security Improvements.

The first, VeraCrypt, has addressed several security issues in TrueCrypt. First, the VeraCrypt development team thought the TrueCrypt storage format was too sensitive to attacks and

had developed a new format incompatible with TrueCrypt. Secondly, VeraCrypt has addressed vulnerabilities of arbitrary code execution and privilege escalation found in TrueCrypt.

VeraCrypt is widely used by individuals to protect sensitive personal data, such as financial records, personal documents, and private communications. This ensures that the data is encrypted and thus remains confidential and secure, for instance, when the device is lost or stolen.

VeraCrypt is a tool that is used by businesses to secure sensitive information such as intellectual property, customer data, and internal communications. This is because full disk encryption makes it difficult for any data on company devices to be accessed by unauthorised people, thus minimising the risk of data breaches.

Government and military applications require the highest levels of data security. Due to strong encryption algorithms and a feature for plausible deniability, it is appropriate to use VeraCrypt to encrypt sensitive information and protect national security interests.

Thus, this article shows that free and open-source software is compelling in cryptology, as demonstrated by VeraCrypt. As a result, it can be seen as a viable tool for data protection in various applications due to its strong encryption, transparency and community-based development. Therefore, where data security is a significant concern, tools such as VeraCrypt will be very useful in protecting sensitive information.

References

- [1] VeraCrypt – Free Open source disk encryption with strong security for the Paranoid. [Electronic resource] – Resource access mode: <https://veracrypt.eu/en/Technical%20Details.html>
- [2] "Encryption Algorithms". VeraCrypt Documentation. [Electronic resource] – Resource access mode: <https://www.veracrypt.fr/en/Encryption%20Algorithms.html>
- [3] "Hash Algorithms". VeraCrypt Documentation. IDRIX. [Electronic resource] – Resource access mode: <https://www.veracrypt.fr/en/Hash%20Algorithms.html>

ENHANCING CYBERSECURITY WITH OPEN SOURCE CRYPTOGRAPHIC LIBRARIES

Andrii Zhuravka, Irina Mishchuk
E-mail: andrii.v.zhuravka@lpnu.ua
Lviv, Lviv Polytechnic National University

Unfortunately, cyber threats are becoming increasingly complex today and pose a significant threat to modern information systems. Therefore, reliable information protection is becoming a very important factor in the reliable functioning of contemporary information systems. Open cryptographic libraries are becoming the basis of secure information systems. This is because they are transparent, flexible and free. In today's information environment, open cryptographic libraries have many advantages.

One of the most essential features of open libraries is their transparency. Unlike paid solutions, where the code is often hidden from viewing and editing, open source allows anyone to check and confirm the integrity of the algorithms.

This creates high trust among users. The rapid detection and patching of the Heartble vulnerability in OpenSSL is a powerful testament to the control and security provided by open-source transparency [1].

The open-source model is developing quite dynamically thanks to the joint work of developers from all over the world. This approach not only accelerates the development of new features but also ensures that libraries are resistant to new threats. For example, the Libsodium library has received many improvements from leading cryptanalysts and now offers advanced encryption methods that are both efficient and secure.

In addition, open-source cryptographic libraries provide access to high-quality security tools without the high cost of proprietary software. This affordability is especially useful for small and

medium-sized enterprises that may not have the financial resources to invest in expensive information security solutions [2].

However, it should be noted that effective implementation of cryptographic libraries requires a high level of technical expertise, as incorrect settings can lead to vulnerabilities.

This means that organisations should emphasise training programmes and partnerships with educational institutions to produce more qualified cryptography professionals. This means, therefore, that, for the long-term sustainability of open-source projects, more has to be done. Organisations should establish protocols for regular security audits and timely patching to minimise risks.

Active participation in open-source communities also helps to identify and resolve security issues at an early stage.

Here are some examples of practical applications of cryptographic library open source. Digital communications are protected by libraries such as OpenSSL and GnuTLS, which secure Internet communications using HTTPS and SSL/TLS protocols.

Data is protected by tools such as Libsodium and Botan. Various applications use these libraries, ranging from secure file storage to encrypted communication platforms.

The security of blockchain and cryptocurrencies also depends on these libraries, as they provide transaction authentication, which allows the development of decentralised, secure financial systems.

In the Internet of Things (IoT), cryptographic libraries ensure data protection by encrypting and creating secure communication channels, which reduces the risk of unauthorised access and data loss.

Open cryptographic libraries are becoming the basis of a modern cybersecurity strategy due to their transparency and economic benefits [3]. They are indispensable for organisations that want to improve their security environment. With the help of these libraries, organisations can strengthen their defences against evolving cyber threats.

References

[1] Open Source Cryptography - Amazon Web Services [Electronic resource] – Resource access mode: <https://aws.amazon.com/ru/security/opensource/cryptography>.

[2] Why open-source encryption is better for your privacy | Proton [Electronic resource] – Resource access mode: <https://proton.me/blog/open-source-encryption-privacy>

[3] Comparison of cryptography libraries - Wikipedia [Electronic resource] – Resource access mode: https://en.wikipedia.org/wiki/Comparison_of_cryptography_libraries

THE ROLE OF OPEN-SOURCE SOFTWARE IN ADVANCING CRYPTOGRAPHIC RESEARCH

Andrii Zhuravka, Diana Stupak

E-mail: andrii.v.zhuravka@lpnu.ua

Lviv, Lviv Polytechnic National University

The article discusses the significant impact of Open-Source Software (OSS) on the progress in cryptographic research. Based on the literature and empirical data analysis, the article investigates how OSS promotes innovation, collaboration and practical implementation of cryptographic solutions. The author emphasises the role of open source in accelerating the development of new algorithms, ensuring transparency and reliability of cryptosystems, and promoting the widespread adoption of cryptographic technologies in various industries [1].

Cryptography, as a science of information security, constantly evolves under the influence of new technologies and growing cybersecurity threats. In this context, Open-Source Software (OSS) provides researchers and developers with tools and platforms for experimentation, collaboration, and knowledge sharing. This article aims to explore the impact of OSS on cryptographic research, focusing on its benefits and challenges.

OSS as a Catalyst for Innovation in Cryptography.

Access to advanced tools and algorithms. OSS provides researchers with unprecedented access to the latest cryptographic algorithms and tools. For example, the Open Quantum Safe (OQS) library is a key resource for post-quantum cryptography research, providing implementations of algorithms such as CRYSTALS-Kyber and SABER, which are candidates for standardisation as part of the NIST Post-Quantum Cryptography Standardisation process. This access allows researchers to actively experiment with new methods and evaluate their effectiveness in various scenarios [2].

Accelerated prototyping and iterative development. The nature of OSS facilitates rapid prototyping and iterative development of cryptographic solutions. Log4Shell vulnerability is a vivid example of the need to respond rapidly to new threats. OSS allows researchers to adapt existing libraries, such as OpenSSL quickly, and has become a prime example of the need to react rapidly to new threats. OSS will enable researchers to swiftly adapt existing libraries, such as OpenSSL, to develop and test new defences. The ability to quickly iterate and share results is critical to effectively countering cybersecurity threats.

A global community of researchers and developers. OSS creates an international platform for collaboration between researchers and developers. The Open Crypto Audit Project (OCAP) community is an example of how experts worldwide join forces to audit cryptographic code, identify vulnerabilities, and ensure the reliability of cryptosystems.

Open access to research results and code. The principles of open access are the cornerstone of OSS. Research results, source code, and documentation are freely available, allowing researchers to check, reproduce, and use the work of their colleagues. For example, implementing the ChaCha20 encryption algorithm available on GitHub can be studied and used in various projects, contributing to the dissemination of knowledge and improving cryptographic methods.

Implementation and testing in real-world environments. Projects such as OpenSSL [3] and GnuPG are key components of the Internet security infrastructure. OpenSSL is used to protect millions of websites, and GnuPG [4] is used to encrypt email and files. The open-source nature of these projects allows for independent audits and vulnerability detection, ensuring their reliability and security.

Widespread adoption in the industry. OSS is widely used in various industries to protect data and ensure communication security. For example, Google uses the BoringSSL library in its Chrome and Android products. This shows that OSS is a tool for academic research and an essential component of commercial solutions.

Open-source software plays a critical role in the development of cryptographic research. By providing access to advanced tools, facilitating collaboration, and ensuring the transparency and reliability of cryptosystems, OSS has become a driving force for innovation and adoption of cryptographic technologies in various fields. Further research could focus on the impact of OSS on specific areas of cryptography, such as post-quantum cryptography, homomorphic encryption, and blockchain technologies.

References

[1] Exploring Real-World Cryptography Applications & Innovations [Electronic resource] – Resource access mode: <https://www.certauri.com/exploring-real-world-cryptography-applications-innovations/>

[2] Top 10 Security Risks of Using Open Source Software - WPG Consulting [Electronic resource] – Resource access mode: <https://wpgc.io/blog/top-10-security-risks-of-using-open-source-software/>

[3] Openssl-library [Electronic resource] – Resource access mode: <https://openssl-library.org/>

[4] The GNU Privacy Guard [Electronic resource] – Resource access mode: <https://www.gnupg.org/>

ЗАСОБИ ГЕНЕРАЦІЇ ТА ПЕРЕВІРКИ ЦИФРОВОГО ПІДПISУ

Азаров А. В.

Керівник: Солодовник Г.В.

E-mail: ganna.solodovnyk@hneu.net

Харків, Харківський національний економічний університет імені Семена Кузнеця

Вступ. Швидкий розвиток електронного документообігу та електронної комерції призвів до значного зростання кількості електронних документів, які циркулюють в інформаційному просторі. Для того, щоб забезпечити їхню юридичну силу та захистити від підробок, необхідні надійні засоби аутентифікації. Цифровий підпис як технологія, що дозволяє підтвердити авторство та цілісність електронного документа, відіграє ключову роль у забезпеченні довіри до електронних взаємодій. Цифровий підпис гарантує, що документ не був підроблений або змінений після підписання, а його автор є саме тією особою, яка вказана в підписі.

Актуальність дослідження програмних засобів генерації та перевірки цифрового підпису обумовлена стрімким розвитком цифрових технологій та зростанням кіберзагроз. Перехід до безпаперового документообігу потребує надійних засобів для підтвердження автентичності та цілісності електронних документів. Власне це і гарантує цифровий підпис. Крім того, законодавство багатьох країн, у тому числі й України, дедалі більше регулює використання електронного підпису, що висуває додаткові вимоги до безпеки та надійності систем цифрового підпису. Розробка власних програмних рішень в галузі інформаційної безпеки дозволяє зменшити залежність від іноземного програмного забезпечення та підвищити рівень кібербезпеки країни. Таким чином, розробка програми для генерації та перевірки цифрового підпису є актуальним завданням, яке відповідає сучасним вимогам інформаційної безпеки.

Метою роботи є огляд програмного забезпечення, яке забезпечує надійну генерацію та перевірку цифрових підписів. Таке програмне забезпечення має відповідати сучасним вимогам безпеки та ефективності, а також забезпечувати довіру до електронних документів.

Існує багато засобів для генерації та перевірки цифрового підпису, які належать до категорії вільного програмного забезпечення. Одним з них є OpenSSL – це бібліотека з відкритим кодом для реалізації криптографічних функцій, включаючи генерацію та перевірку цифрових підписів. До можливостей цієї бібліотеки належать: підтримка алгоритмів RSA, DSA, ECDSA, створення ключів, сертифікатів та цифрових підписів, перевірка підписаних даних.

З метою генерації та перевірки цифрового підпису можна використовувати також Python-бібліотеки. Криптографічна бібліотека PyCryptodome підтримує цифрові підписи та надає можливість генерації ключів RSA, DSA, ECC, а також створення та перевірки підписів. Інтуїтивно зрозуміла бібліотека для криптографії Cryptography є ще одним інструментарієм Python для роботи з цифровими підписами.

Висновок. Отже, цифровий підпис як надійний інструмент гарантії безпеки електронних документів стає все більш затребуваним у зв'язку зі зростанням кількоберзагроз та переходом до безпаперового документообігу. Подальше дослідження полягає у створенні програмного продукту, який буде відповідати сучасним вимогам безпеки та ефективності, а також сприяти розвитку електронного урядування та електронної комерції. Дослідження має на меті не лише розробку програмного забезпечення, але й аналіз існуючих рішень, вибір оптимальних криптографічних алгоритмів та створення рекомендацій щодо використання цифрових підписів в різних сферах діяльності. Результати роботи можуть бути використані для підвищення рівня кібербезпеки та довіри до електронних документів.

АВТОМАТИЗОВАНІ СИСТЕМИ ПЕРЕВІРКИ БЕЗПЕКИ САЙТІВ

Акуленко А. Є.

Керівник: Старкова О.В.

E-mail: alinkaakulenko@gmail.com

Харків, Харківський національний економічний університет імені Семена Кузнеця

Сучасний світ характеризується стрімким розвитком інформаційних технологій та їх широким впровадженням у діяльність організацій. Веб-сайти стали невід'ємною частиною бізнесу, виконуючи функції представництва в Інтернеті, залучення клієнтів та партнерів, а також забезпечення інформаційного обміну. Проте, зростаюча залежність від веб-ресурсів також підвищує ризики кіберзлочинності, спрямованої на злом сайтів, крадіжку даних та інші зловживання. У зв'язку з цим, питання забезпечення безпеки веб-сайтів організацій набуває особливої актуальності. Ефективним інструментом для вирішення цієї задачі є автоматизація процесу аналізу безпеки, яка дозволяє своєчасно виявляти та усувати вразливості, запобігаючи можливим атакам, та передбачає використання спеціалізованих інструментів та програмних комплексів, які дозволяють проводити сканування веб-ресурсів на предмет вразливостей, аналіз коду, перевірку відповідності стандартам безпеки та інші види перевірок.

Актуальні сканери безпеки веб-сайтів:

1. Acunetix - сканер, який перевіряє веб-сайт на наявність понад 7000 відомих вразливостей, тестує HTML5-сторінки, а також сторінки, для яких потрібна автентифікація. Після завершення сканування сервіс надає звіт із корисною інформацією.

2. ImmuniWeb - сканер перевіряє безпеку веб-сайтів на основі 10 найбільш критичних загроз OWASP. Сервіс надає детальну інформацію про знайдені вразливості та рекомендації щодо їх усунення.

3. AppCheck - сканер, який працює за моделлю SaaS. Сервіс імітує процес ручного тесту на проникнення, забезпечує охоплення OWASP Top 10, перевіряє на вразливості нульового дня та понад 100 000 відомих недоліків безпеки шляхом опитування бази даних CVE.

4. SSL Labs - сервіс перевіряє SSL-сертифікати та налаштування SSL-протоколу. SSL Labs надає детальну інформацію про знайдені проблеми та рекомендації щодо їх вирішення.

5. WPScan - сканер безпеки, який перевіряє наявність вразливостей у плагінах, темах та ядрі WordPress, також надає інформацію про відомі вразливості та рекомендації щодо їх усунення.

6. Invicti - сканер призначений для сканування всіх типів веб-сайтів, програм та API. Інструмент має комбінований підхід до сканування DAST + IAST [1].

Автоматизовані системи перевірки безпеки сайтів є необхідним елементом сучасної стратегії кібербезпеки. Вони здатні сканувати та аналізувати веб-ресурси набагато швидше, ніж людина, що дозволяє оперативно виявляти потенційні вразливості. Такі системи можуть працювати безперервно, забезпечуючи своєчасне виявлення нових загроз та миттєве реагування на них. Їх використання дозволяє значно підвищити рівень захисту веб-ресурсів та мінімізувати ризик кіберінцидентів.

Література

[1] WH-X Technology [Електронний ресурс] – Режим доступу до ресурсу: <https://www.h-x.technology/ua/blog-ua/23-website-security-quick-check-services-ua>

КРОСПЛАТФОРМНІ ФАЄРВОЛИ ДЛЯ КІБЕРБЕЗПЕКИ: АНАЛІЗ, ПОРІВНЯННЯ ТА ВИБІР ОПТИМАЛЬНОГО РІШЕННЯ

Балим Г.В.

E-mail: balym@hrtt.kh.ua

Харків, Харківський радіотехнічний фаховий коледж

Захист інформаційних систем є одним з найважливіших викликів сучасного цифрового середовища. Фаєрволи (мережеві екрани) відіграють ключову роль у забезпеченні безпеки комп'ютерних систем, контролюючи трафік та блокуючи несанкціоновані з'єднання. З розвитком інформаційних технологій збільшуються загрози, пов'язані з кібербезпекою [1]. Кіберзлочинці постійно вдосконалюють методи атак, використовуючи такі техніки, як фішинг, соціальна інженерія, атаки на відмову в обслуговуванні (DDoS) та експлуатація вразливостей у програмному забезпеченні [2]. Це створює серйозні ризики для бізнесу, державних установ і звичайних користувачів. Втрата або компрометація даних може призвести до фінансових втрат, юридичних наслідків і шкоди репутації компаній. Тому захист даних і забезпечення безпеки інформаційної інфраструктури є пріоритетним завданням для системних адміністраторів та ІТ-фахівців [3].

Фаєрволи є основним механізмом контролю мережевого трафіку, що забезпечує фільтрацію, блокування та аналіз потенційно небезпечних з'єднань. Вони дозволяють створювати політики доступу до мережі, обмежувати або дозволяти певний трафік та забезпечувати детальний моніторинг активності. Окрім того, сучасні фаєрволи мають можливість інтеграції з системами виявлення та запобігання вторгненням (IDS/IPS), що додатково підвищує рівень безпеки. Нові тенденції у сфері кібербезпеки включають впровадження штучного інтелекту (AI) для виявлення аномалій у мережевому трафіку, використання машинного навчання для ідентифікації загроз та автоматизацію управління політиками безпеки.

Багато сучасних операційних систем включають вбудовані засоби контролю трафіку, такі як Windows Defender Firewall, Linux iptables та macOS Packet Filter. Однак вони не завжди забезпечують гнучкість конфігурації та широкі можливості захисту. Тому вибір універсального фаєрвола залишається важливим питанням для адміністраторів мереж та ІТ-спеціалістів [4].

На основі аналізу існуючих рішень виділено три універсальні фаєрволи, які можуть працювати на різних операційних системах (важливо зазначити, що на даний час pfSense, OPNsense та IPFire не знаходяться під заборонаю в Україні. Вони є відкритими рішеннями, розробленими міжнародними спільнотами, і їх використання не порушує чинного законодавства України [5]):

1. pfSense – мережевий екран на базі FreeBSD, що забезпечує розширені можливості маршрутизації та безпеки [6].
2. OPNsense – сучасна альтернатива pfSense, що надає додаткові функції моніторингу та аналітики [7].
3. IPFire – легке, але потужне рішення для серверних та настільних платформ [8].

Таблиця 1. Порівняння універсальних фаєрволів

Фаєрвол	Підтримка ОС	VPN	IDS/IPS	Легкість налаштування	Призначення
pfSense	Linux, Windows, macOS (через віртуалізацію)	+	Suricata, Snort	4/5	Корпоративні мережі
OPNsense	Linux, Windows, macOS (через віртуалізацію)	+	Suricata	4/5	Бізнес, хмарні рішення
IPFire	Linux, Windows, macOS	+	Snort	3/5	Домашні мережі, малі компанії

Огляд провідних універсальних фаєрволів:

- pfSense – корпоративний рівень захисту. pfSense є одним із найпотужніших безкоштовних фаєрволів, який забезпечує високий рівень контролю мережевого трафіку. Він підтримує OpenVPN, IPsec, WireGuard, інтегрується з Suricata та Snort для аналізу загроз і має гнучкі правила безпеки.
- OPNsense – баланс між функціональністю та простотою. OPNsense є альтернативою pfSense із покращеною підтримкою Suricata, NetFlow, VPN та можливістю інтеграції з хмарними сервісами AWS, Azure.
- IPFire – компактне рішення для малих мереж. IPFire – це легкий фаєрвол, що використовує Snort для захисту від загроз, OpenVPN для безпечного підключення та має зручний веб-інтерфейс.

На основі аналізу можна зробити такі висновки та рекомендації щодо вибору універсального фаєрвола для різних категорій користувачів:

- Великі компанії та корпоративні мережі: pfSense забезпечує широкий функціонал безпеки, підтримку VPN, інтеграцію з Suricata та Snort, що робить його ідеальним вибором для корпоративних мереж з високими вимогами до безпеки та продуктивності.
- Малий та середній бізнес: OPNsense є збалансованим рішенням між продуктивністю та простотою керування. Він містить інтуїтивний інтерфейс, підтримує Suricata та NetFlow, що дозволяє ефективно відстежувати загрози в мережі.
- Домашні користувачі та малі офіси: IPFire – це легке та ефективне рішення, що підтримує Snort для аналізу загроз та забезпечує швидке налаштування VPN, що підходить для домашнього використання або невеликих офісних мереж.
 - pfSense – найкращий варіант для великих компаній та корпоративних мереж.
 - OPNsense – оптимальне рішення для малого бізнесу та середніх підприємств.
 - IPFire – відмінний вибір для домашніх мереж та малого офісу.

Використання будь-якого з цих рішень дозволяє значно підвищити рівень кібербезпеки мережевої інфраструктури та зменшити ризики атак.

Література

- [1] Коваленко І. П. Інформаційна безпека комп'ютерних систем. – Київ: Техніка, 2020.
- [2] Сидоренко О. В. Захист інформації в комп'ютерних мережах. – Харків: Основа, 2021.
- [3] Білоусов В. С. Основи кібербезпеки: навчальний посібник. – Львів: ЛНУ імені І. Франка, 2019.
- [4] Український центр кібербезпеки. Рекомендації щодо налаштування фаєрволів. – <https://cybersecurity.gov.ua/>, 2023.
- [5] Офіційний сайт Держспецзв'язку України. Перелік заборонених програмних рішень. – <https://cip.gov.ua/>, 2024.
- [6] Netgate. pfSense Official Documentation [Електронний ресурс] – Режим доступу до ресурсу: <https://docs.netgate.com>.
- [7] OPNsense Project. OPNsense Documentation [Електронний ресурс] – Режим доступу до ресурсу: <https://docs.opnsense.org>.
- [8] IPFire Project. IPFire Documentation [Електронний ресурс] – Режим доступу до ресурсу: <https://www.ipfire.org/docs>.

АЛГОРИТМИ ШИФРУВАННЯ В СУЧАСНИХ МЕТОДАХ ПЕРЕВІРКИ АВТЕНТИЧНОСТІ ЦИФРОВИХ ПІДПИСІВ

Білошапка А.С.

Керівник: Долгова Н.Г.

E-mail: artem.bel236@gmail.com

Харків, Харківський Національний Економічний Університет імені Семена Кузнеця

Цифровий підпис – це сучасний інструмент, який забезпечує ідентифікацію сторін, а також цілісність цифрових документів і повідомлень. Його основна ідея базується на використанні алгоритмів шифрування, які дозволяють підтвердити авторство відправника та гарантувати, що дані не були змінені під час передачі. У цій доповіді розглядається роль алгоритмів шифрування в сучасних методах автентифікації цифрових підписів.

Цифровий підпис є більш надійним, ніж звичайний рукописний підпис. Він створюється за допомогою асиметричного шифрування, яке використовує пару ключів: закритий ключ для підпису та відкритий ключ для перевірки. Процес підписування включає хешування даних, їх шифрування закритим ключем і додавання отриманого підпису до повідомлення. Одержувач може розшифрувати підпис за допомогою відкритого ключа та перевірити співпадіння хеш-значень, що підтверджує автентичність і цілісність даних.

Серед найпоширеніших алгоритмів, які використовуються для створення цифрових підписів, можна виділити наступні:

- RSA - один із найвідоміших алгоритмів асиметричного шифрування. Він базується на складності факторизації великих простих чисел. У контексті цифрових підписів RSA використовується для шифрування хешу даних закритим ключем відправника. Одержувач розшифровує підпис за допомогою відкритого ключа та перевіряє хеш. Незважаючи на свою надійність, проте RSA має недолік — використання довгих ключів, що може уповільнювати процес обробки даних[1].

- ECDSA - сучасний алгоритм, який базується на криптографії еліптичних кривих (ECC). Він забезпечує той самий рівень безпеки, що й RSA, але з меншим розміром ключа, що робить його більш ефективним з точки зору обчислювальних ресурсів. Цей алгоритм широко використовується в умовах обмежених ресурсів, наприклад, у блокчейні та мобільних додатках[1][2].

- DSA - федеральний стандарт для цифрових підписів, розроблений Національним інститутом стандартів і технологій США (NIST). Він базується на математичній складності задачі дискретного логарифмування. Хоча DSA є надійним, він поступається RSA та ECDSA за ефективністю і використовується переважно в урядових та корпоративних системах, а також у застарілих інфраструктурах[3][5].

Хешування є важливим етапом у створенні цифрових підписів. Воно перетворює дані у фіксований набір бітів, який потім шифрується для формування підпису. Серед найпоширеніших алгоритмів хешування можна виділити:

- SHA-256: Частина сімейства SHA-2, цей алгоритм широко використовується завдяки своїй швидкості та високому рівню безпеки.

- SHA-3: Найновіший алгоритм із сімейства SHA, який забезпечує покращену стійкість до криптографічних атак.

- Цифрові підписи знаходять застосування в різних сферах, наприклад:

- Електронна комерція: Забезпечення безпеки транзакцій та підтвердження автентичності договорів.

- Блокчейн[4]: Перевірка цілісності транзакцій та смарт-контрактів.

- Розробка програмного забезпечення: Підтвердження авторства та цілісності програмних оновлень.

- Урядові та юридичні документи: Забезпечення неспростовності та автентичності цифрових документів.

Незважаючи на високу надійність сучасних алгоритмів шифрування, існують потенційні загрози, такі як квантові обчислення, які можуть зламати традиційні криптографічні схеми. У відповідь на ці виклики розвивається пост-квантова криптографія, яка займається створенням алгоритмів, стійких до квантових атак. Крім того, впровадження більш ефективних алгоритмів, таких як ECDSA, та вдосконалення методів хешування продовжують формувати майбутнє цифрових підписів.

Алгоритми шифрування є основою цифрових підписів, забезпечуючи їх автентичність, цілісність і неспростовність. Від RSA до ECDSA, ці алгоритми забезпечують надійний захист цифрових комунікацій. З розвитком технологій і появою нових загроз, таких як квантові обчислення, криптографія продовжує еволюціонувати, щоб забезпечити безпеку цифрового світу[1].

Література

[1] Wikipedia. RSA [Електронний ресурс] – Режим доступу до ресурсу: <https://uk.wikipedia.org/wiki/RSA>

[2] Wikipedia. ECDSA [Електронний ресурс] – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/Elliptic_Curve_Digital_Signature_Algorithm

[3] Wikipedia. DSA [Електронний ресурс] – Режим доступу до ресурсу: <https://uk.wikipedia.org/wiki/DSA>

[4] Wikipedia. Blockchain [Електронний ресурс] – Режим доступу до ресурсу: <https://uk.wikipedia.org/wiki/%D0%91%D0%BB%D0%BE%D0%BA%D1%87%D0%B5%D0%B9%D0%BD>

[5] NIST. Digital Signature Standard (DSS) [Електронний ресурс] – Режим доступу до ресурсу: <https://www.nist.gov/publications/digital-signature-standard-dss-2>

РОЗРОБКА ВЕБ-ЗАСТОСУНКУ КЕРУВАННЯ ФАЄРВОЛОМ

Бойко В.В.

Керівник: Леуенко О.В.

E-mail: vadyu.boiko.1@hneu.net, oleksii.Leuuenko@hneu.net

Харків, Харківський національний економічний університет імені Семена Кузнеця

У сучасному світі цифрових технологій кібербезпека є надзвичайно важливою. Фаєрволи або брандмауери є ключовим інструментом для захисту інформаційних систем. Вони контролюють доступ до мережі, блокують шкідливий трафік та запобігають несанкціонованому проникненню.

Таким чином одним з перших кроків створення безпечної мережі є налаштування правил мережі, проте кількість кібератак зростає та кількість фахівців ще не є достатньою[1], тому для часткового вирішення проблеми кадрів та зменшення витрат на налаштування мережевих фільтрів є системи керування фаєрволами.

Для спрощення адміністрування та підвищення рівня захисту мережі, розроблено веб-застосунок для централізованого керування фаєрволом. Цей інструмент [2] надає можливість централізовано налаштувати правила мережі, що значно зменшує кількість помилок, які можуть виникнути під час ручного налаштування кожного окремого фаєрвола. Крім того, система автоматизує низку важливих завдань, таких як створення резервних копій та відновлення налаштувань для мережевого екрану. Це не тільки підвищує безпеку, але й звільняє цінний час системних адміністраторів, дозволяючи їм зосередитися на інших важливих аспектах роботи.

Використання даного веб-застосунку також сприяє зменшенню ресурсів, необхідних для налаштування мережевого екрану. Завдяки централізації та автоматизації, потреба в ручному втручанні та, відповідно, витрати на обслуговування, значно скорочуються.

Впровадження системи централізованого керування фаєрволом є важливим кроком до підвищення рівня кібербезпеки та оптимізації роботи з мережею.

Система дозволить генерувати звіти про стан мережі, та аналізувати події у мережі. Звіти допомагають оцінити ефективність системи безпеки та прийняти обґрунтовані рішення щодо її покращення та оптимізації.

Також за допомогою даної системи можна навчати людей, оскільки система не дозволяє створювати не вірні правила мережі, тп може пояснити як працюють налаштування мережевого фільтру.

Переваги використання централізованої системи керування фаєрволом [3]

- Зручне налаштування
- Віддалена робота спеціалістів із мережевої безпеки
- Масштабування
- Централізоване управління

Дане рішення може допомогти наступним типам установ:

- Великі підприємства, які хочуть централізувати управління правил мережі.
- Провайдери мереж, які хоуть централізувати безпеку мереж своїх клієнтів.
- Державні установи для захисту критичної інфраструктури та інформації.
- Маленькі компанії, які хочуть зробити свою мережу біль захищеною та не хочуть витратити великі кошти для налаштування правил мережі.
- Навчальні установи, для пояснення як працюють мережеві екрани, та які навчають працювати із фаєрволами.

Стосовно вибору технологій, було обрано наступні:

- Операційна система – Linux, оскільки більша частина серверів працює на даній операційній системі [4]
- Мова програмування – Node.js, оскільки має достатбо прав для взаємодії із ОС та мережевим екраном відповідно
- Назва мережевого екрану з яким буде взаємодіяти система – UFW [5], оскільки є досить зручним
- База даних, яка зберігає інформацію про користувачів – MongoDB
- Фреймворки – Nest.js, GraphQL, Mongoose, React

В результаті даної конфігурації, система має наступний вигляд взаємодії рис. 1

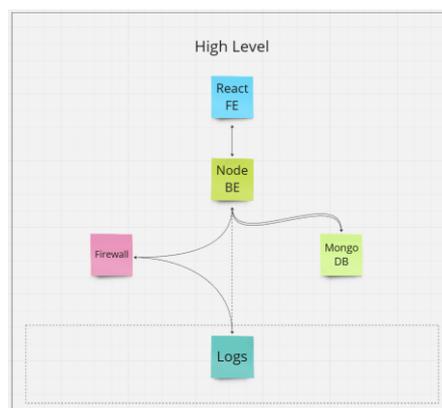


Рисунок 1 – Схема взаємодії системи між собою

Таким чином веб застосунок керування фаєрволом дозволить ефективно забезпечувати безпеку мережевої інфраструктури та дозволить централізовано контролювати трафік та впроваджувати політики безпеки на основі аналітичних даних.

Література

[1] NationalUniversity [Електронний ресурс] – Режим доступу до ресурсу: <https://www.nu.edu/blog/cybersecurity-statistics/>

[2] GitHub [Електронний ресурс] – Режим доступу до ресурсу:
<https://github.com/boykovm/firewall-manager>

[3] Zenarmor [Електронний ресурс] – Режим доступу до ресурсу:
<https://www.zenarmor.com/docs/network-security-tutorials/what-is-firewall-as-a-service-fwaas>

[4] PhoenixNAP [Електронний ресурс] – Режим доступу до ресурсу:
<https://phoenixnap.com/kb/server-operating-system>

[5] Wikipedia [Електронний ресурс] – Режим доступу до ресурсу:
https://en.wikipedia.org/wiki/Uncomplicated_Firewall

РОЗРОБКА ІНТЕРАКТИВНОЇ СИСТЕМИ ВІЗУАЛІЗАЦІЇ ЦИФРОВОГО СЛІДУ ДЛЯ ОЦІНКИ РИЗИКІВ КОНФІДЕНЦІЙНОСТІ ТА ПІДВИЩЕННЯ КІБЕРОБІЗНАНОСТІ

Ваталінський Д.А.

Керівник: Муржа Д.Ю.

E-mail: dima.dimon202202@gmail.com

Харків, Харківський національний економічний університет імені Семена Кузнеця

Збільшення цифрового сліду користувачів через активне використання онлайн-сервісів, соціальних мереж і мобільних додатків створює нові виклики для конфіденційності та кібербезпеки. Відсутність зручних і доступних інструментів для наочної оцінки цих ризиків ускладнює усвідомлення потенційних загроз [1]. Саме тому розробка інтерактивної системи візуалізації цифрового сліду є актуальним напрямом, що може суттєво підвищити рівень кіберобізнаності користувачів.

Метою цієї роботи є створення інструменту, який дозволить користувачам оцінювати свій цифровий слід, аналізувати можливі ризики конфіденційності та отримувати персоналізовані рекомендації для покращення безпеки в мережі. Для цього система повинна збирати та обробляти дані про активність користувача в онлайн-середовищі, представляючи їх у зручному форматі за допомогою графіків, діаграм та карт взаємозв'язків. Важливим аспектом є також можливість оцінки рівня ризику конфіденційності на основі отриманих даних і впровадження навчальних механізмів, що допоможуть користувачам свідоміше керувати своєю присутністю в мережі [2-3].

Для реалізації системи використовуватимуться сучасні технології та алгоритми аналізу цифрового сліду. Обробка лог-файлів, застосування методів машинного навчання та статистичних моделей дозволять виявляти потенційні загрози. Фронтенд буде побудований на основі JavaScript і бібліотек для візуалізації даних, таких як D3.js або React, що забезпечить інтерактивний та інтуїтивно зрозумілий інтерфейс. Серверна частина працюватиме на Python із використанням бібліотек pandas і scikit-learn, що забезпечить ефективний аналіз даних. Для збереження конфіденційності планується впровадження механізмів анонімізації та безпечного зберігання інформації.

Очікувані результати проєкту включають створення зручного та доступного інструменту для візуалізації цифрового сліду, що допоможе користувачам краще розуміти, як їхні дані використовуються в мережі. Це сприятиме підвищенню рівня цифрової грамотності, зменшенню ризиків витоку персональних даних і формуванню більш відповідального підходу до кібербезпеки.

Література

[1] Гуцалюк М. В., Король В. А. Методологія аналізу цифрового сліду для оцінки кіберризиків. Вісник НТУУ «КПІ». Серія: Інформаційні технології. 2022. № 3. С. 45–52.

[2] Вітюк В. І., Третяк А. О. Застосування методів машинного навчання для аналізу загроз конфіденційності. Комп'ютерні науки та інформаційні технології. 2023. № 5. С. 68–75.

[3] NIST Special Publication 800-122. Guide to Protecting the Confidentiality of Personally Identifiable Information (PII). National Institute of Standards and Technology, 2010. 53 p.

ОГЛЯД ІСНУЮЧИХ СИСТЕМ ПЕРЕВІРКИ НАДІЙНОСТІ ПАРОЛЯ

Войтенко С.Р.

Керівник: Почанський О.М.

E-mail: vojtenkos24@gmail.com

Харьков, Харківський національний економічний університет імені Семена Кузнеця

У сучасній цифровій системі гарантування достовірності паролів користувачів є надзвичайно важливим для завдання інформаційної безпеки. Дана робота присвячена вивченню систем і методів, що використовуються в даний час для перевірки надійності паролів, їх порівняльної характеристики та основних підходів до оцінки безпеки паролів.

База даних Have I Been Pwned використовує базу даних зламаних паролів, а також перевіряє, чи ваш пароль не був викрадений раніше під час деяких відомих порушень даних. Він також пропонує API для інтеграції в інші служби, підтримує регулярно оновлену базу даних із понад 613 мільйонами унікальних паролів і значно полегшує масову перевірку паролів для корпоративних клієнтів [1].

Система zxcvbn використовує комплексний алгоритм оцінки складності пароля, враховуючи такі фактори як: наявність послідовностей, повторень, спеціальних символів, а також перевірку на наявність слів із різних мов. Особливістю zxcvbn є можливість роботи на стороні клієнта без необхідності відправки пароля на сервер, що підвищує безпеку. Система також враховує популярні заміни символів та розпізнає дати, поштові індекси та інші поширені патерни [2].

Microsoft Password Checker - корпоративне рішення для оцінки надійності пароля. Система використовує технологію машинного навчання для вивчення шаблонів паролів і їх потенційної вразливості. На додаток до цього, система має механізми для запобігання повторному використанню пароля та контролю дотримання політик складності [3].

Google Password Checkup пропонує один із способів перевірити безпеку пароля, об'єднавши функцію перевірки з браузером Chrome. Він дозволяє перевіряти пароль за допомогою криптографічних протоколів, що означає, що паролі не надсилатимуться у вигляді відкритого тексту. Серед особливостей цієї системи – постійний моніторинг нових витоків даних; він автоматично сповіщає користувачів про потенційні загрози. Він також рекомендує способи покращення надійності пароля та пропонує безпечні альтернативи з автоматичною генерацією [4].

LastPass Password Generator [5] пропонує комплексний підхід до створення та перевірки паролів. Система включає:

- генерацію випадкових паролів із заданими параметрами;
- оцінку сили існуючих паролів за multiple факторами;
- перевірку на відповідність галузевим стандартам;
- інтеграцію з корпоративними системами безпеки.

Як висновок можна сказати, що ефективність системи перевірки надійності пароля значною мірою залежить від комплексного застосування різних методів аналізу та постійного оновлення баз даних та алгоритмів відповідно до нових загроз та вимог безпеки.

Література

[1] Have I Been Pwned API Documentation [Електронний ресурс] – Режим доступу до ресурсу: <https://haveibeenpwned.com/API/v3>.

[2] Official zxcvbn Documentation [Електронний ресурс] – Режим доступу до ресурсу: <https://github.com/dropbox/zxcvbn>.

[3] Microsoft Security Guidelines [Електронний ресурс] – Режим доступу до ресурсу: <https://www.microsoft.com/en-us/security/blog/2020/07/08/microsoft-password-guidance>.

[4] Google Security Blog [Електронний ресурс] – Режим доступу до ресурсу: <https://security.googleblog.com/2019/02/protect-your-accounts-from-data.html>.

[5] LastPass Security Documentation - [Електронний ресурс] - [Електронний ресурс] – Режим доступу до ресурсу: <https://www.lastpass.com/security/password-security-generator>.

РОЗРОБКА МОДЕЛІ УПРАВЛІННЯ ІНЦИДЕНТАМИ БЕЗПЕКИ З ВИКОРИСТАННЯМ XDR СИСТЕМ

Гребельний Р.С.

Керівник: Долгова Н.Г.

E-mail: romangrebelnij06@gmail.com

Харків, Харківський Національний Економічний Університет імені Семена Кузнеця

У сучасному цифровому світі з'являється все більше кіберзагроз, які ставлять під загрозу безпеку даних, інфраструктури та конфіденційність користувачів. Одним із найважливіших засобів захисту від цих загроз є системи управління інцидентами. Серед них особливе місце займають рішення XDR (Extended Detection and Response), які мають унікальні можливості аналізу, виявлення та реагування на кіберінциденти [1].

Модель управління кіберінцидентами описує набір стратегій та процедур, які використовуються для виявлення, розслідування та реагування на кіберінциденти.

- Перша модель, реактивна, передбачає реагування на кіберінциденти лише після їх виникнення [2].
- Друга модель, проактивна, спрямована на запобігання кіберінцидентам [3].
- Третя модель, превентивна, спрямована на створення інформаційної системи, яка стійка до кіберінцидентів [4].

Вибір моделі та методів управління кіберінцидентами повинен враховувати розмір організації, її бюджет, галузь діяльності та рівень ризику, це показано на малюнку.

XDR пропонує ряд безпекових переваг, які забезпечують підприємствам повний, адаптивний та ефективний захист від загроз. Інтегруючи свої команди, інструменти та процеси з системами XDR, підприємства можуть покращити свій кіберзахист у різних аспектах[5].

Переваги системи:

- Підвищена видимість;
- Швидке виявлення загроз і негайне реагування;
- Розроблені процеси SecOps;
- Система XDR зменшує складність операцій та витрат на безпеку;
- XDR автоматично оцінює та підкреслює тривалі інциденти з високим ризиком;
- XDR надає центру операцій з безпеки (SOC) потужність штучного інтелекту та автоматизації;
- XDR пропонує набір можливостей, що автоматизують повторювані завдання.

У ході проведеного дослідження виявлено, що системи управління інцидентами XDR та Wazuh є ключовими компонентами в галузі кібербезпеки в сучасному цифровому середовищі [2].

У практичній частині роботи був проведений аналіз переваг та недоліків використання XDR, включаючи огляд процесу впровадження та розгляд компонентів системи.

Особлива увага була приділена системі Wazuh, яка є ще одним важливим інструментом у галузі кібербезпеки[3].

Загальний висновок полягає в тому, що як XDR, так і Wazuh є ефективними інструментами для виявлення та реагування на кіберінциденти. Вони допомагають підвищити кібербезпеку для користувачів та організацій, забезпечуючи найвищий рівень захисту даних, інфраструктури та конфіденційності в цифровому просторі.

Література

[1] Palo Alto Networks. "What is XDR?" [Електронний ресурс] – Режим доступу до ресурсу: <https://www.paloaltonetworks.com/cyberpedia/what-is-xdr>

[2] MITRE ATT&CK Framework for Incident Management. [Електронний ресурс] – Режим доступу до ресурсу: <https://attack.mitre.org/>

[3] Wazuh Documentation. "Open-source security monitoring platform". [Електронний ресурс] – Режим доступу до ресурсу: <https://documentation.wazuh.com/>

[4] Crowley M., Young D. Incident Response and Cyber Resilience: Proactive and Reactive Strategies. Wiley, 2021.

[5] Anton Chuvakin, Augusto Barros, Gary Hayslip. Security Operations Center: Building, Operating, and Maintaining Your SOC. Addison-Wesley, 2020.

КОНТЕКСТНО-ОРІЄНТОВАНІ СИСТЕМИ БАГАТОФАКТОРНОЇ АУНТИФІКАЦІЇ ДЛЯ ГЕТЕРОГЕННИХ ІНФОРМАЦІЙНИХ

Гришко М.С.

Керівник: Розломій І.О.

E-mail: nikitagrisko4@gmail.com

Черкаси, Черкаський державний технологічний Університет

Оскільки кіберзагрози стають дедалі складнішими, інтеграція контекстно-залежних механізмів у системи MFA примітна своєю здатністю забезпечувати як надійну безпеку, так і більш оптимізовану роботу користувача, вирішуючи критичні проблеми, з якими стикаються традиційні методи автентифікації. Важливість контексту в автентифікації підкреслюється його здатністю виявляти незвичні спроби доступу та зменшувати потенційні ризики для безпеки. Наприклад, фінансова установа може вимагати додаткової перевірки, якщо користувач намагається ввійти з нерозпізаного місця, незважаючи на використання правильного пароля [1].

Цей адаптивний підхід не лише покращує безпеку, розпізнаючи аномалії та реагуючи на них, але також зменшує непотрібні перешкоди для користувачів, які отримують доступ до своїх облікових записів зі знайомих і надійних середовищ.

Відповідно, контекстно-залежні системи MFA все частіше застосовуються в різних секторах, включаючи фінанси та охорону здоров'я, де захист конфіденційних даних є першорядним. Однак реалізація контекстно-залежних систем MFA не позбавлена проблем. Занепокоєння щодо конфіденційності користувачів, потенційних збоїв у роботі та складності інтеграції в існуючу інфраструктуру створюють значні перешкоди для організацій, які прагнуть застосувати ці розширені заходи безпеки.

Більше того, потреба у збалансованому підході, який забезпечує зручність для користувача, забезпечуючи при цьому надійні заходи безпеки, ще більше ускладнює розгортання контекстно-залежних систем.

Ці суперечки підкреслюють постійний діалог навколо етичних наслідків і практичних аспектів впровадження технологій контекстно-залежної автентифікації. У міру розвитку ландшафту кібербезпеки очікується, що роль контекстно-залежних систем MFA буде розширюватися завдяки прогресу в області штучного інтелекту та машинного навчання. Ця еволюція обіцяє підвищити адаптивність і ефективність протоколів безпеки, прокладаючи шлях для більш інтелектуальних систем, які можуть динамічно реагувати на поведінку користувачів і фактори навколишнього середовища, зберігаючи при цьому відповідність нормативним нормам, таким як Загальний регламент захисту даних (GDPR).

Зрештою, розробка та впровадження контекстно-залежних систем MFA означає критичний зсув до більш інтуїтивно зрозумілого та безпечного досвіду користувачів у все більш цифровому світі [2].

Системи контекстно-залежної багатофакторної автентифікації (MFA) представляють значний прогрес у захисті цифрових взаємодій шляхом використання контекстної інформації для покращення процесів перевірки користувачів. Фундаментальна концепція контекстно-залежних обчислень, представлена Шілітом і Теймером у 1994 році, заклала основу для

розуміння того, як пристрої можуть розумно реагувати на потреби користувачів на основі ситуаційної обізнаності.

Література

[1] Loske, M., Rothe, L., & Gertler, D. G. (2019, April). Context-aware authentication: State-of-the-art evaluation and adaption to the IIoT. In 2019 IEEE 5th world forum on Internet of Things (WF-IoT), pp. 64-69.

[2] Liu, Z., Bonazzi, R., & Pigneur, Y. (2016). Privacy-based adaptive context-aware authentication system for personal mobile devices. Journal of mobile multimedia, pp. 159-180.

ВИКОРИСТАННЯ SNORT ДЛЯ ЗАХИСТУ ІОТ-ПРИСТРОЇВ: ІНТЕГРАЦІЯ З ДОМАШНІМИ МАРШРУТИЗАТОРАМИ ТА ВИЯВЛЕННЯ БОТНЕТ-АТАК

Довбня М.В.

Керівник: Леуенко О. В.

E-mail: maksym.dovbnia@hneu.net, Oleksii.Leunencko@hneu.net

Харків, Харківський національний економічний університет імені Семена Кузнеця

З розвитком Інтернету речей (IoT) зростає потреба у надійних методах захисту підключених пристроїв від кіберзагроз. У даній роботі розглядається застосування системи виявлення та запобігання вторгненням Snort для безпеки IoT-пристроїв. Основна увага приділяється інтеграції Snort із домашніми маршрутизаторами та механізмам виявлення ботнет-атак.

Інтернет речей (IoT) швидко поширюється, забезпечуючи автоматизацію та зручність у повсякденному житті. Проте, із збільшенням кількості IoT-пристроїв зростає і кількість кіберзагроз [2]. Багато IoT-пристроїв мають обмежені можливості безпеки, що робить їх вразливими до атак, таких як ботнети. Для підвищення рівня безпеки домашніх мереж із IoT-пристроями доцільно використовувати системи виявлення та запобігання вторгненням (IDS/IPS), такі як Snort [1].

Snort є однією з найпопулярніших систем для виявлення та запобігання вторгненням. Це безкоштовне рішення з відкритим кодом, що здійснює аналіз мережевого трафіку у реальному часі. [1] Включає механізми аналізу за сигнатурами, перевірку мережевих протоколів і виявлення підозрілих аномалій. Може функціонувати у декількох режимах, зокрема як система моніторингу мережевого трафіку або реєстрації пакетів.

Для захисту IoT-пристроїв у домашній мережі Snort можна інтегрувати з маршрутизаторами, наприклад, використовуючи pfSense — безкоштовний дистрибутив на базі FreeBSD, призначений для налаштування маршрутизаторів і брандмауерів. pfSense підтримує встановлення пакета Snort, що дозволяє реалізувати функції IDS/IPS безпосередньо на маршрутизаторі.

Етапи встановлення Snort на pfSense:

- Встановлення пакета Snort: у веб-інтерфейсі pfSense перейти до "System" > "Package Manager" > "Available Packages". Знайти Snort і встановити його. [2]
- Налаштування інтерфейсів: після встановлення перейти до "Services" > "Snort". Додати інтерфейси, на яких працюватиме Snort (наприклад, WAN і LAN).
- Налаштування правил та оновлень: активувати необхідні правила для виявлення ботнет-атак та інших загроз.

Інтеграція Snort у pfSense дозволяє аналізувати весь вхідний і вихідний трафік, забезпечуючи надійний захист IoT-пристроїв.

Snort використовує сигнатурний метод виявлення атак, ґрунтуючись на заздалегідь визначених правилах. Для ідентифікації ботнет-активності застосовуються такі методи:

- Аналіз аномального трафіку;
- Виявлення підключень до відомих командно-контрольних серверів (C&C);

- Виявлення спроб сканування портів та інших підозрілих дій.

Крім того, Snort підтримує використання додаткових модулів для підвищення ефективності виявлення складних загроз.

Використання Snort у поєднанні з домашніми маршрутизаторами (наприклад, pfSense) забезпечує ефективний спосіб захисту IoT-пристроїв у домашніх мережах. Інтеграція Snort дозволяє своєчасно виявляти та запобігати ботнет-атакам і іншим кіберзагрозам, підвищуючи загальний рівень безпеки мережі.

Література

[1] Snort – Вікіпедія [Електронний ресурс] – Режим доступу до ресурсу: <https://uk.wikipedia.org/wiki/Snort>

[2] Tutorial – Snort Installation auf Pfsense [Schritt für Schritt]. [Електронний ресурс] – Режим доступу до ресурсу: <https://techexpert.tips/uk/pfsense/snort-installation/>

[3] Огляд Snort для виявлення вторгнень [Електронний ресурс] – Режим доступу до ресурсу: <https://vaiti.io/obzor-snort-dlya-obnaruzheniya-vtorzhenij/>

[4] Intrusion detection systems for IoT-based smart environments: a survey [Електронний ресурс] – Режим доступу до ресурсу: <https://journalofcloudcomputing.springeropen.com/articles/10.1186/s13677-018-0123-6>

[5] Використання штучного інтелекту в IPS та IDS системах [Електронний ресурс] – Режим доступу до ресурсу: https://elartu.tntu.edu.ua/bitstream/lib/44382/2/IMSTT_2023_Humeniuk_V_R-Using_artificial_intelligence_34.pdf

ДОСЛІДЖЕННЯ ПОТЕНЦІЙНИХ КІБЕРЗАГРОЗ ТА МЕТОДІВ ЗАХИСТУ ЗАГАЛЬНИХ ПЛОЩАДОК ЕЛЕКТРОННОЇ ТОРГІВЛІ

Донченко А.О.

Керівник: Семенов С.Г.

E-mail: cleverman2215@gmail.com

Харків, Харківський національний економічний університет імені Семена Кузнеця

Сучасний електронний бізнес є важливим інструментом для розвитку підприємництва, однак також стає мішенню для кіберзлочинців. З кожним роком обсяги торгівлі в Інтернеті збільшуються, що приваблює увагу не лише бізнес-власників, а й злочинців. Це зумовлює необхідність досліджень потенційних кіберзагроз та розробку ефективних методів захисту електронних торгових платформ.

Метою дослідження була розробка теоретичних положень та практичних рекомендації щодо потенційних кіберзагроз та методів захисту загальних площадок електронної торгівлі.

Перша частина дослідження включає аналіз сучасних загроз, таких як фішинг, шкідливе ПЗ, атаки на відмову в обслуговуванні (DDoS) та інші методи кіберзлочинців, спрямовані на електронну торгівлю.

Наступний розділ присвячено методам захисту електронної торгівлі. Зокрема, описано різні методи захисту:

- Використання SSL/TLS протоколів для забезпечення захищеного з'єднання;
- Впровадження багатофакторної аутентифікації;
- Регулярні оновлення та патчі системного ПЗ;
- Використання фаєрволів та систем виявлення вторгнень (IDS/IPS).

Третя частина саме про проектування та розробку платформи для електронної торгівлі.

Описано процес вибору інструментів для розробки, проектування структури бази даних, внутрішньої структури платформи та графічного інтерфейсу користувача.

Результати дослідження можуть бути використані для покращення кібербезпеки на існуючих та нових платформах електронної торгівлі, що сприятиме зменшенню ризиків для бізнесу та споживачів.

В роботі досліджено функції потенційних кіберзагроз та методи захисту загальних площадок електронної торгівлі. Запропоновано практичні рекомендації, що можуть бути впроваджені для покращення безпеки у сфері електронної торгівлі.

Ці тези охоплюють основні аспекти дослідження та надають короткий огляд структури та змісту дипломної роботи, яка присвячена аналізу кіберзагроз та методам їх захисту на платформах електронної торгівлі.

ПРОГРАМНА РЕАЛІЗАЦІЯ ЗДІЙСНЕННЯ БАГАТОЕТАПНОГО ВИБОРУ В УМОВАХ РИЗИКУ

Єфімов М.Ю.

Керівник: Солодовник Г.В.

E-mail: ganna.solodovnyk@hneu.net

Харків, Харківський національний економічний університет імені Семена Кузнеця

Актуальність. Процес управління передбачає підготовку та ухвалення рішень, які базуються на результатах інших, ще не реалізованих рішень. Таким чином виникає додатковий чинник невизначеності та ризику, пов'язаний з відсутністю повної інформації щодо результатів здійснення попередніх запланованих заходів. В цьому випадку утворюється ланцюг взаємопов'язаних рішень, для яких успіх реалізації кожного наступного рішення обумовлюється результатами попереднього та багатьма іншими стохастичними факторами. Задача здійснення вибору в цій ситуації може бути розв'язана в рамках багатоетапних ігор з природою за допомогою побудови дерева рішень [1].

Метою роботи є розробка програмної реалізації розв'язання задачі здійснення багатоетапного вибору в умовах невизначеності за допомогою дерева рішень.

Сформульована в роботі задача полягає у визначенні необхідності проведення додаткових ринкових досліджень фірмою, яка виробляє обчислювальну техніку. Після здійснення попереднього аналізу ринку нової високопродуктивної техніки було визначено розмір прибутків (або збитків) у разі сприятливого та несприятливого стану ринку для двох альтернатив: виробництва великої та невеликої партій техніки. За відсутності додаткової інформації щодо майбутнього ринкового стану суб'єкт управління вважає обидва ринкові стани рівноймовірними, проте додаткові ринкові дослідження можуть уточнити ці ймовірності та повисити ефективність рішення. Такі дослідження потребують додаткових капіталовкладень, тому перш ніж приймати рішення щодо розміру партії, яку слід випускати необхідно визначитися з тим чи проводити додаткові дослідження. Розміри прибутків (або збитків) від виробництва великої та невеликої партій техніки є ймовірнісними величинами, оскільки залежать від ринкового стану, тому рішення приймаються в умовах ризику та невизначеності. У сформульованій таким чином задачі утворюється послідовність рішень, для прийняття яких слід скористатися математичним апаратом теорії ігор, а саме методом прийняття рішень за допомогою дерева рішень.

З метою автоматизації розв'язку даної задачі було розроблено програму, робота якої складається з таких етапів:

- введення вхідних даних (очікуваний прибуток або збиток від випуску великої та невеликої партій техніки, ймовірності сприятливих та несприятливих ринкових умов, витрати на додаткове обстеження ринку);
- побудова дерева рішень (використовується бібліотека Graphviz для візуалізації дерева рішень, кожен вузол якого відображає певне рішення і очікувані прибутки);
- розрахунки очікуваних грошових оцінок для кожної гілки дерева (обчислення для двох основних варіантів: якщо обстеження ринку не проводиться та якщо обстеження ринку

проводиться, і враховуються прогнози сприятливих і несприятливих умов із ймовірностями, наданими експертом);

- аналіз результатів (на підставі порівняння значень очікуваних грошових оцінок програма визначає, чи варто замовляти обстеження ринку, яку максимальну суму можна виплатити експерту, а також розраховує очікувану грошову оцінку найкращого рішення);
- збереження результатів (побудоване дерево рішень зберігається як зображення у форматі PNG) (рис. 1).



Рисунок 1 – Дерево рішень

Програмна реалізація була здійснена мовою Python, яка є вільною та відкритою мовою програмування та розповсюджується під ліцензією Python Software Foundation License (PSFL), тобто дозволяє безкоштовне використання, модифікацію та розповсюдження [2]. Вихідний код Python доступний на GitHub, що спрощує його перегляд, зміну та покращення. Перевагою Python є його кросплатформність: працює на Windows, macOS, Linux, а також на мобільних ОС (Android, iOS через спеціальні обгортки). Наразі Python має понад 450 000 бібліотек у PyPI, які також є відкритими (NumPy, Pandas, Flask, TensorFlow тощо). Оновлення Python координуються Python Software Foundation (PSF).

В процесі автоматизації також було використано бібліотеку Graphviz, яка є відкритим програмним забезпеченням для візуалізації графів [3]. Візуалізація графів – це спосіб представлення структурної інформації як діаграми абстрактних графіків та мереж, має важливі застосування в мережах, біоінформатиці, програмній інженерії, базах даних та веб-дизайні, а також в машинному навчанні та візуальних інтерфейсах для інших технічних областей. Graphviz має кілька основних програм компонування графів, а також веб та інтерактивні графічні інтерфейси, допоміжні інструменти, бібліотеки та мовні прив'язки. Програми верстки Graphviz виконують описи графіків простою текстовою мовою і роблять діаграми в декількох корисних форматах, таких як зображення і SVG для веб-сторінок, Postscript для включення в PDF або інші документи. Graphviz надає можливості відображення в інтерактивному переглядачі графіків.

Graphviz підтримує багато мов програмування, і його можна інтегрувати у Python (graphviz або pygraphviz), C/C++, Java, JavaScript (d3-graphviz), Go, R, Haskell, Ruby, PHP, Perl та багато інших. Крім того Graphviz підтримує діалект XML GXL.

Висновок. Розроблена програма призначена для формування правильної техніко-економічної стратегії в умовах ризику та невизначеності. Побудоване дерево рішень чітко демонструє всі можливі варіанти розвитку подій і очікувані результати. Використання дерева рішень дозволяє враховувати ймовірності подій і ризику. Розроблена програма відповідає на ключові економічні запитання, допомагаючи обрати оптимальну стратегію. Такий підхід може бути адаптований для інших бізнес-задач, що потребують аналізу умов невизначеності. Виконана робота підтверджує ефективність використання математичних моделей у прийнятті управлінських рішень.

Програму реалізовано мовою Python, що через свою відкритість розвивається завдяки глобальній спільноті розробників, яка підтримує бібліотеки, виправляє баги та додає нові можливості.

Література

- [1] Теорія прийняття рішень : конспект лекцій / О. В. Горда. – Київ : КНУБА, 2023. – 120 с.
- [2] Python [Електронний ресурс] – Режим доступу до ресурсу: <https://www.python.org/>
- [3] Graphviz [Електронний ресурс] – Режим доступу до ресурсу: <https://graphviz.org/>

КРИТИЧНА РОЛЬ ТЕСТУВАННЯ РІВНЯ ЗАХИЩЕНОСТІ ВЕБ-РЕСУРСІВ

Єфременков К.О.

Керівник: Лимаренко В.В.

E-mail: viacheslav.lymarenko@hneu.net

Харків, Харківський національний економічний університет імені Семена Кузнеця

Веб-ресурси це будь які об'єкти, які можна знайти за унікальною адресою. Вони відіграють важливу роль у цифровому середовищі, забезпечуючи доступ до інформації, послуг і комунікацій. До веб-ресурсів відносяться усі об'єкти в мережі, починаючи від маленьких фотографій та закінчуючи цілими системами й базами даних. [1]

Нажаль зловмисники налаштовані порушити сервіс, знаходячи вразливості та атакуючи слабкі точки веб-сайтів. Це в результаті може призвести до шкоди обслуговуванню, спотворенню інформаційного контенту та витоку даних. У разі порушення безпеки можуть бути пошкоджені або вкрадені дані. Нажаль успішні атаки часто стають причиною масштабних витоків даних та фінансових втрат. [3]

Одними з найпоширеніших кібератак є:

- Дос та ДДоС
- Міжсайтовий скриптінг
- SQL Ін'єкції
- Ransomware
- Атака нульового кліку

Кібератаки особливо небезпечні під час нульового дня, але таких втрат можна уникнути завдяки гарно підготовленому захисту, котрий буде створений для супротиву поширеним атакам. Щоб зрозуміти з чого починати та що потрібно захищати, для цього є тестування рівня безпеки веб-ресурсів. [2]

Основними видами тестування безпеки котрі допоможуть з сучасними кібератаками є:

- Виявлення вразливостей для пошуку слабких точок у системах шляхом поверхневого аналізу.
- Тестування на проникнення, що полягає у імітації реальних атак для оцінки безпеки веб-ресурсів на більш глибокому рівні.
- Перевірка регулювання трафіку системи на перенавантаження

Тестування рівня захисту і вживання заходів для покращення безпеки допоможе власникам вебсайтів збільшити шанси уникнення атак нульового дня.

Література

- [1] Wikipedia. Поняття веб-ресурсу [Електронний ресурс] – Режим доступу до ресурсу: https://simple.wikipedia.org/wiki/Web_resource
- [2] Р. Дубинецький. "Що таке веб-тестування?". [Електронний ресурс] – Режим доступу до ресурсу: <https://embo.com.ua/uk/blog/what-is-web-testing/>
- [3] С. М. Alliance. "January 2025: Recent Cyber Attacks, Data Breaches, Ransomware Attacks". [Електронний ресурс] – Режим доступу до ресурсу: <https://www.cm-alliance.com/cybersecurity-blog/january-2025-recent-cyber-attacks-data-breaches-ransomware-attacks>

БЕЗКОШТОВНІ СЕРВІСИ ДЛЯ ОЦІНКИ СКЛАДНОСТІ ТА ГЕНЕРАЦІЇ ПАРОЛІВ

Загнібеда А.О.

Керівник: Міхєєв І.А.

E-mail: anastasiia.zagnibeda@icloud.com

Харків, Харківський національний економічний університет імені Семена Кузнеця

У сучасному світі розвиток хакерських технологій, зокрема атаки грубої сили та аналіз витоків даних, значно підвищує ризик несанкціонованого доступу до облікових записів користувачів. Згідно зі звітом Digital Defense Report компанії Microsoft у 2021 році Україна посіла друге місце у рейтингу країн, які найчастіше зазнавали хакерських атак, а вже у 2024 році в Україні було зафіксовано 4315 кібератак, що на 69,8% більше порівняно з 2023 роком (рис. 1) [1-2].

Приблизно 60% кібератак спрямовані на паролі, що охоплює фішинг, атаки методом підбору (brute force), повторне використання паролів і виток даних. Використання слабкого пароля підвищує ймовірність витоків даних до 80%, а повторне використання паролів призводить до 30% компрометацій через фішингові атаки. Попри ризики, показники повторного використання паролів залишаються високими – 13% користувачів використовують однакові паролі для різних облікових записів, проте паролі, що містять 12 символів зламати у 62 трильйони разів складніше, ніж пароль із 6 символів. [3]

- Україна посіла друге місце у рейтингу країн за кількістю кібератак у 2021 році (19%).
- У 2024 році кількість кібератак зросла на 69,8%.
- 60% кібератак спрямовані на паролі користувачів.
- Слабкі паролі стали причиною понад 80% витоків даних організацій.
- 70% слабких паролів можуть бути зламані хакерами менш ніж за 1 секунду.
- До 30% витоків даних в організаціях відбуваються через фішингові атаки.
- Пароль із 12 символів зламати у 62 трильйони разів складніше, ніж пароль із 6 символів.

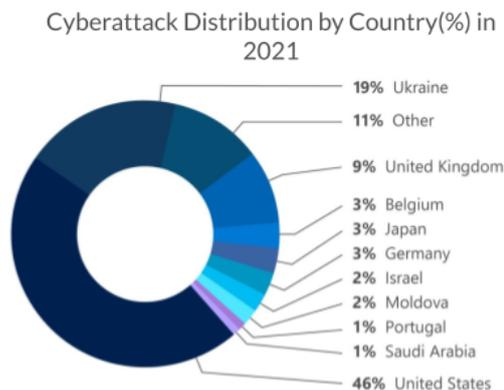


Рисунок 1 – Цифри і факти про кібератаки

Зазначені загрози свідчать про зростання потреби у використанні інструментів для створення надійних та складних для зламування паролів.

У роботі планується розглянути два основних види сервісів щодо теми дослідження.

Сервіси для оцінки складності пароля [4-7]. Такі сервіси як 2ip.io, Password Monster, UIC та Security.org, допомагають оцінити стійкість пароля та надають як кількісну, так і якісну оцінку його надійності, враховуючи такі фактори, як довжина пароля, наявність різних типів символів (великі та малі літери, цифри, спеціальні символи). Однак, деякі з них мають додаткові особливості:

- сервіс UIC – можливість приховати та показати пароль.
- сервіс Password Monster – можливість приховати та показати пароль, а також опис кількості символів і типів, що використовуються.

Для порівняння результатів аналізу було сформовано декілька критеріїв, що є важливими для подібних сервісів. Результат порівняльного аналізу за ключовими критеріями наведено в табл. 1.

Таблиця 1. Результати порівняльного аналізу сервісів для оцінки паролів

	2ip.io	Password Monster	UIC	Security.org
Функція приховування пароля	✘	✓	✓	✓
Функція відкриття пароля	✓	✓	✓	✘
Кількісна оцінка	✓	✓	✓	✓
Якісна оцінка	✓	✓	✓	✓
Мова інтерфейсу	UKR	ENG	ENG	ENG

Сервіси для генерації паролів [8-11]. Такі сервіси як Хостинг Україна, 2ip.ua, LastPass, Password Generator Plus 3.0, допомагають створити надійний пароль, що відповідає вимогам безпеки, враховуючи такі фактори, як довжина пароля, наявність різних типів символів (великі та малі літери, цифри, спеціальні символи). Однак, деякі з них мають додаткові особливості:

- Хостинг Україна – багато варіантна генерація паролів на основі заздалегідь визначеного набору символів, можливість виключення схожих символів та генерація пулу унікальних паролів.
- LastPass – генерація паролів для зручної вимови, створення паролів для спрощеного сприйняття та прочитання.
- Password Generator Plus 3.0 – можливість обрати, з чого починається пароль, виключення схожих, повторних та послідовних символів, автоматична генерація паролів при першому відкритті сервісу, можливість вибору кількості паролів та збереження налаштувань пароля.

Для порівняння результатів аналізу було сформовано декілька критеріїв, що є важливими для подібних сервісів. Результат порівняльного аналізу за ключовими критеріями наведено в табл. 2

Таблиця 2. Результати порівняльного аналізу сервісів для генерації паролів

	Хостинг Україна	2ip.ua	LastPass	Password Generator Plus 3.0
Довжина паролю	✓	✓	✓	✓
Цифри	✓	✓	✓	✓
Верхній регістр	✓	✓	✓	✓
Нижній регістр	✓	✓	✓	✓
Спеціальні символи	✓	✓	✓	✓
Кількість паролів	✘	✓	✘	✓
Мова інтерфейсу	UKR	UKR	ENG	ENG

Проаналізувавши сервіси, можна зробити висновок, що кожен сервіс має свої недоліки, переваги та особливості, які визначають його ефективність залежно від обставин. Також варто зазначити, що використання одного сервісу не дає повної гарантії захисту. Генерація складного пароля залежить від сценарію, обраного користувачем, і не завжди результатом буде саме складний пароль. Виходячи з переваг різних сервісів, можна зробити висновок, що для підвищення безпеки варто комбінувати їх, використовуючи як для генерації, так і для оцінки паролів. Використання вищезазначених інструментів допомагає користувачам залишатися обізнаними у сфері кібербезпеки та надійно захищати дані від несанкціонованого доступу. Результати дослідження будуть використані для побудови веб-сервісу із відповідним функціоналом.

Література

[1] Офіційний сайт Microsoft // Microsoft Digital Defense Report // What we're seeing [Електронний ресурс] – Режим доступу до ресурсу: <https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/FY21-Microsoft-Digital-Defense-Report.pdf>

[2] Офіційний сайт Forbes Ukraine [Електронний ресурс] – Режим доступу до ресурсу: <https://forbes.ua/news/v-ukraini-za-rik-kilkist-kiberatak-zrosla-na-70-nauposhirenishi-tipi-intsidentiv-i-golovni-tsili-khakeriv-08012025-26137>

[3] JumpCloud Blog [Електронний ресурс] – Режим доступу до ресурсу: <https://jumpcloud.com/blog/password-statistics-trends>

[4] 2IP.io [Електронний ресурс] – Режим доступу до ресурсу: <https://2ip.io/ua/passcheck/>

[5] Password Monster [Електронний ресурс] – Режим доступу до ресурсу: <https://www.passwordmonster.com/>

[6] UIC [Електронний ресурс] – Режим доступу до ресурсу: <https://www.uic.edu/apps/strong-password/>

[7] Security.org [Електронний ресурс] – Режим доступу до ресурсу: <https://www.security.org/how-secure-is-my-password/>

[8] Хостинг Україна [Електронний ресурс] – Режим доступу до ресурсу: <https://www.ukraine.com.ua/info/tools/passwdgenerate/>

[9] 2IP.ua [Електронний ресурс] – Режим доступу до ресурсу: <https://2ip.ua/ua/services/useful-service/password-generator>

[10] LastPass [Електронний ресурс] – Режим доступу до ресурсу: <https://www.lastpass.com/features/password-generator>

[11] Password Generator Plus 3.0 [Електронний ресурс] – Режим доступу до ресурсу: <https://passwordsgenerator.net/>

РОЗРОБКА МОДЕЛІ ДЛЯ ПРОТИДІЇ СПАМУ НА ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІ СИСТЕМИ

Іванько А.С.

Керівник: Старкова О.В.

E-mail: vzai044@gmail.com

Харків, Харківський національний економічний університет імені Семена Кузнеця

Спам – це масове розсилання небажаних або шкідливих повідомлень через електронні канали зв'язку, такі як електронна пошта, месенджери, соціальні мережі. Відповідно до "Великого тлумачного словника української мови", спам -це небажана кореспонденція, що заважає ефективному функціонуванню інформаційних систем [1].

З розвитком цифрових технологій спам стає дедалі складнішим, створюючи загрози для конфіденційності, фінансової безпеки та стабільності інформаційних ресурсів. Він використовується для фішингу, поширення шкідливого програмного забезпечення, шахрайських схем і дезінформації. Окрім цього, він перевантажує каналів зв'язку, що знижує продуктивності інформаційних систем.

Для протидії впливу спаму використовують різні методи: чорні списки (Blacklists), які блокують відомі джерела спаму; байєсівські фільтри, що аналізують зміст повідомлень; евристичного аналіз, який виявляє підозрілі закономірності; алгоритми машинного навчання, що автоматично розпізнають спам [2].

Оскільки сучасні кіберзлочинці постійно вдосконалюють методи обходу спам-фільтрів, традиційні методи виявлення спаму потребують удосконалення та адаптації до нових загроз. Перспективним напрямком у боротьбі зі спамом є використання штучного інтелекту та глибокого навчання, що дозволяє виявляти складні патерни у спамових повідомленнях і підвищувати ефективність їхньої ідентифікації. Також важливим є аналіз мета-даних повідомлень, таких як частота надсилання, поведінкові характеристики відправників, структура тексту та рівень довіри до джерела повідомлення.

На даному етапі дослідження основна увага приділяється аналізу існуючих методів боротьби зі спамом та їх недоліків. Вивчаються різні підходи, їх ефективність та проблеми реалізації. Подальші дослідження будуть спрямовані на розробку власної моделі протидії спаму, яка поєднуватиме кілька методів для підвищення ефективності фільтрації та виявлення нових загроз.

Література

[1] Великий тлумачний словник української мови / уклад. і голов. ред. Бусел В.Т. Київ; Ірпінь : Перун, 2009. – 1736 с.

[2] Солодовник Г.В. Методи та системи штучного інтелекту : навчальний посібник. – Харків: ТОВ «ДІСА ПЛЮС», 2021. – 177 с.

[3] ДСТУ 8302:2015 Інформація та документація. Бібліографічне посилання. Загальні положення та правила складання. – Київ: ДП УкрНДНЦ, 2016. – 17 с.

ЗАСТОСУВАННЯ ДИФЕРЕНЦІАЛЬНОЇ ПРИВАТНОСТІ ДЛЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

Клюєв В. О.

Керівник: Розломий І. О.

E-mail: v.o.kliuiev.fitis23@chdtu.edu.ua

Черкаси, Черкаський державний технологічний університет

Захист персональних даних у сучасних інформаційних системах є критично важливим завданням. Одним із перспективних підходів є використання диференціальної приватності. Ця технологія дозволяє зберігати анонімність користувачів навіть при аналізі великих обсягів інформації. Основна ідея полягає у внесенні контрольованого шуму до даних, що унеможливорює ідентифікацію окремих осіб, зберігаючи при цьому статистичну корисність інформації [1].

Методи диференціальної приватності знаходять широке застосування в різних галузях. Наприклад, у сфері охорони здоров'я цей підхід дозволяє аналізувати медичні дані без розкриття особистої інформації пацієнтів. У фінансовому секторі забезпечується захист транзакційних записів, що сприяє зниженню ризиків витоку конфіденційних відомостей. В освітніх та наукових дослідженнях ця технологія допомагає збирати дані про успішність студентів без компрометації їхньої конфіденційності. Крім того, компанії, що працюють у сфері цифрового маркетингу, можуть використовувати диференціальну приватність для аналізу поведінкових даних споживачів без ризику порушення їхніх прав.

Практична реалізація диференціальної приватності включає кілька підходів. Один із них — механізм Лапласа, що додає випадковий шум до відповідей запитів до бази даних. Інший варіант — механізм Гаусса, який також застосовує стохастичні зміни, але з урахуванням більш точних параметрів розподілу даних. Також існують методи перетворення даних на локальному рівні, що забезпечує конфіденційність ще до їхньої передачі на сервери. Деякі системи використовують алгоритми агрегованого навчання, які дозволяють обробляти дані без необхідності їхньої централізованої обробки, що підвищує рівень безпеки[2].

Головною перевагою диференціальної приватності є можливість отримання корисних статистичних висновків без загрози ідентифікації користувачів. Однак існують і виклики. Оптимальний баланс між рівнем анонімності та точністю аналізу даних залишається відкритим питанням. Надмірне зашумлення може спотворити результати, тоді як недостатній рівень захисту може створювати ризики витоку інформації. Крім того, впровадження таких методів потребує значних обчислювальних ресурсів, що може впливати на продуктивність інформаційних систем.

Дослідження у цій сфері активно розвиваються, оскільки забезпечення конфіденційності даних стає дедалі актуальнішим. Впровадження методів диференціальної приватності в інформаційні системи допомагає вирішити проблему безпеки персональних даних, забезпечуючи баланс між захистом інформації та її аналітичною цінністю. Надалі очікується удосконалення алгоритмів, що дозволить підвищити ефективність аналізу великих даних без загрози порушення конфіденційності.

References

[1] Zhu, T., Ye, D., Wang, W., Zhou, W., & Philip, S. Y. (2020). More than privacy: Applying differential privacy in key areas of artificial intelligence. *IEEE Transactions on Knowledge and Data Engineering*, 34(6), 2824-2843.

[2] ZHU, Tianqing, et al. More than privacy: Applying differential privacy in key areas of artificial intelligence. *IEEE Transactions on Knowledge and Data Engineering*, 2020, 34.6: 2824-2843.

ОГЛЯД СУЧАСНИХ КРИПТОГРАФІЧНИХ АЛГОРИТМІВ

Ключко О.О.

Керівник: Венгіна О.С.

E-mail: sos200oleg@gmail.com

Харків, Харківський національний економічний університет імені Семена Кузнеця

Сучасні веб-застосунки для обміну повідомленнями є невід'ємною частиною повсякденного життя користувачів. Основними вимогами до таких систем є швидкість передавання даних, безпека та конфіденційність. Використання технологій шифрування гарантує захист інформації від несанкціонованого доступу та забезпечує безпечну комунікацію.

Розробка безпечних месенджерів базується на сучасних криптографічних алгоритмах, таких як AES (Advanced Encryption Standard), RSA (Rivest-Shamir-Adleman) та E2EE (End-to-End Encryption). Реалізація наскрізного шифрування гарантує, що повідомлення можуть бути розшифровані лише відправником і отримувачем, навіть якщо дані перехоплені на сервері.

Основні сучасні криптографічні алгоритми

- Advanced Encryption Standard (AES) – симетричний алгоритм шифрування, що забезпечує високу ефективність та надійний захист даних. Він широко застосовується в банківських системах, VPN та Wi-Fi безпеці. AES може шифрувати дані з довжиною ключа 128, 192 і 256 біт, що робить його стійким до атак.

- Rivest-Shamir-Adleman (RSA) – асиметричний алгоритм, який використовується для безпечного обміну ключами та цифрових підписів. Його безпека ґрунтується на складності факторизації великих чисел.

- Еліптична криптографія (ECC) – забезпечує такий самий рівень безпеки, як і RSA, при меншій довжині ключа, що робить її ефективною для мобільних і IoT-пристроїв.

- Хеш-функції (SHA-256, SHA-3) – алгоритми криптографічного хешування, які використовуються для забезпечення цілісності даних і цифрових підписів. Вони є основними компонентами сучасних систем безпеки.

- Постквантова криптографія – напрям, спрямований на створення стійких до атак квантових комп'ютерів алгоритмів шифрування. Оскільки квантові обчислення можуть загрожувати класичним криптографічним методам, активно розробляються нові алгоритми.

Сучасні веб-застосунки для обміну повідомленнями потребують високого рівня захисту даних у цифрових комунікаціях. Криптографічні алгоритми є важливими інструментами для гарантування безпеки інформації. Використання AES, RSA, E2EE та інших технологій дозволяє забезпечити конфіденційність, цілісність та автентифікацію даних. Подальший розвиток криптографії сприятиме створенню ще більш безпечних цифрових сервісів.

Література

[1] Wikipedia. End-to-End Encryption [Електронний ресурс] – Режим доступу до ресурсу: https://wikipedia.org/wiki/End-to-end_encryption

[2] AES Encryption Standard [Електронний ресурс] – Режим доступу до ресурсу: <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf>

[3] Post-Quantum Cryptography [Електронний ресурс] – Режим доступу до ресурсу: <https://csrc.nist.gov/Projects/Post-Quantum-Cryptography>

РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ВИЯВЛЕННЯ КІБЕРЗАГРОЗ З ВИКОРИСТАННЯМ АЛГОРИТМУ RANDOM FOREST

Костерний В.О.

Керівник: Шаповалова О.О.

E-mail: wetal.kosternoi@gmail.com

Харків, Харківський національний економічний університет імені Семена Кузнеця

У сучасному світі проблема кібербезпеки набуває все більшої актуальності через стрімкий розвиток інформаційних технологій та зростаючу залежність бізнес-процесів від цифрової інфраструктури. Особливої уваги заслуговує питання захисту від розподілених атак відмови в обслуговуванні (DDoS), які становлять значну загрозу для функціонування мережевих сервісів та можуть призвести до суттєвих фінансових втрат [1, 4, 10, 12].

Метою дослідження є розробка ефективного програмного забезпечення для виявлення кіберзагроз, зокрема DDoS-атак, з використанням алгоритму Random Forest [5, 9, 13] та порівняння його ефективності з іншими методами машинного навчання.

Сучасний кіберпростір характеризується різноманітністю загроз [6,7], серед яких можна виділити: віруси, трояни, програми-вимагачі, фішингові атаки та DDoS-атаки. Останні представляють особливий інтерес через їх масштабність та складність виявлення. DDoS-атаки спрямовані на порушення доступності сервісів шляхом генерації великої кількості запитів, що перевищують можливості обробки цільової системи.

Вибір DDoS-атак як об'єкта дослідження обумовлений наступними факторами [1]:

- зростання кількості та потужності атак (у 2024 році зафіксовано збільшення на 30% порівняно з попереднім роком);
- складність своєчасного виявлення через різноманітність векторів атаки;
- значні економічні збитки для бізнесу (середній час простою сервісу становить 6-8 годин);
- постійна еволюція методів проведення атак, що вимагає вдосконалення систем захисту.

Сучасні методи виявлення кіберзагроз можна розділити на кілька категорій:

- статистичні методи аналізу трафіку;
- сигнатурні методи;
- методи машинного навчання;
- гібридні підходи.

Особлива увага приділяється методам машинного навчання, зокрема порівнянню ефективності згорткових нейронних мереж (CNN) [2,9] та алгоритму Random Forest. CNN демонструють високу ефективність у розпізнаванні патернів у даних, проте вимагають значних обчислювальних ресурсів та часу на навчання. Random Forest, у свою чергу, пропонує ряд переваг [5]:

- висока точність класифікації;
- стійкість до перенавчання;
- можливість паралельної обробки даних;
- прозорість прийняття рішень.

У рамках дослідження розроблено програмне забезпечення на основі алгоритму Random Forest, яке аналізує мережевий трафік за наступними параметрами:

- інтенсивність пакетів;
- розмір пакетів;
- ентропія заголовків;
- статистичні характеристики потоків даних;
- часові характеристики з'єднань.

Архітектура розробленої системи включає наступні компоненти:

- модуль захоплення та попередньої обробки трафіку;
- підсистема виділення ознак;
- класифікатор на основі Random Forest;
- модуль візуалізації та звітності;
- система сповіщення про виявлені загрози.

Експериментальна перевірка системи проводилась на наборі даних, що містить зразки нормального трафіку та різні типи DDoS-атак. Порівняльний аналіз ефективності алгоритмів Random Forest та CNN показав наступні результати:

- за точністю виявлення Random Forest показав 97.8%, CNN - 96.5%;
- за швидкістю обробки (пакетів/сек) Random Forest показав 15000 пакетів/сек, CNN- 8000 пакетів/сек;
- за кількістю використаних ресурсів Random Forest показав помірне використання, CNN – високе;
- час навчання моделі Random Forest складає 45 хвилин, CNN - 6 годин.

Результати експериментів демонструють, що розроблене програмне забезпечення на основі Random Forest забезпечує високу точність виявлення DDoS-атак при меншому споживанні ресурсів порівняно з CNN. Особливо важливим є факт швидшої обробки трафіку, що критично для систем реального часу.

Практична цінність роботи полягає у створенні ефективного інструменту виявлення кіберзагроз, який може бути інтегрований у існуючі системи захисту. Подальші дослідження можуть бути спрямовані на:

- оптимізацію параметрів алгоритму;
- розширення спектру виявлення інших типів атак;
- впровадження механізмів автоматичного оновлення моделі;
- інтеграцію з хмарними системами безпеки.

Література

- [1] Сучасні методи виявлення та запобігання DDoS-атак: Монографія / За ред. В.Л. Бурячка. - Київ: НАУ, 2023. - 286 с.
- [2] Stallings W. Network Security Essentials: Applications and Standards, 7th Edition. - Pearson, 2024. - 448 p.
- [3] Kumar S., Singh M. "Anomaly Detection in Network Traffic using Machine Learning Techniques" // International Journal of Network Security. - 2023. - Vol. 25, No. 2. - pp. 312-325.
- [4] Zhao Y., Jin H. "A Comprehensive Survey of Deep Learning Approaches for DDoS Detection" // IEEE Communications Surveys & Tutorials. - 2023. - Vol. 25, Issue 3. - pp. 1678-1702.
- [5] Random Forest Applications in Cybersecurity: From Theory to Practice / Ed. by J. Anderson. - O'Reilly Media, 2023. - 394 p.
- [6] Chen X., Li K. "Comparative Analysis of ML Algorithms for Network Intrusion Detection" // Journal of Cybersecurity. - 2024. - Vol. 10, Issue 1. - pp. 45-62.
- [7] Miller D.R. Essential Cybersecurity Science: Build, Test, and Evaluate Secure Systems. - Wiley, 2023. - 528 p.
- [8] Національний стандарт України ДСТУ ISO/IEC 27001:2022 "Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою".
- [9] Wang L., Wu H. "Performance Evaluation of CNN vs Random Forest in Network Security Applications" // Security and Communication Networks. - 2023. - Vol. 2023. - Article ID 9876543.
- [10] Cloud Security Alliance. "DDoS Attack Trends Report 2024". - CSA, 2024.
- [11] Методичні рекомендації щодо впровадження систем виявлення та запобігання вторгнень / Державна служба спеціального зв'язку та захисту інформації України. - Київ, 2023.

[12] Zhang R., Liu Q. "Deep Learning Approaches for DDoS Attack Detection: A Systematic Review" // IEEE Access. - 2023. - Vol. 11. - pp. 12345-12367.

[13] Artificial Intelligence in Cybersecurity: Current Trends and Future Perspectives / Ed. by M. Thompson. - Springer, 2024. - 456 p.

[14] Cisco Annual Internet Report (2023-2028) / Cisco Systems, Inc. - 2023.

[15] Hassan M.M. "Real-time DDoS Attack Detection using Machine Learning: A Performance Analysis" // Computer Networks. - 2024. - Vol. 215. - pp. 109567.

ПЛАТФОРМА КЕРУВАННЯ ОНЛАЙН-ОГОЛОШЕННЯМИ

Линник Я. І.

Керівник: Науменко С. В.

E-mail: lynnyk.yaroslav1121@vu.edu.ua

Черкаси, Черкаський національний університет імені Богдана Хмельницького

Платформа керування онлайн-оголошеннями – спеціальний застосунок, що дозволяє користувачам розміщувати свої речі у вигляді оголошень на платформі і в зручному вигляді купувати та обирати те що потрібно.

Застосунок побудований за принципами мікросервісної архітектури, що дозволяє розподіляти навантаження між окремими сервісами, підвищувати масштабованість та забезпечувати стійкість системи.

Основні компоненти системи:

- Сервіс пошуку та перегляду товарів – забезпечує пошук оголошень за ключовими словами, категоріями, ціною, місцезнаходженням тощо. Використовує Elasticsearch [1] для швидкого пошуку.

- Сервіс створення оголошень – надає користувачам можливість публікувати нові оголошення, додавати фото, опис та контактні дані. Дані зберігаються у PostgreSQL [2], а пошукові індекси оновлюються через Kafka [3]. Передбачено можливість редагування та видалення власних оголошень.

- Сервіс чату – реалізує обмін повідомленнями між продавцем і покупцем, що дозволяє узгоджувати деталі угоди в режимі реального часу. Використовує Чат зберігає історію повідомлень у базі даних для можливості перегляду в майбутньому.

- Сервіс профілю користувача – містить інформацію про користувача, його активні оголошення, історію продажів/покупок, а також налаштування облікового запису.

- Сервіс оформлення замовлення – дозволяє покупцям оформити угоду, підтвердити замовлення та відстежувати його статус. Містить функцію підтвердження отримання товару та можливість залишити відгук.

- Сервіс безпеки та автентифікації – забезпечує реєстрацію, вхід у систему та верифікацію користувачів. Використовує JWT для безпечної автентифікації та реалізує механізм відновлення пароля.

Література

[1] Офіційна документація Elasticsearch [Електронний ресурс] – Режим доступу до ресурсу: <https://www.elastic.co/docs>

[2] Офіційна документація PostgreSQL [Електронний ресурс] – Режим доступу до ресурсу: <https://www.postgresql.org/docs/>

[3] Офіційна документація Apache Kafka [Електронний ресурс] – Режим доступу до ресурсу: <https://kafka.apache.org/documentation/>

QUAD9 ЯК ПРОГРАМА ДЛЯ ЗАПОБІГАННЯ ФІШИНГУ В EMAIL

Літвінов В.Д.

Керівник: Лимаренко В.В.

E-mail: litvinov.valeriy.d@hneu.net, viacheslav.lymarenko@hneu.net

Харків, Харківський національний економічний університет імені Семена Кузнеця

Фішингові атаки становлять серйозну загрозу для безпеки користувачів електронної пошти, спрямовані на викрадення конфіденційної інформації. У цій роботі розглядається безкоштовне рішення Quad9, яке забезпечує захист від фішингових атак шляхом блокування доступу до відомих шкідливих доменів. Проаналізовано принципи роботи, переваги та результати застосування цього сервісу [1].

З розвитком цифрових технологій фішингові атаки стають дедалі витонченішими, націленими на обман користувачів для отримання їхніх особистих даних. Традиційні методи захисту не завжди ефективні проти нових загроз. У цьому контексті використання безкоштовних сервісів, таких як Quad9, є актуальним рішенням для підвищення безпеки електронної пошти [2].

Аналіз існуючих методів боротьби з фішингом. Основні підходи до виявлення фішингових атак включають:

- Фільтрація за чорними списками – перевірка домену відправника за базою відомих шкідливих сайтів.
- Аналіз поведінкових характеристик – перевірка URL-адрес у листах, виявлення переадресацій та маніпуляцій із посиланнями.
- Використання системи доменних імен (DNS) для блокування шкідливих доменів – сервіси, такі як Quad9, автоматично блокують доступ до відомих фішингових сайтів на рівні DNS.

Сервіс Quad9 надає безкоштовний захист, перенаправляючи запити до шкідливих доменів на безпечні сервери, тим самим запобігаючи доступу до фішингових ресурсів [3].

Методологія використання Quad9 для запобігання фішингу. Використання Quad9 не потребує встановлення додаткового програмного забезпечення. Основні етапи впровадження:

- Налаштування DNS – заміна стандартних DNS-серверів на сервери Quad9 (IP-адреса: 9.9.9.9) у налаштуваннях мережі користувача або організації [4].
- Моніторинг та оновлення – Quad9 постійно оновлює базу шкідливих доменів, забезпечуючи актуальний захист від нових загроз.

Тестування Quad9 показало високу ефективність у блокуванні доступу до відомих фішингових сайтів. Користувачі відзначають зниження кількості шкідливих листів та підвищення загальної безпеки при використанні електронної пошти. Важливо зазначити, що Quad9 є додатковим рівнем захисту і не замінює інші методи безпеки, такі як антивірусне програмне забезпечення та навчання користувачів [5].

Література

[1] Що таке фішинг і фішингова атака [Електронний ресурс] – Режим доступу до ресурсу: <https://hostiq.ua/blogukr/internet-phishing/>

[2] Фішинг: поширена загроза для пристроїв та облікових записів [Електронний ресурс] – Режим доступу до ресурсу: <https://parties.cyberhandbook.org/uk/topics/securing-accounts-devices/fishynh-poshyrena-zahroza-dlya-prystroyiv-ta-oblikovykh-zapysiv>

[3] Quad9 [Електронний ресурс] – Режим доступу до ресурсу: <https://www.quad9.net>

[4] IP-адреса DNS-сервера: 9.9.9.9 [Електронний ресурс] – Режим доступу до ресурсу: <https://uk.ipshu.com/dns-ip/9.9.9.9>

[5] Quad9 висновок [Електронний ресурс] – Режим доступу до ресурсу: <https://sysadmin.pm/quad9/>

ЙМОВІРНІСНИЙ ПІДХІД ДО ВИЗНАЧЕННЯ ПРАЦЕЗДАТНОСТІ ІС

Мазепа І.В.

Керівник: Солодовник Г.В.

E-mail: ganna.solodovnyk@hneu.net

Харків, Харківський національний економічний університет імені Семена Кузнеця

Ризик відмови у працездатності технічного обладнання можна оцінювати як за суб'єктивними так і за об'єктивними показниками. Прикладом об'єктивного показника є ймовірність виходу з ладу певного технічного інформаційного засобу або компоненти ІС у певний проміжок часу.

Припустимо, що під час аналізу функціонування технічного забезпечення ІС було визначено, що певна компонента може перебувати в одному з наступних станів: S_0 – компонента є справною та вільною (простій), S_1 – компонента є справною та зайнятою (обробка), S_2 – компонента є справною, але відбувається оновлення програмного забезпечення, S_3 – компонента є несправною (відмова у функціонуванні). Задача полягає у визначенні ймовірностей перебування компоненти в кожному з вказаних станів за заданих інтенсивностей відповідних потоків подій: завершення відновлення компоненти після відмови у функціонуванні λ_0 ; надходження замовлення на обробку даних λ_1 ; завершення оновлення програмного забезпечення λ_2 ; відмова у функціонуванні λ_3 .

Метою роботи є автоматизація процесу визначення фінальних ймовірностей перебування компоненти в кожному з визначених станів.

Сформульована задача може бути описана марківським випадковим процесом, оскільки момент відмови у функціонуванні або час, затрачений на відновлення компоненти або оновлення програмного забезпечення так само як і момент надходження замовлення на обробку даних у майбутньому не залежать від стану компоненти у попередніх періодах часу, а лише від того в якому зі станів компонента перебуває в теперішній час.

За припущення, що перехід компоненти з одного стану в інший відбувається практично миттєво у ймовірнісні моменти часу, такий марківський процес можна вважати ймовірнісним процесом з дискретними станами та неперервним часом.

Це задача на знаходження стаціонарних (фінальних) ймовірностей станів компоненти Маркова. Для її розв'язання використовується баланс ймовірностей, який визначає відносини між станами.

Процес розв'язання задачі полягає у побудові розміченого графа станів компоненти з метою подальшого формування системи рівнянь Колмогорова. Потім відбувається перехід до стаціонарних ймовірностей станів, які мають сенс середнього відносного часу перебування компоненти в певному стані. Стаціонарні ймовірності – це ймовірності станів компоненти при $t \rightarrow \infty$, для компоненти, яка перебуває в граничному стаціонарному режимі, в якому випадковим чином змінюються її стани, але ймовірності вже не залежать від часу. Сума стаціонарних ймовірностей має дорівнювати одиниці.

Для розв'язання системи рівнянь Колмогорова було використано матричний підхід або підстановки, для автоматизації обчислень використано мову С#.

За наступних вхідних даних: $\lambda_0=1$, $\lambda_1=2$, $\lambda_2=2$, $\lambda_3=3$, за допомогою розробленої автоматизації розв'язання задачі було отримано такі значення фінальних ймовірностей перебування компоненти в кожному зі станів: ймовірність того, що компонента є справною і вільною $P_0 = 0,15$; ймовірність того, що компонента є справною і зайнятою $P_1 = 0,10$; ймовірність того, що компонента є справною, але потребує оновлення $P_2 = 0,10$; ймовірність того, що компонента є несправною $P_3 = 0,65$.

Розроблена в роботі програма дозволяє легко змінювати інтенсивності переходів і повторно виконувати розрахунки.

ІНТЕГРАЦІЯ EDGE ТА FOG ОБЧИСЛЕНЬ ДЛЯ РОЗПОДІЛЕНОГО ЗАХИСТУ ДАНИХ У РЕАЛЬНОМУ ЧАСІ

Малига З.П.

Керівник: Розломій І.О

E-mail: z.p.malyha.fitis23@chdtu.edu.ua

Черкаси, Черкаський державний технологічний університет

В роботі досліджується можливість використання обчислювальних ресурсів на периферії мережі (Edge) та в її проміжних шарах (Fog) для організації розподілених систем моніторингу та захисту даних.

Сучасні технології кібербезпеки активно використовують обчислювальні ресурси на периферії мережі (Edge) та в її проміжних шарах (Fog) для моніторингу та захисту даних. Такий підхід дозволяє ефективно розподіляти навантаження між центральними дата-центрами та локальними пристроями, забезпечуючи швидке виявлення загроз і миттєву реакцію на інциденти [1].

Edge Computing – це концепція, за якої обробка даних відбувається безпосередньо на пристроях, що генерують інформацію. Завдяки цьому зменшується затримка передачі даних і підвищується швидкість виконання операцій. Такий підхід особливо корисний для систем, що працюють у режимі реального часу, наприклад, у сфері Інтернету речей (IoT), відеоспостереження та розумних міст.

Fog Computing доповнює периферійні обчислення, додаючи проміжний рівень між Edge та хмарними сервісами. Цей рівень дозволяє зменшити навантаження на основну мережеву інфраструктуру, виконуючи попередню обробку та фільтрацію даних перед передачею до центральних серверів. Завдяки цьому забезпечується гнучкість і масштабованість системи.

Розподілений захист даних у таких архітектурах досягається через використання локальних механізмів аутентифікації, шифрування інформації на рівні пристроїв і виявлення аномальної активності. Інтеграція штучного інтелекту дозволяє автоматично аналізувати потенційні загрози та запобігати кібернападам у режимі реального часу.

Одним з ключових викликів є узгодження стандартів безпеки між Edge, Fog і центральними обчислювальними ресурсами. Для цього застосовуються технології блокчейну, які гарантують цілісність даних, а також децентралізовані механізми керування доступом.

Інтеграція Edge та Fog обчислень відкриває нові можливості для підвищення ефективності кібербезпеки [2]. Використання цих технологій у комплексі дозволяє створювати гнучкі та адаптивні системи захисту, які швидко реагують на загрози та мінімізують ризики втрати конфіденційної інформації.

Окрім цього, застосування технологій машинного навчання у розподілених обчислювальних системах дозволяє прогнозувати потенційні вразливості та автоматично оновлювати політики безпеки. Це сприяє підвищенню загального рівня захисту даних і зменшенню ризиків кіберінцидентів.

Важливим аспектом є розвиток правових і нормативних стандартів для регулювання використання Edge та Fog обчислень у сфері безпеки. Спільна робота державних органів та комерційних компаній сприятиме створенню ефективних механізмів контролю та захисту інформації.

Література

[1] Kuchuk, H., & Malokhvii, E. (2024). INTEGRATION OF IOT WITH CLOUD, FOG, AND EDGE COMPUTING: A REVIEW. *Advanced Information Systems*, 8(2), pp. 65-78.

[2] Laroui, M., Nour, B., Mounghla, H., Cherif, M. A., Afifi, H., & Guizani, M. (2021). Edge and fog computing for IoT: A survey on current research activities & future directions. *Computer Communications*, 180, pp. 210-231.

БЛОКЧЕЙН ТА РОЗПОДІЛЕНІ РЕЄСТРИ ДЛЯ ЗАБЕЗПЕЧЕННЯ НЕЗМІННОСТІ ТА АУДИТУ ДАНИХ У ГІБРИДНИХ ХМАРНИХ СИСТЕМ

Маліщук А. Р.

Керівник: Розломій І. О.

E-mail: a.r.malishchuk.fitis.23@chdtu.edu.ua

Черкаси, Черкаський державний технологічний університет

Блокчейн та розподілені реєстри є потужними технологіями для забезпечення незмінності та аудиту даних, особливо в контексті гібридних хмарних систем. Гібридні хмари об'єднують переваги приватних та публічних хмар, надаючи організаціям гнучкість та масштабованість, але водночас ставлять нові вимоги до безпеки та прозорості даних. Блокчейн є ефективним інструментом для вирішення цих проблем, оскільки його ключовою характеристикою є незмінність записів після того, як вони були зафіксовані в реєстрі. Це дозволяє гарантувати, що інформація, яка зберігається в гібридних хмарах, не може бути змінена або знищена без того, щоб це не стало очевидним для всіх учасників мережі [1].

Блокчейн забезпечує прозорість, оскільки всі транзакції та зміни записуються в розподілений реєстр, що дозволяє всім користувачам або учасникам системи перевіряти історію змін. Важливою перевагою є те, що дані, що зберігаються в блокчейні, неможливо змінити без підтвердження з боку інших учасників, що робить ці записи максимально надійними. Це також є основою для аудиту, оскільки всі дії з даними, такі як зміни або доступ до інформації, можуть бути перевірені в будь-який час. Таким чином, блокчейн дозволяє створити надійну систему для перевірки історії змін даних, що особливо важливо для забезпечення відповідності нормативним вимогам і політикам безпеки в гібридних хмарах.

Використання блокчейну в гібридних хмарах допомагає забезпечити контрольованість доступу до даних. Наприклад, записи в блокчейні можуть містити інформацію про те, хто та коли здійснив зміну або отримав доступ до конкретних даних, що дозволяє організаціям ефективно управляти доступом та захищати конфіденційну інформацію. Застосування розподілених реєстрів у таких системах підвищує рівень безпеки, оскільки дані зберігаються не в одному місці, а на численних вузлах мережі, що ускладнює їх несанкціоновану зміну [2].

Проте інтеграція блокчейн-технологій у гібридні хмари не позбавлена викликів. Одним з основних є питання масштабованості, оскільки блокчейн може мати обмеження щодо кількості транзакцій, які він здатен обробляти за одиницю часу. Це може стати проблемою для великих хмарних систем, де обсяг даних і кількість операцій є величезними. Крім того, енергоспоживання, особливо у випадку використання консенсусних алгоритмів, таких як proof-of-work, може стати важливим фактором, який обмежує використання цієї технології в певних сферах.

У підсумку, блокчейн та розподілені реєстри надають потужні інструменти для забезпечення незмінності та аудиту даних у гібридних хмарних системах. Вони дозволяють підвищити рівень безпеки, прозорості та довіри до даних, але для їх ефективного використання необхідно враховувати існуючі виклики, такі як масштабованість, енергоспоживання та інтеграцію з іншими технологіями.

Література

[1] Zou, J., He, D., Zeadally, S., Kumar, N., Wang, H., & Choo, K. R. (2021). Integrated blockchain and cloud computing systems: A systematic survey, solutions, and challenges. *ACM Computing Surveys (CSUR)*, 54(8), 1-36.

[2] Muzammal, M., Qu, Q., & Nasrulin, B. (2019). Renovating blockchain with distributed databases: An open source system. *Future generation computer systems*, 90, 105-117.

РОЗРОБКА ІНСТРУМЕНТІВ ЗАПОБІГАННЯ АТАКАМ, ЗАСНОВАНИХ НА МАНІПУЛЯЦІЇ ЛЮДЬМИ

Мамон К.Д.

Керівник: Муржа Д.Ю.

E-mail: puffjylogan@gmail.com

Харків, Харківський національний економічний університет імені Семена Кузнеця

Атаки, засновані на маніпуляції людьми (соціальна інженерія), становлять одну з найбільших загроз для кібербезпеки, оскільки вони спрямовані не на технічні вразливості, а на людський фактор. Хакери використовують психологічні методи для отримання доступу до конфіденційної інформації, змушуючи жертву добровільно розкрити паролі, фінансові дані чи інші критично важливі відомості. Традиційні засоби кіберзахисту часто неефективні проти таких атак, тому необхідно розробляти спеціалізовані інструменти для їхнього виявлення та запобігання [1-3].

Метою цього дослідження є створення системи, яка дозволить аналізувати, прогнозувати та блокувати атаки соціальної інженерії за допомогою методів штучного інтелекту та поведінкової аналітики. Для цього система повинна вміти розпізнавати підозрілі шаблони комунікації, аналізувати текстові повідомлення на наявність маніпулятивних технік, а також виявляти аномальну поведінку користувачів, що може свідчити про компрометацію облікових записів.

Розробка інструменту передбачає використання машинного навчання для класифікації загроз, аналізу мови (NLP) для виявлення емоційного тиску, термінів, пов'язаних із шахрайством, та інших ознак соціальної інженерії. Фронтенд-система може бути реалізована на основі веб-інтерфейсу, що дозволить користувачам отримувати миттєві попередження про потенційні загрози. Серверна частина працюватиме на Python із використанням бібліотек для аналізу тексту (spaCy, transformers) і моделювання аномальної поведінки (scikit-learn, TensorFlow). Також буде реалізована інтеграція з корпоративними комунікаційними платформами для моніторингу та фільтрації підозрілих повідомлень.

Очікуваними результатами проекту стане створення ефективного інструменту для автоматичного виявлення загроз соціальної інженерії, що допоможе зменшити кількість успішних атак, спрямованих на людський фактор. Така система сприятиме підвищенню рівня обізнаності користувачів щодо методів маніпуляції та дозволить компаніям і приватним особам ефективніше захищати свої дані.

Література

[1] ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection — Information security controls [Електронний ресурс] – Режим доступу до ресурсу: <https://www.iso.org/standard/75652.html>

[2] NIST Special Publication 800-63B. Digital Identity Guidelines: Authentication and Lifecycle Management. [Електронний ресурс] – Режим доступу до ресурсу: <https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-63b.pdf>

[3] OWASP Foundation. Social Engineering: What If The User Opens Back Doors To Strangers? [Електронний ресурс] – Режим доступу до ресурсу: <https://god.owasp.de/2023/schedule/slides/Christina%20Lekati%20--%20What%20if%20the%20User%20Opens%20Back%20Door%20to%20Strangers.pdf>

ОГЛЯД СИСТЕМ ВИЯВЛЕННЯ ТА БЛОКУВАННЯ ПРИХОВАНИХ КІБЕРАТАК У РЕАЛЬНОМУ ЧАСІ

Матюшечко М.В.

Керівник: Солодовник Г.В.

E-mail: ganna.solodovnyuk@hneu.net

Харків, Харківський національний економічний університет імені Семена Кузнеця

Актуальність. Стрімкий розвиток інформаційного суспільства призвів до проникнення цифрових технологій у всі сфери життєдіяльності сучасної людини. Приховані кібератаки становлять серйозну загрозу безпеці як в бізнесі так і в пересічному житті. Постійне зростання рівня складності цих атак дозволяє їм залишатися непомітними для стандартних засобів захисту, що призводить до втрати конфіденційних даних, фінансових збитків та значних репутаційних ризиків для організацій. Традиційні методи кіберзахисту часто не здатні ефективно виявляти та блокувати такі загрози у режимі реального часу, що зумовлює необхідність розробки сучасних систем, здатних адаптуватися до динаміки загроз та забезпечувати проактивний захист інформації.

Іншим аспектом актуальності роботи є розвиток технологій аналізу даних та машинного навчання, які відкривають нові можливості для створення систем, що здатні ефективно виявляти приховані патерни, притаманні кібератакам. Розробка та впровадження таких систем є важливим кроком у забезпеченні надійності цифрових інфраструктур. Предметом дослідження даної роботи є системи виявлення прихованих загроз та їх блокування за допомогою інноваційних підходів.

Метою роботи є огляд систем виявлення та блокування прихованих кібератак у режимі реального часу із застосуванням сучасних методів аналізу даних та алгоритмів машинного навчання. Такі системи спрямовані на автоматизацію процесів моніторингу та аналізу мережевого трафіку для ідентифікації аномальних патернів, що можуть свідчити про активність прихованих атак.

Наразі існує велика кількість типів систем виявлення та блокування прихованих кібератак у режимі реального часу (RTDMI – Real-Time Detection and Mitigation of Intrusions). Одними з них є спеціалізовані системи для виявлення та запобігання несанкціонованих дій: система виявлення вторгнень (Intrusion Detection System), яка аналізує мережевий трафік, шукаючи аномалії або підозрілі активності, але не блокує загрози та система запобігання вторгнень (Intrusion Prevention System), яка активно блокує загрози після їх виявлення. Прикладом таких систем є Snort, яка належить до класу вільного програмного забезпечення та слугує для виявлення та запобігання атак і поєднує в собі методи зіставлення за сигнатурами, інструментарій інспекції протоколів і засоби виявлення аномалій [1].

Сучасні системи управління інформацією та подіями безпеки збирають, аналізують і корелюють дані з різних джерел (систем, пристроїв, мереж), виявляють аномалії на основі шаблонів, поведінкових моделей або індикаторів компрометації (IoC). Такі системи можуть використовувати штучний інтелект для передбачення прихованих атак. Аналогом таких систем з класу програмного забезпечення з відкритим кодом є проект OpenSearch створений фірмою Amazon [2].

Моніторинг процесів, файлів та мережевих з'єднань в режимі реального часу забезпечують платформи, які працюють на кінцевих пристроях. Прикладом таких засобів з класу вільних програм є Wazuh, який об'єднує історично окремі функції в єдину архітектуру агента і платформи [3]. Wazuh надає детальну інформацію про підозрілу активність і може блокувати атаки.

Системи виявлення мережевих аномалій та реагування (Network Detection and Response) фокусуються на аналізі мережевого трафіку. У своїй роботі такі системи використовують методи машинного навчання для виявлення аномалій у поведінці мережі. Прикладом таких систем є Suricata – це програмне забезпечення для аналізу мережі з

відкритим кодом, яке використовується більшістю приватних та громадських організацій та вбудоване великими постачальниками для захисту своїх активів [4].

У реальних сценаріях зазвичай використовують комбінацію таких систем для максимального захисту від прихованих кібератак. Моделювання процесів виявлення та блокування кібератак в умовах динамічного розвитку кіберзагроз базується на різних підходах. Одним із ключових є поведінковий аналіз, що дозволяє оцінювати дії користувачів та систем для виявлення відхилень від нормальної поведінки. Використання алгоритмів машинного навчання забезпечує можливість автоматичного навчання на основі попередніх даних про загрози, що значно підвищує ефективність системи у реальних умовах.

Машинне навчання дозволяє створювати моделі, які здатні виявляти не лише відомі типи атак, але й адаптуватися до нових загроз, які раніше не зустрічалися. Для цього розглядаються методи класифікації, кластеризації та прогнозування спрямовані на виявлення аномальних патернів у поведінці мережевого трафіку.

Розглянуті системи зазвичай оперують трьома ключовими компонентами: джерела загроз, канали поширення та механізми реагування. Використання цих компонентів дозволяє створювати динамічну матрицю ризиків, що стає основою для прийняття рішень у реальному часі.

Серед прикладів застосування розроблених систем можна виділити захист корпоративних мереж від атак типу «відмова в обслуговуванні» (DDoS), виявлення спроб несанкціонованого доступу до конфіденційних даних, а також моніторинг дій внутрішніх користувачів з метою попередження інсайдерських загроз.

Існуючі комерційні рішення у сфері кібербезпеки, такі як Palo Alto Networks або Splunk, надають ефективні інструменти аналізу та моніторингу, але часто вимагають значних фінансових витрат і не адаптовані для малого та середнього бізнесу. Тому впровадження відкритих платформ для аналізу даних дозволяє зменшити витрати та підвищити доступність сучасних технологій кіберзахисту.

Наведені системи враховують важливість доступності програмних рішень, які базуються на відкритих технологіях, і демонструють потенціал для значного підвищення рівня кіберзахисту організацій, незалежно від їхніх розмірів чи фінансових можливостей.

Висновок. В ході роботи було розглянуто різні системи виявлення та блокування прихованих кібератак у реальному часі, які використовують сучасні методи аналізу даних та алгоритми машинного навчання. Застосування поведінкових моделей, аналізу великих обсягів даних і адаптивних алгоритмів дозволяє забезпечити ефективність та високу точність виявлення загроз. Визначено актуальність розробки системи здатної автоматично адаптуватися до змін у поведінці зловмисників, здійснювати проактивне виявлення загроз та реагувати на них у режимі реального часу.

Розглянутий підхід сприяє підвищенню рівня кіберзахисту організацій, забезпеченню безперервності їхньої діяльності та мінімізації ризиків, пов'язаних із витоками конфіденційних даних та іншими наслідками кібератак. Таким чином, запропонована система може стати важливим інструментом у забезпеченні інформаційної безпеки в умовах сучасних викликів.

Література

[1] Сайт Snort // Documents [Електронний ресурс] – Режим доступу до ресурсу: <https://www.snort.org/documents>

[2] Сайт Opensearch // Find the meaning in your data [Електронний ресурс] – Режим доступу до ресурсу: <https://opensearch.org/>

[3] Сайт Wazuh // The Open Source Security Platform [Електронний ресурс] – Режим доступу до ресурсу: <https://wazuh.com/>

[4] Сайт Suricata [Електронний ресурс] – Режим доступу до ресурсу: <https://suricata.io/>

АНАЛІЗ СУЧАСНИХ СИСТЕМ ВИЯВЛЕННЯ ТА ЗАПОБІГАННЯ КІБЕРЗАГРОЗАМ НА ОСНОВІ АНАЛІЗУ ПОВЕДІНКИ КОРИСТУВАЧІВ

Ментяник Д.О.

Керівник: Солодовник Г.В.

E-mail: ganna.solodovnyk@hneu.net

Харків, Харківський національний економічний університет імені Семена Кузнеця

Актуальність. Сучасні корпоративні мережі стикаються з постійно зростаючими загрозами кібербезпеки. Збільшення кількості кіберзагроз, їх складності та шкідливого впливу вимагають інноваційних підходів до забезпечення безпеки інформаційних систем. Традиційні методи, засновані на сигнатурному аналізі, вже не забезпечують достатнього рівня захисту. Аналіз поведінки користувачів, відомий як User Behavior Analytics (UBA), відкриває нові можливості для ідентифікації аномальної активності та раннього виявлення потенційних загроз.

Метою роботи є аналіз існуючих систем виявлення та запобігання кіберзагрозам на основі аналізу поведінки користувачів, з подальшою розробкою системи яка дозволить своєчасно ідентифікувати загрози, оцінювати ризики та знижувати вплив інцидентів на корпоративну інфраструктуру.

Сучасні методології дослідження та розробки систем виявлення та запобігання кіберзагрозам на основі аналізу поведінки користувачів ґрунтуються на наступних принципах:

- під час збору даних такі системи мають забезпечувати обробку великих обсягів логів, які включають дії користувачів, мережеву активність, доступ до файлів та ресурсів;
- системи мають здійснювати аналіз поведінки трафіку із застосуванням алгоритмів машинного навчання для виявлення відхилень від нормальної поведінки;
- системи мають передбачати автоматичне реагування на інциденти з метою блокування загроз у реальному часі.

До складу систем виявлення та запобігання кіберзагрозам можуть входити наступні модулі: модуль збору даних, який забезпечує інтеграцію з джерелами даних (SIEM, Active Directory, журнали серверів); модуль аналізу, який вміщує в себе алгоритми машинного навчання для класифікації поведінкових патернів (кластеризація для виявлення аномалій, алгоритми раннього попередження); модуль реагування, призначений для автоматизованого виконання правил реагування (блокування акаунтів, ізоляція пристроїв).

В якості інструментарію практичної реалізації системи виявлення та запобігання кіберзагрозам на основі аналізу поведінки користувачів планується використовувати наступні ресурси вільного програмного забезпечення:

- мову програмування Python (для аналізу даних та реалізації моделей машинного навчання);
- пошуковий сервер Elasticsearch (для обробки великих обсягів логів);
- плагін Kibana (для візуалізації змісту проіндексованого кластером Elasticsearch);
- платформи кібербезпеки ELK Stack або Splunk Free (для інтеграції через API, аналізу і моніторингу даних).

Очікувані результати розробки системи виявлення та запобігання кіберзагрозам полягають у знизенні часу виявлення інцидентів, підвищенні точності виявлення загроз, можливості запобігання атакам до моменту їхнього впливу на бізнес.

Висновок. Розробка системи аналізу поведінки користувачів відкриває нові можливості в управлінні кібербезпекою. Така система може стати основним інструментом для забезпечення стабільності корпоративних мереж у сучасному світі.

RIPE ATLAS – НЕЗАМІННИЙ ІНСТРУМЕНТ ДЛЯ МОНІТОРИНГУ ІНТЕРНЕТ-МЕРЕЖ

Мерлак О.В., Литвиненко Є.М.

E-mail: olena.merlak@hneu.net

Харків, Харківський національний економічний університет імені Семена Кузнеця

RIPE Atlas – це глобальна розподілена система моніторингу інтернет-мереж, яка дозволяє користувачам проводити вимірювання продуктивності та доступності різних сегментів мережі. Вона була створена RIPE NCC (Réseaux IP Européens Network Coordination Centre) для надання відкритого доступу до реальних даних про стан інтернету.

- RIPE Atlas – це потужний інструмент для моніторингу та аналізу інтернет-мереж у глобальному масштабі. Його використовують оператори зв'язку, адміністратори мереж, дослідники та навіть звичайні користувачі для оцінки продуктивності інтернет-з'єднання та вирішення мережевих проблем.

Одним із ключових застосувань RIPE Atlas є безперервний моніторинг роботи інтернет-провайдерів та великих автономних систем (AS). За допомогою цієї платформи можна: визначати стабільність мережевого з'єднання – отримувати дані про втрати пакетів та зміну часу відповіді; виявляти зміни у маршрутизації – перевіряти, чи змінився маршрут трафіку між джерелом та отримувачем; оцінювати якість інтернет-послуг – аналізувати, як швидко відповідають сервери та наскільки стабільне з'єднання у різних регіонах світу.

Трасування маршрутів (Traceroute) та аналіз трафіку – один із найпоширеніших методів діагностики проблем у мережі. RIPE Atlas дозволяє визначати, через які вузли проходить трафік між двома точками; виявляти «вузькі місця» в інтернет-інфраструктурі, які можуть спричинити затримки або втрати пакетів; перевіряти роботу маршрутів BGP – оцінювати, чи правильно працює маршрутизація між автономними системами (AS).

RIPE Atlas дозволяє проводити високоточні вимірювання затримки (Ping, Latency) та втрат пакетів між будь-якими двома точками в інтернеті. Це особливо корисно для операторів зв'язку, які хочуть оцінити якість своїх міжнародних з'єднань; компаній, що надають онлайн-сервіси (наприклад, стрімінгові платформи, хмарні сервіси), які потребують низької затримки для якісного обслуговування користувачів; геймерів, які можуть перевіряти, наскільки стабільне їхнє з'єднання з ігровими серверами.

DNS (Domain Name System) є критично важливим компонентом інтернет-інфраструктури, і RIPE Atlas допомагає оцінити його продуктивність. За допомогою вимірювань можна перевіряти швидкість відповіді DNS-серверів у різних регіонах; діагностувати проблеми з кешуванням DNS та визначати, чи коректно працює розподіл трафіку; виявляти проблеми з доступністю доменів – якщо DNS-сервер не відповідає, це може впливати на доступність сайтів та інших онлайн-сервісів.

RIPE Atlas дозволяє виявляти проблеми з маршрутизацією та геолокацією IP-адрес. Це допомагає боротися з мережевими атаками (наприклад, BGP-хіджакінгом), коли зловмисники перенаправляють трафік через небажані маршрути; перевіряти коректність геолокації IP-адрес, що особливо важливо для контент-провайдерів (наприклад, потокові сервіси, які обмежують доступ за географічною ознакою); досліджувати проблеми з доступом до сайтів, особливо якщо виникають регіональні блокування або помилки маршрутизації.

Інтернет-обмінні точки (IXP) є критично важливими вузлами для зменшення затримок у глобальному інтернеті. RIPE Atlas використовується для оцінки ефективності роботи IXP та перевірки, як добре взаємодіють провайдери у певному регіоні; підвищення якості маршрутизації шляхом аналізу, через які точки проходить трафік; допомоги у прийнятті рішень про підключення до певних IXP – провайдери можуть використовувати дані RIPE Atlas, щоб визначити, які точки обміну будуть найбільш вигідними.

RIPE Atlas дозволяє проводити тести доступності веб-сайтів та онлайн-сервісів у різних частинах світу. Це допомагає компаніям оцінювати якість доставки контенту (наприклад, для CDN-систем); діагностувати регіональні проблеми – якщо сайт доступний у одних країнах, але недоступний у інших; визначити проблеми з мережевими блокуваннями (наприклад, урядові або корпоративні фільтри).

RIPE Atlas є важливим джерелом відкритих даних для наукових досліджень та інтернет-аналітики. Він використовується для аналізу глобальних збоїв в інтернеті, наприклад, під час великих кібер-атак або природних катастроф; для вивчення довготривалих змін у маршрутизації, що допомагає визначити загальні тенденції розвитку інтернету; для оцінки впливу нових технологій, таких як IPv6, DNSSEC, QUIC тощо.

Завдяки API RIPE Atlas можна інтегрувати отримані дані з іншими інструментами мережевого моніторингу (наприклад, Zabbix, Grafana, Prometheus). Це дозволяє автоматизувати виявлення аномалій у роботі мережі; створення автоматичних звітів про продуктивність; реагування на зміни у маршрутизації в реальному часі.

RIPE Atlas має розподілену архітектуру, яка дозволяє ефективно збирати, аналізувати та візуалізувати дані про роботу інтернет-мережі. Вона складається з трьох ключових компонентів.

Вимірювальні вузли (Probes та Anchors) є основою RIPE Atlas. Вони встановлюються користувачами в різних точках світу та виконують вимірювання за певними параметрами. Вузли поділяються на:

- RIPE Atlas Probes – малі фізичні пристрої або програмні агенти, які користувачі розміщують у своїх мережах. Вони працюють у фоновому режимі, виконуючи вимірювання, які ініціюють інші користувачі або RIPE NCC;

- RIPE Atlas Anchors – потужніші пристрої, які використовуються як опорні точки вимірювань. Вони розташовані в критично важливих точках мережі, таких як інтернет-обмінні вузли (IXP), дата-центри та вузлові мережеві точки. Anchors відіграють ключову роль у забезпеченні стабільності вимірювань і надають точніші дані.

Центральна інфраструктура (RIPE NCC Backend) – ця частина архітектури складається з серверів RIPE NCC, які збирають, обробляють і аналізують отримані дані. Основні функції цієї інфраструктури:

- координація вимірювань – сервери отримують запити на вимірювання та розподіляють їх серед probes та anchors;

- обробка та збереження даних – результати вимірювань надходять у базу даних, де вони аналізуються та індексуються;

- забезпечення доступу до даних – користувачі можуть отримувати результати вимірювань через веб-інтерфейс або API.

Інтерфейси для користувачів – RIPE Atlas надає кілька способів доступу до даних та керування вимірюваннями:

- веб-інтерфейс – основний спосіб взаємодії користувачів із системою. Він дозволяє переглядати результати, запускати вимірювання та аналізувати дані за допомогою візуалізацій;

- API RIPE Atlas – інструмент для автоматизації та інтеграції даних RIPE Atlas з іншими системами моніторингу. API дозволяє створювати користувацькі вимірювання, отримувати дані в реальному часі та аналізувати історичні записи;

- клієнтські утиліти – окремі програмні засоби, що допомагають працювати з RIPE Atlas через командний рядок, дозволяючи швидко отримувати результати вимірювань.

RIPE Atlas є незамінним інструментом для моніторингу інтернет-мереж. Він допомагає провайдерам, адміністраторам мереж та дослідникам аналізувати маршрутизацію, продуктивність DNS, затримку з'єднання, доступність веб-сайтів та багато іншого. Використання RIPE Atlas дозволяє швидко знаходити проблеми та приймати обґрунтовані рішення для покращення якості зв'язку у глобальній інтернет-мережі.

ІНСТРУМЕНТИ КІБЕРБЕЗПЕКИ НА ОСНОВІ LINUX-ДИСТРИБУТИВІВ: KALI, OPENVAS, WIRESHARK

Мінаєв А. І., Латанська Л. О.

E-mail: minaiiev.andrii@gmail.com, liudmyla.latanska@nuos.edu.ua

Миколаїв, Національний університет кораблебудування імені адмірала Макарова

Інструменти кібербезпеки на базі дистрибутивів Linux є важливими компонентами для виявлення, аналізу та нейтралізації кіберзагроз. Серед найвідоміших рішень – Kali Linux, OpenVAS та Wireshark. Вони надають можливості для тестування на проникнення, оцінювання вразливостей та моніторингу мережевого трафіку. Ці інструменти широко використовуються як у наукових дослідженнях, так і в практиці фахівців з інформаційної безпеки.

Kali Linux – спеціалізований GNU/Linux дистрибутив типу LiveCD, який виник у результаті об'єднання проєктів WHAX і Auditor Security Collection. Kali включає в себе велику кількість інструментів для аналізу безпеки, серед яких є OpenVAS. Таким чином, Kali надає готове середовище для використання OpenVAS та багатьох інших засобів, що робить дистрибутив популярним вибором серед професіоналів з кібербезпеки [1, 2]. Kali Linux має безліч попередньо встановлених утиліт для різних аспектів тестування:

- Сканування та аналіз мереж: Nmap, Netcat, Nikto.
- Пошук загроз: OpenVAS, Metasploit Framework.
- Виявлення вразливостей: Armitage, Exploit-db.
- Атаки грубої сили: Hydra, John the Ripper, Hashcat.
- Інструменти для аналізу Wi-Fi, наприклад Aircrack-ng, Kismet, Fern WiFi Cracker.

OpenVAS – це сканер вразливостей, що використовується для виявлення проблем безпеки в мережах і серверах. Він допомагає адміністраторам проводити комплексну оцінку захищеності систем, знаходити вразливості та аналізувати рівень ризиків. Інструмент працює шляхом сканування мережі, аналізуючи відкриті порти, сервіси та конфігурації. OpenVAS порівнює зібрані дані з базою вразливостей (Vulnerability Tests) і формує звіти з детальною інформацією про знайдені ризики, вказуючи їхній рівень критичності. Хоча система забезпечує високий рівень точності, процес сканування може бути вимогливим до ресурсів і впливати на продуктивність цільової системи [2].

Wireshark – це аналізатор мережевого трафіку, який дозволяє досліджувати дані, що передаються через мережу в реальному часі. Wireshark може розбивати пакети даних на фрейми та сегменти, надаючи детальну інформацію про біти та байти в пакеті. Wireshark підтримує всі основні мережеві протоколи та типи даних. Також його можна використовувати як інструмент для аналізу пакетів, якщо є адміністратор мережі загального користування. Wireshark має доступ до всієї мережі, підключеної до роутера. Програма поширюється за вільною ліцензією GNU GPL і використовує кросплатформену бібліотеку GTK+ для графічного інтерфейсу, з перспективою переходу на Qt. Вона підтримує GNU/Linux, Windows та інші UNIX-подібні системи, зокрема macOS, Solaris і BSD. Програма має широкий набір функцій [3]:

- Підтримка Windows, Linux, macOS, Solaris, FreeBSD, NetBSD та інших платформ.
- Аналіз захоплених даних через графічний інтерфейс або утиліту TShark у режимі командного рядка.
- Фільтри відображення та розширений VoIP аналіз.
- Читання/запис файлів захоплення різних форматів (tcpdump, Pcap NG, Cisco IDS, Microsoft Network Monitor тощо).
- Підтримка стиснення файлів gzip із розпакуванням на льоту.
- Захоплення трафіку з Ethernet, Wi-Fi, Bluetooth, USB та інших протоколів.
- Дешифрування IPsec, TLS, WPA2, Kerberos та інших протоколів.

Отже, Kali Linux є універсальним рішенням для комплексної роботи з безпеки, OpenVAS спеціалізується на скануванні вразливостей, а Wireshark надає інструменти для поглибленого аналізу мережевого трафіку. Ці інструменти можна використовувати для різних завдань, таких як загальне тестування, оцінка безпеки та моніторинг мережі.

Література

[1] Kali Linux. Kali Documentation [Електронний ресурс] – Режим доступу до ресурсу: <https://www.kali.org/docs/>

[2] OpenVAS. Open Vulnerability Assessment System [[Електронний ресурс] – Режим доступу до ресурсу: <https://www.openvas.org>

[3] Wireshark. Network Protocol Analyzer [Електронний ресурс] – Режим доступу до ресурсу: <https://www.wireshark.org>

АНАЛІЗ БЕЗПЕКИ СМАРТ-КОНТРАКТІВ ДЛЯ ДЕЦЕНТРАЛІЗОВАНИХ ФІНАНСОВИХ ОПЕРАЦІЙ (DeFi)

Налігацьких М. М.

Керівник: Долгова Н.Г.

E-mail: Naligatskih133@gmail.com

Харків, Харківський національний економічний університет імені Семена Кузнеця

Децентралізовані фінанси (DeFi) пропонують нові можливості для фінансових операцій, але їх безпека залишається критично важливим питанням. Дана робота присвячена аналізу безпеки смарт-контрактів для DeFi, включаючи огляд існуючих рішень, обґрунтування проектних рішень та практичну реалізацію системи безпеки. Розглянуто основні загрози безпеці DeFi, проаналізовано існуючі методи та інструменти захисту, запропоновано комплексну архітектуру безпечної DeFi-інфраструктури.

DeFi базуються на смарт-контрактах, що автоматизують виконання фінансових операцій. Проте, вразливості в смарт-контрактах можуть призвести до серйозних збитків [1]. Тому аналіз безпеки смарт-контрактів для DeFi є актуальною та важливою задачею.

Метою дослідження є аналіз безпеки смарт-контрактів для DeFi та розробка рекомендацій щодо підвищення рівня безпеки.

Для досягнення мети були поставлені наступні завдання:

- Провести аналіз існуючих рішень для забезпечення безпеки DeFi.
- Обґрунтувати проектні рішення та розробити архітектуру безпечної DeFi-інфраструктури.
- Реалізувати систему безпеки та протестувати її на реальних DeFi-протоколах.
- Оцінити ефективність розробленої системи та порівняти її з існуючими рішеннями.

Існуючі рішення для забезпечення безпеки DeFi включають в себе:

- OpenZeppelin: бібліотека безпечних смарт-контрактів, що надає готові, перевірені компоненти для розробки DeFi-додатків [2].
- CertiK: платформа для аудиту безпеки смарт-контрактів, що використовує формальну верифікацію та інші методи для виявлення вразливостей.
- ConsenSys Diligence: набір інструментів для аналізу та тестування безпеки смарт-контрактів, включаючи Slither та Mythril [3].
- Trail of Bits: компанія, що спеціалізується на безпеці блокчейн-технологій та проводить аудити безпеки смарт-контрактів.
- PeckShield: компанія, що займається безпекою блокчейну та надає послуги з аудиту безпеки, аналізу вразливостей та реагування на інциденти.

Проте, існуючі рішення мають свої недоліки, такі як обмежена функціональність, висока вартість або недостатня інтеграція між різними інструментами.

В даній роботі пропонується комплексний підхід до забезпечення безпеки DeFi, який включає в себе наступні компоненти:

Захист від атак: розроблено алгоритми для виявлення та запобігання відомим видам атак на DeFi-інфраструктуру, таким як:

- Атаки повторного виконання (Replay Attacks)
- Атаки на оракулів (Oracle Attacks)
- Атаки на міжпротокольні взаємодії (Cross-Protocol Attacks)
- Атаки типу "сендвіч" (Sandwich Attacks)
- Атаки з використанням флеш-кредитів (Flash Loan Attacks) [4].

Виявлення вразливостей: створено систему для автоматичного аналізу смарт-контрактів на наявність вразливостей, використовуючи статичний та динамічний аналіз, а також формальну верифікацію.

Система включає в себе наступні інструменти

- Slither
- Mythril
- Oyente
- Securify
- Formal verification tools (e.g., K Framework, Isabelle/HOL)

Таким чином розроблено систему для моніторингу транзакцій та виявлення аномалій, що може свідчити про атаку або зловживання. Система використовує машинне навчання для виявлення підозрілих патернів поведінки [5]. Також розроблено план дій на випадок виявлення атаки або вразливості, який включає в себе процедури блокування уражених контрактів, відновлення втрачених коштів та інформування спільноти. Окремо слід відзначити, що впроваджено принципи безпечної розробки програмного забезпечення, такі як:

- Мінімізація коду
- Використання перевірених бібліотек
- Ретельне тестування
- Безпечне кодування

Література

[1] Atzei, A., Bartoletti, L., & Cimoli, M. (2017). A Survey of Attacks on Ethereum Smart Contracts. *International Workshop on Software Engineering and Blockchain (SEB)*, pp. 25-34.

[2] Zamfir, D., & Gervais, A. (2021). A Survey of Security Issues in Ethereum Smart Contracts. *Journal of Cybersecurity and Mobility*, 10(1), pp. 1-27.

[3] Cheng, X., Zhou, L., & Liu, F. (2020). A Comprehensive Survey on Smart Contract Vulnerabilities. *IEEE Access*, 8, pp. 107898-107919.

[4] Luu, L., et al. (2016). A Secure Smart Contract Platform. *Financial Cryptography and Data Security*, pp. 562-580.

[5] Weber, I., et al. (2019). Security and Privacy in Blockchain Systems. *IEEE Transactions on Knowledge and Data Engineering*, 31(6), pp. 1183-1207.

ІННОВАЦІЙНИЙ МЕТОД ПОБУДОВИ S-BOX ДЛЯ ПОЛЕГШЕНИХ БЛОКОВИХ ШИФРІВ У ВБУДОВАНИХ ПРИСТРОЯХ

Науменко С.В., Розломій І.О.

E-mail: naumenko.serhii1122@vu.cdu.edu.ua

Черкаси, Черкаський національний університет ім. Б. Хмельницького

Інноваційна конструкція S-box для захисту вбудованих пристроїв відноситься до розробки нових методів для проектування блоків заміни (S-box), що має вирішальне значення для безпеки криптографічних алгоритмів, особливо в сфері криптографії з симетричним ключем. S-блоки є невід'ємною частиною для впровадження нелінійності в криптографічні системи, значно підвищуючи їх стійкість до різних форм атак, таких як диференціальний і лінійний криптоаналіз. Важливість конструкції S-box полягає в її прямому впливі на продуктивність, безпеку та ефективність, зокрема, полегшених систем шифрування. Такі системи шифрування використовуються у вбудованих пристроях, які стають все більш поширеними в таких секторах, як охорона здоров'я, автомобільна промисловість та Інтернет речей (IoT).

Важливість цієї теми підкреслюється розвитком ландшафту кібербезпеки, який вимагає надійних заходів безпеки у вбудованих системах через їхню вразливість до атак. Помітні досягнення включають дослідження 5-розрядних S-блоків, які є компромісом між вищою безпекою великих конфігурацій та економічною ефективністю менших проектів, а також методи, що використовують хаотичні системи та методи на основі матриць для підвищення випадковості та стійкості [1].

Протиріччя щодо конструкції S-box часто виникають через компроміс між безпекою та продуктивністю. Хоча більші S-блоки забезпечують більшу безпеку, вони також вимагають більше обчислювальних ресурсів, що може бути обмежуючим фактором у вбудованих середовищах. І навпаки, менші S-блоки можуть не запропонувати адекватний захист від нових криптоаналітичних методів. Проблемою залишається створення S-блоків, які відповідають суворим вимогам безпеки, зберігаючи низькі накладні витрати в обмежених середовищах. S-блоки (блоки заміни) служать основними компонентами в криптографічних алгоритмах, зокрема в рамках криптографії з симетричним ключем. Їх основною функцією є забезпечення нелінійності в мережах заміни-перестановки, підвищуючи стійкість алгоритму до різних форм криптоаналізу, включаючи лінійні та диференціальні атаки [2].

Конструкція S-блоків безпосередньо впливає як на безпеку, так і на ефективність усієї криптографічної системи. Існують різні конфігурації S-box, від 3-х до 8-бітних, кожна з яких представляє унікальні переваги та виклики, що стосуються безпеки та ефективності використання ресурсів. У багатьох сучасних криптографічних стандартах, таких як Advanced Encryption Standard (AES), S-блоки відіграють вирішальну роль. S-блок AES генерується з мультиплікативного обернення над полем Галуа з подальшим афінним перетворенням. Цей метод підкреслює важливість математичних методів у створенні ефективних S-блоків, оскільки ефективність апаратних реалізацій часто залежить від таблиць пошуку (LUT), які можуть споживати значні ресурси пам'яті [3].

Розробка S-box, який відповідає конкуруючим вимогам економічності та міцності безпеки, створює значні проблеми для дослідників. Хоча 8-розрядним S-блокам часто віддають перевагу через їхні надійні можливості безпеки, вони мають високі витрати на впровадження. І навпаки, S-блоки меншого розміру (3- або 4-розрядні) є ресурсоефективними, але демонструють уразливості, які можуть поставити під загрозу безпеку. Дослідження 5-бітних S-блоків стало багатообіцяючою альтернативою, яка пропонує баланс між вимогами до ресурсів і функціями безпеки. Нещодавні дослідження показують, що 5-бітні S-блоки можуть забезпечити значну гнучкість, зберігаючи при цьому високий ступінь нелінійності, що є критичним атрибутом безпечного шифрування. Оскільки галузь криптографії продовжує розвиватися, інноваційні підходи до побудови S-box, такі як

використання теорії хаосу та матричних методів, набувають популярності. Ці досягнення спрямовані на створення S-блоків, які не тільки відповідають криптографічним вимогам, але й добре адаптуються до обмежень середовищ з обмеженими ресурсами, таких як вбудовані системи. Ці триваючі дослідження мають важливе значення для розробки безпечних криптографічних систем, здатних захищати конфіденційну інформацію у дедалі більш вимогливих технологічних умовах.

Розглянемо інноваційні підходи до побудови S-box.

- Відстань Хеммінга та нелінійність. Відстань Хеммінга служить ключовим показником для оцінки відстані між парами вводу-виводу S-блоку, яка визначається як кількість різних бітів між входом і виходом у кожній позиції (i), де (i) коливається від (0) до (n), загальної кількості бітів. У S-блоках бажаний високий ступінь нелінійності, із запропонованою конструкцією, що демонструє середню відстань Хеммінга 2,75, що вказує на сильні нелінійні властивості. Генерація S-блоків керується алгоритмами, які забезпечують додавання кандидатів на основі суворих критеріїв, включаючи відсутність у S-блоку [1].

- Диференціальний криптоаналіз і лавинний ефект. Диференціальний криптоаналіз вивчає зміни у виході криптографічних функцій у відповідь на невеликі зміни у вхідних даних. Щоб посилити захист від таких аналізів, важливо досягти високого ефекту лавини, коли зміна одного вхідного біта змінює щонайменше 50% вихідних бітів. Запропонований S-box демонструє середній ефект Avalanche 0,52, таким чином задовольняючи суворі вимоги до критерію Avalanche (SAC), який є життєво важливим для підтримки криптографічної цілісності.

- Хаотичне використання карти. Конструкція S-box використовує хаотичні системи, зокрема нелінійні карти дискретного часу, такі як Enhanced Logistic Map (ELM). Ці карти мають перевагу завдяки своїй детермінованій природі та здатності генерувати складні псевдовипадкові послідовності, виконуючи ключові цілі безпеки в рамках криптографічних алгоритмів. Властивості, притаманні хаотичним системам, такі як динамічна нестабільність і топологічне змішування, узгоджуються з принципами плутанини та дифузії Шеннона, ще більше підвищуючи надійність S-box.

- Критерій бітової незалежності. Критерій незалежності біта (BIC) є ще одним важливим аспектом оцінки сили Avalanche, зосереджуючись на тому, як зміни окремих бітів впливають на вихідні дані. Він визначається як ступінь, до якої зміна одного вхідного біта незалежно впливає на вихідні дані. Запропонований S-блок демонструє значення матриці BIC-SAC навколо радіуса 0,5, в середньому 0,525, що вказує на високу відповідність необхідним вимогам до ефекту лавини.

Безпека вбудованих систем стала першорядною проблемою, зокрема через швидке поширення пристроїв IoT і дедалі складніші кіберзагрози. Оскільки ці пов'язані пристрої стають все більш поширеними, ризики для цілісності даних і конфіденційності користувачів значно зростають, що спонукає розробників вбудованих систем надавати пріоритет надійним заходам безпеки. Такі стратегії, як апаратні функції безпеки, безпечні процедури завантаження та алгоритми шифрування, все частіше застосовуються для захисту цих систем від вразливостей і атак.

Література

[1] El Gaabouri, Ismail, et al. "A new S-box pattern generation based on chaotic enhanced logistic map: case of 5-bit S-box." *Cybersecurity 7.1* (2024): 1-14.

[2] Yarmilko, A., Rozlomii, I., & Naumenko, S. (2024, May). Dependability of Embedded Systems in the Industrial Internet of Things: Information Security and Reliability of the Communication Cluster. In *International Scientific-Practical Conference "Information Technology for Education, Science and Technics"* (pp. 235-249). Cham: Springer Nature Switzerland.

[3] Rozlomii, I., Yarmilko, A., & Naumenko, S. (2024, April). Data security of IoT devices with limited resources: challenges and potential solutions. In *doors* (pp. 85-96).

СУЧАСНІ ТЕХНОЛОГІЇ ЗАХИСТУ ДАНИХ У ВБУДОВАНИХ ПРИБОРАХ З ОБМЕЖЕНИМИ РЕСУРСАМИ

Науменко С.В., Михайловський Є.В.

Керівник: Стабецька Т.А.

E-mail: nauhenko.serhii1122@vu.cdu.edu.ua

Черкаси, Черкаський національний університет ім. Б. Хмельницького

Сучасні технології захисту даних у вбудованих пристроях з обмеженими ресурсами зосереджені на захисті конфіденційної інформації в середовищах, обмежених пам'яттю, потужністю обробки та доступністю енергії. Оскільки вбудовані пристрої поширюються в різних додатках – від пристроїв Інтернету речей (IoT) до критичних систем безпеки в автомобілях – необхідність ефективних стратегій захисту даних стає першочерговою [1]. Ця галузь відома не лише своїми технічними проблемами, але й впливом на конфіденційність, безпеку та відповідність нормативним вимогам, оскільки організації прагнуть орієнтуватися в середовищі загроз, що швидко змінюється.

В основі сучасного захисту даних у вбудованих системах лежать методи шифрування, надійні механізми автентифікації та системи контролю доступу, пристосовані для ефективної роботи в межах обмежень цих пристроїв. Технології автентифікації, включаючи багатофакторну автентифікацію та цифрові сертифікати, підвищують безпеку, забезпечуючи доступ до конфіденційних ресурсів лише авторизованим користувачам і пристроям. Крім того, ефективні заходи контролю доступу запобігають несанкціонованому доступу до даних шляхом визначення дозволів користувачів на основі ролей в організації. Незважаючи на досягнення, у впровадженні цих технологій захисту даних залишаються проблеми.

Обмеження ресурсів часто перешкоджають інтеграції комплексних заходів безпеки, що вимагає розробки полегшених криптографічних рішень, які зберігають конфіденційність даних без шкоди для продуктивності чи енергоефективності. Крім того, вразливість ланцюга постачання та відповідність суворим нормам, таким як Загальний регламент захисту даних (GDPR), додають складності, які організації повинні вирішити, щоб забезпечити безпечну роботу вбудованих пристроїв.

Впровадження захисту даних у сучасних вбудованих пристроях, особливо тих, що мають обмежені ресурси, створює кілька серйозних проблем. Ці виклики виникають через властиві обмеження вбудованих систем, включаючи пам'ять, обчислювальну потужність і доступність енергії, а також мінливий ландшафт загроз безпеці. Багато вбудованих пристроїв працюють із надзвичайно обмеженою пам'яттю, часто лише в кількох кілобайтах. Це обмеження ускладнює інтеграцію комплексних заходів захисту даних, оскільки як програмний код, так і дані виконання повинні вміщатися в цей невеликий розмір. Енергоспоживання є критично важливим фактором, особливо для пристроїв IoT, що працюють від батареї. Механізми безпеки часто вимагають додаткової обчислювальної потужності та енергії, що може значно скоротити термін служби акумулятора [2].

Шифрування відіграє вирішальну роль у захисті конфіденційних даних, що зберігаються на вбудованих пристроях, а також у забезпеченні конфіденційності та цілісності зв'язку між ними. Щоб запровадити надійні механізми шифрування та дешифрування, важливо використовувати надійні алгоритми шифрування, застосовувати належні методи керування ключами та використовувати безпечні апаратні та програмні компоненти. Цей комплексний підхід важливий для захисту вбудованих пристроїв від витоку даних і несанкціонованого доступу [3].

Окрім шифрування, для запобігання несанкціонованому доступу до вбудованих пристроїв та їхніх конфіденційних даних необхідні надійна автентифікація та контроль доступу. Зловмисники можуть легко використати слабкі паролі або погано реалізовані механізми автентифікації. Таким чином, впровадження надійних методів автентифікації,

таких як двофакторна автентифікація та цифрові сертифікати, має вирішальне значення для підтримки безпеки вбудованих систем.

Регулярні оновлення програмного забезпечення необхідні для усунення відомих вразливостей і підтримки загальної безпеки вбудованих пристроїв. Однак багатьом системам не вистачає ефективних механізмів для оновлення мікропрограм або програмного забезпечення, через що вони піддаються загрозам. Забезпечення своєчасного та безпечного оновлення програмного забезпечення є критично важливим компонентом ефективної стратегії захисту даних у вбудованих системах.

З огляду на те, що вбудовані пристрої часто підключаються до Інтернету чи інших мереж, використання безпечних протоколів зв'язку, таких як SSL/TLS і SSH, є обов'язковим для захисту від таких атак, як прослуховування. Для забезпечення конфіденційності та цілісності до конфіденційних даних як під час передачі, так і в спокої слід застосовувати надійне шифрування [4].

Ефективне керування ключами шифрування має першочергове значення для безпеки вбудованих систем. Це передбачає використання безпечних рішень для зберігання ключів і забезпечення ротації та видалення ключів за потреби. Автоматизація керування ключами також може допомогти спростити цей процес і покращити загальну структуру безпеки. Дотримуючись цих найкращих практик, організації можуть значно посилити заходи захисту даних у своїх вбудованих пристроях, забезпечуючи конфіденційність і цілісність у цифровому середовищі, що швидко розвивається.

Використання полегшеної криптографії важливе для захисту вбудованих пристроїв з обмеженими ресурсами. Цей підхід адаптує криптографічні алгоритми відповідно до обмежень пристроїв із низьким енергоспоживанням і низькою здатністю обробки, наприклад тих, що використовуються в медичних технологіях і системах розумного дому. Наприклад, Національний інститут стандартів і технологій (NIST) рекомендував полегшені криптографічні стандарти, придатні для невеликих пристроїв, наголошуючи на необхідності рішень безпеки, які можуть бути ефективно реалізовані в таких середовищах. Це має широкі наслідки для різних додатків, включаючи пристрої охорони здоров'я та промислову автоматизацію, де надійні механізми безпеки є вирішальними.

Таким чином, захист даних у вбудованих пристроях з обмеженими ресурсами потребує комплексного підходу, що охоплює полегшені криптографічні методи, надійні механізми автентифікації, безпечний процес завантаження та регулярне оновлення програмного забезпечення. Враховуючи динамічний розвиток технологій IoT і дедалі ширше використання вбудованих пристроїв у критично важливих галузях (медицина, промисловість, транспорт), впровадження енергоефективних рішень для шифрування й управління ключами набуває особливої актуальності. Успішна реалізація цих підходів передбачає тісну взаємодію апаратних і програмних рішень, а також дотримання відповідних нормативних вимог і стандартів безпеки.

Література

[1] De Micco, L., Vargas, F. L., & Fierens, P. I. (2019). A literature review on embedded systems. *IEEE Latin America Transactions*, 18(02), 188-205.

[2] Lacamera, D. (2018). *Embedded Systems Architecture: Explore architectural concepts, pragmatic design patterns, and best practices to produce robust systems*. Packt Publishing Ltd.

[3] Rozlomii, I., Yarmilko, A., Naumenko, S., & Mykhailovskyi, P. (2024, September). Hardware encryptors and cryptographic libraries for optimizing security in IoT. In *Proceedings of the 12th International Conference Information Control Systems & Technologies (ICST 2024)*, Odesa, Ukraine (pp. 99-109).

[4] Panagiotou, P., Sklavos, N., Darra, E., & Zaharakis, I. D. (2020). Cryptographic system for data applications, in the context of internet of things. *Microprocessors and Microsystems*, 72, 102921.

АДАПТИВНІ КРИПТОГРАФІЧНІ ПРОТОКОЛИ З ДИНАМІЧНОЮ ГЕНЕРАЦІЄЮ КЛЮЧІВ ДЛЯ ГІБРИДНИХ БАЗ ДАНИХ.

Норенко М.С.

Керівник: Розломій І.О.

E-mail: maksnorenko9@gmail.com

Черкаси, Черкаський державний технологічний університет

Адаптивні криптографічні протоколи з динамічною генерацією ключів для гібридних баз даних є важливим напрямком у розвитку безпеки сучасних інформаційних систем. Вони дозволяють забезпечити надійний захист даних в умовах постійних змін, що відбуваються в таких середовищах, як розподілені бази даних та хмарні сервіси. Завдяки таким підходам можна адаптувати криптографічні рішення до конкретних умов використання і змінюваних загроз, що виникають у процесі зберігання та обробки даних[1].

Динамічна генерація ключів є ключовою складовою в адаптивних криптографічних протоколах. Вона дає змогу автоматично оновлювати криптографічні ключі залежно від зміни умов, що дозволяє підтримувати високий рівень захисту інформації в умовах, коли доступ до даних здійснюється з різних джерел і різними користувачами. Зокрема, це дозволяє знижувати ризики компрометації ключів, забезпечуючи їхню своєчасну зміну у відповідь на зловмисні спроби доступу або інші зовнішні загрози.

Інноваційні підходи до розробки таких протоколів зосереджуються на використанні гібридних баз даних, які поєднують в собі різні типи зберігання даних. Це дає змогу поєднувати переваги реляційних і нереляційних баз, оптимізуючи процеси доступу та обробки великих обсягів інформації[2]. Адаптивність у контексті цих баз даних дозволяє динамічно налаштовувати криптографічні методи відповідно до типу даних і вимог до їх захисту, що робить систему більш гнучкою і надійною.

Важливою перевагою адаптивних криптографічних протоколів є можливість інтеграції з різними стандартами і технологіями захисту даних. Це дозволяє забезпечити високий рівень безпеки, навіть у випадку змін у зовнішньому середовищі або при появі нових вразливостей. Наприклад, протоколи можуть бути налаштовані для використання сучасних криптографічних методів, таких як квантова криптографія, що робить їх стійкими до можливих загроз, які з'являються з розвитком новітніх технологій [3].

Таким чином, дослідження в галузі адаптивних криптографічних протоколів з динамічною генерацією ключів для гібридних баз даних відкриває нові можливості для створення більш безпечних і ефективних систем зберігання та обробки даних. Вони дозволяють підтримувати високу стійкість до атак і забезпечують гнучкість при використанні різних типів даних і технологій, що робить їх актуальними в умовах швидко змінюваного інформаційного середовища.

Література

[1] Arora, S., Singh, P., & Gupta, A. J. (2016). Adaptive selection of cryptographic protocols in wireless sensor networks using evolutionary game theory. *Procedia Computer Science*, 78, 358-366. Spring. Spring Tool Suite [Електронний ресурс] – Режим доступу до ресурсу: spring.io/tools/sts

[2] PRIYA, S. Suga; VIJAYABHASKER, R.; RAJARAM, A. Advanced Security and Efficiency Framework for Mobile Ad-Hoc Networks Using Adaptive Clustering and Optimization Techniques. *Journal of Electrical Engineering & Technology*, 2025, 1-12.

[3] Battagliola, M., Borin, G., Di Crescenzo, G., Meneghetti, A., & Persichetti, E. (2025). Enhancing Threshold Group Action Signature Schemes: Adaptive Security and Scalability Improvements. *Cryptology ePrint Archive*.

РОЗРОБКА ФІЛЬТРА КОНТЕНТУ ДЛЯ ЗАХИСТУ ВІД ФІШИНГУ

Підмурняк М.В.

Керівник: Шаповалова О.О.

E-mail: *Pidmurniak14@gmail.com*

Харків, Харківський національний економічний університет імені Семена Кузнеця

Фішингові атаки є однією з найбільш поширених загроз у сфері кібербезпеки, що спричиняють значні фінансові втрати та компрометацію конфіденційних даних користувачів[1]. Традиційні методи блокування фішингових сайтів, такі як чорні списки або сигнатурний аналіз, часто виявляються недостатньо ефективними через постійне оновлення шахрайських ресурсів та зміну їхньої структури[2]. Тому актуальним є розробка нових підходів, заснованих на методах машинного навчання та обробки природної мови (NLP), які дозволяють більш точно ідентифікувати потенційно небезпечні веб-сайти[3].

Метою дослідження є розробка інтелектуального фільтра контенту для захисту від фішингових сайтів, який аналізує веб-сторінки та визначає їхню безпечність на основі вмісту, структури URL та HTML-коду. Основні завдання роботи включають:

- збір та аналіз даних про фішингові веб-сайти[2];
- визначення ключових ознак фішингових ресурсів[3];
- реалізацію алгоритму машинного навчання для автоматичної класифікації сайтів[4];
- інтеграцію розробленого рішення у браузерне розширення або мережевий шлюз безпеки[1].

Огляд існуючих методів виявлення фішингових сайтів включає використання чорних списків (Google Safe Browsing API, OpenPhish)[1], евристичних методів аналізу URL та доменів[4], а також застосування машинного навчання[3]. Обробка природної мови дозволяє аналізувати текстовий вміст сторінок за допомогою TF-IDF, Word2Vec, BERT, що, в свою чергу, допомагає знаходити невідповідності у стилі написання текстів, характерні для фішингових сайтів[3]. Використання глибоких нейромереж (CNN, LSTM, трансформерних моделей) може покращити якість аналізу та зменшити кількість хибнопозитивних результатів[4]. Розроблене програмне забезпечення включає три основні модулі: модуль збору даних (парсинг HTML-структури, API-запити до баз даних фішингових сайтів)[2], модуль аналізу (класифікація за допомогою алгоритмів машинного навчання та NLP)[3] та модуль інтеграції (браузерне розширення або серверна реалізація). Навчання моделі базується на реальних датасетах (PhishTank, OpenPhish, APWG)[2], а оцінка ефективності виконується за метриками Precision, Recall, F1-score[4]. Результати дослідження показали, що використання NLP та машинного навчання дозволяє значно підвищити точність виявлення фішингових сайтів у порівнянні з класичними методами. Інтеграція розробленого рішення у браузерне розширення може забезпечити ефективний захист користувачів в режимі реального часу[1]. Подальший розвиток дослідження передбачає впровадження гібридного підходу (поєднання машинного навчання та евристичних методів)[4], а також інтеграцію з корпоративними системами кібербезпеки[2].

Література

[1] Google Safe Browsing API. [Електронний ресурс] – Режим доступу до ресурсу: <https://developers.google.com/safe-browsing>

[2] PhishTank Database. [Електронний ресурс] – Режим доступу до ресурсу: <https://www.phishtank.com/>

[3] Bahnsen A.C., Torroledo D., Camacho-Collados M., et al. Detecting Phishing Attacks using Natural Language Processing and Machine Learning. – 2018.

[4] Zouina S., Outtaj B. Phishing Detection Using Support Vector Machines and Random Forest. – 2017.

РОЗРОБКА ПРОГРАМНОЇ МОДЕЛІ СИСТЕМИ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ В МЕРЕЖАХ ЗВ'ЯЗКУ СТАНДАРТУ GSM

Попов В.Ю.

Керівник: Семенов С.Г.

E-mail: vladislav.lllove@gmail.com

Харків, Харківський національний економічний університет імені Семена Кузнеця

У сучасному світі забезпечення безпеки інформації у мережах зв'язку стандарту GSM має вирішальне значення. З метою забезпечення конфіденційності та цілісності переданих даних розробляється програмна модель системи криптографічного захисту. У межах дослідження проводиться аналіз ефективності цієї моделі з метою її оптимізації та підвищення надійності захисту інформації. Розроблена програмна модель спрямована на забезпечення високого рівня безпеки та приватності користувачів у мережах GSM, що робить її актуальною та необхідною у сучасному інформаційному суспільстві.

Актуальність теми дослідження полягає у зростаючій потребі захисту конфіденційності та безпеки інформації у мережах зв'язку стандарту GSM. З огляду на широке використання мобільних телефонів із підтримкою GSM, зловмисникам стає легше отримати несанкціонований доступ до особистих даних та конфіденційної інформації користувачів. Тому розробка програмної моделі системи криптографічного захисту стає важливою для забезпечення приватності та безпеки користувачів у цих мережах.

У межах дослідження проводиться розробка програмної моделі системи криптографічного захисту інформації, призначеної для використання у мережах зв'язку стандарту GSM. Ця модель включає в себе алгоритми шифрування та аутентифікації, які забезпечують конфіденційність та цілісність переданих даних, а також захищають мережевий трафік від несанкціонованого доступу [1].

Аналіз ефективності розробленої програмної моделі дозволяє оцінити її здатність забезпечити високий рівень захисту інформації у мережах GSM. Це включає в себе перевірку стійкості криптографічних алгоритмів до атак, швидкість обробки даних, а також визначення вразливостей системи та шляхів їх вирішення.

Загальне значення цього дослідження полягає у покращенні безпеки та конфіденційності інформації у мережах зв'язку стандарту GSM. Розробка ефективної програмної моделі криптографічного захисту сприятиме забезпеченню приватності користувачів та запобіганню несанкціонованому доступу до їх особистих даних.

Основний напрямок дослідження включає розробку програмної моделі системи криптографічного захисту інформації для мереж зв'язку стандарту GSM. Ця модель буде включати в себе алгоритми шифрування та аутентифікації, які забезпечують безпеку та конфіденційність переданих даних в мережі.

Важливий компонент дослідження - це аналіз сучасних методів криптографічного захисту, що застосовуються в мережах зв'язку стандарту GSM. Це включає в себе вивчення та оцінку стійкості алгоритмів шифрування та методів аутентифікації, щоб забезпечити ефективний захист інформації.

Крім того, проводиться аналіз поточних загроз безпеці в мережах GSM, таких як атаки з використанням перехоплення даних або зламу системи аутентифікації. Це допомагає виявити потенційні вразливості системи та розробити ефективні заходи захисту [2].

У результаті дослідження розробляється програмна модель, яка буде здатна забезпечити високий рівень захисту інформації в мережах GSM, зменшуючи ризик несанкціонованого доступу та збереження конфіденційності даних.

Аналіз ефективності розробленої програмної моделі показав, що вона дійсно здатна забезпечити високий рівень захисту інформації у мережах GSM. Це стосується як стійкості криптографічних алгоритмів до атак, так і швидкості обробки даних, а також виявлення та вирішення вразливостей системи.

Загальне значення цього дослідження полягає у підвищенні безпеки та конфіденційності інформації, що передається у мережах зв'язку стандарту GSM. Розроблена програмна модель криптографічного захисту допоможе запобігти несанкціонованому доступу до особистих даних користувачів і сприятиме покращенню їх приватності та безпеки в цих мережах.

Література

[1] Гапак О. М. Визначення довжини періоду генераторів псевдовипадкових послідовностей на основі GSM. 2017. 92 – 97 с.

[2] NIST SP 800-22rev1a. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, 2020, 131 p.

РОЗРОБКА ЗАХИЩЕНОЇ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ СИСТЕМИ ДЛЯ МОНІТОРИНГУ СТАНУ БУДІВЕЛЬНИХ КОНСТРУКЦІЙ НА ОСНОВІ ІОТ

Пугач Т.А.

E-mail: 388karuno@gmail.com

Харків, Харківський національний економічний університет імені Семена Кузнеця

У сучасному світі цифрові технології відіграють важливу роль у забезпеченні безпеки та довговічності будівельних конструкцій. Інтернет речей (IoT) дозволяє створювати системи моніторингу, які відстежують стан об'єктів у реальному часі. Однак одним із ключових викликів таких систем є забезпечення їх захищеності від несанкціонованого доступу та кібератак.

Мета дослідження – розробка безпечної IoT-системи моніторингу будівельних конструкцій, що забезпечує захист від кібератак та несанкціонованого доступу.

Основні завдання дослідження:

- Аналіз сучасних методів моніторингу будівельних конструкцій та їх безпекових ризиків.
- Вибір оптимальної архітектури IoT-системи з урахуванням вимог безпеки.
- Розробка механізмів аутентифікації, шифрування та контролю доступу.
- Реалізація прототипу системи та її тестування.

Система моніторингу базується на мережі IoT-пристроїв, що використовують датчики для збору інформації про фізичний стан будівельних конструкцій (температура, вологість, деформація тощо). Для передачі даних застосовуються бездротові технології (Wi-Fi, LoRaWAN, Zigbee) [1].

Безпека IoT-системи забезпечується такими методами:

- Використання шифрування AES-256 для захисту даних при передачі.
- Впровадження механізмів аутентифікації на основі X.509-сертифікатів.
- Захист від атак типу «man-in-the-middle» (MITM) та DDoS.
- Виявлення аномальної активності за допомогою машинного навчання [2].

Практична реалізація. ESP32, які відрізняються низькою вартістю, енергоефективністю та мають вбудовані модулі Wi-Fi та Bluetooth, що робить їх ідеальними для застосування в IoT-пристроях. Для забезпечення обміну даними між мікроконтролерами та сервером використовується протокол MQTT (Message Queuing Telemetry Transport), який є легким та ефективним протоколом, спеціально розробленим для IoT-пристроїв з обмеженими ресурсами. MQTT забезпечує надійну доставку повідомлень та підтримує зв'язок між великою кількістю пристроїв. Особлива увага в розробці системи приділяється питанням кібербезпеки. Для централізованого моніторингу та аналізу даних щодо безпеки використовується платформа Wazuh. Wazuh є потужним інструментом для виявлення вторгнень, аналізу журналів безпеки та моніторингу цілісності файлів. Завдяки Wazuh,

система забезпечує високий рівень захисту від кіберзагроз, що є критично важливим для систем, що контролюють стан критичної інфраструктури[3].

Розроблена IoT-система забезпечує надійний моніторинг будівельних конструкцій та має високий рівень захисту від кіберзагроз. Запропоновані рішення можуть бути впроваджені у реальних умовах для підвищення безпеки критичної інфраструктури. Подальші дослідження спрямовані на оптимізацію алгоритмів безпеки та розширення функціональності системи.

Література

[1] Lee, J., Bagheri, B., & Kao, H. A. (2015). A Cyber-Physical Systems architecture for Industry 4.0-based manufacturing systems. *Manufacturing Letters*, 3, 18-23.

[2] Liu, P., Yang, C., & Wu, J. (2020). Security and Privacy Challenges in IoT-based Smart Homes. *IEEE Access*, 8, 23456-23470.

[3] Wazuh. Open Source Security Monitoring Platform. [Електронний ресурс] – Режим доступу до ресурсу: <https://wazuh.com>

ВИЗНАЧЕННЯ ПОГОДЖЕНОСТІ ДУМОК ЕКСПЕРТІВ ЗАСОБАМИ ВІЛЬНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Пчолка В.Е.

Керівник: Солодовник Г.В.

E-mail: ganna.solodovnyuk@hneu.net

Харків, Харківський національний економічний університет імені Семена Кузнеця

Актуальність. В умовах постійного тиску з боку кіберзагроз, які можуть спричинити фінансові втрати, витік даних або репутаційні збитки керівники повинні приймати рішення на основі аналізу ризиків, оцінки потенційних загроз і розробки ефективних стратегій захисту. З цією метою використовуються методи моделювання кіберзагроз, система управління ризиками (Cyber Risk Management) та принципи адаптивної безпеки, які дозволяють зменшити ймовірність атак та мінімізувати їх наслідки. Використання об'єктивних методів оцінювання ризиків значно підвищує ефективність рішень завдяки науковому обґрунтуванню. Проте такий підхід вимагає наявності певної інформації про умови реалізації рішень. За відсутності такої інформації використовують суб'єктивні методи оцінювання ризиків, на підставі думок експертів. В цьому випадку виникає проблема довіри наданим оцінкам, тобто необхідність визначення їх достовірності. Одним з показників достовірності оцінок є погодженість думок експертів, яка зазвичай визначається за використання колективних методів експертних оцінювань.

Мета роботи полягає у створенні програмної реалізації розв'язання задачі визначення погодженості думок експертів в процесі оцінювання інформаційних ризиків.

Якщо кількість експертів більша за двох, а кількість об'єктів оцінювання перевищує значення 3, то доцільно використовувати коефіцієнт конкордації W – загальний коефіцієнт рангової кореляції для групи з m експертів та кількості об'єктів оцінювання n . Значення цього показника належить інтервалу $[0,1]$ та розраховується за формулою:

$$W = \frac{12 S}{m^2 n (n^2 - 1)},$$

де S – сума квадратів відхилень всіх оцінок рангів кожного об'єкта експертизи від середньої думки.

Чим ближче значення коефіцієнта конкордації до одиниці, тим думки експертів більш погоджені, тим вищим є рівень довіри наданим оцінкам, а значить їх можна використовувати для прийняття рішень [1].

Розроблена програмна реалізація дозволяє вводити кількість експертів та кількість об'єктів оцінювання, а також в діалоговому режимі вводити значення рангів. За даних, введених під час проведення тестового експерименту з програмою, було визначено $W=0.1675$. Це свідчить про низький рівень узгодженості думок експертів щодо ранжування ризиків. Недостатня узгодженість може бути ризиком для прийняття остаточного рішення на основі цих даних, тому рекомендується проведення повторної експертизи або додаткового аналізу з метою уточнення сформованих ризиків.

Програмна реалізація написана мовою Python, яка належить до програмного забезпечення з відкритим кодом [2].

Висновок. Використання вільних програмних засобів допомагає підвищувати ефективність рішень в багатьох сферах людської діяльності без витрачання зайвих фінансових засобів.

Література

[1] Studfile // Метод Кендала [Електронний ресурс] – Режим доступу до ресурсу: <https://studfile.net/preview/6059770/page:19/>

[2] Python [Електронний ресурс] – Режим доступу до ресурсу: <https://www.python.org/>

БЕЗКОШТОВНІ СИСТЕМИ ВИЯВЛЕННЯ ВТОРГНЕНЬ У КОМП'ЮТЕРНИХ МЕРЕЖАХ

Рихва В.

Керівник: Солодовник Г.В.

E-mail: volodymyr.rykhva@hneu.net

Харків, Харківський національний економічний університет імені Семена Кузнеця

Виявлення вторгнень – це процес моніторингу подій, що відбуваються в комп'ютерній системі чи мережі, та їх аналізу на ознаки вторгнень, які визначаються як спроби порушити конфіденційність, цілісність, доступність або обійти механізми безпеки комп'ютера чи мережі. Системи виявлення вторгнень (IDS) – це програмні або апаратні продукти, які автоматизують процес моніторингу та аналізу. [1]

IDS поділяються на кілька основних типів [2]:

- Network intrusion detection system (NIDS) – розгортається у стратегічних точках мережі організації для моніторингу вхідного та вихідного трафіку. Виявляє підозрілі дії у всьому мережевому середовищі.
- Host intrusion detection system (HIDS) – встановлюється на окремих пристроях, що підключені до мережі, та дозволяє аналізувати пакети даних, які не може побачити NIDS.
- Signature-based intrusion detection system (SIDS) – порівнює мережеві пакети з базою відомих загроз і виявляє атаки за їхніми сигнатурами.
- Anomaly-based intrusion detection system (AIDS) – аналізує трафік мережі та порівнює його з базовими показниками "нормальної" поведінки. Використовує машинне навчання для виявлення нових, ще не відомих загроз.
- Perimeter intrusion detection system (PIDS) – розміщується на периметрі критичної інфраструктури та фіксує спроби вторгнення.
- Virtual machine-based intrusion detection system (VMIDS) – відстежує трафік та підозрілі дії у віртуальному середовищі, забезпечуючи моніторинг трафіку між віртуальними машинами.
- Stack-based intrusion detection system (SBIDS) – інтегрується у протокол TCP/IP, що дозволяє IDS відстежувати та блокувати шкідливі пакети ще до того, як вони будуть оброблені операційною системою або додатками.

Найбільш поширені на сьогодні програмні IDS, що працюють на NIDS:

- Система Zeek, раніше відома як Bro, є результатом багаторічних досліджень та розробок у галузі мережевої безпеки [3]. Розпочата в 1995 році в Національній лабораторії

Лоуренса в Берклі, США, вона стала одним із найпотужніших інструментів для аналізу мережевого трафіку та виявлення аномалій. Основним методом, що використовується в Zeek, є глибокий аналіз протоколів і подій на різних рівнях мережевої моделі. Система не просто шукає відомі сигнатури атак, а моделює поведінку мережевих з'єднань, дозволяючи виявляти складні та нові загрози.

- Snort – це відкрита система виявлення та запобігання вторгнень (IDS/IPS) [4], розроблена Мартіном Роешем у 1998 році. З моменту свого створення Snort стала однією з найпоширеніших систем IDS у світі, завдяки своїй гнучкості, продуктивності та підтримці спільноти. Основним методом, що використовується в Snort, є сигнатурний аналіз мережевого трафіку з використанням правил, які описують характерні ознаки відомих атак. Система також підтримує аналіз на основі аномалій через використання препроцесорів та модулів розширення.

- Suricata – це високопродуктивна система виявлення вторгнень та запобігання атак (IDS/IPS), розроблена Open Information Security Foundation (OISF) [5]. Проект розпочато в 2009 році з метою створення сучасної та гнучкої IDS з відкритим кодом. Основний метод, що використовується в Suricata, – це сигнатурний аналіз мережевого трафіку з використанням правил, подібних до правил Snort. Однак Suricata також підтримує розширені функції, такі як глибокий аналіз пакетів та розпізнавання протоколів на основі контексту.

- Security Onion – це інтегрована платформа з відкритим кодом для моніторингу мережевої безпеки, яка поєднує в собі кілька інструментів для виявлення вторгнень, аналізу журналів та реагування на інциденти [6]. Проект розпочато в 2008 році та активно розвивається спільнотою спеціалістів з безпеки. Основний метод роботи Security Onion полягає в комбінуванні різних інструментів та технологій для створення комплексного рішення з моніторингу та аналізу безпеки.

- Wazuh – це платформа з відкритим кодом для виявлення вторгнень на основі агентів, моніторингу безпеки та відповідності вимогам [7]. Вона є розвитком проекту OSSEC, розпочатого в 2008 році. Основний метод роботи Wazuh – це збір та аналіз даних з кінцевих вузлів за допомогою встановлених агентів, що дозволяє контролювати цілісність файлів, аналізувати журнали та виявляти аномалії.

Найбільш поширеною IDS на NIDS рівні є OSSEC. Вона забезпечує моніторинг подій на рівні хостів, аналізуючи журнали подій, зміни у файловій системі, спроби отримання несанкціонованого доступу та виявляє руткити (rootkit). OSSEC інтегрується з SIEM-системами, що робить її ефективним рішенням для комплексного моніторингу безпеки.

Головна відмінність між IDS і брандмауером полягає в їхньому функціональному призначенні. Брандмауер є механізмом контролю, який блокує або дозволяє трафік відповідно до встановлених правил на основі IP-адрес, портів, протоколів або додатків. Він працює як бар'єр, що запобігає несанкціонованому доступу. Натомість IDS є системою моніторингу та виявлення загроз. Вона аналізує трафік на предмет підозрілої активності або ознак атак. IDS не блокує трафік самостійно, а лише генерує сповіщення для подальшого аналізу та реагування. Деякі IDS-системи, наприклад Suricata, можуть працювати в режимі IPS (Intrusion Prevention System) і виконувати функції брандмауера, активно блокуючи загрози. Оптимальне розміщення IDS залежить від потреб безпеки: найчастіше його встановлюють після брандмауера, що знижує навантаження на систему та дозволяє фокусуватися на внутрішніх загрозах. Рідше IDS розміщують перед брандмауером, що забезпечує раннє виявлення загроз, але потребує більше ресурсів [8].

Література

[1] Rebecca Bace, Peter Mell Intrusion Detection Systems, 2001. [Електронний ресурс] – Режим доступу до ресурсу: <https://www.govinfo.gov/app/details/GOVPUB-C13-PURL-LPS72073>

[2] What Is An Intrusion Detection System (IDS)? [Електронний ресурс] – Режим доступу до ресурсу: <https://www.fortinet.com/resources/cyberglossary/intrusion-detection-system>

[3] Zeek. [Електронний ресурс] – Режим доступу до ресурсу: <https://github.com/zeek/zeek>

[4] Snort [Електронний ресурс] – Режим доступу до ресурсу: <https://www.snort.org>

[5] Suricata [Електронний ресурс] – Режим доступу до ресурсу: <https://suricata.io>

[6] Security Onion [Електронний ресурс] – Режим доступу до ресурсу: <https://securityonionsolutions.com/software>

[7] Wazuh. [Електронний ресурс] – Режим доступу до ресурсу: <https://github.com/wazuh/wazuh>

[8] Intrusion Detection System in Cyber Security, [Електронний ресурс] – Режим доступу до ресурсу: <https://www.stamus-networks.com/intrusion-detection-system-in-cyber-security>

ЕФЕКТИВНИЙ ARX ПІДХІД ДО ЗАХИСТУ ІНФОРМАЦІЇ В СЕРЕДОВИЩІ З ОБМЕЖЕНИМИ РЕСУРСАМИ

Розломій І.О., Науменко С.В.

E-mail: inna-roz@ukr.net

Черкаси, Черкаський державний технологічний університет

Ефективний підхід ARX (Addition-Rotation-XOR) до захисту інформації в середовищах з обмеженими ресурсами – це структура, розроблена для підвищення безпеки даних у середовищах з обмеженими обчислювальними ресурсами та доступом до мережі. З розвитком Інтернету речей (IoT) ці середовища стикаються з проблемами щодо безпеки та конфіденційності, що робить ефективні методології захисту даних необхідними для пом'якшення таких ризиків, як витік даних та внутрішні загрози [1].

Відомий завдяки інтеграції легких криптографічних методів, підхід ARX пропонує ефективне рішення для захисту конфіденційної інформації з відносно невеликими витратами обчислювальних ресурсів. Використовуючи прості математичні операції, алгоритми ARX забезпечують надійне шифрування, зберігаючи при цьому низьку затримку та обчислювальні витрати, що робить їх особливо придатними для пристроїв з обмеженою потужністю та можливостями обробки.

Ефективність ARX відрізняється від традиційних криптографічних методів, які часто вимагають більш складних операцій і значних ресурсів. Структура охоплює різні стратегії, спрямовані на захист конфіденційності, цілісності та доступності даних протягом усього життєвого циклу. До них належать розширені протоколи шифрування, контроль доступу на основі ролей і регулярні оцінки вразливості, які сприяють зміцненню захисту від нових кіберзагроз. Однак реалізація ARX не позбавлена проблем; він повинен враховувати потенційні ризики, пов'язані з людськими помилками та технічними обмеженнями, шляхом ретельного тестування та постійного моніторингу. Оскільки попит на безпечне керування даними зростає із розширенням кількості пристроїв IoT, підхід ARX позиціонується як важливий внесок у розробку надійних інфраструктур безпеки, які можуть ефективно захищати конфіденційні дані в середовищах з обмеженими ресурсами. Його здатність оптимізувати керування доступом і підвищити відповідність нормативним вимогам ще більше підкреслює його важливість у сучасному цифровому ландшафті [2].

В останні роки поширення Інтернету речей (IoT) значно змінило спосіб збору, зберігання та використання даних. Однак цей швидкий прогрес створює кілька проблем, зокрема щодо безпеки та конфіденційності в середовищах з обмеженими ресурсами.

Відсутність належного шифрування є основною вразливістю багатьох додатків Інтернету речей, що робить передачу даних чутливою до перехоплення та використання зловмисниками [3]. Щоб вирішити ці проблеми, необхідно включити надійні протоколи шифрування для захисту конфіденційної інформації під час передачі та зберігання. Крім того, підтримка цілісності та доступності даних має важливе значення для того, щоб операції були надійними та доступними для авторизованих користувачів, особливо в сценаріях, коли зловмисні операції можуть призвести до апаратних збоїв або програмних атак [4].

Інфраструктура ARX пропонує комплексні стратегії для покращення захисту даних у цих середовищах. Він охоплює різні методології, спрямовані на забезпечення конфіденційності, цілісності та доступності інформації протягом усього життєвого циклу.

Підхід ARX, який включає передові стратегії шифрування та управління ризиками, спрямований на зміцнення механізмів захисту даних від широкого спектру кіберзагроз і вразливостей. Завдяки інтеграції надійних функцій безпеки ARX значно зменшує потенційну вразливість організаційних систем, підвищуючи ефективність роботи та забезпечуючи відповідність нормативним вимогам.

ARX забезпечує підвищену безпеку за рахунок впровадження надійних засобів контролю безпеки, проактивних заходів запобігання загрозам і постійного моніторингу. Ці функції призначені для зменшення кіберризиків і захисту критично важливих даних. Використовуючи надійні протоколи безпеки, ARX захищає конфіденційні дані від зловмисних атак і несанкціонованого доступу. Крім того, він проводить регулярні оцінки вразливості та навчає персонал найкращим практикам безпеки, сприяючи зміцненню безпеки проти нових кіберзагроз. Інфраструктура ARX забезпечує покращену відповідність, дотримуючись суворих політик безпеки та нормативних вимог.

ARX оптимізує керування доступом за допомогою захищених каналів зв'язку та контролю доступу на основі ролей. Це забезпечує ефективні процеси авторизації та зводить до мінімуму несанкціонований доступ до конфіденційних даних. Інтеграція ARX з існуючою інфраструктурою має вирішальне значення для уникнення збоїв у роботі та підвищення загальної ефективності. Оскільки ARX розширює свої послуги, вона також повинна вирішувати проблеми масштабованості шляхом ретельного планування та розподілу ресурсів.

Незважаючи на переваги ARX, існують ризики, такі як можливе неправильне використання через людські помилки або технічні обмеження. Щоб зменшити ці ризики, ARX використовує ретельне навчання, суворе тестування та постійний моніторинг. Система використовує передові методи шифрування та багаторівневі стратегії захисту, включаючи системи виявлення вторгнень і брандмауери, для захисту конфіденційної інформації та швидкого реагування на підозрілі дії.

На практиці ARX забезпечує безпечний доступ до конфіденційних даних, контрольований доступ до корпоративних мереж і захист хмарної інфраструктури. Ефективно керуючи дозволами користувачів, ARX обмежує доступ до даних лише авторизованому персоналу, використовуючи розширене шифрування для захисту даних під час передачі та зберігання. Повна інтеграція ARX спрощує процес керування доступом на різних платформах, таким чином підвищуючи безпеку роботи.

Порівнюючи алгоритми ARX з іншими криптографічними рішеннями, однією помітною перевагою є їх затримка швидкості. Алгоритми ARX зазвичай демонструють меншу затримку під час криптографічних операцій порівняно зі звичайними шифрами, які потребують великих обчислювальних ресурсів для шифрування та дешифрування. Зокрема, алгоритм SPECK на основі ARX, забезпечує кращу продуктивність з точки зору затримки швидкості, виконуючи операції швидше, ніж інші методи. Ця ефективність може бути критичною в додатках, які потребують обробки даних у реальному часі. Крім того, швидкість розкладу ключів, яка вимірює ефективність процесу генерації ключів алгоритмом, також надає перевагу алгоритмам ARX. Цей показник вказує на те, що методи ARX можуть генерувати ключі швидше, ніж багато традиційних алгоритмів, що ще більше підвищує їх практичність у середовищах із суворими обмеженнями ресурсів.

Література

[1] Seo, H., Jeong, I., Lee, J., & Kim, W. H. (2018). Compact implementations of ARX-based block ciphers on IoT processors. *ACM Transactions on Embedded Computing Systems (TECS)*, 17(3), 1-16.

[2] Rozlomii, I., Yarmilko, A., Naumenko, S., & Mykhailovskyi, P. (2024, September). Hardware encryptors and cryptographic libraries for optimizing security in IoT. In *Proceedings of*

the 12th International Conference Information Control Systems & Technologies (ICST 2024), Odesa, Ukraine (pp. 99-109).

[3] Pattanaik, R. K., Mohanty, M. N., Mohapatra, S. K., & Pattanayak, B. K. (2023). Nonlinear Dynamic System Identification of ARX Model for Speech Signal Identification. *Comput. Syst. Sci. Eng.*, 46(1), 195-208.

[4] Naru, E. R., Saini, H., & Sharma, M. (2017, February). A recent review on lightweight cryptography in IoT. In 2017 international conference on I-SMAC (IoT in social, mobile, analytics and cloud)(I-SMAC) (pp. 887-890). IEEE.

РОЗРОБКА ВЕБ-ЗАСТОСУНКУ ДЛЯ ЗАХИСТУ ВІД DDoS-АТАК У РЕЖИМІ РЕАЛЬНОГО ЧАСУ

Романов І.Р.

Керівник: Борисенко Д.В.

E-mail: illia.romanov@hneu.net

Харків, Харківський національний економічний університет імені Семена Кузнеця

У сучасному цифровому світі зростає кількість кіберзагроз, серед яких розподілені атаки на відмову в обслуговуванні (DDoS) є одними з найпоширеніших. Веб-застосунки, що працюють у реальному часі, стають першочерговими цілями таких атак, що потребує розробки ефективних механізмів захисту. У цьому дослідженні розглядається підхід до створення веб-застосунку для виявлення та нейтралізації DDoS-атак у режимі реального часу.

Актуальні проблеми:

- Збільшення складності DDoS-атак: Використання ботнетів, експлуатація вразливостей та атаки рівня додатків ускладнюють виявлення та запобігання.
- Необхідність роботи в реальному часі: Класичні методи аналізу трафіку не завжди забезпечують оперативну реакцію на загрози.
- Оптимізація продуктивності: Важливо знайти баланс між швидкістю обробки трафіку та споживаними ресурсами.
- Зменшення хибнопозитивних спрацьовувань: Використання штучного інтелекту та машинного навчання може допомогти підвищити точність виявлення атак.

Для розробки та реалізації веб-застосунку застосовуються такі методи:

- Збір та аналіз даних про DDoS-атаки (використання датасетів, таких як CICDDoS2019, CAIDA, UNSW-NB15).
- Впровадження алгоритмів виявлення атак (методи поведінкового аналізу, аномального виявлення, машинного навчання).
- Розробка веб-застосунку з інтегрованими механізмами захисту від DDoS (Node.js, Python, Flask, Django).
- Тестування та оптимізація (використання тестових середовищ для моделювання атак, таких як LOIC, HOIC, Slowloris).

Використані технології:

- Інструменти аналізу трафіку: Wireshark, Zeek, Suricata.
- Фреймворки для обробки трафіку: Scapy, Netfilter, iptables.
- Машинне навчання: TensorFlow, PyTorch, scikit-learn.
- Архітектура: CloudFlare API, AWS Shield, Google Cloud Armor для інтеграції хмарного захисту.
- Моніторинг та логування: ELK Stack (Elasticsearch, Logstash, Kibana), Prometheus, Grafana.

Очікувані результати:

- Створення ефективного веб-застосунку для виявлення та запобігання DDoS-атакам у режимі реального часу.

- Підвищення точності виявлення атак за рахунок використання машинного навчання.
- Можливість інтеграції з існуючими системами моніторингу та безпеки мережі.
- Зменшення впливу DDoS-атак на продуктивність веб-ресурсів.

Розробка веб-застосування для захисту від DDoS-атак у режимі реального часу є критично важливою задачею для сучасних інформаційних систем. Використання машинного навчання, поведінкового аналізу та ефективних алгоритмів виявлення атак дозволяє значно підвищити рівень кібербезпеки та мінімізувати ризики для веб-додатків.

РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ ВИЯВЛЕННЯ АТАК ТИПУ DOS/DDOS

Россол О.С.

Керівник: Лимаренко В.В.

E-mail: sr09906@gmail.com

Харків, Харківський національний економічний університет імені Семена Кузнеця

Сучасні інформаційні системи зазнають постійних загроз з боку атак типу DoS та DDoS, які спрямовані на порушення доступності ресурсів через перевантаження інфраструктури. З розвитком цифрової економіки та зростанням кількості онлайн-сервісів ці атаки стають дедалі складнішими, використовуючи як масовані потоки запитів, так і складніші методи обходу традиційних засобів захисту. В умовах масштабного переходу бізнесу та державних послуг у цифровий простір, забезпечення ефективного виявлення та нейтралізації таких атак є ключовою задачею кібербезпеки.

Важливість створення ефективних систем виявлення DoS/DDoS атак зумовлена тим, що традиційні методи захисту, такі як фільтрація трафіку або чорні списки IP-адрес, уже не завжди є ефективними. Сучасні атаки можуть бути добре замасковані під легітимний трафік, використовувати зашифровані з'єднання та навіть генерувати запити від справжніх користувачів через ботнети або зламані пристрої. Це вимагає нових підходів до моніторингу мережевого трафіку, аналізу логів та виявлення аномальної активності в реальному часі.

У межах цього дослідження розглядатимуться сучасні методи виявлення DDoS-атак, які поєднують поведінковий аналіз, аналіз мережевого трафіку та логів. Використання багаторівневого підходу до виявлення аномалій дозволяє значно підвищити ефективність виявлення атак і мінімізувати ризик помилкових спрацьовувань.

До уваги необхідно взяти безкоштовні утиліти та сервіси, які можуть бути інтегровані в загальну систему кіберзахисту.

Хмарні сервіси, такі як Cloudflare Free Plan [1], забезпечують базовий захист веб-додатків, фільтруючи підозрілий трафік та запобігаючи перевантаженню серверів. Водночас, інструменти на зразок FastNetMon Community [2] дозволяють здійснювати моніторинг великих обсягів трафіку в реальному часі, що дозволяє виявляти розподілені атаки на рівні інтернет-провайдерів або корпоративних мереж.

Серед локальних рішень необхідно приділити увагу IDS/IPS-системам, таким як Snort та Suricata, які аналізують вхідний трафік і виявляють шаблони атак. Вони можуть працювати як у сигнатурному режимі, розпізнаючи відомі загрози, так і в режимі аналізу аномалій, що дозволяє реагувати на нові, невідомі атаки. Використання таких інструментів у поєднанні з аналізаторами трафіку на зразок Wireshark [3] допомагає детально дослідити характер атак та знаходити слабкі місця в мережевій інфраструктурі.

Окремий напрям дослідження пов'язаний з аналізом логів, оскільки саме в логах серверів та мережевого обладнання можна знайти цінні дані про спроби атак. Для цього застосовуються платформи, такі як ELK Stack (Elasticsearch, Logstash, Kibana) [4], які дозволяють централізовано збирати, обробляти та візуалізувати дані про підозрілі події в системі. Додатково, легкі та швидкі утиліти, такі як GoAccess [5], можуть використовуватися для аналізу веб-трафіку в реальному часі.

У свою чергу необхідно згадати про автоматизоване блокування шкідливих запитів. Наприклад, Fail2Ban [6, 7] дозволяє автоматично блокувати IP-адреси, які надсилають надмірну кількість запитів або намагаються підібрати паролі до сервера.

Розробка власного програмного забезпечення для виявлення DoS/DDoS атак має ґрунтуватися на поєднанні кількох підходів: аналізу мережевого трафіку, поведінкового аналізу та обробки логів. У межах цього дослідження планується розробити рішення, яке базуватиметься на згаданих підходах та забезпечить більш ефективне виявлення атак у режимі реального часу. 2

Одна з ключових перспектив розвитку програмного забезпечення для виявлення DoS/DDoS атак полягає в інтеграції технологій машинного навчання та штучного інтелекту для глибшого аналізу мережевого трафіку та поведінкових аномалій. Використання нейронних мереж і алгоритмів самонавчання дозволить значно покращити точність виявлення атак, зменшуючи кількість хибних спрацьовувань. Крім того, розвиток технологій блокчейну може сприяти створенню розподілених систем захисту, які будуть стійкими до централізованих атак. Також варто враховувати перспективи впровадження автоматизованих відповідей на загрози, що дозволить не тільки виявляти атаки, а й миттєво застосовувати заходи захисту без залучення людини.

Література

[1] Cloudflare. Cloudflare Free Plan [Електронний ресурс] – Режим доступу до ресурсу: <https://www.cloudflare.com/plans/free/>

[2] FastNetMon Community [Електронний ресурс] – Режим доступу до ресурсу: <https://fastnetmon.com/guides/>

[3] Wireshark [Електронний ресурс] – Режим доступу до ресурсу: <https://www.wireshark.org>

[4] Elastic. ELK Stack (Elasticsearch, Logstash, Kibana) [Електронний ресурс] – Режим доступу до ресурсу: <https://www.elastic.co/elastic-stack>

[5] GoAccess [Електронний ресурс] – Режим доступу до ресурсу: <https://goaccess.io>

[6] Вікіпедія. Fail2ban [Електронний ресурс] – Режим доступу до ресурсу: <https://uk.wikipedia.org/wiki/Fail2ban>

[7] GitHub. Fail2ban [Електронний ресурс] – Режим доступу до ресурсу: <https://github.com/fail2ban/fail2ban/blob/master/README.md>

БАГАТОРІВНЕВИЙ АНАЛІЗ ПОВЕДІНКОВИХ ПАТЕРНІВ КОРИСТУВАЧІВ ЯК ІНСТРУМЕНТ ПОПЕРЕДЖЕННЯ КІБЕРАТАК

Ротань К. В.

Керівник: Розломий І. О.

E-mail: k.v.rotan.fitis23@chdtu.edu.ua

Черкаси, Черкаський державний технологічний університет

Ландшафт кібербезпеки постійно розвивається, зумовлений швидким технологічним прогресом та зростаючою витонченістю кіберзлочинців. Це потребує глибшого розуміння поведінки користувачів як критичної складової ефективного виявлення та запобігання загрозам. Відповідно до Національної ініціативи кар'єри та досліджень кібербезпеки, кібербезпека охоплює діяльність та можливості, необхідні для захисту інформаційно-комунікаційних систем від несанкціонованого доступу та експлуатації [1]. Комплексний підхід передбачає не лише захист від зовнішніх загроз, але й розуміння внутрішньої поведінки, що може призвести до порушень безпеки.

Аналіз поведінки користувачів служить основою для ефективного виявлення інсайдерської загрози, що дозволяє організаціям встановити, що є "нормальною" поведінкою серед їх користувачів. Моніторинг таких заходів, як шаблони входу, час доступу до файлів та

використання системи, організації можуть створити базову лінію, яка допомагає виявити відхилення, що вказують на потенційні загрози [2]. Платформа Living Security Unify демонструє цей підхід, відстежуючи понад 250 дискретних поведінок у різних категоріях, забезпечуючи таким чином цілісний погляд на діяльність користувачів та пов'язані з цим ризики [2].

Кібербезпека стикається з численними проблемами, особливо у царині виникаючих загроз. Організації намагаються йти в ногу з динамічним характером цих загроз, які можуть включати фішинг, атаки зловмисного програмного забезпечення та інсайдерські загрози [1, 3]. Виявлення та реагування на аномалії є важливими, оскільки такі технології, як штучний інтелект та аналітика поведінки користувачів та юридичних осіб (UEBA), виявляються корисними для виявлення незвичних зразків, які можуть означати порушення безпеки. Більше того, зростання підключених пристроїв та віддалена робота розширили поверхню атаки, зробивши традиційні механізми оборони недостатніми [3].

Оскільки професіонали з кібербезпеки обробляють конфіденційну інформацію, вони повинні орієнтуватися на етичні дилеми щодо конфіденційності та розкриття даних. Нещодавній Закон про консолідовані асигнування 2022 року підкреслює необхідність прозорості у повідомленні про відомі кібератаки, підкреслюючи баланс між захистом конфіденційних даних та правом громадськості на інформацію. Етичні міркування є першорядними, особливо з огляду на серйозні наслідки, які можуть виникнути внаслідок несанкціонованого розкриття інформації, включаючи крадіжку особи та фінансові шахрайства.

Література

[1] Shelke, P., & Hämäläinen, T. (2024). Analysing multidimensional strategies for cyber threat detection in security monitoring. In Proceedings of the European Conference on Cyber Warfare and Security (Vol. 23, No. 1). Academic Conferences International Ltd.

[2] Sarkar, K. R. (2010). Assessing insider threats to information security using technical, behavioural and organisational measures. information security technical report, 15(3), 112-133.

[3] Enberg, P. (2024). Behavior Analytics in Cyber Security.

ОГЛЯД СПЕЦІАЛІЗОВАНОГО ПЗ ДЛЯ АНАЛІЗУ ВРАЗЛИВОСТЕЙ СМАРТ-КОНТРАКТІВ

Селегей О. Є.

Керівник: Долгова Н.Г.

E-mail: sealeksandr14@gmail.com

Харків, Харківський Національний Економічний Університет імені Семена Кузнеця

Актуальність забезпечення безпеки смарт-контрактів зростає, через те, що блокчейн-технологій стають все більш популярними в загальному цифровому просторі.

Смарт-контракти стали важливою частиною блокчейн-технологій, забезпечуючи автоматизацію угод та виконання умов між сторонами без потреби у посередниках. Вони стали ключовим елементом для розвитку децентралізованих фінансів, токенизації активів, а також інших цифрових сервісів, таких як постачання та електронна комерція.

Однак з ростом популярності таких технологій виникають нові виклики, пов'язані з безпекою смарт-контрактів. Будь-які помилки або вразливості в коді смарт-контрактів можуть призвести до серйозних втрат або зловживань, оскільки блокчейн є незмінним середовищем і після публікації контракту його код неможливо змінити [1].

Вибір смарт-контрактів обумовлений такими факторами як:

- Зростання популярності блокчейн технологій.
- Ріст капіталізація криптоактивів.
- Інтеграція блокчейн технологій в повсякденний вид веб простору як частина Веб

3.

На ринку зараз існує два розв'язання проблеми ідентифікації вразливостей в смарт-контрактах, наймання вузько направлених спеціалістів та використання спеціалізованого програмного забезпечення для аналізу смарт-контрактів на вразливості. З програмного забезпечення зараз найактуальніші проекти які вирішують проблему пошуку вразливостей це MythX, Slither, Securify's [1][3].

Плюсами найму спеціалістів є:

- Максимально якісний аналіз.
- Звітність створюється людиною та може пояснюватися більш простими словами.
- Може самостійно виправити вразливість в смарт-контракті.

Недоліки найму спеціалістів:

- Великі витрати фінансового ресурсу.
- Час на аналіз.
- Складність пошуку та найму спеціалістів.

Плюси наявного програмного забезпечення:

- Автоматизація процесу.
- Детальний аналіз.
- Легка інтеграція.

Недоліки наявного програмного забезпечення:

- Вузька спеціалізація (підтримка тільки однієї мови створення смарт-контрактів).
- Складність для новачків.
- Вартість.
- Складність розширення вразливостей.

Описанні переваги та недоліки як найму спеціалістів, так і використання наявного програмного забезпечення вказують на відсутність універсального рішення, яке об'єднувало б автоматизацію, універсальність і ефективність у роботі з різними мовами програмування та для смарт-контрактів.

Уніфікація смарт-контрактів передбачає в собі такий процес, код смарт-контракту компілюється у байт-код з використанням Python-бібліотек, таких як `py-solc` або `web3.py`. Конвертація байт-коду здійснюється шляхом розбору байт-коду в граф виконання (Control Flow Graph, CFG), де кожна вершина відображає дію, а ребра можливі переходи між діями, що дає логічне представлення дії смарт-контракту [4].

Аналіз на вразливості передбачає прохід по CFG за допомогою алгоритму який шукає логічний патерн вразливості, та помічає його [2].

Генерація звітності дозволить представити результат аналізу в зрозумілому для людини вигляді.

Перевагами даного підходу є:

- У порівнянні з існуючими рішеннями, такими як MythX, Slither чи Securify's , запропонований підхід абстрагується від мов програмування та зосереджується на структурі логіки контракту.
- Аналіз виконується без потреби в знанні специфічних мов (Solidity чи Vyper), що знижує залежність від вузькоспеціалізованих експертів.

CFG є універсальною структурою, яку можна доповнювати новими правилами аналізу для виявлення нових типів вразливостей. Це дає можливість інтегрувати нові алгоритми для виявлення специфічних уразливостей або нових типів атак [4].

Це спеціалізоване програмне забезпечення повинно дозволити:

- автоматизувати процес аналізу смарт-контрактів різних блокчейн-платформ;
- мінімізувати ризики, пов'язані з вразливостями;
- знизити потребу у спеціалістах із кібербезпеки при перевірці коду;
- підвищити безпеку блокчейн-додатків на етапі розробки.

Література

- [1] DL ACM. Securify: Practical Security Analysis of Smart Contracts [Електронний ресурс] – Режим доступу до ресурсу: <https://dl.acm.org/doi/abs/10.1145/3243734.3243780>
- [2] Ethereum. Formal verification of smart contracts [Електронний ресурс] – Режим доступу до ресурсу: <https://ethereum.org/ru/developers/docs/smart-contracts/formal-verification/>
- [3] Trail of Bits Blog. Slither: The Leading Static Analyzer for Smart Contracts [Електронний ресурс] – Режим доступу до ресурсу: <https://blog.trailofbits.com/2019/05/27/slither-the-leading-static-analyzer-for-smart-contracts/>
- [4] CSC110/111. Application: Control Flow Graphs [Електронний ресурс] – Режим доступу до ресурсу: <https://www.cs.toronto.edu/~david/course-notes/csc110-111/17-graphs/08-control-flow-graphs.html>

ПЕРЕВАГИ ТА НЕДОЛІКИ ІНСТРУМЕНТІВ ДЛЯ ВИЯВЛЕННЯ ЗАГРОЗ У МЕРЕЖЕВИХ ТА ХОСТОВИХ СЕРЕДОВИЩАХ

Сивуха А.Л.

Керівник: Венгріна О.С.

E-mail: anastasiasivuha7@gmail.com

Харків, Харківський національний економічний університет імені Семена Кузнеця

У сучасному цифровому світі забезпечення кібербезпеки є важливим завданням через постійне зростання складності та кількості кібератак. Для ефективного моніторингу та виявлення загроз використовуються різні інструменти, які дозволяють аналізувати мережевий трафік та активність на хостах.

В даному дослідженні було виділено наступні популярні інструменти: Snort, Suricata, Wireshark, Bro/Zeek та OSSEC, які забезпечують широкий функціонал для аналізу загроз. Відкритий характер цих систем дозволяє адаптувати їх до потреб користувачів, що робить їх доступними для багатьох організацій. Snort та Suricata забезпечують ефективну роботу у мережевих середовищах, Wireshark використовується для глибокого аналізу трафіку, Bro/Zeek орієнтований на детальний аналіз подій, а OSSEC фокусується на захисті хостів.

Ці інструменти надають можливість для глибокого розуміння мережевої активності, виявлення аномалій та протидії потенційним кіберзагрозам. Оскільки відкриті джерела відіграють ключову роль у розвитку та адаптації технологій кібербезпеки, низка безкоштовних інструментів, доступних на ринку, стають незамінними помічниками для фахівців у цій галузі.

Автором цього дослідження було розглянуто переваги та недоліки, які представлено у табл. 1. Ці дані демонструють перелік популярних інструментів для виявлення загроз у мережевих та хостових середовищах.

Таблиця 1. Переваги та недоліки

Інструмент	Перевага	Недолік
Snort	Потужна система виявлення вторгнень	Високе споживання ресурсів у великих мережах
Wireshark	Інтерактивний аналіз мережевого трафіку	Не автоматизує виявлення загроз
Bro/Zeek	Детальний аналіз на прикладному рівні	Складність конфігурації
Suricata	Підтримка багатопоточності для високої продуктивності	Вимогливість до ресурсів
OSSEC	Ефективне виявлення атак на хостах	Не аналізує мережевий трафік

РОЗРОБКА СИСТЕМИ МОНІТОРИНГУ ТА ПРОТИДІЇ АТАКАМ НА БЕЗДРОТОВІ МЕРЕЖІ З ВИЯВЛЕННЯМ ШКІДЛИВИХ ТОЧОК ДОСТУПУ

Синявський К.Є.

Керівник: Муржа Д.Ю.

E-mail: kirill.ciniavskiub3@gmail.com

Харків, Харківський національний економічний університет імені Семена Кузнеця

Зі зростання використання бездротових мереж значно підвищується ризик кібератак, спрямованих на компрометацію переданих даних та несанкціонований доступ до мережевої інфраструктури. Однією з найбільш небезпечних загроз є створення шкідливих точок доступу (rogue AP), які імітують легітимні мережі та обманним шляхом змушують користувачів підключатися до них. Це може призвести до перехоплення трафіку, крадіжки конфіденційних даних і розповсюдження шкідливого програмного забезпечення. Традиційні механізми безпеки часто виявляються недостатніми для ефективного виявлення таких загроз, тому актуальним є розроблення системи моніторингу та протидії атакам на бездротові мережі.

Метою цього дослідження є створення системи, що дозволить у реальному часі виявляти шкідливі точки доступу, аналізувати їхню поведінку та запобігати можливим атакам. Запропоноване рішення має забезпечувати моніторинг бездротового спектра, аналізувати аномальну активність мережевих пристроїв і автоматично сповіщати адміністратора про потенційні загрози.

Розробка системи передбачає використання методів пасивного та активного сканування бездротових мереж. Пасивне сканування дозволить аналізувати характеристики точок доступу, такі як SSID, MAC-адреси, рівень сигналу та канали зв'язку, що допоможе виявити аномалії, пов'язані з атаками. Активне сканування передбачає перевірку рівня шифрування, підроблених аутентифікаційних запитів та інших підозрілих дій. Важливим компонентом системи стане використання машинного навчання для класифікації мережевих загроз на основі зібраних даних.

Технічна реалізація системи включатиме використання бездротових аналізаторів, таких як Wireshark і Kismet, разом із Python-бібліотеками для обробки мережевого трафіку (Scapy, PyShark). Фронтенд буде реалізовано у вигляді веб-інтерфейсу для наочного відображення загроз та надання адміністративних інструментів для реагування на атаки. Також планується інтеграція з SIEM-системами для автоматизованого аналізу інцидентів і сповіщень.

Очікуваними результатами роботи стане створення ефективного рішення для виявлення шкідливих точок доступу та запобігання атакам на бездротові мережі. Впровадження такої системи дозволить суттєво знизити ризики несанкціонованого доступу, підвищити рівень безпеки корпоративних і публічних Wi-Fi-мереж, а також сприятиме загальному зміцненню захисту інформаційних систем.

РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ АНАЛІЗУ УРАЗЛИВОСТЕЙ КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

Скрипніков Є.М.

Керівник: Муржа Д.Ю.

E-mail: Egvarakcin@gmail.com

Харків, Харківський Національний Економічний Університет імені Семена Кузнеця

Розробка програмного забезпечення для аналізу уразливостей корпоративних інформаційних систем є важливим аспектом сучасної кібербезпеки. Це програмне

забезпечення дозволяє виявляти та аналізувати потенційні слабкі місця в інформаційних системах, що допомагає запобігти кібератакам та захистити корпоративні дані.

Ця система була розроблена з метою автоматизації процесу виявлення уразливостей та надання детальних звітів з рекомендаціями щодо їх усунення. Програмне забезпечення включає в себе модулі для сканування мережі, аналізу даних та генерації звітів.

Основні функції програмного забезпечення:

- Ідентифікація уразливостей: Використання автоматизованих сканерів для виявлення потенційних слабких місць у мережах та системах.
- Аналіз ризиків: Оцінка рівня загрози для кожної виявленої уразливості та пріоритизація їх за ступенем критичності.
- Генерація звітів: Створення детальних звітів з рекомендаціями щодо усунення виявлених проблем.
- Автоматизація процесу: Спрощення процесу аналізу та зменшення людського фактора завдяки інтеграції з існуючими системами безпеки.

Програмне забезпечення було протестовано на реальних корпоративних системах, що дозволило внести необхідні корективи та покращити його функціональність. Інтерфейс користувача розроблений з урахуванням зручності використання для адміністраторів безпеки.

Програмне забезпечення для аналізу уразливостей є ефективним інструментом для підвищення безпеки корпоративних інформаційних систем. Воно дозволяє значно зменшити час на виявлення уразливостей та надає детальні звіти для прийняття рішень керівництвом.

ПРОГРАМНА РЕАЛІЗАЦІЯ ВИБОРУ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ ЗА КРИТЕРІЄМ РИЗИКОВАНОСТІ

Супрун М.В.

Керівник: Солодовник Г.В.

E-mail: ganna.solodovnyk@hneu.net

Харків, Харківський національний економічний університет імені Семена Кузнеця

Актуальність. Прийняття управлінських рішень в сфері захисту інформації передбачають здійснення вибору в умовах ризику, який обумовлений багатьма чинниками, в тому числі й принциповою індетермінованістю процесів, які впливають на безперебійне функціонування засобів інформатизації.

Проблема полягає у виборі найкращої системи заходів безпеки інформації за заданого значення інтегрального показника ефективності. Формулювання проблеми передбачає наявність декількох альтернативних варіантів системи захисту, а значення їх показників ефективності є випадковими величинами.

Метою роботи є автоматизація процесу вибору найкращої системи інформаційного захисту за критеріями ефективності та ризикованості.

В ході роботи було розроблено застосунок вхідними даними якого є: кількість альтернатив системи захисту, можливі значення показника ефективності та відповідні ймовірності для кожної альтернативи. В якості тестового прикладу було проведено розрахунки середньозваженої за ймовірностями ефективності та ризикованості для трьох альтернативних систем (А, В, С). Оскільки кількість альтернатив більша за дві, то для наочності вибору доцільним є графічне зображення результатів розрахунків, а саме: представлення кожної з систем точкою в координатах ризикованість-середньозважений за ймовірностями показник ефективності (рис. 1).

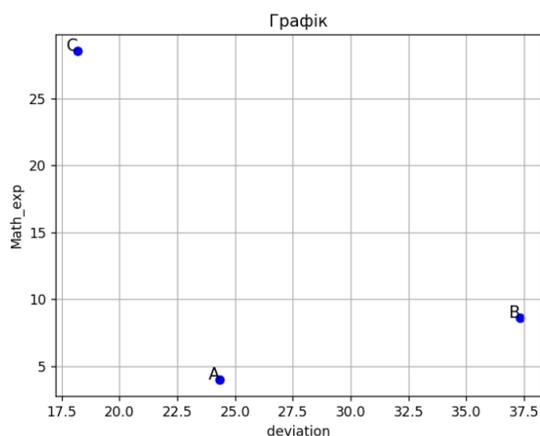


Рисунок 1 – Графічне відображення результатів розрахунків

За математичний інструментарій в роботі використано апарат теорії ймовірності: математичне сподівання для визначення середньозваженого за ймовірностями показника ефективності ME та середньоквадратичне відхилення D для визначення ризикованості альтернатив. Автоматизація реалізована засобами мови програмування Python, яка належить до категорії вільно розповсюдженого програмного забезпечення.

Висновок. Автоматизація математичного апарату теорії ймовірності дозволила визначити найкращу систему безпеки за критеріями середньозваженого за ймовірностями показника ефективності та ризикованості. За наведених вхідних даних такою системою є система C, оскільки вона має найменше значення ризикованості ($DA=24,3$; $DB=37,3$; $Dc=18,1$) та найбільше значення прогнозованого показника ефективності ($MEA= 4$; $MEB=9,6$; $MEc=28,55$). Автоматизація розв'язку дозволяє легко отримувати результати вибору за різних вхідних даних, а графічне відображення результатів сприяє їх наочності для суб'єкта прийняття рішення.

СТАТИСТИЧНИЙ АНАЛІЗ ТА ОПТИМІЗАЦІЯ МЕТОДІВ ВИЯВЛЕННЯ ТА ЗАХИСТУ ВІД СОЦІАЛЬНО-ІНЖЕНЕРНИХ АТАК У СУЧАСНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ

Таласкаєв Д.І.

Керівник : Лимаренко В.В

E-mail: pro100gamer2014@gmail.com

Харків Харківський економічний національний університет імені Семена Кузнеця

Надаючи величезні можливості, інформаційні технології несуть у собі небезпеку, великий набір можливих загроз, реалізація яких може призвести до непередбачуваних і катастрофічних наслідків. Наприклад, збій в інформаційних технологіях, що застосовуються в управлінні атомними станціями або хімічними підприємствами, може призвести до екологічних катастроф [1, 2].

Сам факт використання інформаційних технологій, наприклад, у банківській сфері стає неможливим без організації відповідного рівня захищеності інформаційних ресурсів, що забезпечує конфіденційність, цілісність та доступність інформації [1, 2]. Будь-яка сучасна комп'ютерна система складається з трьох складових компонент: апаратна складова (Hardware), програмне забезпечення (Software) та людина (оператор, користувач, або фахівець, який обслуговує роботу системи) [1, 2]. Для забезпечення захисту перших двох компонентів відомо досить багато програмно-апаратних рішень та продуктів, а третя компонента (людина), в силу своїх особливостей, є слабкою ланкою в системі захисту та забезпечення комп'ютерної безпеки системи в цілому. Будь-яка автоматизована інформаційна система (АІС), незалежно від характеру інформації, що обробляється,

складається не тільки з програмно-технічних засобів і інфраструктури, що підтримує роботу АІС, але і з обслуговуючого персоналу та користувачів інформаційної системи [1, 3].

У цих умовах набули поширення хакерські атаки з використанням прийомів отримання необхідного (несанкціонованого) доступу до інформації, що засновані на використанні слабкостей людського фактору. Набір таких прийомів та методів маніпулювання поведінкою людини отримав назву «соціальна інженерія».

Яким би відмінним не був програмно-апаратний захист, завжди залишається у вразливості людина. За даними статистики, серед вдалих зламів інформаційних систем 80% посідає використання соціальної інженерії [2-4]. Таким чином, розробка та реалізація засобів захисту комп'ютерних систем від атак соціальних хакерів та соціальної інженерії є актуальним завданням на сучасному етапі. Статистика успішно проведених атак на комп'ютерні системи показує, що найслабшою ланкою захисту комп'ютерних систем з точки зору безпеки є людина.

В рамках дослідження планується провести аналіз сучасних методів проведення соціально-інженерних атак, та засобів захисту від них, створити навчальну систему протидії атакам методами соціальної інженерії під назвою «АнтиХак», що призначена для навчання та тестування співробітників різних компаній в галузі інформаційної безпеки, з метою підвищення якості їх знань та можливості протидії атакам соціальної інженерії.

Література

[1] Жарков Я.М. Кібербезпека особистості, суспільства, держави / Я.М. Жарков, М.Т. Дзюба, І.В. Замаруєва та ін. – К. : Видавничо-поліграфічний центра Київський університет», 2018. – 256 с.

[2] Presentation Social Engineering [Електронний ресурс] – Режим доступу до ресурсу: https://owasp.org/www-pdf-archive/Presentation_Social_Engineering.pdf

[3] Social Engineering. What is social engineering [Електронний ресурс] – Режим доступу до ресурсу: <https://www.imperva.com/learn/application-security/social-engineering-attack/>

[4] Данільян О.Г. Національна безпека України: структура та напрямки реалізації: [навч. посібник] / О.Г. Данільян, О.П. Дзьобань, М.І. Панов. : Фоліо, 2022. – 285 с.

ІНТЕГРАЦІЯ КВАНТОВИХ КРИПТОГРАФІЧНИХ ПРОТОКОЛІВ З ГЛИБОКИМ НАВЧАННЯМ ДЛЯ ПРОГНОЗУВАННЯ КІБЕРЗАГРОЗ

Ткаченко Д.В.

Керівник: Розломій І.О.

E-mail: d.v.tkachenko.fitis23@chdtu.edu.ua

Черкаси, Черкаський державний технологічний університет

Інтеграція квантових криптографічних протоколів із глибоким навчанням — це розвиваюча сфера, яка спрямована на вирішення критичної потреби в безпечних комунікаціях в епоху, яка все більше визначається кіберзагрозами. Оскільки організації переходять на хмарні обчислення, потенціал витоку даних зростає, особливо в таких конфіденційних сферах, як охорона здоров'я, де захист конфіденційної інформації пацієнтів є першочерговим [1].

Квантова криптографія являє собою значний прогрес у сфері безпечного зв'язку, використовуючи принципи квантової механіки для встановлення незламних каналів зв'язку. Основою цієї технології є Quantum Key Distribution (QKD), яка забезпечує безпечний обмін криптографічними ключами між сторонами з додатковою можливістю виявлення спроб прослуховування.

Основоположну концепцію QKD вперше представили Чарльз Беннетт і Жиль Brassar у 1984 році через їхній протокол BB84. Цей протокол дозволяє двом сторонам генерувати спільний секретний ключ, який використовується для шифрування та дешифрування

повідомлень. Безпека QKD ґрунтується на квантовій механіці: будь-яка спроба підслухати процес розподілу ключів неминуче порушить квантовий стан, тим самим попереджаючи сторони, що спілкуються, про потенційне порушення.

Квантова криптографія використовує кілька ключових принципів квантової механіки. Зокрема, для підвищення безпеки він використовує такі явища, як суперпозиція та заплутування. Суперпозиція дозволяє частинкам існувати в кількох станах одночасно, тоді як заплутаність гарантує, що пов'язані частинки можуть впливати одна на одну, незалежно від відстані між ними. Ця структура підтримує виявлення прослуховування та забезпечує теоретично безпечний засіб зв'язку [2].

Оскільки квантові технології розвиваються, поточні дослідження спрямовані на усунення цих обмежень, сприяючи інтеграції квантових криптографічних протоколів із новими технологіями, такими як глибоке навчання, для посилення заходів кібербезпеки проти майбутніх загроз.

Однією з головних проблем є внутрішні обмеження квантових обчислювальних ресурсів, які можуть обмежувати масштабованість наборів даних, які можна обробити, і складність моделей машинного навчання, які можна ефективно реалізувати. Це обмеження може суттєво вплинути на обсяг і можливість узагальнення експериментальних результатів, потенційно перешкоджаючи екстраполяції результатів на ширші програми кібербезпеки

Інтеграція квантових криптографічних протоколів із глибоким навчанням для прогнозування кіберзагроз є новою сферою, яка має великі перспективи для посилення заходів кібербезпеки. Оскільки організації стикаються з дедалі складнішими загрозами, використання обчислювальних переваг квантових технологій разом із передбачуваними можливостями глибокого навчання може прокласти шлях до більш стійких систем.

Література

[1] Пашорін, Валерій, "МЕТОДИ ТА ЗАСОБИ ВИКОРИСТАННЯ НЕЙРОННИХ МЕРЕЖ ДЛЯ КРИПТОГРАФІЇ." Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка» 4.24 (2024): 298-311.

[2] Нікітченко, Б. Ю. (2023). Дослідження застосування методів пост-квантової криптографії для розподілених систем авторизації.

ГІБРИДНІ АЛГОРИТМИ НЕЙРОННИХ МЕРЕЖ ТА СТАТИСТИЧНОГО АНАЛІЗУ ДЛЯ ВИЯВЛЕННЯ АНОМАЛІЙ У ВЕЛИКИХ ДАНИХ.

Троян К. С.

Керівник: Розломій І. О.

E-mail: k.s.troian.fitis23@chdtu.edu.ua

Черкаси, Черкаський державний технологічний університет

Гібридні алгоритми нейронних мереж та статистичного аналізу стають важливим інструментом для виявлення аномалій у великих даних. Поєднання цих двох підходів забезпечує високу точність аналізу, дозволяючи оперативно ідентифікувати потенційні загрози та кібератаки. Нейронні мережі ефективно працюють із нелінійними залежностями, тоді як статистичні методи забезпечують строгий математичний підхід до виявлення відхилень від норми [1].

Одним із ключових аспектів цього підходу є можливість адаптивного навчання моделі в реальному часі. Використання глибоких нейронних мереж дозволяє виявляти складні взаємозв'язки між параметрами системи, тоді як статистичний аналіз допомагає встановити порогові значення, що сигналізують про потенційно небезпечні зміни в поведінці системи. Таким чином, система не лише реагує на відомі загрози, а й здатна прогнозувати нові типи аномалій.

Гібридний підхід передбачає багаторівневу обробку даних. На першому етапі нейронна мережа аналізує вхідні параметри, виділяючи ключові особливості. Далі

статистичні методи оцінюють відхилення від нормального функціонування, порівнюючи отримані дані із заздалегідь визначеними шаблонами або історичними показниками. Така комбінація методів дозволяє значно зменшити кількість хибнопозитивних спрацьовувань, покращуючи якість класифікації загроз. Крім того, застосування методів самонавчання дозволяє системі постійно вдосконалювати свої алгоритми та адаптуватися до нових загроз, що робить її надзвичайно ефективною в умовах швидко змінюваного інформаційного середовища.

Практичне застосування цього підходу включає аналіз мережевого трафіку, поведінковий аналіз користувачів та моніторинг промислових систем. У сфері кібербезпеки такі алгоритми дозволяють швидко виявляти спроби несанкціонованого доступу, шкідливе програмне забезпечення та DDoS-атаки. У фінансовому секторі вони допомагають розпізнавати підозрілі транзакції, запобігаючи фінансовим шахрайствам. У сфері охорони здоров'я подібні системи можуть аналізувати показники життєдіяльності пацієнтів, попереджаючи лікарів про можливі ускладнення. У промисловості застосування гібридних моделей дозволяє виявляти технічні несправності обладнання, що дає змогу уникнути аварій та мінімізувати фінансові втрати [2].

Інноваційність такого методу полягає у можливості його застосування для широкого спектра завдань, що потребують оперативного аналізу великих обсягів інформації. Використання гібридних моделей дозволяє підвищити безпеку даних і зробити процес моніторингу більш гнучким та ефективним. Подальші дослідження в цій галузі можуть сприяти вдосконаленню алгоритмів та їх впровадженню в ще більш складні та відповідальні сфери, що вимагають найвищого рівня безпеки та надійності. Такі системи можуть інтегруватися із засобами автоматизованого управління, штучним інтелектом та великими базами даних, що відкриває нові горизонти для підвищення ефективності виявлення загроз і оптимізації процесів безпеки.

Література

[1] Al Jallad, K., Aljnidi, M., & Desouki, M. S. (2020). Anomaly detection optimization using big data and deep learning to reduce false-positive. *Journal of Big Data*, 7, 1-12.

[2] Oprea, S. V., Bâra, A., Puican, F. C., & Radu, I. C. (2021). Anomaly detection with machine learning algorithms and big data in electricity consumption. *Sustainability*, 13(19), 10963.

ДЕЦЕНТРАЛІЗОВАНЕ ЗБЕРІГАННЯ ДАНИХ У ЗАХИЩЕНИХ МЕСЕНДЖЕРАХ

Харитонов Г.Д.

Керівник: Лимаренко В.В.

E-mail: viacheslav.lymarenko@hneu.net

Харків, Харківський національний економічний університет імені Семена Кузнеця

Децентралізація зберігання даних є перспективною методологією, що забезпечує високий рівень конфіденційності й безпеки у системах обміну повідомленнями. Вона дозволяє створювати платформи для комунікації, які не залежать від централізованих серверів та зменшують ризик витоку інформації. [1]

Однією з головних переваг децентралізації даних є збереження повідомлень у зашифрованому вигляді в розподіленій мережі, що запобігає легкому доступу до них сторонніми особами. Також це гарантує володіння власним криптографічним ключем кожним користувачем, що захищає інформацію навіть у разі компрометації окремих вузлів. [2]

Системи децентралізації є менш вразливими до DDoS-атак та зломів завдяки розподіленню даних у кількох незалежних вузлах мережі. Використання наскрізного шифрування (наприклад, AES-256) забезпечує повну конфіденційність обміну повідомленнями між відправником і отримувачем. [3]

Нижче наведені ключові елементи розробки програмного забезпечення:

- Використання протоколів Peer-to-Peer (P2P) для передачі даних напряму між користувачами. Протоколи P2P дозволяють обмінюватися даними між пристроями без необхідності проходження через централізовані сервери.
- Blockchain – це розподілений реєстр, який дозволяє реєструвати події, транзакції або повідомлення у вигляді блоків, захищених криптографією. Застосування blockchain дозволяє мінімізувати ризики підробки повідомлень, а також забезпечує прозорість та довіру між користувачами.
- Наскрізне шифрування (E2EE) забезпечує повну конфіденційність комунікацій, адже дані шифруються безпосередньо на пристрої відправника і розшифровуються лише на пристрої отримувача.

Основними переваги E2EE слід зазначити:

- Шифрування на стороні клієнта – повідомлення кодується перед надсиланням, і ключ для його розшифрування є тільки у отримувача.
- Алгоритм AES-256 (Advanced Encryption Standard) для симетричного шифрування та алгоритм ECDH (Elliptic Curve Diffie-Hellman) для обміну ключами.
- Приватність – оператор платформи чи постачальник сервісу не мають доступу до вмісту повідомлень.

Література

[1] Schneier B. "Applied Cryptography: Protocols, Algorithms, and Source Code in C". Wiley, 2020.

[2] Nakamoto S. "Bitcoin: A Peer-to-Peer Electronic Cash System". – [Електронний ресурс] – Режим доступу до ресурсу: <https://bitcoin.org/bitcoin.pdf>

[3] Wikipedia. Наскрізне шифрування [Електронний ресурс] – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/Наскрізне_шифрування

ГОМОМОРФНЕ ШИФРУВАННЯ В РОЗПОДІЛЕНИХ БАЗАХ ДАНИХ ДЛЯ КОНФІДЕНЦІЙНИХ ОБЧИСЛЕНЬ.

Чікін Д.М

Керівник: Розломій І.О

E-mail: d.m.chikin.fitis23@chdtu.edu.ua

Черкаси, Черкаський державний технологічний університет

Гомоморфне шифрування є однією з ключових технологій для забезпечення конфіденційних обчислень у розподілених базах даних і хмарних середовищах, де безпека інформації є критичною. На відміну від традиційних криптографічних методів, які вимагають розшифрування даних перед їх опрацюванням, гомоморфні алгоритми дозволяють виконувати обчислення безпосередньо над зашифрованою інформацією, що мінімізує ризики витоку конфіденційних відомостей. Це особливо актуально для розподілених систем, де дані зберігаються та обробляються на стороні сторонніх провайдерів, що підвищує ймовірність атак зловмисників або внутрішніх загроз. За словами Gentry С., гомоморфне шифрування вперше стало можливим завдяки використанню ґраткових криптографічних схем, що забезпечили проведення довільних обчислень над зашифрованими даними без втрати їхньої цілісності [1].

Впровадження гомоморфного шифрування у сфері фінансових технологій, медицини та державного управління дозволяє підвищити рівень довіри до цифрових сервісів, оскільки користувачі можуть бути впевнені у безпеці своїх даних навіть під час їх опрацювання. Наприклад, у сфері охорони здоров'я цей метод дає змогу проводити аналіз медичних записів без розкриття персональних даних пацієнтів, що відповідає вимогам нормативних актів щодо конфіденційності інформації. У фінансовому секторі гомоморфні технології забезпечують захищене виконання аналітичних операцій над банківськими транзакціями без

розголошення особистої інформації клієнтів. Brakerski Z. та Vaikuntanathan V. зазначають, що подальші дослідження у цій сфері спрямовані на оптимізацію алгоритмів для зниження обчислювальних витрат та забезпечення більш ефективного шифрування у великих системах [2].

Попри значні переваги, широке впровадження гомоморфного шифрування стримується високими обчислювальними витратами, оскільки існуючі алгоритми потребують значних ресурсів для виконання навіть базових математичних операцій. Тому актуальними є дослідження, спрямовані на оптимізацію методів шифрування та створення апаратних рішень, що підвищують швидкість обчислень. Важливим аспектом є також розробка адаптивних моделей, які дозволяють ефективно поєднувати гомоморфне шифрування з іншими механізмами безпеки, такими як політики розмежування доступу, багатофакторна аутентифікація та аналіз поведінкових патернів користувачів. За результатами дослідження Acar A. та співавторів, поєднання гомоморфного шифрування з іншими криптографічними методами може значно покращити безпеку та продуктивність розподілених систем, що працюють у хмарному середовищі [3].

Література

[1] Gentry, C. (2019). Fully Homomorphic Encryption Using Ideal Lattices. Proceedings of the 41st Annual ACM Symposium on Theory of Computing (STOC'09), 169-178.

[2] Brakerski, Z., & Vaikuntanathan, V. (2024). Efficient Fully Homomorphic Encryption from (Standard) LWE. SIAM Journal on Computing, 43(2), 831-871.

[3] Acar, A., Aksu, H., Uluagac, A. S., & Conti, M. (2018). A Survey on Homomorphic Encryption Schemes: Theory and Implementation. ACM Computing Surveys, 51(4), 1-35.

ПАРОЛІ ЯК КРИТИЧНИЙ ФАКТОР УРАЗЛИВОСТІ В КІБЕРБЕЗПЕЦІ

Чуєва А.О.

Керівник: Долгова Н.Г.

E-mail: anzhelika.chuieva@hneu.net

Харків, Харківський національний економічний університет імені Семена Кузнеця

У сучасному світі паролі відіграють суттєву роль у захисті даних і водночас є найслабшою ланкою в системі кібербезпеки. Для входу в облікові записи, що містять конфіденційну та особисту інформацію, користувачі використовують паролі, які можуть піддатися кібератакам.

Існують певні критерії, яким повинен відповідати надійний пароль [1]:

- довжина повинна відповідати щонайменше 12 символів;
- містить цифри, спеціальні символи, великі та малі літери;
- не повинен містити особисту інформацію, яку хакери можуть легко вгадати;
- для кожного веб-сайту слід використовувати унікальний пароль.

Також є додаткові механізми автентифікації для захисту даних: двофакторна, багатофакторна, біометрична автентифікація та за допомогою апаратних пристроїв (смарт-картки та USB-ключі). Але є недоліки цих методів, чим складніші вони, тим складніше користувачам ними керувати. Постійна потреба у повторній автентифікації та зміні паролів у різних програмах створює додаткові незручності як для звичайних користувачів, так і для ІТ-адміністраторів [2].

Менеджери паролів допомагають керувати та зберігати всі паролі в одному безпечному місці, однак їхня популярність серед користувачів відносно низька. Це пов'язано з деякими чинниками: користувачі не знають, який менеджер обрати, не хочуть витратити кошти на платні рішення або побоюються, що їхні дані будуть зламані, крім того, потрібно додатково встановлювати програму або розширення, та запам'ятовувати один складний пароль. Навіть значна частина організацій (близько половини) не впроваджує менеджери

паролів, висловлюючи про негативний вплив на продуктивність, складність керування, впровадження та зручність використання [1].

Проте більшість людей нехтує рекомендаціями щодо надійності паролів та додатковими методами захисту, тому використання слабких паролів є дуже поширеним. В роботі [1] було проаналізовано понад 15 мільярдів паролів отриманих внаслідок витоків даних, з них найуживанішим є «123456», який можна зламати за декілька секунд. Однак відносно надійні паролі також можуть бути вразливі до атак, якщо їх не змінювати та не використовувати додаткові механізми захисту, які були наведені вище. Так для паролю з 8 знаків, для якого може бути використаний один з 36 різних символів (латинські літери одного регістру і цифри). Кількість можливих унікальних комбінацій становитиме 2,8 трлн (36^8). Методом повного перебору (брутфорсом) сучасний процесор з обчислювальною потужністю 6,7 млрд хешей на секунду зламає такий пароль за 7 хвилин, а така відеокарта як RTX 4090 подолає завдання всього за 17 секунд. А враховуючи те, що потужність обладнання навіть на рівні персональних комп'ютерів постійно зростає, статистика проаналізованих викрадених паролів свідчить про те, що 6 з 10 паролів можуть бути зламані менш ніж за одну годину і для цього знадобляться лише сучасна відеокарта та початкові знання кількох простих алгоритмів на кшталт bruteforce_corr, zxcvbn, unogram, gram_seq, ngram_seq та інших.

У зв'язку з поширенням практики віддаленої роботи та дистанційного навчання зростає і кількість облікових даних у різних сервісах, завдяки яким стає можливий такий формат роботи та навчання, що потребує нових паролів. Врешті це призводить до нової проблеми, коли користувачі відчувають «втому від паролів». Так дослідження [3] показує, що майже половина користувачів Інтернету вважає керування паролями проблемою. Це зумовлено складністю запам'ятовування складних паролів, що змушує людей використовувати повторно їх або створювати прості, що збільшує ризики. До того ж витрати часу на введення та відновлення забутих паролів створюють додатковий стрес.

В свою чергу, ризики витоку паролів завдають значних збитків для компаній та сайтів, які мають їх зберігати, призводячи до штрафів, судових розглядів та втрати репутації, що зумовлює втрату клієнтів. За статистикою, скомпрометовані паролі є причиною понад половини всіх витоків даних.

Розглянемо детальніше статистику витоків даних, пов'язаних з паролями, яка розглядалася у роботі [4]:

- 70% крадіжок паролів відбувається через фішинг;
- 30% витоків даних спричинені внутрішніми факторами;
- 20% випадків зумовлені атаками грубою силою;
- 10% витоків стаються через автоматичний підбір облікових даних.

Середня вартість подолання наслідків витоку даних для компаній становить 4 мільйони доларів, але реальність може бути набагато вищою. Розглянемо деякі з найбільших витоків даних, що сталися у 2024 році. RockYou2024 став найбільшим витоком паролів та був опублікований на онлайн-форумі у вигляді текстового файлу, що містить 10 мільярдів паролів. Була здійснена атака грубою силою хакером, щоб отримати доступ до мережі Dell через бекдор у клієнтському порталі торгового посередника Dell, що призвело до витоку даних клієнтів і платіжної інформації в Інтернет. У травні 2024 року особисті та фінансові дані мільйонів клієнтів були викрадені з бази даних Ticketmaster у зв'язку з атакою підміни облікових даних [4].

Таким чином можна зробити висновок, що паролі залишаються вразливим елементом в системі кібербезпеки, які завдають великих збитків, а альтернативні рішення часто створюють незручності для користувачів та IT-адміністраторів. Проблеми та незручності, які виникають через необхідність створювати, зберігати та відновлювати паролі дійшли до критичної межі і ситуація з паролями з кожним днем тільки погіршується, що вимагає пошуку нових, більш ефективних та зручних підходів до захисту даних та автентифікації без пароля. Враховуючи сучасні тенденції розвитку Інтернет згідно концепції web 3.0, подібне

рішення має базуватися на таких технологіях як блокчейн та штучний інтелект, адже саме ці технології можуть стати основою для створення більш безпечних та зручних систем автентифікації.

Література

[1] 50+ Password Statistics: The State of Password Security in 2024 [Електронний ресурс] – Режим доступу до ресурсу: <https://explodingtopics.com/blog/password-stats>

[2] Annoying but necessary: How to decrease the burden of authentication requirements [Електронний ресурс] – Режим доступу до ресурсу: <https://www.eset.com/blog/new-products/annoying-but-necessary-how-to-decrease-the-burden-of-authentication-requirements-1/>

[3] Password & Login Fatigue Explained [Електронний ресурс] – Режим доступу до ресурсу: <https://www.beyondencryption.com/blog/password-login-fatigue-explained>

[4] 50+ Password Statistics & Trends to Know in 2024 [Електронний ресурс] – Режим доступу до ресурсу: <https://jumpcloud.com/blog/password-statistics-trends>

ВИКОРИСТАННЯ ОПЕРАЦІЙНОЇ СИСТЕМИ TAILS ДЛЯ ЗАБЕЗПЕЧЕННЯ АНОНІМНОСТІ РОБОТИ В ІНТЕРНЕТ ТА ПЕРЕДАВАННЯ ДАНИХ

Шапо В.Ф.¹, Воловщиків В.Ю.²

E-mail: ¹vladlen.shapo@gmail.com, ²valvol98@gmail.com

¹*Одеса, Інститут Військово-Морських Сил*

²*Харків, Національний технічний університет “Харківський політехнічний інститут”*

Велика кількість людей у всьому світі з різних причин вимушені приховувати свою активність в мережі Інтернет та використовувати застарілі комп'ютерні системи для роботи. До першої групи можна віднести журналістів, що розслідують неблаговидні дії різноманітних чиновників, корпорацій, урядів, а також поліцейських, військових, суддів та адвокатів і т.ін., яким необхідно приховати факти свого доступу до різних ресурсів та матеріалів Інтернет. До другої групи можна віднести співробітників організацій, які не мають сучасного парку комп'ютерних систем, та не можуть забезпечити комп'ютером кожного співробітника, або студентів, які вимушені по черзі використовувати один і той самий комп'ютер. При цьому на таких комп'ютерах вже виконані відповідні налаштування, регулярно змінювати які неможливо або не має сенсу.

У зв'язку з нападом Росії на Україну в українських військових з'явилася необхідність, з одного боку, працювати в Інтернеті анонімно, щоб ворог не міг відслідкувати їхні дії, а з другого, – або використовувати будь-які морально та фізично застарілі комп'ютерні системи самостійно (головний критерій в таких випадках, – хоча б мінімальна працездатність), або працювати в таких умовах, коли користувачі навіть таких систем постійно змінюються.

Одним з можливих шляхів виходу з вказаного становища є використання Linux-подібних операційних систем (ОС) Tails (The Amnesic Incognito Live System) [1]. Головним критерієм їхнього використання є можливість завантаження з зовнішнього накопичувача, підключеного по шині USB (флеш-накопичувач або жорсткий диск), або з використанням CD/DVD-приводу (7-10 років тому не можна було уявити собі комп'ютер без такого приводу, тоді як завантаження ОС з зовнішнього USB-пристрою було не завжди можливим).

9.01.2025 р. випущено дистрибутив ОС Tails 6.11, орієнтований на конфіденційність, заснований на пакетній базі Debian 12 і призначений для анонімної роботи в Інтернет. У Tails всі вихідні з'єднання забезпечуються браузером Tor, а всі неанонімні блокуються. ОС Tails повинна для завантажуватися з LiveCD чи LiveUSB і не залишає слідів на комп'ютері, де використовувалася. Для зберігання даних користувача застосовується шифрування. Розмір ISO-образу дистрибутива Tails становить близько 1 ГБ. У версії Tails 6.11 до версії 14.0.4 оновлено браузер Tor і поштовий клієнт Thunderbird (до версії 128.6.0). Усунуто вразливості, виявлені при зовнішньому аудиті безпеки (для експлуатації цих вразливостей нападник

повинен отримати доступ до локального оточення, наприклад, використовуючи доступну вразливість в одному із застосунків):

уразливість у Tails Upgrader, яку можна використати для встановлення модифікованого оновлення дистрибутива та отримання постійного контролю над системою;

проблеми з окремими застосунками, які можуть призвести до деанонізації та відстеження активності користувача: через застосунок Onion Circuits можна отримати відомості про ланцюжки підключення в Tor, через Unsafe Browser можна підключитися до сайтів в обхід Tor, через браузер Tor можна відстежувати дії користувача в браузері, через Tor Connection можна переналаштувати з'єднання;

проблема, пов'язана з можливістю зміни налаштувань постійного сховища.

6.02.2025 р. випущено ОС Tails 6.12 з оновленим браузером Tor (версія 14.0.5), до додатка About додано кнопку перевірки наявності оновлень, додано комбінацію клавіш Ctrl+Alt+T для відкриття емулятора терміналу, забезпечено запуск коду на мові Python в ізольованому режимі, унеможливлено зависання екрана привітання входу в систему при активації постійного сховища, підвищено надійність синхронізації часу під час перезапуску Tor. Два оновлення протягом практично одного місяця свідчать про постійний розвиток ОС Tails і наявність зацікавленості в ній великої кількості користувачів. Усі підключення Tails ОС проходять через мережу TOR, використовуються новітні криптографічні інструменти для шифрування файлів, електронної пошти, обміну миттєвими повідомленнями та приховування всіх файлів і каталогів на електронному носії.

Для встановлення ОС Tails потрібен флеш-накопичувач USB розміром від 8 ГБ і програма Etcher [2] згідно з рекомендаціями розробників ОС Tails. Її інтерфейс інтуїтивно зрозумілий: потрібно вибрати образ ОС, флеш-диск і запустити встановлення. Після завантаження образу потрібно, не відключаючи USB, перезавантажити комп'ютер, увійти в BIOS і вибрати флеш-диск як завантажувальний пристрій, після чого завантажитися з нього.

Меню Greeting відкриватиметься при кожному вході в систему. Далі бажано встановити пароль адміністратора, підміну MAC-адреси, з'єднання через Tor і мости (рис. 1).



Рисунок 1 – Меню встановлення паролю адміністратора в ОС Tails

ОС Tails не розрахована на збереження встановлених у неї програм, налаштувань і файлів під час вимкнення. Але існує можливість зберегти дані в розділі, створеному заздалегідь. Наприклад, щоб встановити програму, треба відкрити менеджер пакетів Synaptic, вказати новий репозиторій програм і вибрати потрібну. Для збереження файлів їх треба перемістити в Home/Persistent. Хоча сам сеанс роботи під час вимкнення комп'ютера не

зберігається, АРТ-пакети (налаштування, розширення браузера тощо) за правильних налаштувань зберігаються в персистентному розділі. Це робить можливим розгортання всіх необхідних програм під час завантаження ОС.

Persistent Volume зашифровано за замовчуванням. Прихований розділ не дуже зручний у використанні. Розробники Tails радять користуватися Cryptsetup, але розділ, створений ним, прихований недостатньо добре. При цьому розділ, створений інструментом TrueCrypt, неможливо виявити. Розділ TrueCrypt прихований так, що ОС його не знайде, поки не буде введено пароль. Під час запису файлів у прихований розділ він може бути пошкоджений. Щоб уникнути цього, треба використовувати опцію, представлену на рис. 2.

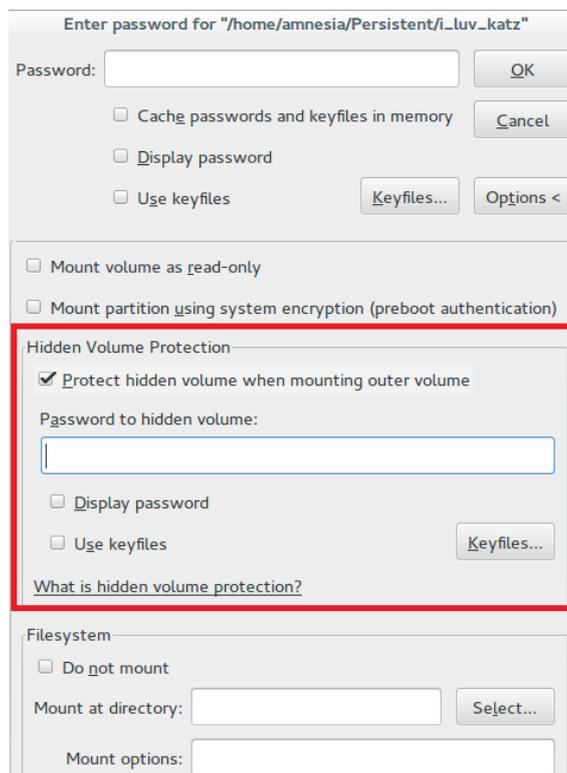


Рисунок 2 – Меню налаштування доступу до прихованого розділу

Браузер TOR відомий усім, хто намагався обійти різні блокування. Тор має завжди працювати в режимі приватного перегляду, захист від відстеження має бути ввімкнений, як і підроблений та обманний вміст. TorButton дає змогу вибрати максимальний рівень захисту. Додатки захищають від стеження під час роботи в Інтернеті, шкідливі сайти будуть заблоковані. Disconnect (Конфіденційний Блокувальник Реклами) блокує Google Analytics, Яндекс Статистику, – основні засоби стеження за відвідуванням сайтів, місцезнаходженням. Adblock Plus блокує трекери, майнінг, рекламу. User-Agent Switcher автоматично змінює fingerprint комп'ютера/браузера. Man in the Middle захищає від перехоплення Інтернет трафіку/МІТМ-атаки. Disable WebRTC: протокол WebRTC видає справжню IP-адресу, ланцюг з'єднань TOR та інші дані, навіть якщо використовуються інші засоби захисту. NoScript: це розширення треба налаштовувати залежно від необхідного рівня захисту. Https Everywhere потрібно вмикати. User-Agent Switcher: вибрати розкид 25% і всі UserAgents.

Для спілкування із зовнішнім світом ОС Tails має чат-клієнт зі встановленим доповненням для шифрування повідомлень Pidgin, систему обміну файлами OnionShare і поштовий клієнт Thunderbird. Додаткова програма MAT стирає метадані файлів, які можуть розкрити інформацію про творця. У систему також входять LibreOffice, Gimp та Inkscape.

Вказане вище робить ОС Tails дуже зручним інструментом для роботи в найрізноманітніших умовах для вирішення дуже широкого спектру задач.

Література

- [1] Tails is a portable operating system that protects against surveillance and censorship. [Електронний ресурс] – Режим доступу до ресурсу: <https://tails.net/>
- [2] BalenaEtcher [Електронний ресурс] – Режим доступу до ресурсу: <https://etcher.balena.io/>

ОГЛЯД ІНТЕРАКТИВНИХ ЗАСОБІВ НАВЧАННЯ ОСНОВАМ КІБЕРБЕЗПЕКИ

Шарун П.В.

Керівник: Солодовник Г.В.

E-mail: ganna.solodovnyk@hneu.net

Харків, Харківський національний економічний університет імені Семена Кузнеця

Актуальність. У сучасному світі цифрові технології відіграють ключову роль у всіх сферах життя: починаючи особистим спілкуванням і закінчуючи прийняттям рішень у сферах бізнеса, державного управління та освітніх послуг. Розвиток цифрового суспільства кидає нові виклики, серед яких кіберзагрози займають провідне місце. Кількість кібератак, які спрямовані на викрадення персональних даних, компрометацію інформаційних систем, порушення конфіденційності або нанесення фінансових збитків, стрімко зростає [1]. За статистикою, значна частина таких атак відбувається через недостатню обізнаність користувачів у питаннях кібербезпеки.

Людський фактор є одним із найслабших місць в системі інформаційного захисту. Навіть найсучасніші технічні засоби захисту не можуть гарантувати безпеку, якщо користувачі не дотримуються базових правил кібергігієни. Наприклад, використання слабких паролів, недовіра до оновлень програмного забезпечення або бездумне відкриття сумнівних посилань створює додаткові ризики [2, 3]. Такий стан речей обумовлює необхідність розробки ефективних способів підвищення рівня обізнаності користувачів щодо основ кібербезпеки.

Україна, як країна, що активно інтегрується у глобальний інформаційний простір, стикається із суттєвими викликами у сфері кібербезпеки. За останні роки ми стали свідками масштабних кібератак, спрямованих як на державні установи, так і на приватний сектор [4]. У таких умовах підвищення цифрової грамотності населення стає пріоритетним завданням національної безпеки [1].

Традиційні підходи до навчання, такі як лекції, статичні навчальні матеріали чи односторонні презентації, часто є недостатньо ефективними, через те, що користувачі звикли до інтерактивного споживання інформації [5]. У зв'язку з цим виникає необхідність використання сучасних методів навчання, які базуються на поєднанні інтерактивних технологій, ігрових елементів та практичних завдань [6].

Метою роботи є розробка інтерактивного застосунку, який буде сприяти навчанню користувачів основам кібербезпеки. Застосунок має забезпечити ефективне засвоєння ключових принципів та практик інформаційної безпеки, таких як захист персональних даних, безпека мереж, використання надійних паролів, а також реагування на потенційні кіберзагрози.

Наукова та практична значущість розробки інтерактивного застосунку для навчання основам кібербезпеки полягає в його внеску в підвищення рівня цифрової грамотності користувачів та зменшення ризиків, пов'язаних із людським фактором. Такий застосунок зможе стати ефективним інструментом у формуванні стійких навичок безпечного використання інформаційних технологій.

Наразі існує достатня кількість застосунків інтерактивного навчання основам кібербезпеки. Наведемо стислий огляд найпопулярніших з цих ресурсів.

Інтерактивна платформа CyberStart [7] пропонує ігровий підхід до навчання кібербезпеці. Містить завдання для аналізу даних, криптографії, зламів та інших аспектів

захисту інформації. Особливістю ресурсу є його орієнтація на новачків та підлітків, а також наявність гейміфікованих сценаріїв.

Ресурс, який дозволяє створення спілок та обмін досвідом з іншими студентами – TryHackMe [8]. Ця навчальна програма організована у вигляді інтерактивних кімнат, які охоплюють теми від мережевого захисту до проникнення в системи. Позитивними рисами програми є: практичні завдання, які містять реальні сценарії атак, а також докладні та чіткі пояснення теорії, які передують практиці.

Отримання практичних навичок протидії кіберзагрозам від початкового рівня до просунутих сценаріїв можливе завдяки ресурсу Hack The Box [9]. Ця платформа призначена для навчання етичному зламу через практичні завдання, які передбачають злам віртуальних машин і мереж. Особливість платформи – використання реальних викликів для вдосконалення навичок проникнення в системи.

Навчання, практичні заняття та отримання досвіду в сфері кіберзахисту пропонує платформа Cybrary – освітня платформа, яка надає інтерактивні курси з кібербезпеки, включаючи захист мереж, етичний злам, криптографію та управління ризиками [10]. Цей ресурс містить курси для новачків та професіоналів, сертифікаційні програми.

Google Cybersecurity Career Certificate – онлайн-курс від Google, який навчає базовим аспектам кібербезпеки, зокрема управлінню ризиками та виявленню загроз [11]. Головною особливістю є акцент на практичному застосуванні, орієнтований на початківців.

Висновок. Таким чином, розробка інтерактивного додатку є не лише актуальним, а й необхідним кроком для забезпечення кібербезпеки як на індивідуальному, так і на національному рівнях. Враховуючи зростаючу популярність мобільних і веб-застосунків, запропоноване рішення сприятиме поширенню знань серед широкої аудиторії, незалежно від віку, професії чи рівня підготовки користувачів.

Література

[1] Офіційний вебпортал парламенту України // Закон України "Про основні засади забезпечення кібербезпеки України" [Електронний ресурс] – Режим доступу до ресурсу: <https://zakon.rada.gov.ua>

[2] Сайт McAfee // The Importance of Cybersecurity Training in Combating Human Error. [Електронний ресурс] – Режим доступу до ресурсу: <https://www.mcafee.com>

[3] Сайт Symantec // The Role of User Education in Preventing Cybersecurity Breaches. [Електронний ресурс] – Режим доступу до ресурсу: <https://www.symantec.com>

[4] Юрченко О.В., Сидоренко І.Г. Розробка навчальних застосунків для підвищення обізнаності в кібербезпеці. // Інформаційні технології та безпека, 2021, №3, С. 25-30.

[5] Харченко В.С. Використання гейміфікації у навчанні основам кібербезпеки. // Науково-освітні тренди у цифрову епоху, 2022, С. 78-85.

[6] Павлов А.М. Кібербезпека в цифрову епоху: навчання через інтерактивні технології. // Технології і суспільство, 2021, №2, С. 65-72.

[7] Сайт Cyberstart [Електронний ресурс] – Режим доступу до ресурсу: <https://cyberstart.com>

[8] Сайт Tryhackme [Електронний ресурс] – Режим доступу до ресурсу: <https://tryhackme.com/>

[9] Сайт Hackthebox [Електронний ресурс] – Режим доступу до ресурсу: <https://www.hackthebox.com/>

[10] Сайт Cybrary [Електронний ресурс] – Режим доступу до ресурсу: <https://www.cybrary.it/>

[11] Сайт Cyberseclabs [Електронний ресурс] – Режим доступу до ресурсу: <https://cyberseclabs.co.uk/>

ВИКОРИСТАННЯ БЕЗКОШТОВНИХ ПЛАТФОРМ АНАЛІЗУ КІБЕРЗАГРОЗ ДЛЯ ПІДВИЩЕННЯ ЗАХИСТУ ОРГАНІЗАЦІЙ

Шелестова А. М., Лубенець С. В.

E-mail: anna.shelestova@karazin.ua, s.lubenec@karazin.ua

Харків, Харківський національний університет імені В. Н. Каразіна

Використання безкоштовних платформ аналізу кіберзагроз (Threat Intelligence Platforms, TIPs) стало важливою стратегією для організацій, які прагнуть посилити свою кібербезпеку без значних фінансових витрат. Ці платформи надають важливу інформацію про постійно змінюваний ландшафт кіберзагроз, а це, в свою чергу, дозволяє організаціям ефективніше ідентифікувати, аналізувати та знижувати потенційні ризики [1, 2].

Для виявлення кіберзагроз застосовують інструменти та методи кіберрозвідки. Кіберрозвідка поділяється на кілька основних типів, кожен з яких виконує специфічну роль у захисній стратегії організації [1].

Стратегічна кіберрозвідка охоплює високорівневі, нетехнічні інсайти, які інформують керівників організацій та підрозділів про загальний ландшафт загроз, включаючи тенденції та мотиви зловмисників [1].

Тактична кіберрозвідка містить детальну інформацію про тактики, техніки та процедури, які застосовують зловмисники. Так, цей вид кіберрозвідки допомагає розробити відповідні заходи захисту [1, 2].

Операційна та технічна кіберрозвідки зосереджені на конкретних деталях потенційних атак, включаючи інформацію про вразливості, сигнатури шкідливого програмного забезпечення та індикатори компрометації (IoCs) [1, 3].

Безкоштовні платформи аналізу кіберзагроз пропонують низку важливих функцій, які є корисними для організацій під час виявлення кіберзагроз [4, 5]:

- Інтеграція з існуючими системами безпеки (SIEM, IDS/IPS);
- Оновлення даних у реальному часі;
- Автоматизовані сповіщення про нові загрози;
- Гнучкість налаштування та масштабованість;
- Доступ до даних спільноти кібербезпеки.

Основними перевагами використання таких платформ є [1, 3, 6, 8]:

- Економічна ефективність, що особливо важливо для організацій з обмеженим бюджетом;
- Можливість проактивного виявлення загроз;
- Доступ до різних типів розвідувальних даних;
- Співпраця зі спільнотою фахівців з кібербезпеки.

Тим не менш при впровадженні безкоштовних TIPs організації стикаються з певними викликами [3, 6, 7]. Одним із викликів є якість та точність даних, так як інформація може вимагати значних зусиль для фільтрації та перевірки, оскільки якість і глибина даних можуть варіюватися [7]. Наступним викликом є обмеженість ресурсів, це пов'язано із тим, що управління чисельними потоками даних може перевантажувати організації та команди з обмеженим бюджетом і штатом [8]. Ще один виклик – брак експертизи, що проявляється у недостатності внутрішньої експертизи для ефективного аналізу даних і це може призвести до пропущених загроз або затримок у реагуванні [7, 8]. І ще один виклик – перевантаження інформацією виникає, коли великий обсяг даних може ускладнювати виокремлення значущої інформації [9].

Враховуючи вище наведені виклики, фахівці пропонують застосовувати певні стратегії впровадження платформ аналізу кіберзагроз, а саме рекомендується [12, 14, 15]:

- Провести ретельну оцінку потреб організації та бажаних результатів.
- Вибрати платформу, яка відповідає технічним вимогам та стратегічним цілям організації.

- Забезпечити всебічне навчання співробітників.
- Інтегрувати платформу з існуючими в організації системами безпеки.
- Постійно вдосконалювати та налаштовувати систему під потреби організації.

Дотримання та ефективна реалізація таких заходів дозволить організаціям отримувати більш ефективну віддачу від платформ аналізу кіберзагроз, при цьому не витрачаючи великі ресурси.

За спостереженнями фахівців в галузі кібербезпеки у розвитку платформ аналізу кіберзагроз окреслюються наступні тенденції [9, 10, 11]:

- Активне впровадження технологій штучного інтелекту та машинного навчання;
- Покращення користувацького досвіду та інтерфейсу;
- Розширення можливостей налаштування та інтеграції;
- Посилення автоматизації процесів розвідки;
- Підвищена увага до конфіденційності даних і відповідності нормативам.

Як висновок слід зазначити, впровадження безкоштовних платформ аналізу кіберзагроз є важливим кроком у посиленні кібербезпеки організації. Незважаючи на певні обмеження, правильний підхід до вибору та впровадження таких платформ може значно підвищити здатність організації протистояти сучасним кіберзагрозам [12, 13].

Література

[1] 11 Free Threat Intelligence Tools for 2023. Security Boulevard [Електронний ресурс] – Режим доступу до ресурсу: <https://securityboulevard.com/2023/06/11-free-threat-intelligence-tools-for-2023/>

[2] 11 Free Threat Intelligence Tools for 2023. ImmuniWeb [Електронний ресурс] – Режим доступу до ресурсу: <https://www.immuniweb.com/media/11-free-threat-intelligence-tools-for-2023.html>

[3] Best Open Source Threat Intelligence Platforms and Feeds [Електронний ресурс] – Режим доступу до ресурсу: <https://www.zenarmor.com/docs/network-security-tutorials/best-open-source-threat-intelligence-platforms-and-feeds>

[4] From Noise to Knowledge: Tackling Challenges in Cyber Threat Intelligence [Електронний ресурс] – Режим доступу до ресурсу: <https://www.picussecurity.com/resource/blog/from-noise-to-knowledge-tackling-challenges-in-cyber-threat-intelligence>

[5] Ibrahim A, Thiruvady D, Schneider J-G and Abdelrazek M. The Challenges of Leveraging Threat Intelligence to Stop Data Breaches // Front. Comput. Sci. 2020. 2:36 [Електронний ресурс] – Режим доступу до ресурсу: <https://www.frontiersin.org/journals/computer-science/articles/10.3389/fcomp.2020.00036/full>

[6] How Actionable Threat Intelligence Helps in Incident Response [Електронний ресурс] – Режим доступу до ресурсу: <https://threatintelligencelab.com/blog/how-actionable-threat-intelligence-helps-in-incident-response/>

[7] 5 Best Threat Intelligence Feeds in 2025 (Free & Paid Tools). Comparitech [Електронний ресурс] – Режим доступу до ресурсу: <https://www.comparitech.com/net-admin/best-threat-intelligence-feeds/>

[8] 6 Free Threat Intelligence Sources You Can't Live Without in 2025 [Електронний ресурс] – Режим доступу до ресурсу: <https://nomicnetworks.com/blog/6-free-threat-intelligence-sources-you-cant-live-without-in-2025>

[9] Top 11 Cyber Threat Intelligence Tools in 2025. Sprinto [Електронний ресурс] – Режим доступу до ресурсу: <https://sprinto.com/blog/cyber-threat-intelligence-tools/>

[10] CTI4U: A Practical Introduction to Starting a Cyber Threat Intelligence Program – Part 2 [Електронний ресурс] – Режим доступу до ресурсу: <https://www.spartanssec.com/post/cti4u-part-2>

[11] The Art of Incident Response: Best Practices. Simeononsecurity [Електронний ресурс] – Режим доступу до ресурсу: <https://simeononsecurity.com/articles/the-art-of-incident-response/>

[12] How to use cyber threat intelligence platforms to strengthen your cyber defense [Електронний ресурс] – Режим доступу до ресурсу: <https://www.dataguard.com/blog/use-cyber-threat-intelligence-platforms-to-strengthen-your-cyber-defense/>

[13] Incorporating Threat Intelligence into Your Incident Response Strategy [Електронний ресурс] – Режим доступу до ресурсу: <https://www.cyberriskinsight.com/cyber-incident/incorporating-threat-intelligence-incident-response/>

[14] How to Integrate Threat Intelligence Platforms for Enhanced Security [Електронний ресурс] – Режим доступу до ресурсу: <https://www.datasecurityintegrations.com/integration-approaches/integrate-threat-intelligence-platforms-enhanced/>

[15] Threat Intelligence Platforms: A Comprehensive Review [Електронний ресурс] – Режим доступу до ресурсу: <https://www.depththreatanalytics.com/cyber-threat-intelligence/threat-intelligence-platforms-comprehensive-review/>

ФУНКЦІОНАЛ MONGODB ДЛЯ ВИЯВЛЕННЯ ФІШИНГУ

Шерстнюк А.В.

Керівник: Шаповалова О.О.

E-mail: sherstnuk1@gmail.com

Харків, Харківський національний економічний університет імені Семена Кузнеця

MongoDB – це сучасна нереляційна (NoSQL) база даних, що забезпечує гнучке зберігання даних у форматі JSON-подібних документів. Завдяки масштабованості, високій продуктивності та зручності використання, вона стала популярним вибором для розробки веб-додатків, Big Data-аналітики та хмарних сервісів.

MongoDB була розроблена компанією 10gen (тепер MongoDB Inc.) та вперше представлена у 2009 році. Це документоорієнтована база даних, яка не використовує традиційні таблиці та SQL-запити, а натомість працює з гнучкими документами у форматі BSON (бінарний аналог JSON).

Основні особливості MongoDB:

- Гнучка модель даних – документи не вимагають жорсткої схеми, що спрощує зберігання структурованої, напівструктурованої та неструктурованої інформації.
- Масштабованість – підтримка горизонтального масштабування через шардинг (sharding).
- Висока продуктивність – кешування та індексація забезпечують швидке зчитування та запис даних.
- Автоматичне управління реплікаціями – механізм реплікації Replica Set гарантує високу доступність і захист від збоїв.
- Інтеграція з мовами програмування – підтримка драйверів для Python, JavaScript (Node.js), Java, C# та інших мов.

MongoDB складається з наступних ключових компонентів:

- Колекції – аналоги таблиць у реляційних базах, містять документи.
- Документи – окремі записи у форматі BSON.
- Індеси – прискорюють пошук даних.
- Шарди – розподіляють дані між серверами для балансування навантаження.
- Replica Set – група серверів, що підтримують автоматичне резервування даних.

Сфери застосування MongoDB:

- Веб-розробка – використовується для створення веб-додатків із динамічними даними.
- Big Data та аналітика – забезпечує зберігання та обробку великих обсягів інформації.
- Інтернет речей (IoT) – зберігання потокових даних від датчиків.

- Електронна комерція – управління каталогами товарів, транзакціями та користувачами.
- Соціальні мережі – швидке збереження та пошук контенту, коментарів, лайків тощо.

MongoDB є потужним інструментом для сучасних застосунків, які потребують гнучкості, масштабованості та швидкодії. Її нереляційний підхід дозволяє ефективно працювати з великими обсягами даних та забезпечує високу продуктивність у різних сферах бізнесу та технологій.

MongoDB добре підходить для зберігання та аналізу великих обсягів неструктурованих даних, таких як лог-файли, HTTP-запити та інші дані, пов'язані з кібербезпекою. В контексті виявлення фішингу MongoDB можна використати для низки завдань кібербезпеки.

Збереження фішингових доменів та URL. Створення бази з відомими фішинговими сайтами. Автоматичне оновлення чорного списку з відкритих джерел (наприклад, PhishTank, OpenPhish).

```
{
  "url": "http://fakebank-login.com",
  "category": "phishing",
  "date_added": "2025-02-08T12:00:00Z",
  "source": "PhishTank"
}
```

Аналіз HTTP-запитів. MongoDB можна використовувати для зберігання та аналізу логів мережевого трафіку. Виявлення підозрілих запитів на основі шаблонів фішингових атак.

```
{
  "ip": "192.168.1.10",
  "user_agent": "Mozilla/5.0",
  "request_url": "http://login-secure-bank.com",
  "referrer": "http://unknown-site.com",
  "timestamp": "2025-02-08T12:30:00Z"
}
```

Зіставлення за атрибутами. Використання MongoDB Aggregation Framework для виявлення фішингових сайтів за схожістю з легітимними сайтами (наприклад, схожі домени, підроблені логотипи).

```
{
  "domain": "paypal-security-check.com",
  "similar_to": "paypal.com",
  "score": 0.92
}
```

Використання машинного навчання. MongoDB можна інтегрувати з моделями машинного навчання для аналізу тексту, метаданих сайтів, виявлення підозрілих шаблонів запитів. Наприклад, зберігати векторні представлення сайтів (зокрема TF-IDF для аналізу контенту).

Побудова SIEM-системи (Security Information and Event Management). MongoDB може виступати як основа для системи збору логів та кореляції подій для виявлення фішингових атак у реальному часі.

Таким чином, MongoDB добре підходить для виявлення фішингу завдяки можливості зберігання великої кількості напівструктурованих даних, гнучкості запитів та підтримці аналітичних операцій. Оптимальним підходом є інтеграція MongoDB з машинним навчанням, SIEM-системами та джерелами фішингових загроз для виявлення та блокування підозрілих сайтів у реальному часі.

Література

[1] MongoDB Офіційна документація: Детальна інформація про встановлення, налаштування та використання MongoDB. [Електронний ресурс] – Режим доступу до ресурсу: <https://docs.mongodb.com/>

[2] PhishTank: Спільнота, яка збирає та обмінюється інформацією про фішингові сайти. [Електронний ресурс] – Режим доступу до ресурсу: <https://www.phishtank.com/>

[3] OpenPhish: Автоматизований фід фішингових URL-адрес для захисту від фішингу. [Електронний ресурс] – Режим доступу до ресурсу: <https://openphish.com/>

[4] Elastic Security: SIEM Guide: Посібник з налаштування системи виявлення та реагування на загрози з використанням Elastic Stack. [Електронний ресурс] – Режим доступу до ресурсу: <https://www.elastic.co/guide/en/siem/guide/current/index.html>

[5] scikit-learn: Machine Learning in Python: Бібліотека машинного навчання для Python, яка може бути використана для створення моделей виявлення фішингу. [Електронний ресурс] – Режим доступу до ресурсу: <https://scikit-learn.org/stable/>

ВИКОРИСТАННЯ ОПЕРАЦІЙНОЇ СИСТЕМИ PARROT ДЛЯ ПІДВИЩЕННЯ КВАЛІФІКАЦІЇ З КІБЕРГІГІЄНИ ТА КІБЕРБЕЗПЕКИ

Шестопалов М.А.¹, Шапо В.Ф.², Воловщиков В.Ю.³

E-mail: ¹shestopalovmikhailo@gmail.com, ²vladlen.shapo@gmail.com, ³valvol98@gmail.com

^{1,2}Одеса, Інститут Військово-Морських Сил

³Харків, Національний технічний університет “Харківський політехнічний інститут”

На протязі останніх 10-15 років в усьому світі невпинно зростає кількість кіберзлочинів, хакерських атак, вторгнень в корпоративні, офісні, промислові мережі передавання даних, інформаційні системи і т. ін. Особливо цей процес прискорився у зв'язку зі вторгненням Росії в Україну. Оскільки різноманітні комп'ютерні системи відіграють все більшу роль в діяльності людини, і майже неможливо уявити якусь діяльність, що виконується без використання комп'ютерів та мереж передавання даних, кількість цілей для кіберзлочинців швидко зростає, як і ціна відновлення працездатності після зламу інформаційних систем та мереж, втрати даних і т. д. Взагалі кожна хвилина простоювання робочих комп'ютерів може мати суттєве значення, а результати їх непрацездатності можуть бути не виправними і вести до втрати бізнесу або програшу бою на війні з величезними фінансовими збитками та втратою технічних засобів, обладнання, озброєння та навіть людських життів.

Під час війни виявилось, що безліч військових інформаційних систем, безпілотні повітряні, наземні, підводні та надводні апарати та сучасне комп'ютеризоване озброєння, що коштує мільйони доларів/євро, також потребують постійного кіберзахисту.

Для підвищення якості підготовки фахівців з кіберзахисту та підвищення загального рівня кібергігієни та кіберкультури навіть для непрофесіоналів в цих областях в дисципліні на кшталт «Інформатика», «Інформатика та основи програмування» та ін. для 1-го або 2-го курсів університетів доцільно ввести окремий модуль з кібергігієни обсягом в 10-16 аудиторних академічних годин, якщо нема можливості ввести подібну дисципліну окремо. Також доцільним є введення дисциплін «Кібербезпека», «Основи кібербезпеки» та ін. для 4-го курсу бакалаврату, коли студенти вже мають підвищений рівень відповідальності, або для 1-го чи 2-го курсів магістратури з обсягом в 4-6 кредитів. Отриманий досвід говорить, що подібний підхід є доцільним, своєчасним та правильним в сучасних умовах.

Для забезпечення якісного кіберзахисту вкрай бажано використовувати широкий спектр апаратних пристроїв, операційних систем, прикладного програмного забезпечення, що дозволить застосовувати багатoshаровий захист відповідних систем з різних сторін. Для перевірки якості побудованого кіберзахисту також вкрай бажано використовувати різні інструменти, що дозволить спростити пошук та виявлення слабких місць. Одним з таких комплексних інструментів є операційна система (ОС) Parrot Security, або скорочено Parrot.

Parrot ОС [1] – це вільнодоступна операційна система сімейства Linux на базі дистрибутива Debian, яка створена спеціально для роботи з кібербезпекою та тестуванням на проникнення в комп'ютерну систему ззовні. Вона надає величезний набір інструментів для аналізу мереж передавання даних, криптографії, аналізу вразливостей, кіберрозвідки,

етичного хакінгу, інструментів для тестування на проникнення, цифрової криміналістики, приватності в Інтернеті та широкого спектру інших задач, взагалі пов'язаних з кібербезпекою та кібергігієною. Останньою версією є Parrot 6.3, випущена 31 січня 2025 р. ОС має інтуїтивно зрозумілий інтерфейс і дозволяє швидко опанувати систему навіть новачкам, забезпечує високий рівень безпеки за рахунок використання шифрування та анонімізації, а вбудовані утиліти та програми охоплюють більшість основних аспектів кібербезпеки.

Актуальним є використання Parrot ОС для вивчення кібергігієни (набору підходів, які допомагають користувачам захистити свої пристрої та особисту інформацію, комп'ютерні системи та мережі від загроз та атак, у т.ч. в Інтернеті). Parrot ОС дозволяє вивчати та використовувати вбудовані антивірусні програми та міжмережні екрани (firewall, фایрвол, хоча також досить часто зустрічається німецький термін Brandmauer), виконувати аналіз мережевого трафіку для виявлення потенційних загроз, проводити регулярні аудити безпеки системи.

Можливим є також використання Parrot ОС для вивчення кібербезпеки (забезпечення конфіденційності, цілісності та доступності інформаційних систем) шляхом проведення тестів на проникнення для оцінки захищеності систем (пентестинг, або penetration testing), використання в цифровій криміналістиці шляхом виявлення та аналізу цифрових доказів для розслідування інцидентів, ідентифікації, аналізу та виправлення вразливостей у програмному забезпеченні.

Parrot ОС має вбудовані застосунки Nmap [2] для сканування мереж, Wireshark [3] для аналізу трафіку (остання версія 4.4.3, випущена 9 січня 2025 р.), Metasploit [4] для проведення тестів на проникнення (остання версія 6.4.46, випущена 23 січня 2025 р.), Burp Suite [5], що дозволяє практикувати навички виявлення та усунення вразливостей.

Вбудовані інструменти для цифрової криміналістики дозволяють аналізувати системи та відновлювати дані, що важливо для розслідування кіберзлочинів.

Parrot ОС має застосунки I2P, Tor та Anonsurf для забезпечення анонімності, що дозволяє користувачам навчатися захисту приватності в Інтернеті.

Практичне використання Parrot може бути реалізовано шляхами, наведеними нижче.

- Використання Parrot ОС у навчальних лабораторіях дозволяє студентам вчитися кібергігієні та кібербезпеці в безпечному середовищі.
- Багато онлайн курсів з кібербезпеки використовують Parrot ОС як основний інструмент для практичних занять.
- Участь у кібербезпекових конкурсах та змаганнях допомагає відточити навички та підвищити власну кваліфікацію в кібергігієні.

Взагалі Parrot ОС містить понад 700 інструментів для тестування безпеки, включаючи сканування портів, аналіз вразливостей, тестування на проникнення. ОС надає можливість використовувати віртуальні машини для тестування різних сценаріїв загроз та має власне захищене середовище, що забезпечує безпечну роботу користувача.

Система розроблена таким чином, щоб бути звичною для експерта з безпеки та простою у використанні для новачка, але вона не намагається приховати свої внутрішні елементи, як це намагаються зробити інші дистрибутиви загального призначення.

Parrot ОС можна використовувати як щоденну систему. Він надає всі програми для повсякденних завдань, включаючи спеціальну версію системи Parrot Home Edition, яка не містить інструментів безпеки.

Система має власне сховище програм, включаючи всі пакети, які підтримує Debian, а також багато інших програм та інструментів, які Debian не надає. Усі вони доступні безпосередньо з менеджера пакетів APT (Advanced Packaging Tool, утиліта в Debian-подібних системах, що виконує встановлення, оновлення пакетів та відслідковування їх залежностей).

Parrot ОС підтримує Snap [6], систему розповсюдження пакетів, яка забезпечує легкий доступ до багатьох інших програм, які дистрибутиви GNU/Linux не завжди постачають у своїх архівах програмного забезпечення.

Також підтримується Flatpak [7], – універсальний магазин програмного забезпечення, схожий на Snap. Його можна встановити з офіційного репозиторію Parrot.

Parrot також підтримує Wine (первинно абревіатура “Wine Is Not an Emulator”), додатковий об’єкт або рівень сумісності [8] для спрощення запуску програм Windows у середовищах GNU/Linux. Останньою версією Wine є 10.1, випущена 7.02.2025.

На відміну від типових, звичних та розповсюджених дистрибутивів Linux, Parrot не намагається приховати жодних внутрішніх елементів, тобто система включає в себе багато автоматизованих інструментів, які полегшують використання, але все одно дають гарне уявлення про те, що є в самій системі.

Хорошим прикладом цього є Parrot Update Reminder, – простий, але потужний додаток, який пропонує користувачам перевіряти наявність оновлень системи раз на тиждень. Однак замість приховування процесу оновлення за індикатором виконання він показує користувачеві повний процес оновлення з результатів тесту на профпридатність. Ще одна важлива відмінність полягає в тому, що Parrot за замовчуванням вимикає всі мережеві служби, попередньо встановлені в системі. Це робиться для того, щоб зменшити зайнятий обсяг оперативної пам’яті і підвищити продуктивність та запобігти впливу на роботу служб у цільовій мережі. Кожну мережеву службу користувач має запускати вручну за потреби. Дистрибутив Parrot Pentest відомий тим, що в ньому інтегровані лише інструменти безпеки, що забезпечує легкий доступ з правами суперкористувача і усуває всі бар’єри безпеки, які могли б вплинути на роботу пентестера.

Parrot ОС створена як дуже комфортне середовище для фахівців з безпеки та дослідників. Дистрибутив включає в себе багато базових програм, які використовуються щодня, але зазвичай не входять до складу дистрибутивів для пентестування (менше одного гігабайта додаткової пам’яті). Цей вибір зроблений не тільки для того, щоб зробити Parrot ОС хорошою системою для тестування безпеки, але і для того, щоб зробити її зручним середовищем для написання звітів, створення власних інструментів і безперешкодного спілкування з колегами по команді без необхідності в додаткових комп’ютерах, операційних системах або конфігураціях. Головна ціль Parrot ОС, – дозволити професійному пентестеру провести повний тест безпеки від початку до звіту лише за допомогою ISO Parrot і середнього за можливостями апаратного забезпечення ноутбука.

Parrot Security постачається зі спеціальними профілями захисту та конфігураціями для AppArmor [9] та інших технологій захисту Linux і бере приклад з інших проектів, які забезпечують найвищий рівень безпеки в сценарії GNU/Linux, як Tails і Whonix для пісочниці системи та доставки рівень безпеки вище середнього.

Таким чином, ОС Parrot може бути з успіхом використана експертами з безпеки та цифрової криміналістики, студентами широкого кола ІТ-спеціальностей та викладачами дисциплін з вивчення програмування, мереж передавання даних, кібергігієни та кібербезпеки, дослідниками в ІТ-галузі, білими (етичними) хакерами, які шукають недоліки у захисті програмного забезпечення, т. зв. Wannabe-хакерів (спотворене англійське «want to be», буквально «хочу бути», тобто починаючих хакерів, або людей, що намагаються показати всім свою високу кваліфікацію ІТ-спеціаліста широкого профілю, хоча насправді це не відповідає дійсності), розробниками програмного забезпечення.

Література

[1] PARROTSEC Operation System [Електронний ресурс] – Режим доступу до ресурсу: <https://www.parrotsec.org/>

[2] NMAP Network scanner [Електронний ресурс] – Режим доступу до ресурсу: <https://nmap.org/download>

[3] Wireshark [Електронний ресурс] – Режим доступу до ресурсу: <https://www.wireshark.org/download.html>

[4] RAPID7 Metasploit [Електронний ресурс] – Режим доступу до ресурсу: <https://www.metasploit.com/download>

[5] Burp Suite [Електронний ресурс] – Режим доступу до ресурсу: <https://portswigger.net/burp>

[6] Canonical Snapcraft [Електронний ресурс] – Режим доступу до ресурсу: <https://snapcraft.io/>

[7] Flatpak – the future of application distribution [Електронний ресурс] – Режим доступу до ресурсу: <https://flatpak.org/>

[8] WINE HQ [Електронний ресурс] – Режим доступу до ресурсу: <https://www.winehq.org/>

[9] AppArmor [Електронний ресурс] – Режим доступу до ресурсу: <https://ubuntu.com/server/docs/apparmor>

ЗАСОБИ ПРОТИДІЇ SQL-ІН'ЄКЦІЯМ ТА XSS-АТАКАМ

Шишлов А.С.

Керівник: Солодовник Г.В.

E-mail: ganna.solodovnyk@hneu.net

Харків, Харківський національний економічний університет імені Семена Кузнеця

Актуальність теми розробки веб-застосунків із вбудованими механізмами боротьби з SQL-ін'єкціями та XSS-атаками зумовлена стрімким розвитком цифрових технологій та підвищенням вимог до кібербезпеки. Наразі Інтернет є необхідним інструментарієм спілкування, обміну інформацією, фінансових операцій і доступу до державних та бізнес-послуг. Зловмисники постійно вдосконалюють свої методи, створюючи нові загрози, які можуть завдати значної шкоди бізнесу, державним організаціям і кінцевим користувачам. SQL-ін'єкції та XSS-атаки є одними з найпоширеніших типів атак, які дозволяють зловмисникам отримати доступ до конфіденційної інформації, змінити дані в базі даних, підробити вміст сторінки або зламати веб-програму для розповсюдження шкідливого програмного забезпечення [1]. SQL-ін'єкція призначена для використання вразливостей у взаємодії веб-програми з базою даних, що дозволяє виконувати неавторизовані запити. Навпаки, XSS-атаки використовують уразливість під час перевірки вхідних даних, щоб ін'єктувати шкідливий код на веб-сторінки, видимі для користувачів [2].

Розробка веб-застосунків із вбудованим захистом від таких типів атак є важливою не лише для зменшення ризику зловживання, але й для створення довгострокової основи для розробки безпечного програмного забезпечення. Ця проблема охоплює різні галузі, зокрема фінанси, медицину, електронну комерцію, уряд, освітні платформи тощо. Застосунки, які використовуються в цих сферах призначені для обробки значних обсягів конфіденційних даних, таких як особисті дані, історія хвороби, фінансові операції та навіть результати наукових досліджень.

Дотримання правил загального регламенту з захисту даних (GDPR) у Європі, вимагає від розробників забезпечення високого рівня захисту персональних даних, вимагаючи інтеграції передових інструментів кібербезпеки протягом всього життєвого циклу програмного продукту. Це допомагає підвищити загальну довіру до цифрових послуг, а також уникнути значних фінансових та репутаційних втрат у разі витоку даних.

Враховуючи вищезазначене, розробка веб-застосунків із вбудованими механізмами захисту від SQL-ін'єкції та XSS-атак є не лише актуальним, а й стратегічно важливим завданням для забезпечення безпеки мережі в сучасному інформаційному середовищі.

Метою роботи є аналіз вбудованих засобів протидії SQL-ін'єкціям та XSS-атакам для подальшого їх використання в процесі розробки захищеного веб-застосунку.

Сучасні методи боротьби з SQL-ін'єкціями та XSS-атаками базуються на використанні відповідних методів програмування, таких як параметризовані запити, перевірка даних, очищення вхідних даних і обмеження доступу до бази даних [3]. Ключову роль у розробці також відіграють автоматизовані засоби та платформи, які забезпечують інтеграцію механізмів безпеки на всіх етапах створення програмного забезпечення.

Параметризовані (або підготовлені) запити гарантують, що введені користувачем дані обробляються як параметри, а не як частина SQL-запиту. Такі запити можуть бути реалізовані мовою php, яка є проектом відкритого програмного забезпечення.

Одним із основних підходів до запобігання впровадження SQL є використання бібліотеки ORM (об'єктно-реляційне відображення), яка обробляє запити до бази даних за допомогою параметризованих методів [4]. Інструменти ORM (наприклад, Hibernate, Django ORM, SQLAlchemy) абстрагують доступ до бази даних і дозволяють уникнути написання "сирого" SQL-коду. Перевагою таких інструментів є те, що вони автоматично обробляють дані так, щоб запобігти SQL-ін'єкціям.

Захист від атак XSS передбачає кодування вмісту HTML, використання політики безпеки вмісту, а також регулярний моніторинг і оновлення використовуваних бібліотек [5]. Так, наприклад, екранування (escaping) виводу забезпечує безпечне відображення даних, введених користувачем, шляхом заміни небезпечних символів їхніми HTML-еквівалентами. Це запобігає виконанню коду, який користувач міг вставити у вхідні дані.

Валідація та фільтрація вхідних даних призначені для перевірки даних, які були введені користувачем, на коректність перед їхнім збереженням або обробкою. Підвищення надійності джерел запуску скриптів можливо завдяки використанню заголовків Content Security Policy (CSP) [6]. Це обмежує типи вмісту, які можуть виконуватися на веб-сторінці, запобігаючи виконанню шкідливого JavaScript-коду. Використання шаблонізаторів (наприклад, Twig або Handlebars) дозволяє автоматично екранувати вміст, який додається до HTML та убезпечувати вставку даних у веб-сторінку.

Проведений аналіз показав, що для автоматизації процесів протидії SQL-ін'єкціям та XSS-атакам слід використовувати сучасні засоби розробки з відкритим кодом. Прикладом таких інструментів є платформи, які забезпечують тестування на проникнення та можливості виявлення вразливостей. В рамках роботи пропонується інтегрувати механізми безпеки безпосередньо у веб-застосунк за допомогою мов програмування Python та JavaScript.

Програмний продукт, який розробляється, передбачає використання фреймворків, таких як Django або Flask, для захисту запитів до бази даних, а також бібліотек для запобігання атак XSS, таких як DOMPurify або Helmet.js. Для тестування програми використовуватимуться сучасні інструменти, такі як OWASP ZAP і Burp Suite.

Висновок

Розробка веб-застосунку з вбудованими механізмами захисту від атак SQL і XSS дозволяє не лише підвищити рівень кібербезпеки, але й забезпечує відповідність сучасним стандартам захисту даних. Використання інструментів з відкритим кодом сприяє економії ресурсів, масштабованості та гнучкості рішень. Автоматизація цих процесів є важливим кроком у розробці програмного забезпечення, яке відповідає сучасним вимогам безпеки інформації.

Література

[1] Сайт OWASP Ukraine. Рекомендації щодо безпеки веб-додатків. [Електронний ресурс] – Режим доступу до ресурсу: <https://owasp.org>.

[2] Сайт European Commission // General Data Protection Regulation (GDPR). [Електронний ресурс] – Режим доступу до ресурсу: <https://gdpr-info.eu>.

[3] Сайт Django Software Foundation // Django Documentation. [Електронний ресурс] – Режим доступу до ресурсу: <https://docs.djangoproject.com>.

[4] Сайт IT Cluster Ukraine // Захист даних у сучасних веб-технологіях. Київ: ІТКУ, 2021.

[5] Сайт OWASP Foundation // OWASP Testing Guide. [Електронний ресурс] – Режим доступу до ресурсу: <https://owasp.org>.

[6] Content Security Policy (CSP) // Quick Reference Guide [Електронний ресурс] – Режим доступу до ресурсу: <https://content-security-policy.com/>

Секція 2

BANDIT: AUTOMATED STATIC SECURITY ANALYZER FOR PYTHON CODE

Kolotii M.O.

Supervisor: Leunenکو O.V.

E-mail: mykyta.kolotii@hneu.net, Oleksii.Leunenکو@hneu.net

Kharkiv, Simon Kuznets Kharkiv National University of Economics

Bandit is a great open source for threat discovery in python code to use. It performs source code analysis, building an Abstract Syntax Tree (AST) from the source code then verifying every element against a list of dangerous patterns.

As is for the tool beyond some pretty basic things Bandit does. It can tell you lots of things: weak cryptographic algorithms, injection attacks and problems with permission management in a somewhat development friendly way. The configuration is so flexible that the checks can be designed per project, so that only the most relevant security points are checked. Adding this tool to your CI/CD pipeline stops insecure code from being implemented early on in the development cycle.

Bandit allows a plug-ins system for extending functionality. Developers have the chance to write its own project-specific checking scenario that fits well to their present needs. In addition Bandit support the ability to set issue severity and confidence levels to all found issue, this allows teams identify the most important security issues. In addition, configuration files allow for how you want the scans to be executed and which ones should be ignored which provides a good level of the flexibility in analysis. You can even configure it — the settings are stored in configuration files, and you can define specific analysis parameters the software has to implement and until what/which directories or files to ignore during the scan.

In order to use Bandit during development, you need to install it with pip and patch the relevant scripts to run checks. It natively outputs to JSON and HTML among other things, which makes it easy to consume as part of an larger ecosystem of tools/reporting systems.

The active community actively maintains updates to Bandit regularly, adds hundreds of checks, and improving thousands more.

The security quality control process for the automated analyzer is pitched faster, by a lot. Bandit-with Github actions or other CI/CD pipeline generator automatically tests each commit and reports the issues as well as logs right away. This ensures that developers can quickly address serious issues and have minimal delay in software release.

Bandit's results can also be published into external monitoring and analysis systems like Splunk, Snyk, the ELK stack (Elasticsearch, Logstash and Kibana) to extend its feature and capabilities. This gives you sight not only at playing counter to the vulnerabilities you have found but also from deeper nature of security trends investigations, to find broader procedural errors inside the code base so Bandit was an unique factor to take part in secured code culture.

References

[1] GitHub – PyCQA/bandit: Bandit is a tool designed to find common security issues in Python code. GitHub. [Электронний ресурс] – Режим доступу до ресурсу: <https://github.com/PyCQA/bandit> (date of access: 08.02.2025).

[2] Welcome to Bandit – Bandit documentation. [Электронний ресурс] – Режим доступу до ресурсу: <https://bandit.readthedocs.io/> (date of access: 08.02.2025).

COMPARATIVE ANALYSIS OF OPEN SOURCE INFRASTRUCTURE AS CODE (IAC) TOOLS FOR MANAGING HETEROGENEOUS CLOUD RESOURCES

Yenhalychev S.O., Leunencko O.V.

*E-mail: engalichev.sergiy@hneu.net, oleksii.leunencko@hneu.net
Kharkiv, Simon Kuznets Kharkiv National University of Economics*

Cloud computing has completely reshaped modern IT infrastructure, allowing businesses to access scalable and on-demand resources without the need for heavy upfront investments. As organizations move toward multi-cloud and hybrid cloud strategies, they can take advantage of multiple cloud providers or combine private and public cloud services for greater flexibility. That's why effective cloud management has become a crucial part of IT operations, helping companies stay agile, cost-effective, and resilient in an ever-evolving digital landscape.

Terraform is an open source Infrastructure as Code (IaC) tool developed by HashiCorp that enables users to define, provision, and manage infrastructure across multiple cloud providers using a declarative configuration language. It has become a cornerstone in modern DevOps practices by automating complex, multi-cloud deployments efficiently. In 2023, HashiCorp made changes to the licensing model for Terraform's enterprise offerings, a decision that has generated significant debate in the tech community [1].

Advantages of Terraform:

- **MultiCloud:** One of the biggest strengths of Terraform is its ability to work with multiple cloud providers, making it flexible tool for managing cloud infrastructure. Whether a company is using AWS, Azure, Google Cloud etc., Terraform makes it easier to manage everything from one place.
- **Declarative Configuration Language:** Terraform uses HashiCorp Configuration Language (HCL), which lets users define their infrastructure in a simple, clear, and structured way. This declarative approach means you just describe the final setup you want, and Terraform takes care of making it happen.
- **Strong Ecosystem & Community:** Terraform benefits from an active open-source community and extensive collection of modules and providers, which allows for faster development through code reuse.
- **State Management & Plan/Apply Workflow:** The plan/apply workflow enables users to review and visualize changes before applying them, minimizing errors and increasing transparency. The state is stored naturally, tracking infrastructure changes for easier maintenance.
- **Extensibility & Modularity:** Terraform is based on a modular approach and allows the user to create reusable components with less duplication and better organization. It is this kind of model that makes large-scale infrastructure management both efficient and scalable.

Disadvantages of Terraform

- **Complexity of State Files:** These files are crucial for infrastructure management. Problems like state drift, short-term changes, or the deletion of state information can create problems within multi-users environments or multi-complex deployments.
- **HCL Limitations:** every new tool comes with a learning curve to it and HCL is no different. It has the curve that people new to imperative programming environment. HCL is excellent for configuration, but not as powerful for complex logic or behaviors.
- **Interdependencies and Order of Operations** — Although Terraform's dependency graph is powerful, it does not contain enough information on the complex structure of modern infrastructures, leading to challenges around controlling dependencies and order of operations for provisioning resources.
- **Recent Licensing Changes for Enterprise Features:** The core Terraform product continues to be open source through the Mozilla Public License (MPL) 2.0, but HashiCorp has

recently made some licensing adjustments to some of its enterprise products. This change has led to discussions within the community, especially regarding the balance between open source collaboration and monetization within the enterprise.

- **Error Handling and Debugging:** One of the major downsides of Terraform is that its error messaging outputs can be confusing stranding users to lose their time debugging an issue. Longer debug sessions if working with complex infrastructure or rare cloud provider combinations.

This balanced view of Terraform highlights its strengths in managing heterogeneous cloud infrastructures while also acknowledging areas where challenges may arise. Understanding these pros and cons can help practitioners make informed decisions about integrating Terraform into their infrastructure management workflows [2].

OpenTofu is a community-driven, open source Infrastructure as Code (IaC) tool designed to manage multi-cloud and heterogeneous infrastructures much like Terraform. Developed with the same configuration language and workflow, OpenTofu seeks to be a drop-in replacement for Terraform. OpenTofu focuses on transparent and community-driven governance to preserve a pure open source philosophy which can be attractive for users who desire an open source tool, controlled only with community governance without the burdensome aspects of proprietary licensing schemes [3].

Advantages of OpenTofu

- **Community Governance and Transparency:** OpenTofu is governed by the community, ensuring that its development is transparent and driven by the needs of its users rather than commercial pressures.

- **Terraform Compatible – Drop-in Replacement:** OpenTofu is purposefully built to reflect the syntax and workflows of Terraform’s configuration language so existing users can move to the alternative provider with few changes to their existing IaC configurations.

- **Multi-Cloud Flexibility:** OpenTofu, as with Terraform, supports multiple cloud providers – allowing users to effectively manage heterogeneous environments.

Disadvantages of OpenTofu

- **Ecosystem Maturity:** As a newer entrant compared to Terraform, OpenTofu might have a smaller ecosystem, including fewer community modules, integrations, and less mature documentation.

- **Tooling and Integration Challenges:** Certain third-party tools and integrations that are built specifically for Terraform might not fully support OpenTofu immediately.

- **Adoption and Stability** While OpenTofu shows great promise, it still faces stability and adoption challenges as it continues to grow.

OpenTofu is an alternative to Terraform that offers similar features with a strong focus on community management and open source transparency. However, its relative newness means it still has some hurdles to overcome before it can be widely adopted.

Pulumi is an Infrastructure as Code (IaC) tool that distinguishes itself from Terraform and OpenTofu by enabling developers to define infrastructure using general-purpose programming languages such as TypeScript, Python, Go, and C# [4].

Key Differences from Terraform and OpenTofu:

- **Programming Language Flexibility:** Pulumi allows users to leverage familiar programming languages with full language features—such as loops, conditionals, and rich abstractions – providing greater flexibility and expressiveness. In contrast, Terraform and OpenTofu use declarative configuration languages that emphasize simplicity and a clear, desired-state model.

- **Imperative vs. Declarative Approach:** Pulumi's use of imperative programming can make it easier for developers to integrate infrastructure management into existing software development practices. However, this may come at the cost of introducing complexity in ensuring idempotence and predictability, which are inherent strengths of the declarative approach used by Terraform and OpenTofu.

- **Ecosystem and Community:** While Terraform and OpenTofu have a mature ecosystem and extensive community-driven modules, Pulumi is rapidly growing its community and library of packages. Pulumi model appeals especially to teams with strong software development backgrounds.

Advantages of Pulumi

- **Familiarity for Developers:** Enables developers to use their preferred programming languages, which can shorten the learning curve and facilitate deeper integration with existing codebases and CI/CD pipelines.
- **Rich Language / Programming Constructs:** In-depth programming constructs (e.g., loops, conditionals, functions etc.) allows for dynamic and DRY infrastructure definitions.
- **DevOps-Friendly:** Pulumi integrates unit testing, code reviews and new DevOps tooling.

Disadvantages of Pulumi

- **Complexity and Learning Curve:** The flexibility of using general-purpose languages can introduce complexity, especially for operations teams more accustomed to declarative configurations.
- **Risk of imperative errors:** Imperative code can sometimes result in less transparent infrastructure changes, making debugging and state management more difficult than the simple plan/apply model in declarative systems.
- **Ecosystem Maturity:** Although growing quickly, Pulumi's ecosystem is not as mature or extensive as Terraform's, which may mean fewer pre-built modules and community resources for certain cloud providers or niche use cases.

Pulumi stands out as a strong alternative to Terraform and OpenTofu, especially for teams that prefer using general-purpose programming languages to manage infrastructure. Its approach fits well with modern software development practices, offering greater flexibility and power. However, this also adds complexities that need to be carefully managed to maintain stable and predictable deployments.

Following its latest updates, Terraform is still the best tool to manage different cloud environments. Considering the future, Pulumi gives you the flexibility with general-purpose programming languages, whereas OpenTofu encourages open-source transparency without licensing restrictions. The future is likely to see a mix of Terraform's stability, Pulumi's flexibility and OpenTofu's transparency driving the next generation of cloud management tooling.

References

[1] HashiCorp adopts Business Source License | Terraform [Electronic resource] – Resource access mode: <https://www.hashicorp.com/en/blog/hashicorp-adopts-business-source-license>

[2] Terraform Consulting : Advantages and disadvantages of terraform [Electronic resource] – Resource access mode: <https://ismiletechnologies.com/technology/terraform-consulting-advantages-and-disadvantages-of-terraform/>

[3] OpenTofu vs Terraform : Key Differences and Comparison [Electronic resource] – Resource access mode: <https://spacelift.io/blog/opentofu-vs-terraform>

[4] Pulumi vs. Terraform : Key Differences and Comparison [Electronic resource] – Resource access mode: <https://spacelift.io/blog/pulumi-vs-terraform>

[5] Pulumi vs OpenTofu [Electronic resource] – Resource access mode: <https://medium.com/@DiggerHQ/pulumi-vs-opentofu-6c0be5aced99>

DEVELOPMENT OF METHODS FOR DYNAMIC LOAD BALANCING DURING THE TRANSFER OF LARGE VOLUMES OF DATA: A COMPARATIVE STUDY OF APACHE KAFKA AND RABBITMQ

Yenhalychev S.O., Leunenکو O.V.

*E-mail: engalichev.sergiy@hneu.net, oleksii.leunenکو@hneu.net
Kharkiv, Simon Kuznets Kharkiv National University of Economics*

The explosive growth of data-intensive applications demands efficient and adaptive implementations of transferring resource-hungry jobs across heterogeneous Cloud systems. This thesis tries to tackle the challenge by proposing new dynamic load-balancing techniques and resilient data transfer models. Ultimately, the study presents a comparative analysis between two widely adopted open-source models, Apache Kafka, and RabbitMQ, fielded by combining theoretical concepts of load balancing and data routing with real-world applications. The objective is to determine the most effective approach for modeling and managing the transfer of large volumes of data in diverse cloud environments.

Modern cloud architectures are heterogeneous regarding nodes, computational power, storage capacity, and network bandwidth. In these scenarios, it is important to model data transfer for such resource-heavy operations. An effective load-balancing system prevents any single system in a distributed resource from facing latency and bottlenecks, ensuring optimal usage pooling and efficiency. Resource awareness, latency optimization, and fault tolerance are theoretical models for Load balancing and Data Routing, which are used to solve these problems [1].

In this thesis, we then investigate dynamic load-balancing strategies for diverse data transmission in heterogeneous cloud systems. Our main objective turns around grounding these theoretical models over empirical, open-source message brokers – namely Apache Kafka and RabbitMQ – to determine their efficiency in practice. This paper will provide insights on using these channels to pursue scalable and robust data transfer for resource-constrained workloads.

A cloud environment needs to have effective data transfer mechanisms for data-hungry tasks (e.g., real-time analytics, video processing, complex simulations) to work right.

There are a few core elements to modeling the data transfer process:

- **Resource Awareness:** however, the model should consider the different functionalities of different nodes in a heterogeneous cloud. Adaptive algorithms optimize CPU, memory, and network bandwidth for the most efficient processing of each task as it is received
- **Latency Optimization:** reducing transmission delays is crucial. It uses strategies to guide the data through routes that add minimal latency, ensuring timely processing of data-intensive tasks.
- **Fault Tolerance and Scalability:** since the cloud enables dynamic environments, the model should gracefully handle node failure and scalable operation. Nodes enter and leave the system, at which point work gets dynamically redistributed, and loads get rebalanced.

Such theories form the basis of dynamic load-balancing algorithms that will adjust to changing workloads and resource availability [3]. The above models combined together with messaging systems like Apache Kafka and RabbitMQ gives a realistic approach to seamlessly transfer data between heterogeneous systems.

Apache Kafka is a distributed streaming platform, which is designed for high-throughput, low-latency data processing. It is built on the partitioned log mechanism that segments the data into topics and partitions. With a design like this, dynamic load balancing is fundamentally supported by consumer groups that dynamically adjust the assignment of partitions and their consumers.

Some of the major benefits of Kafka are:

- **Scalability:** Kafka's use of partitioning guarantees near-linear scalability and is designed for scale-out (with increasing connected data streams).
- **Dynamic rebalancing:** the consumer group mechanism automatically evenly distributes partitions when consumers either join or leave the group.

- High throughput & fault tolerance: the architecture of Kafka enables high data throughput and strong fault tolerance, which is critical for expensive workloads [2].

RabbitMQ is a general-purpose message broker based on a queue-based architecture and exchange-based routing mechanisms. It also allows you to route messages based on content or rules, such as filtering out certain messages or sending them to different destinations based on their properties.

Its features include:

- Flexible routing: RabbitMQ implements four delivery semantics (direct, topic, fanout & headers), so applications can have very complex routing strategies that can be custom configured.
- Clustering and high availability: contingent on clustering, many RabbitMQ nodes, message queues, and loads can be allocated and balanced dynamically in real-time.
- Protocol support: RabbitMQ supports multiple messaging protocols, making it compatible with a broader range of applications than Kafka, albeit with potentially weaker performance in extremely high-throughput scenarios [3].

The theoretical models of load balancing and data routing, as outlined above, can be combined with the two distributed systems, Apache Kafka and RabbitMQ, to improve resilience for moving tasks with high requirements:

- Models that require scalability and fault tolerance – Apache Kafka fits the bill. Its ability to split data up into partitioned sections and dynamically rebalance consumer groups meant it was the perfect scenario for use cases with high data throughput to be delivered quickly.
- RabbitMQ is especially beneficial in cases that require intricate routing logic and process flexibility. The exchange-based routing can be configured to maximize performance by minimizing latency and ensuring data is delivered to appropriate tasks.

The analysis demonstrates the selection of either Kafka or RabbitMQ should be determined by the unique needs of the context in which these technologies will be applied, be it in the processing of large amounts of data with little delay, or in the management of sophisticated routing for heterogeneous tasks.

Conclusion. Cloud system resources typically require significant effort to be allocated towards particular tasks, and the models that try to optimize such allocation in distributed systems are sophisticated challenges that lay within the scope of this thesis. For this work, I analyzed methods for dynamic load balancing based on resource awareness and optimization latency. The comparative analysis of Apache Kafka and RabbitMQ also sought to understand what the platforms have to offer in terms of dynamic load balancing. As anticipated, there are various trade-offs, with Apache Kafka users gaining higher value from scaling and increased throughput when working with high-volume data streams as compared to those who use RabbitMQ, who are better off with sophisticated routing and protocol flexibility. Empirical testing and benchmarking are the next steps in improving the models that have been developed by trying to figure out how best to hybridize the two systems.

References

[1] Tanenbaum, A. S., & van Steen, M. (2007). Distributed Systems: Principles and Paradigms. [Electronic resource] – Resource access mode: <https://www.distributed-systems.net/>

[2] Apache Kafka Official Documentation. [Electronic resource] – Resource access mode: <https://kafka.apache.org/documentation>

[3] RabbitMQ Official Documentation. [Electronic resource] – Resource access mode: <https://www.rabbitmq.com/documentation.html>

ОСОБЛИВОСТІ ПОБУДОВИ ПРИВАТНОЇ ХМАРИ НА ОСНОВІ ТЕХНОЛОГІЇ KUBERNETES

Алексієв В.О.

E-mail: vlah@hneu.edu.ua

Харків, Харківський національний економічний університет імені Семена Кузнеця

Для більшості сучасних компаній та розвитку їх бізнесу завжди є у пріоритеті побудова цифрових активів та забезпечення їх захисту. Публічна хмара фактично може надати всі необхідні ресурси та засоби для розгортання ефективних рішень й створення IT-інфраструктури компанії. Поруч з цим, як частина послуг, хмарне рішення надає певні практики та рекомендації щодо кібербезпеки. Звичайно між публічною хмарою та користувачем є взаємний поділ відповідальності щодо забезпечення безпеки. Однак, безпека вже є складовою послуг хмарного провайдера.

Слід відмітити, що не завжди публічна хмара є остаточним рішенням, наприклад, завдяки регіональним законам або специфіці компанії можливим рішенням може стати застосування приватної хмари або гібридного рішення. Тому актуальним стає питання розгортання хмарних рішень на ресурсах компанії. Якщо подивитися на розвиток сучасних цифрових технологій, то фактично сучасна приватна хмара будується на основі засобів віртуалізації. Традиційно це є віртуалізація на базі гіпервізору. Однак, світ стрімко змінюється й на сьогодні є ефективна альтернатива – віртуалізація рівня операційної системи або контейнерна віртуалізація. Фактично LXC (Linux container), Docker (<https://docs.docker.com/>), Podman (<https://podman.io/>) та ін. виступають як стала альтернатива традиційному гіпервізору. Однак, контейнери більш швидкі, потребують менш продуктивних ресурсів та дуже зручні у процесах DevOps [1].

У разі застосування віртуалізації як основи побудови приватної хмари, одним з варіантів може бути впровадження технології OpenStack (<https://www.openstack.org/>). Такий підхід може задовольнити потреби відносно великих компаній та організацій. Порівняно менші масштаби розгортання приватної хмари забезпечує рішення Proxmox Virtual Environment (<https://www.proxmox.com/>). Такі рішення дозволяють балансувати між залученням гіпервізору та застосуванням контейнерної віртуалізації. Поруч з цим, для невеликих компаній актуальним є залучення ресурсів у розмірі, що перевищує декілька контейнерів, які працюють, наприклад у Docker. Типовим рішенням для такого випадку стає запуск невеличкого кластеру контейнерів, який в змозі обробляти одне-два рішення, наприклад, що будуються на базі технології мікросервісів.

Таким чином, відкрита технологія Kubernetes (<https://kubernetes.io/>), як відповідь на вимоги до надійності, доступності та керуєності мікросервісів, фактично де-факто стає універсальною платформою для бізнесу. Слід зазначити, що контейнерна віртуалізація не достатньо ефективна для застосунків, які потребують складних зав'язків між серверними компонентами, їх конфігуруванню та вимог у залученні продуктивних платформ виконання, але це є дуже суперечливим й залежить від певного завдання. Тому впровадження Kubernetes повинно бути обґрунтованим [2, 3]. Відповідно стає прикладне питання, яким чином можна швидко ознайомитися з технологією Kubernetes та на її базі побудувати приватну хмару або рішення для Edge computing (крайові/граничні обчислення)?

Звичайно, можна зразу почати з роботи на кластері Kubernetes, який є сервісом хмарного провайдера, наприклад: Amazon Elastic Container Service for Kubernetes (EKS), Google Kubernetes Engine (GKE), Azure Kubernetes Service (AKS) та ін. Однак, вивчення технологічних рішень Kubernetes доцільно виконувати на ресурсах, які підтримуються звичайним персональним комп'ютером, й надають розуміння побудови рішення та дозволяють оцінити взаємодію компонентів кластеру. Це фактично надає універсальності для швидкого опанування засобами роботи з кластером, що забезпечує запуск, виконання та керування роботою контейнерів.

Слід виділити майже традиційні для IT-індустрії рішення щодо вивчення роботи й особливостей побудови кластеру Kubernetes:

- minikube (<https://minikube.sigs.k8s.io/>) – найвідоміше рішення для вивчення кластера Kubernetes, яке дозволяє розгорнути дослідницьке оточення у середовищі гіпервізору або за допомогою вузлів на базі контейнерів, фактично є універсальним рішенням для побудови фізичної моделі кластеру.

- kind (<https://kind.sigs.k8s.io/>) – дозволяє розгорнути модель кластеру Kubernetes у середовищі контейнерної віртуалізації, наприклад, Docker.

- Kubernetes The Hard Way (<https://github.com/kelseyhightower/kubernetes-the-hard-way>) – проєкт Kelsey Hightower, який призначений для вивчення особливостей побудови кластеру Kubernetes на основі виконання його покрокового розгортання.

У більшості варіантів розгортання та управління кластером Kubernetes у промислових застосуваннях виконується за допомогою штатної утиліти kubectl або ін. Також автоматизація розгортання кластеру може бути виконано за допомогою проєкту Kubespray (<https://kubespray.io/>), який надає попередньо налаштовані плейбуки Ansible для розгортання рішення. Такий підхід доцільний для великих за масштабами рішень. Для невеликих проєктів доцільно звернути увагу на технології:

- K3s (<https://k3s.io/>) – проєкт націлений на рішення завдань галузі Інтернету речей та ін. впровадженнь високодоступних рішень з обмеженнями ресурсів.

- MicroK8s (<https://microk8s.io/compare>) – легкий дистрибутив Kubernetes від компанії Canonical, націлений на рішення крайових обчислень та Інтернету речей.

- k0s (<https://k0sproject.io/>) – проєкт компанії Mirantis, який є простим, надійним і рішенням побудови кластеру Kubernetes та містить мінімум додаткових компонентів.

Фактично K3s є розробкою на основі технологій Kubernetes, який спеціалізований для галузі Інтернету речей. Рішення MicroK8s базується на кодовій базі Kubernetes та розгортається завдяки менеджеру пакетів snap, який ізолює залежності бібліотек. У свою чергу, k0s – мінімалістична зборка для побудови кластеру, яка містить тільки один файл, що може зацікавити розробників рішень на базі кластеру Kubernetes простотою та мінімалізмом проєкту.

Таким чином, різноманіття засобів для розгортання приватної хмари на основі технології Kubernetes дозволяють створити кластер, який буде налаштовано та пристосовано до рішення певної задачі. Уніфікація рішення дозволяє виконати розгортання застосунків компанії на різних платформах хмари, а гнучкість кластера Kubernetes дозволяє масштабувати рішення. Фактично це стає ефективним рішенням приватної хмари компанії. Як розвиток такого підходу може бути залучення парадигми мультікластеру [4]. Робота з декількома кластерами Kubernetes не відрізняється принципово. Звичайно вона відбувається за допомогою штатної утиліти kubectl та перемикання контексту на потрібний кластер, що визначається у конфігурації kubeconfig. Це робить вибір контейнерної віртуалізації, як основи для побудови цифрового простору сучасної компанії чи організації, більш зручним, гнучким та універсальним.

Література

[1] Mikael Krief. Learning DevOps. Second Edition. – Packt Publishing, 2022. – 534 p.

[2] Gineesh Madapparambath, Russ McKendrick. The Kubernetes Bible. Second Edition. – Packt Publishing, 2024. – 683 p.

[3] Marc Boorshtein, Scott Surovich. Kubernetes – An Enterprise Guide. Third Edition. – Packt Publishing, 2024. – 647 p.

[4] What is Kubernetes multi-cluster? [Електронний ресурс] – Режим доступу до ресурсу: <https://www.mirantis.com/cloud-native-concepts/getting-started-with-kubernetes/what-is-kubernetes-multi-cluster/>

ВЕБЗАСТОСУНОК ДЛЯ КООРДИНАЦІЇ СПІВПРАЦІ МІЖ ФРІЛАНСЕРАМИ ТА ЗАМОВНИКАМИ

Антонюк О.А.

Керівник: Науменко С.В.

E-mail: antonyk063@gmail.com

Черкаси, Черкаський національний університет імені Богдана Хмельницького

В наш час, вебзастосунок для координації співпраці між фрілансерами та замовниками, є дуже актуальними. Особливої популярності онлайн-платформи такого виду набули за часів COVID-19. Пандемія спричинила глобальні локдауни по всьому світу, що змусило багато фахівців різних професій шукати альтернативні способи заробітку грошей. Найпопулярнішим та найвигіднішим варіантом стало надання своїх послуг онлайн, з використанням відповідних онлайн-платформ.

Перевагами їх використання - є гнучкий робочий час. Фрілансери не мають певного робочого дня, вони, наприклад, можуть працювати чотири дні в тиждень, або відпочивати вранці та працювати тільки ввечері. Ще однією з переваг є те, що фрілансери працюють самі на себе. Це означає, що вони самі вирішують за яку роботи братися, яку винагороду за виконану роботу отримувати. Також важливим є те, що фрілансери можуть вирішувати в якому їм напрямку краще розвиватися.[1] Недоліками - є відсутність оплачуваних відпусток, лікарняних чи медичного страхування. Фрілансери, зазвичай, заробляють менше грошей ніж люди, що працюють в компаніях. Крім того, при пошуку роботи, весь досвід роботи на фрілансі не грає великої ролі, що значно знижує відсоток успішного прийому на роботу.[2] Також слід зазначити, що всі онлайн-платформи мають певну комісію чи платні підписки, що значно впливає на заробіток.

Ключовою функцією вебзастосунку є забезпечення ефективної та безпечної співпраці між фрілансерами та замовниками. Це включає в себе:

- зручну та ефективну систему пошуку, що надає можливість виконання пошуку за назвою сервісу або з використанням фільтрів, що включають в себе категорії, мови якими розмовляє виконавець, рейтинг виконавців, ціновий сегмент;
- механізм платежів, який забезпечує надійних перенаправлення грошей від виконавця на банківський рахунок системи та перенаправлення коштів до фрілансера, тільки у разі успішного виконання роботи або повернення до замовника, у разі відмови;
- інструменти комунікації, що дає можливість виконавцям та замовникам здійснювати спілкування за допомогою текстового або відео зв'язку;
- рейтингову та відгукову систему, яка дозволяє замовникам залишати свої думки, щодо якості та вчасного виконання роботи, оцінювати їх за п'ятибальною шкалою;
- адмінпанель, де адміністратор зможе вирішувати спірні моменти, які виникають між замовниками та фрілансерами під час відміни замовлення, блокування користувачів або сервісів, що порушують правила платформи, перегляд усіх замовлень для виявлення шахраїв та їх покарання.

Отже, в даному дослідженні було виконано огляд вебзастосунку для координації співпраці між фрілансерами та замовниками, розглянуто його найголовніші функції та важливі компоненти роботи, що допоможе в майбутній розробці онлайн-платформи.

Література

[1] The Thriving Creative. Pros and Cons of Freelancing [Електроний ресурс] – Режим доступу до ресурсу: <https://thethrivingcreative.com/pros-and-cons-of-freelancing/>

[2] Вікіпедія. Freelancer [Електроний ресурс] – Режим доступу до ресурсу: <https://en.wikipedia.org/wiki/Freelancer>

РОЗРОБКА ОСВІТНЬОГО ВЕБ-ЗАСТОСУНКУ ДЛЯ ВИВЧЕННЯ ОСНОВНИХ АЛГОРИТМІВ ШИФРУВАННЯ

Бойко С.О.

Керівник: Лимаренко В.В.

E-mail: soffetsoffit@gmail.com

Харків, Харківський національний економічний університет імені Семена Кузнеця

На сучасному етапі розвитку інформаційних технологій знання основ криптографії є важливим елементом підготовки фахівців у сфері кібербезпеки. Однак більшість навчальних матеріалів з цієї тематики є теоретичними, що ускладнює процес засвоєння. Для ефективного засвоєння основних алгоритмів шифрування необхідні інтерактивні навчальні інструменти, що дозволяють користувачам не лише вивчати теоретичний матеріал, а й практично випробувати шифри в дії. Саме з цією метою розробляється освітній веб-застосунок, який містить інтерактивні модулі для вивчення криптографічних алгоритмів.

Основні функціональні можливості веб-застосунку:

- Інтерактивні навчальні модулі, що включають візуалізацію процесів шифрування та дешифрування для простих та складних алгоритмів шифрування (наприклад, шифр Цезаря, шифр Віженера, шифри DES, AES, RSA та інші) [1,2].
- Можливість введення власного тексту для шифрування та дешифрування, що дозволяє користувачам експериментувати з алгоритмами.
- Використання відкритого вихідного коду, що забезпечує прозорість роботи застосунку та можливість його розширення іншими розробниками.
- Адаптивний дизайн, який дозволяє використовувати застосунок як на стаціонарних комп'ютерах, так і на мобільних пристроях.
- Практична частина з імітацією фактичного використання криптографії при різних сценаріях кібербезпеки.

Технологічні аспекти розробки. Застосунок буде реалізований на основі Flask – мікрофреймворку для Python, що дозволяє створювати легкі та гнучкі веб-додатки [3]. Для взаємодії з користувачем використовується HTML, CSS, JavaScript (Vanilla JS).

Головна особливість застосунку – інтерактивні модулі, які дають змогу вводити текстові дані, обирати параметри шифрування та отримувати результати в реальному часі, можливість практичного виконання заснованих на реальних сценаріях завдань кібербезпеки, орієнтованих на криптографію, в умовах обмеженого часу.

Основними перевагами веб-застосунку є:

- інтерактивність;
- простий та зрозумілий інтерфейс;
- гнучкість.

Перспективи розвитку. У майбутньому планується розширення функціоналу застосунку, зокрема покращення безпеки застосунку, включаючи реалізацію HTTPS та захист від XSS-атак, використання бази даних SQLite або іншого рішення для збереження історії операцій користувача, вбудовування віртуальної машини в додаток (для більш глибоких імітацій реальних сценаріїв практичної частини) та удосконалення теоретичного аспекту додатку за допомогою Ai-помічника, що надаватиме теоретичні завдання з відкритою відповіддю та перевірятиме рівень знань користувача. Також розглядається можливість співпраці з навчальними закладами для впровадження застосунку у навчальний процес.

Таким чином, розробка освітнього веб-застосунку для вивчення алгоритмів шифрування сприятиме покращенню рівня знань у сфері криптографії, популяризації відкритого програмного забезпечення та підвищенню загальної обізнаності у питаннях інформаційної безпеки.

Література

- [1] Al Sweigart. Cracking Codes with Python: An Introduction to Building and Breaking Ciphers / Al Sweigart. – No Starch Press, 2018. – XX p.
- [2] Ferguson, N., Schneier, B., Kohno, T. Cryptography Engineering: Design Principles and Practical Applications / Ferguson, N., Schneier, B., Kohno, T. – Wiley, 2010. – XX p.
- [3] Flask Documentation [Electronic resource]. – Resource access mode: <https://flask.palletsprojects.com/>

GIT – СИСТЕМА КЕРУВАННЯ ВЕРСІЯМИ: GITHUB, GITLAB

Бондаренко В.В, Голуб Д.А, Єгоян В.Б.
E-mail: bondarenko.valeriia@vu.cdu.edu.ua

Черкаси, Черкаський національний університет імені Богдана Хмельницького

У сучасній розробці програмного забезпечення важливу роль відіграє контроль версій (Git), завдяки можливості відстеження змін у коді та рятівника в критичних ситуаціях, наприклад, коли нова функція змусила перестати програму працювати. У такому випадку є можливість повернутись до попередньої версії та поглянути за яких умов відбуваються неполадки.

На відміну від централізованих систем контролю версій (наприклад, Subversion), Git реалізує принципи VCS (Version Control System) за допомогою розподіленої архітектури. Це означає, що кожен користувач має повноцінну копію репозиторію, включно з усіма комітами, історією змін та гілками. Такий підхід забезпечує надійність, оскільки не існує єдиної точки відмови – навіть якщо центральний сервер стане недоступним, локальні копії дозволяють продовжувати роботу на своєму девайсі [1].

Основні завдання VCS:

- збереження історії змін – кожна модифікація файлу реєструється, що дає змогу аналізувати еволюцію коду;
- спільна робота – кілька розробників можуть працювати над одним проектом без ризику конфліктів;
- гілкування та злиття – дозволяє створювати окремі версії проекту для тестування або розробки нових функцій;
- відстеження та відкат змін – спрощує виправлення помилок та повернення до стабільних версій.

Git складається з трьох основних компонентів, які реалізують роботу системи контролю версій: commit, tree та blob. Вони формують внутрішню структуру даних і визначають спосіб збереження, організації та керування історією змін у репозиторії.

У цій системі commit є найвищим рівнем ієрархії. Він містить посилання на tree, яке представляє структуру проекту в конкретний момент часу. У свою чергу, tree зберігає посилання на окремі файли, які представлені у вигляді blob. Таким чином, знаючи хеш певного коміту, можна отримати доступ до відповідного дерева, а через нього – до конкретних файлів у репозиторії.

Blob відповідає за збереження вмісту файлів без будь-яких додаткових метаданих, таких як ім'я чи розташування. Кожен blob ідентифікується унікальним хешем і зберігається у спеціальній директорії, перша частина якої збігається з початковими символами його хеш-коду. Вміст файлів у blob зберігається у стисненому бінарному форматі, що дозволяє оптимізувати використання простору та прискорює доступ до даних [2].

При створенні нового коміту Git створює blob для кожного оновленого файлу та додає посилання на нього у tree. Це дозволяє зберігати файли в ефективному вигляді, використовуючи унікальні хеші для кожного об'єкта. У Git кожен commit є незалежним знімком проекту, що містить посилання на відповідні об'єкти tree та blob. Структуру керування версіями в середині коміту представлено на рисунку 1.

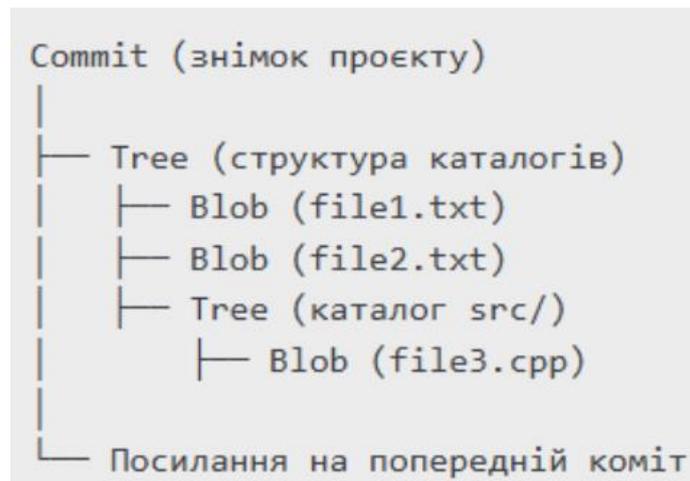


Рисунок 1 – Структура керування версіями в середині коміту

Git має широкий спектр команд, спрямованих на той чи інший функціонал. Хоча Git й надає широкий асортимент можливостей, здебільшого програмісти використовують декілька основних типів команд у своїй роботі, оскільки більшого й не треба. Зокрема, використовуються такі команди:

- базові команди. Сюди входять команди по роботі з репозиторіями, такі як `git init`, `git commit`, `git status`, `git add` та `git clone`. Ці команди спрощують життя під час керування локальними та віддаленими репозиторіями, дозволяючи створювати, оновлювати та переглядати зміни у репозиторії;
- гілкові команди. Завдяки ним можна виконувати маніпуляції з гілками. Завдяки цьому можна створити окрему гілку, в якій будуть проводитись тестування нових функцій, а основна гілка з робочою програмою не буде задіяна. До гілкових команд входять `git branch`, `git checkout`, `git switch`, `git merge` тощо.

GitHub – найбільший хостинг для сховищ Git, що набув популярності серед розробників через свою зручність та велику кількість можливостей. Здебільшого за допомогою GitHub розробники поширюють свої репозиторії для того, щоб показати результати своєї роботи. Для компаній, які розробляють програмне забезпечення також передбачений відповідний функціонал, що включає в себе систему керування доступом, інструменти для код-рев'ю, трекінг завдань тощо.

GitLab — це система керування репозиторіями на основі Git, яка надає можливості для розробки, автоматизації тестування та розгортання, керування проєктами та безпеки коду. Вона є альтернативою GitHub, але з більш розширеними функціями для командної роботи та автоматизації. GitLab має також вбудовану систему для автоматизації тестування та розгортання (CI/CD), підтримку об'єднання змін за допомогою Merge Requests, систему трекінгу задач через Issues та Boards, а також можливість зберігати Docker-образи у Container Registry.

Git став незамінним помічником в сучасній розробці й без нього не обходиться жоден розробник. Завдяки платформам, таким як GitHub та GitLab процес керування версіями став легшим, що в свою чергу дозволило ефективно використовувати технологію Git та розробляти більш кращі застосунки.

Література

[1] VCS основна концепція. [Електронний ресурс] – Режим доступу до ресурсу: <https://about.gitlab.com/topics/version-control/> (дата звернення: 07.02.2025)

[2] Git принцип роботи. [Електронний ресурс] – Режим доступу до ресурсу: <https://www.freecodecamp.org/news/git-under-the-hood/> (дата звернення: 07.02.2025)

ОГЛЯД ФРЕЙМВОРКІВ ТА БІБЛІОТЕК ДЛЯ РОЗРОБКИ ВЕБ-ДОДАТКУ ОНЛАЙН-КІНОТЕАТРУ

Булатов О.С.

Керівник: Гайдаєнко О.В.

E-mail: oksana.gaidaienko@nuos.edu.ua

Миколаїв, Національний університет кораблебудування імені адм.Макарова

У сучасному цифровому світі попит на онлайн-стрімінгові сервіси та кінотеатри стрімко зростає. Впровадження веб-додатку для онлайн-кінотеатру є актуальним рішенням, що відповідає вимогам ринку та змінює підхід до споживання мультимедійного контенту.

Традиційні кінотеатри поступово втрачають аудиторію через розвиток онлайн-платформ, таких як Netflix, Disney+, Amazon Prime. Користувачі віддають перевагу перегляду контенту вдома завдяки зручності доступу з будь-якого пристрою. Веб-додаток дозволяє користувачам переглядати фільми та серіали без прив'язки до місця та часу. Підтримка багатоплатформності (ПК, планшети, смартфони) підвищує доступність сервісу. Використання сучасних технологій (React, Angular, Vue.js, Node.js) дозволяє створювати швидкі та інтерактивні веб-застосунки. Хмарні сервіси та CDN (Content Delivery Network) забезпечують ефективне потокове передавання відео без затримок. Впровадження штучного інтелекту та машинного навчання дозволяє аналізувати вподобання користувачів та рекомендувати релевантний контент. Персоналізований підхід підвищує утримання користувачів та рівень задоволеності сервісом. Веб-додаток може підтримувати різні моделі монетизації:

- передплатна система (Subscription-based) – щомісячна або річна підписка;
- оренда фільмів (Pay-per-view);
- реклама (Ad-supported);
- інтеграція платіжних систем (Stripe, PayPal, LiqPay) дозволяє реалізувати зручну оплату [1].

Додавання функцій коментування, рейтингової системи та рекомендацій друзям робить платформу більш привабливою. Можливість інтеграції з соціальними мережами для спільного перегляду фільмів. Впровадження DRM (Digital Rights Management) для захисту авторських прав. Шифрування даних користувачів та використання безпечних протоколів (HTTPS, OAuth).

Розробка онлайн-кінотеатру вимагає використання сучасних технологій для забезпечення високої продуктивності, масштабованості, безпеки та зручності користувачів:

- Фронтенд (Front-End), це частина, з якою безпосередньо взаємодіє користувач. Для онлайн-кінотеатру важливо забезпечити швидкість, адаптивність та інтуїтивний UX/UI. Фреймворки та бібліотеки які викорисовуються це React.js – найпопулярніша бібліотека для створення інтерфейсів, Vue.js – легкий фреймворк, що дозволяє швидко створювати SPA (Single Page Applications), Angular – потужний фреймворк від Google для великих корпоративних рішень [2].

- Бекенд (Back-End), серверна частина відповідає за бізнес-логіку, авторизацію, управління контентом та обробку запитів. Фреймворки та платформи які використовуються це Node.js + Express.js – швидкий і легкий стек для розробки API, Django + Python – потужний фреймворк для надійних веб-додатків. FastAPI (Python) – високопродуктивний фреймворк для API. Spring Boot (Java) – корпоративне рішення для складних проєктів [3].

- База даних (Database) онлайн-кінотеатру потребує зберігання великих обсягів даних (фільми, користувачі, підписки) рекомендовано використовувати PostgreSQL – реляційна БД з підтримкою JSON та складних запитів. MongoDB – NoSQL-БД, підходить для роботи з гнучкими структурами даних. MySQL – популярна реляційна БД, ефективна для масштабованих проєктів. Redis – кешування запитів та прискорення роботи додатку.

- Стрімінг та відео-хостинг, FFmpeg – обробка та оптимізація відео для стрімінгу. AWS S3 / Cloudflare R2 – зберігання відеофайлів. HLS (HTTP Live Streaming) – технологія потокової передачі. Wowza / Vimeo API / MUX – сервіси для відео-хостингу.

- Для безпеки та авторизації використовується OAuth 2.0 / JWT (JSON Web Token) для безпечної авторизації. Helmet.js використовується для захисту від XSS-атак у Node.js.

- Хмарні сервіси та DevOps використовують Docker для контейнеризації додатку. Kubernetes для управління мікросервісами. AWS / Google Cloud / DigitalOcean – хостинг і обробка серверних запитів. CI/CD (GitHub Actions, GitLab CI/CD) – автоматичне розгортання.

Важливим є питання правильно обраного математичного забезпечення розробки онлайн-кінотеатру, воно потребує застосування різних математичних методів таких як - теорія ймовірностей та статистика для оптимізації роботи системи, аналізу користувацьких даних, управління потоковою передачею відео та забезпечення безпеки. Для аналізу поведінки користувачів (передбачення уподобань, визначення популярності контенту). Для рекомендацій системи (підбір контенту на основі історії переглядів). Моделювання навантаження на сервер (розрахунок кількості одночасних підключень). Для оцінки впливу різних факторів на вибір контенту будемо застосовувати метод дисперсійного аналізу (ANOVA). Для визначення ймовірності підписки користувача після безкоштовного пробного періоду метод біноміального розподілу. Для персоналізації рекомендацій рекомендується використання байєсівської теореми.

Розробка веб-додатку для онлайн-кінотеатру є актуальною, оскільки відповідає сучасним вимогам ринку, покращує доступність контенту, забезпечує персоналізований досвід для користувачів та відкриває нові можливості для монетизації. Враховуючи стрімке зростання популярності стрімінгових сервісів, створення такої системи є перспективним напрямом у сфері цифрових розваг. Для розробки онлайн-кінотеатру варто використовувати React.js + Node.js/Express + PostgreSQL або Vue.js + Django + MongoDB. Для потокового відео важливо інтегрувати HLS або Wowza. Вибір залежить від масштабів проєкту та вимог до продуктивності та безпеки. Математичний апарат онлайн-кінотеатру базується на теорії ймовірностей, машинному навчанні, теорії графів, теорії черг та криптографії. Використання цих методів дозволяє розробити масштабовану, безпечну та ефективну систему.

Література

[1] Бачинський А. В. Розробка кіно-додатку на основі мови програмування JavaScript з використанням технологій html, css: кваліфікаційна робота освітнього рівня «Бакалавр» «126 – інформаційні системи та технології» / А. В. Бачинський. – Тернопіль : ТНТУ, 2023. – 56 с.

[2] Тарасова А. О. Розробка автоматизованої системи онлайн покупки білетів у кінотеатр: автореф. кваліфік. роботи на здобуття освітнього ступеня «Бакалавр»: напрям підготовки 6.050101 «Комп'ютерні науки» / А.О. Тарасова, ЧНУ імені Петра Могили. – Миколаїв, 2019. – 14 с.

[3] HTML и CSS. Разработка и дизайн веб-сайтов / Джон Дакетт – 2021. – 480 с.

НЕО4J – ГРАФОВА БАЗА ДАНИХ

Венгріна О.С., Почанський О.М.

E-mail: olena.venhrina@hneu.net

Харків, Харківський національний економічний університет імені Семена Кузнеця

У сучасному світі обробка великих обсягів даних та складних зв'язків між ними стає все більш актуальною задачею. Традиційні реляційні бази даних часто не справляються з такими викликами, що призводить до необхідності пошуку нових рішень. Одним із таких рішень є графові бази даних, які дозволяють ефективно моделювати та аналізувати складні структури даних.

Neo4j є однією з провідних графових баз даних, яка відзначається своєю унікальною архітектурою та високою продуктивністю. Однією з ключових характеристик Neo4j є її здатність зберігати та обробляти дані у вигляді графів, що дозволяє ефективно моделювати складні зв'язки між об'єктами. Це особливо корисно у випадках, коли дані мають багато взаємозв'язків, таких як соціальні мережі, рекомендаційні системи та управління мережевими ресурсами.

Однією з головних переваг Neo4j є її мова запитів Cypher, яка спеціально розроблена для роботи з графовими даними. Cypher дозволяє легко та інтуїтивно формулювати запити, що робить роботу з базою даних більш зручною та ефективною. Крім того, Neo4j забезпечує високу продуктивність завдяки своїй оптимізованій архітектурі, яка дозволяє швидко виконувати складні запити навіть на великих обсягах даних.

Ще однією важливою перевагою Neo4j є її масштабованість. База даних може легко адаптуватися до зростання обсягів даних та кількості користувачів, що робить її ідеальним рішенням для великих проєктів. Крім того, Neo4j підтримує різноманітні інструменти та інтеграції, що дозволяє легко інтегрувати її з іншими системами та платформами.

Завдяки своїм характеристикам та перевагам, Neo4j знаходить широке застосування у різних галузях, включаючи фінансові послуги, охорону здоров'я, телекомунікації та багато інших. Це підкреслює її універсальність та ефективність у вирішенні різноманітних завдань.

На рисунку 1 представлено частину візуалізації графової бази даних.

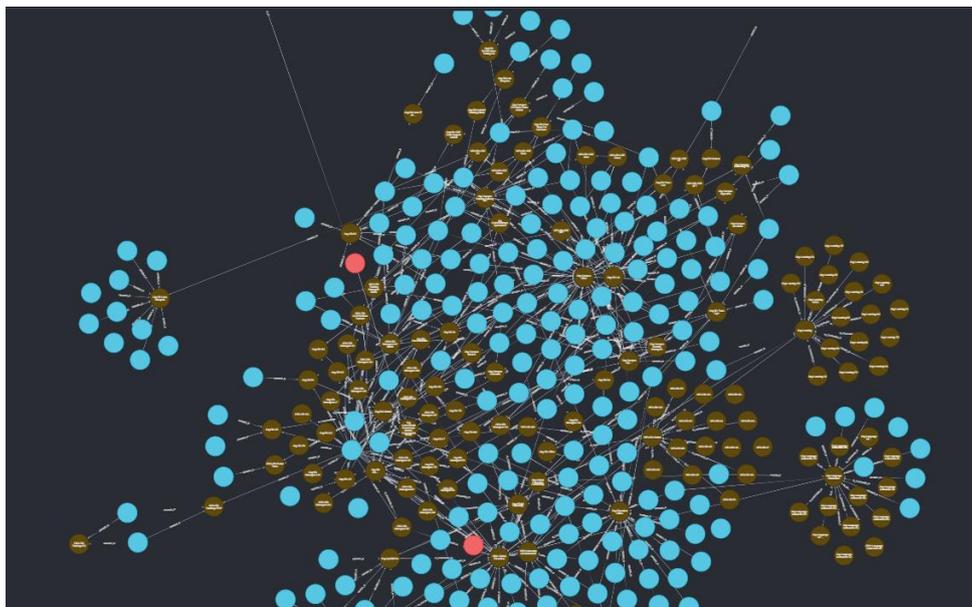


Рисунок 1 – Візуалізація графової бази даних

Література

[1] Graph Database Resources: White Papers, Case Studies & More [Електроний ресурс] – Режим доступу до ресурсу: <https://neo4j.com/resources/>

[2] Graph Databases: Neo4j Analysis - Semantic Scholar [Електроний ресурс] – Режим доступу до ресурсу: <https://pdfs.semanticscholar.org/5164/3300e31bf2c79031c10c8a2007b89c8deb6a.pdf>

[3] Redalyc. Literature review about Neo4j graph database as a feasible alternative for replacing RDBMS [Електроний ресурс] – Режим доступу до ресурсу: <https://www.redalyc.org/pdf/816/81643819017.pdf>

[4] Graph_Databases_2e_Neo4j [Електроний ресурс] – Режим доступу до ресурсу: <https://www.safaribooksonline.com/library/view/graph-databases-2e/9781492044073/>

ПРОБЛЕМИ ЕФЕКТИВНОГО РОЗПОДІЛЕННЯ РЕСУРСІВ В СИСТЕМАХ ОРКЕСТРУВАННЯ ВІРТУАЛЬНИХ КОНТЕЙНЕРІВ

Воєводін Є.В., Стабецька Т.А., Розломій І.О.

E-mail: yevhenii.voievodin@vu.cdu.edu.ua

Черкаси, Черкаський національний університет імені Богдана Хмельницького

Системи оркестрування віртуальних контейнерів (СОВК) відіграють ключову роль у роботі сучасних розподілених систем. Зокрема, їхнє поширення спричинено популярністю та використанням контейнеризованих додатків із застосуванням таких архітектурних підходів, як мікросервісна архітектура [1]. Контейнер являє собою додаток, який є автономним, оскільки, крім самого додатка, містить у собі всі необхідні бібліотеки та засоби мов програмування і середовища, потрібні для його роботи. Це дає змогу використовувати такий додаток на різних операційних системах і платформах [2]. Завдання СОВК полягає в тому, щоб забезпечувати життєвий цикл і роботу таких додатків, маючи певний набір фізичних ресурсів і конфігурацій системи. Серед популярних СОВК – системи з відкритим вихідним кодом, зокрема: Kubernetes, Docker Swarm, Apache Mesos [3].

Один із основних процесів СОВК – це розміщення контейнерів на фізичних вузлах кластера, за що відповідає компонент планування (планувальник). Процес розміщення не є тривіальною задачею та може зіткнутися з наступними викликами.

Послідовність контейнерів для розміщення в кластері є динамічною, тобто наперед невідомою. Наприклад, якщо СОВК застосовується для запуску клієнтських сервісів у кластері хостингової компанії, то саме активність клієнтів генеруватиме динамічну послідовність контейнерів. Або ж, якщо СОВК використовується у межах однієї розподіленої системи з використанням мікросервісної архітектури, у такому випадку команди розробників визначають час, коли нова версія конкретного мікросервісу буде розгортатися, що впливає на послідовність. Оскільки послідовність не є визначеною наперед, не можна заздалегідь підрахувати найкращий варіант розміщення, а отже, залишається простір для застосування більш комплексних стратегій планування, наприклад, з використанням штучного інтелекту [4].

Визначення ефективності розміщення залежить від специфіки системи, яка використовує СОВК. Для одних систем ефективність полягає в тому, щоб використовувати мінімум фізичних ресурсів кластера. Для інших бажаною метрикою ефективності є відмовостійкість системи, тоді для її максимізації розміщувати контейнери, що належать одному й тому ж сервісу, на різних фізичних вузлах. Також чинником може бути безпека [5]: планувальник може брати до уваги рівень критичності сервісу та можливість доступу до нього ззовні. Наприклад, не розміщувати на одному фізичному вузлі контейнери менш критичних і більш критичних сервісів, чи то контейнери сервісів до яких є різний рівень доступу ззовні.

Література

[1] Bushong, V., Abdelfattah, A. S., Maruf, A. A., Das, D., Lehman, A., Jaroszewski, E., ... & Bures, M. (2021). On microservice analysis and architecture evolution: A systematic mapping study. *Applied Sciences*, 11(17), 7856.

[2] Siddiqui, T., Siddiqui, S. A., & Khan, N. A. (2019, November). Comprehensive analysis of container technology. In *2019 4th International Conference on Information Systems and Computer Networks (ISCON)* (pp. 218-223). IEEE.

[3] Mercl, L., & Pavlik, J. (2019). The comparison of container orchestrators. In *Third International Congress on Information and Communication Technology: ICICT 2018, London* (pp. 677-685). Springer Singapore.

[4] Воєводін, Є. В., & Авраменко, В. С. (2018). Порівняння ефективності топологій самоорганізаційних карт Кохонена в системах оркестрування віртуальних контейнерів. *Вчені записки Таврійського національного університету імені ВІ Вернадського. Серія: Технічні науки*, (29 (68), № 1 (1)), 99-105.

[5] Voievodin, Y., & Rozlomii, I. (2024). Application Security Optimization in Container Orchestration Systems Through Strategic Scheduler Decisions.

IFOGSIM: СИМУЛЯЦІЯ РЕСУРСНОГО УПРАВЛІННЯ В СЕРЕДОВИЩАХ ІОТ, EDGE ТА FOG ОБЧИСЛЕНЬ

Волощук С.І.

E-mail: confmail8@gmail.com

Миколаїв, Чорноморський національний університет імені Петра Могили

З розвитком Інтернету речей (ІоТ) зростає потреба у симуляційних інструментах, здатних точно змодельовати продуктивність та поведінку розподілених, ресурсно обмежених мереж. Одним із таких інструментів є iFogSim – безкоштовний та відкритий симуляційний пакет, розроблений для розширення традиційних підходів до моделювання хмарних обчислень з урахуванням можливостей туманових обчислень.

Дослідники зазначають, що iFogSim створено з метою подолання труднощів, пов'язаних із розробкою та впровадженням масштабних ІоТ-систем. Традиційні хмарні симулятори часто не враховують особливості розподілених обчислень, коли необхідно спільно використовувати як централізовані (хмарні), так і децентралізовані (edge або туманові) ресурси. iFogSim заповнює цю прогалину, надаючи можливість створювати віртуальні моделі ІоТ-додатків, що охоплюють від малопотужних сенсорних вузлів до високопродуктивних серверів у хмарі. Такий підхід дозволяє детально аналізувати різні політики планування завдань та стратегії управління ресурсами в реалістичних умовах.

За основу iFogSim покладено модульну архітектуру, що реалізована на Java, що дозволяє дослідникам конфігурувати різноманітні типи пристроїв – сенсорів, виконавчих механізмів, шлюзів та вузлів туману – і задавати власні модулі додатків. Завдяки такій модульності, система здатна змодельовати широкий спектр ІоТ-сценаріїв, від розумних міст до систем моніторингу на виробництві. Крім того, iFogSim інтегрує численні вбудовані алгоритми планування, що допомагають визначити, як завдання розподіляються між хмарними, тумановими та периферійними ресурсами, що дозволяє детально оцінити показники затримок, енергоспоживання та витрат.

Система також характеризується високою масштабованістю та гнучкістю, що дозволяє моделювати як невеликі, так і великі ІоТ-екосистеми, а також легко налаштовувати параметри симуляції для оптимізації продуктивності. Дослідники отримують можливість відстежувати широке коло показників, включаючи загальні затримки, енергоспоживання та виконання сервісних рівнів, що сприяє глибокому аналізу впливу архітектурних рішень на загальну ефективність системи.

iFogSim знаходить застосування у вирішенні практичних завдань, дозволяючи дослідникам досліджувати «що, як якби» сценарії. Наприклад, планувальники розумних міст можуть використовувати його для моделювання мережі сенсорів у місті та оцінки різних стратегій управління транспортом або моніторингу навколишнього середовища. Промислові підприємства можуть перевіряти стратегії розподілу ресурсів і алгоритми планування для профілактичного обслуговування виробничих систем. Віртуальне прототипування таких складних взаємодій допомагає суттєво зменшити час та витрати, пов'язані з впровадженням реальних систем.

Дослідники відзначають, що iFogSim є потужним та надійним інструментом для симуляції ІоТ та туманових обчислень. Його зручність використання у поєднанні з широкими можливостями в області управління ресурсами та оцінки продуктивності робить його популярним як серед наукових дослідників, так і серед розробників, що займаються прототипуванням. Незалежно від того, чи йдеться про проектування невеликої розумної домашньої системи або масштабної мережі розумного міста, iFogSim надає потужну платформу для моделювання, симуляції та оптимізації майбутнього інтегрованих пристроїв.

ПОРІВНЯННЯ СПОЖИВАННЯ ОПЕРАТИВНОЇ ПАМ'ЯТІ У WEB IDE

Гюльмамедов Н.М.

Керівник: Бурлаченко І.С.

E-mail: nikitagulmamedov@gmail.com

Миколаїв, Чорноморський національний університет імені Петра Могили

Web IDE (Integrated Development Environment) стають все більш популярними завдяки доступності та зручності використання. Вони дозволяють розробникам писати, тестувати та відлагоджувати код без потреби встановлення додаткового програмного забезпечення, підтримуючи різні мови програмування [1]. Це забезпечує миттєвий доступ до середовища розробки з будь-якого пристрою, що підключений до Інтернету, та спрощує спільну роботу над кодом через платформи, такі як Replit, CodeSandbox, StackBlitz. Онлайн-середовища [2] ідеально підходять для навчання, адже не вимагають складних налаштувань, а також інтегруються з системами контролю версій, такими як Git, що спрощує управління проєктами. Автоматичне збереження змін та хмарне зберігання захищають код від втрати, а підтримка розширень і плагінів покращує продуктивність розробників. Завдяки цим середовищам можна тестувати код на різних платформах і пристроях, працювати над проєктами в реальному часі та використовувати штучний інтелект для пришвидшення роботи.

Replit – онлайн інтегроване середовище розробки, яке дозволяє користувачам швидко перетворювати свої ідеї на програмне забезпечення за допомогою штучного інтелекту. Replit Agent, передовий штучний інтелект, що допомагає зробити програмування доступним для всіх, дозволяючи користувачам швидко створювати програми та вебсайти. Replit AI допомагає з налагодженням, автозавершенням коду та навіть генеруванням коду з використанням звичайної мови, революціонізуючи спосіб взаємодії розробників із кодом. Користувачі можуть почати з опису програми або сайту, який вони хочуть створити, за допомогою запитів. Штучний інтелект може допомогти покращити ці запити для отримання оптимальних результатів. При автоматизованому створенні плану збірки Replit генерує план, щоб втілити ідею користувача в життя. Користувачі можуть почати з прототипу та додавати функції за допомогою простих запитів. Платформа пропонує простий у використанні чат-інтерфейс для вдосконалення застосунків. Після кожного етапу плану збірки агент шукає зворотний зв'язок та інтегрує запити в подальшу роботу. Replit дозволяє користувачам розгортати сайти або програмне забезпечення на URL-адресу протягом декількох хвилин. Розгортання спрощено, що дозволяє користувачам створювати, тестувати та розгортати вебзастосунки безпосередньо з браузера. Розгортання Replit підтримується Google Cloud.

Робочий вебпростір Replit включає редактор коду, консоль для виконання команд та файлову систему для організації проєктів. Підсвічування синтаксису та автозавершення доступні для полегшення кодування. Replit підтримує понад 50 мов програмування, використовуючи контейнери для забезпечення необхідних інструментів та бібліотек для кожної мови. Декілька користувачів можуть одночасно працювати над одним і тим самим кодом, при цьому зміни відображаються миттєво. Вбудовані ланцюжки дозволяють користувачам коментувати та обговорювати теми зі співавторами безпосередньо в коді. Replit надає інтегровані інструменти, такі як налагодження, контроль версій за допомогою Git та менеджери пакетів для додавання зовнішніх бібліотек.

CodeSandbox – це хмарна платформа розробки, яка дозволяє розробникам швидко кодувати, співпрацювати та запускати проєкти з будь-якого пристрою. Вона надає миттєві хмарні середовища розробки, що дають змогу писати, тестувати та ділитися кодом без потреби локальних інсталяцій. Це популярний вебредактор коду та IDE, який дозволяє користувачам працювати без входу в систему, хоча для збереження роботи це необхідно. CodeSandbox підтримує різні JavaScript фреймворки, такі як React.js, Vue.js та Angular.js, а також може запускати програми Node.js. Він підтримує як фронтенд, так і бекенд

фреймворки. CodeSandbox дає змогу розробникам ділитися кодом, співпрацювати та разом вирішувати проблеми розроблення ПЗ. Кожне середовище працює ізольовано, тому користувачі можуть безпечно запускати ненадійний код, не впливаючи на свою систему. Інфраструктура CodeSandbox розгортає цілі віртуальні машини (VM), клонує їх і відновлює знімки приблизно за 2 секунди. CodeSandbox підтримує роботу в автономному режимі та має вбудовану підтримку npm пакетів, які він автоматично завантажує з репозиторіїв. Платформа дозволяє користувачам легко ділитися кодом через вбудовування, надає доступ до вебтерміналу, дозволяючи запускати NPM скрипти безпосередньо з браузера, та надає користувачам контроль над періодами неактивності перед автоматичною гібернацією. API доступні для створення ізольованих середовищ розробки, які можуть запускати будь-який тип коду.

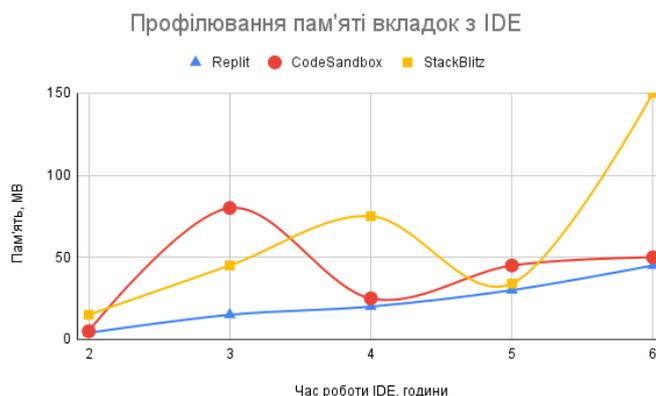


Рисунок 1 – Порівняння споживання пам'яті упродовж робочого дня розробника ПЗ.

StackBlitz - це браузерне IDE для веброзробників, що підтримує спільну роботу та усуває потребу в трудомістких локальних конфігураціях. Це миттєве повностекове веб-IDE для екосистеми JavaScript, що працює на основі Web Containers, першої операційної системи на базі WebAssembly, яка завантажує середовище Node.js за мілісекунди безпечно у вкладці вашого браузера. StackBlitz дозволяє розробникам кодувати, співпрацювати та швидко запускати проекти з будь-якого пристрою. Усі обчислення відбуваються всередині браузера, використовуючи швидкість та інновації в галузі безпеки. Ключові функції включають безпеку, швидкість, функціональність онлайн та офлайн, а також безшовне налагодження за допомогою Chrome Dev Tools як для зовнішніх, так і для внутрішніх застосунків. Він автоматично піклується про налаштування, від розгалуження та встановлення залежностей до конфігурації інструментів збірки та швидкого перезавантаження. Одним клацанням миші StackBlitz IDE запускає повноцінний редактор коду з інтеграцією Git та попереднім переглядом із швидким перезавантаженням. StackBlitz також можна використовувати для додавання інтерактивних прикладів до документації, створення стартових проектів або ефективного відтворення помилок. Термінал StackBlitz дозволяє користувачам запускати команди так само, як вони б це робили на своєму локальному комп'ютері.

Web IDE чудове рішення для студентів і стартапів, оскільки дозволяє заощадити ресурси на інфраструктуру. Проте варто враховувати, що такі інструменти залежать від стабільного інтернет-з'єднання та оперативної пам'яті (рис. 1). Загалом, Web IDE оптимізують робочий процес і суттєво покращують продуктивність розробників.

Література

[1] Most Famous Online IDE for Programming [Електронний ресурс] – Режим доступу до ресурсу: <https://www.geeksforgeeks.org/most-famous-online-ide-for-programming>

[3] Kusumaningtyas, K., Nugroho, E. D., & Priadana, A. (2020). Online Integrated Development Environment (IDE) in supporting computer programming learning process during COVID-19 pandemic: A comparative analysis. IJID (International Journal on Informatics for Development), 9(2), 66–71. doi:10.14421/ijid.2020.09202

САКЕРНР – ФРЕЙМВОРК ДЛЯ ВЕБ-РОЗРОБКИ

Давидов Д.В., Латанська Л.О.

E-mail: den0802200303@gmail.com, liudmyla.latanska@nuos.edu.ua

Миколаїв, Національний університет кораблебудування імені адмірала Макарова

Сучасна веб-розробка вимагає ефективних інструментів для швидкої та якісної розробки програмного забезпечення. Одним із таких інструментів є CakePHP – фреймворк з відкритим кодом для мови PHP, що дозволяє створювати веб-додатки з використанням архітектури Model-View-Controller (MVC) [1].

Спочатку даний фреймворк створювався як клон популярного Ruby on Rails і багато ідей були запозичені саме звідти:

- своя файлова структура;
- абстракція даних (PEAR::DB, ADOdb, власна розробка Cake);
- підтримка різних СКБД: (PostgreSQL, MySQL, SQLite, Oracle).

CakePHP повністю сумісний як з PHP4, так і з PHP5. Це його вигідно відрізняє від таких фреймворків, як Symfony та PHPonTrax [2].

Даний програмний каркас для створення вебзастосунків надає широкий спектр можливостей, що дозволяють скоротити час розробки, забезпечити високу продуктивність і безпеку. Завдяки принципу "конвенція понад конфігурацію" розробникам не потрібно витрачати багато часу на налаштування, що робить CakePHP ідеальним вибором для швидкої розробки. Нижче розглянуті ключові особливості цього фреймворку:

- Завдяки генераторам коду та інтегрованим можливостям автоматизації, розробники можуть швидко створювати веб-додатки без необхідності писати багато повторюваного коду.

- Має вбудовані засоби захисту, такі як захист від SQL-ін'єкцій, міжсайтових підрбок запитів (CSRF) та міжсайтового скриптингу (XSS). Крім того, CakePHP підтримує хешування паролів за допомогою сучасних алгоритмів.

- Полегшує роботу з базами даних завдяки використанню об'єктно-реляційного підходу. Це дозволяє взаємодіяти з базою даних за допомогою об'єктів замість традиційних SQL-запитів, що покращує читабельність коду.

- Дозволяє розширювати функціональність шляхом підключення готових модулів. CakePHP має багатий набір плагінів, які допомагають додавати новий функціонал без необхідності розробки з нуля.

- CakePHP інтегрується з PHPUnit, що дозволяє створювати автоматизовані тести для перевірки працездатності додатка, забезпечуючи стабільність та високу якість коду [3].

CakePHP є потужним інструментом для розробки веб-додатків, що надає розробникам широкий спектр можливостей для швидкої, безпечної та гнучкої розробки. Завдяки відкритому коду та активній спільноті, цей фреймворк залишається одним із найкращих виборів для створення веб-додатків на PHP.

Література

[1] GitHub. CakePHP. [Електронний ресурс] – Режим доступу до ресурсу: <https://github.com/cakephp/cakephp>

[2] Wikipedia. CakePHP. [Електронний ресурс] – Режим доступу до ресурсу: <https://wikipedia.org/wiki/CakePHP>

[4] CakePHP Documentation [Електронний ресурс] – Режим доступу до ресурсу: <https://book.cakephp.org/5/en/index.html>

НАВАНТАЖУВАЛЬНЕ ТЕСТУВАННЯ АГРЕГАТОРУ ДАНИХ З ВИКОРИСТАННЯМ APACHE JMETER

¹Зеленський О.Д., ²Воловщиків В.Ю., ³Шапо В.Ф.

E-mail: ¹oleh.zelenskyi@cs.khpi.edu.ua, ²valeriy.volovshchikov@khpi.edu.ua,
³vladlen.shapo@gmail.com

^{1,2}Харків, Національний технічний університет “Харківський політехнічний інститут”,
³Одеса, Інститут Військово-Морських Сил

Дана робота є логічним розвитком [1, 2] та присвячена питанням навантажувального тестування агрегатора даних з використанням Apache JMeter [3].

На теперішній момент часу різноманітні агрегатори даних стають все більш і більш популярними. Популярність агрегаторів даних пов'язана з забезпеченням кінцевих користувачів агрегованою інформацією з Інтернет джерел (першоджерел). Агрегована інформація у одному місці заощаджує час на пошук та повинна забезпечити користувачів найактуальнішими даними. Найяскравішим представником агрегаторів даних на українському ринку є E-Katalog [4].

Одним з ключових недоліків певного набору агрегаторів даних є надання користувачам неактуальної інформації. Мова йде про відмінність у інформації між першоджерелом та агрегатором. При розгляді агрегаторів електронної комерції можна стверджувати, що, зокрема, може мати місце неактуальність інформації, наприклад, щодо вартості товару. Неактуальність інформації може бути пов'язана з низькою частотою оновлення останньої безпосередньо агрегатором.

Для подолання означеного недоліку пропонується “ініціативу” щодо актуалізації даних на агрегаторі перекласти на першоджерела. Така “ініціатива” може бути реалізована додатковим програмним модулем, який встановлювався би на боці першоджерела та у випадку оновлення даних у автоматичному режимі завантажував їх на бік агрегатору.

Впровадженню у комерційне використання агрегатору та програмних модулів повинно передувати, зокрема, виконання навантажувального тестування агрегатора [5]. Навантажувальне тестування агрегатора забезпечить оцінку його поведінки із заданим очікуваним навантаженням, яке повинно бути тотожним до реальних умов використання.

В роботі проведення навантажувального тестування виконується засобами Apache JMeter [3].

Apache JMeter – це програмне забезпечення з відкритим вихідним кодом, яке засновано на мові Java та має архітектуру, яка підтримує плагіни сторонніх розробників. Останнє дозволяє доповнювати Apache JMeter новими функціями.

Програмне забезпечення використовується для:

- тестування продуктивності – встановлює максимально можливе очікування продуктивності при даній конфігурації інфраструктури;
- тестування навантаження. Це тестування в основному використовується для тестів системи під максимальним навантаженням, для якої вона була розроблена;
- стрес-тестування. В цьому тестуванні виконується спроба зламати систему, перевантажуючи її ресурси;
- тестування на відновлюваність – якщо сервер “впав”, як швидко він відновить роботу та що буде з даними.

До ключових особливостей та переваг Apache JMeter можна віднести:

- вільно доступне програмне забезпечення з відкритим вихідним кодом;
- простий та зрозумілий графічний інтерфейс;
- незалежний від платформи інструмент. У Linux/Unix Apache JMeter може бути викликаний натисканням на скрипт оболонки Apache JMeter. У Windows можна запустити, відкривши файл jmeter.bat;

- повна підтримка Swing та полегшених компонентів (попередньо скомпільований JAR використовує пакети javax.swing. *);
- Apache JMeter зберігає свої плани випробувань у форматі XML. Це означає, що можна створити план тестування за допомогою текстового редактора;
- багатопотокова структура дозволяє одночасну вибірку багатьма потоками та одночасну вибірку різних функцій окремими групами потоків;
- використання для автоматичного та функціонального тестування програм;
- хороша підтримка онлайн-спільноти та наявність навчальних посібників.

В роботі в межах навантажувального тестування була проведена оцінка навантаження агрегатора. Нижче, у якості прикладу, наведено фрагмент ключових вихідних даних навантажувального тестування, яке проводилось шляхом надсилання з боку першоджерел запитів на зміну вартості товару та додавання коментаря для товару. В табл. 1 наведені параметри двох експериментів.

Табл. 1. Показники експериментів

Експеримент	Кількість Інтернет джерел	Час навантажувального тестування, сек.	Середній час обробки запитів, мілісекунда		
			Агреговані дані	Зміна вартості	Додавання коментарю
Перший	300	90	79.5	91	68
Другий	300	50	1550	2991	109

На рис. 1–2 наведені деталізовані та агреговані дані експериментів.

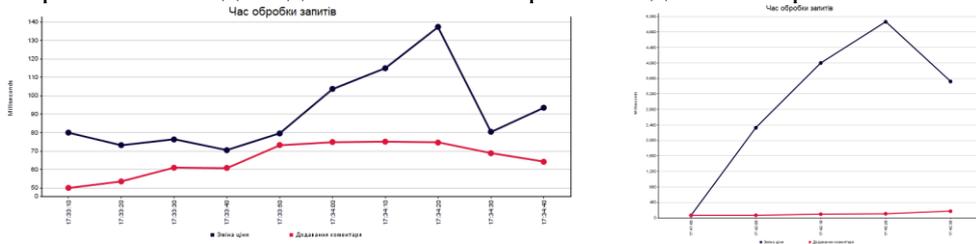


Рис. 1. Деталізовані результати експериментів



Рис. 2. Агреговані результати експериментів

Література

[1] Чухрій В.С., Воловщиків В.Ю., Шапо В.Ф. Стек програмних рішень для агрегування даних з глобальної мережі Internet // Матеріали XIV-ої Міжнародної науково-практичної конференції «Free and Open Source Software», Харків, 14-16 лютого 2023 р. – Харків: ХНЕУ імені Семена Кузнеця, 2023. с. 65-66.

[2] Киблицький Р.Р., Воловщиків В.Ю., Шапо В.Ф. Агрегування даних з Інтернет джерел з використанням стеку безкоштовних програмних рішень // Матеріали XV-ої Міжнародної науково-практичної конференції «Free and Open Source Software», Харків, 13-14 лютого 2024 р. – Харків: ХНЕУ імені Семена Кузнеця, 2024. с.84-85.

[3] Apache JMeter [Електроний ресурс] – Режим доступу до ресурса: <https://jmeter.apache.org/>

[4] E-Katalog [Електроний ресурс] – Режим доступу до ресурса: <https://ek.ua/ua/>

[5] Навантажувальне тестування [Електроний ресурс] – Режим доступу до ресурса: <https://uk.wikipedia.org/wiki/>

РОЗРОБКА ВЕБ-ЗАСТОСУНКУ ДЛЯ УПРАВЛІННЯ РЕЗЕРВНИМИ КОПІЯМИ ТА ВІДНОВЛЕННЯМ ДАНИХ У ХМАРІ

Іванюк В.Р.

Керівник: Борисенко Д.В.

E-mail: valeriia.ivaniuk@hneu.net

Харків, Харківський національний економічний університет імені Семена Кузнеця

У сучасному цифровому світі важливість резервного копіювання та відновлення даних неможливо переоцінити. Пошкодження або втрата даних можуть спричинити значні збитки для компаній та користувачів. Використання хмарних технологій дозволяє створити надійний механізм резервного копіювання, забезпечуючи доступність, безпеку та швидке відновлення інформації. Метою цього проєкту є розробка веб-застосунку для управління резервними копіями та відновленням даних у хмарному середовищі.

Для реалізації веб-застосунку використовуються наступні технології:

- Back-end: Spring Boot – фреймворк для розробки серверної частини Java-застосунків, що забезпечує високу продуктивність та безпеку.
- Front-end: React.js – бібліотека для створення динамічних інтерфейсів користувача.
- База даних: PostgreSQL – надійна реляційна база даних із підтримкою масштабованості.
- Хмарне середовище: AWS S3 – хмарне сховище для збереження резервних копій із високим рівнем доступності.
- Безпека: JWT (JSON Web Token) – механізм аутентифікації та авторизації користувачів.

Основні функціональні можливості

- Створення резервних копій – можливість автоматичного та ручного створення копій даних у хмарному сховищі.
- Керування версіями – збереження декількох версій резервних копій із можливістю вибору потрібної.
- Відновлення даних – швидке відновлення збережених даних із вибором місця відновлення.
- Шифрування та безпека – використання алгоритмів шифрування для захисту даних від несанкціонованого доступу.
- Моніторинг та сповіщення – інтеграція з системами оповіщення про статус резервного копіювання та потенційні загрози.

Розробка веб-застосунку для управління резервними копіями та відновленням даних у хмарі дозволяє підвищити надійність та безпеку збереження важливої інформації. Використання сучасних технологій, таких як Spring Boot, React.js та AWS S3, забезпечує високу продуктивність, гнучкість та масштабованість рішення.

Література

[1] Wikipedia. Cloud Backup Solutions [Електронний ресурс] – Режим доступу до ресурсу: https://wikipedia.org/wiki/Cloud_backup

СЕРВІСИ ГЕНЕРАЦІЇ 3D-МОДЕЛЕЙ

Іщенко Н.Ю.

Керівник: Обухова К.О.

E-mail: niki097875@gmail.com

Миколаїв, Чорноморський національний університет імені Петра Могили

Розвиток комп'ютерних технологій та штучного інтелекту сприяв появі нових інструментів для створення тривимірних моделей, що значно спрощує процес 3D-моделювання для фахівців та аматорів. Одним із таких інструментів є сервіси генерації 3D-моделей, які на основі алгоритмів машинного навчання та глибоких нейронних мереж дозволяють швидко створювати складні об'єкти з високим рівнем деталізації. Використання подібних сервісів відкриває нові можливості в дизайні, архітектурі, медицині, геймдеві та інших сферах, але водночас постає низка викликів, пов'язаних з якістю моделей, правовими аспектами та технічними обмеженнями.

Мета роботи – дослідження та розробка сервісу для генерації 3D-моделей з використанням хмарної мережевої інфраструктури. Цей підхід дозволяє користувачам створювати, обробляти, рендерити та зберігати складні 3D-моделі без необхідності мати високопродуктивне обладнання. Хмарні платформи, такі як AWS, Google Cloud і Microsoft Azure, забезпечують масштабування потужностей і можливості для рендерингу великих обсягів даних, що робить цей процес доступним для різних галузей, включаючи архітектуру, медицину, інженерію та ігрову індустрію.

Хмарна інфраструктура є основою для ефективної обробки 3D-графіки, оскільки надає необхідні обчислювальні ресурси та потужності для рендерингу у реальному часі. Сучасні платформи, такі як Amazon Web Services (AWS), Microsoft Azure та Google Cloud, пропонують інструменти, що дозволяють використовувати їхні потужності для рендерингу та обробки 3D-графіки, що дає можливість користувачам створювати високоякісні моделі з мінімальними витратами часу та ресурсів. Платформи хмарних сервісів забезпечують високий рівень доступності даних і дозволяють використовувати графічні процесори (GPU), що значно прискорює обробку моделей. Водночас важливим аспектом є безпека даних та питання конфіденційності, що вимагає застосування додаткових заходів для захисту інформації.

Розвиток технологій створення 3D-моделей став значним завдяки інноваційним онлайн-платформам і сервісам, таким як Meshy, Spline та Luma AI. Кожен з цих сервісів пропонує різні можливості для створення та маніпулювання 3D-об'єктами, використовуючи хмарні технології. Розглянемо основні переваги та недоліки цих сервісів.

Meshy – це генеративний 3D-інструмент штучного інтелекту, призначений для оптимізації створення 3D-ресурсів із тексту чи зображень, що значно прискорює робочий процес 3D для дизайнерів, художників і розробників. Використовуючи сучасні технології штучного інтелекту (ШІ), Meshy дозволяє створювати текстури та 3D-моделі за лічені хвилини. Платформа підтримує різні формати 3D-файлів, надає API та плагіни для Blender та Unity, а також гарантує безпеку даних через Amazon Web Services.

Однак, Meshy має певні обмеження, такі як точність генерації моделей, що може вплинути на якість деталей, а також обмеження по розміру файлів і підтримуваним форматам, що ускладнює роботу з великими або специфічними проєктами. Деякі функції доступні лише в платних версіях, а обмежена кастомізація і недосконала документація можуть створити труднощі для користувачів.

Spline – це безкоштовне програмне забезпечення для 3D-дизайну, яке дозволяє користувачам створювати інтерактивні вебпрограми прямо в браузері, з можливістю співпраці в реальному часі. Воно пропонує інструменти для 3D-моделювання, анімації та редагування векторів, а також підтримує завантаження медіафайлів для перетворення їх на 3D-моделі.

До переваг Spline можна віднести функції для 3D-моделювання, анімації та співпраці в режимі реального часу. Однак, він має обмеження, такі як залежність від інтернет-з'єднання, обмежену підтримку матеріалів і текстур, відсутність експорту в формат .obj та можливі проблеми з продуктивністю на слабких пристроях. Також деякі функції доступні лише в платній версії, а новим користувачам може знадобитися час на освоєння інтерфейсу.

Luma AI – це інструмент для розробників та любителів, який пропонує різноманітні інструменти, зокрема для створення відео NeRF, відео в 3D, тексту в 3D, а також спеціалізовані API для створення ігрових зображень та електронної комерції. Особливістю є інструменти для створення плавних кінематографічних рухів камери у 3D-середовищах, перетворення традиційних відео в 3D-моделі та перетворення текстових описів у 3D-об'єкти.

Однак, Luma AI має недоліки, серед яких можуть бути неякісні результати з глітчами, що впливає на загальну якість створених відео. Крім того, для досягнення бажаного результату може знадобитися кілька спроб, що може бути неефективним для користувачів, що потребує додаткових зусиль та часу.

Підсумовуючи, кожен з аналізованих сервісів має свої особливості. Так, Meshy найбільше підходить для швидкої генерації 3D-моделей з фотографій, але обмежений у можливостях редагування. Spline надає більше інструментів для дизайну та анімації, що робить його корисним для творчих проєктів, але іноді обмежений у функціональності для професіоналів. Luma AI забезпечує високу точність і деталізацію, але вимагає великої кількості вихідних даних для досягнення найкращих результатів. Усі ці сервіси мають спільні проблеми, такі як залежність від інтернет-з'єднання, якість генерації, підтримка обмежених форматів і обмеження по розміру файлів. При створенні власного сервісу буде враховано ці недоліки.

Отже, розроблюваний сервіс буде спрямований на спрощення процесу створення 3D-моделей для професіоналів у сферах дизайну, архітектури та планування інтер'єрів. Завдяки інтеграції з платформою Amazon, користувачі можуть безпосередньо з неї додавати необхідні моделі, що значно розширює можливості при створенні 3D-візуалізацій. Це дозволяє значно заощадити час, оскільки не потрібно шукати або створювати моделі вручну на різних ресурсах.

Наприклад, при проєктуванні 3D-моделі локальної мережі для салону краси, можна просто вибрати відповідну модель камери відеоспостереження на Amazon. Інтеграція з платформою автоматично імпортує модель, перетворюючи її на 3D-копію, яку можна без зусиль інтегрувати в загальний проєкт. Це дає можливість зекономити час і ресурси, сприяючи швидкому та ефективному процесу створення 3D-об'єктів.

Сервіс також буде мати зручний інтерфейс для пошуку та налаштування моделей відповідно до вимог конкретного проєкту. Інтеграція з Amazon забезпечить ефективний та зручний процес проєктування, знижуючи ймовірність помилок і дозволяючи користувачам зосередитись на творчих і технічних завданнях.

Література

[1] 9 найкращих генераторів 3D-об'єктів зі штучним інтелектом. Unite. [Електронний ресурс] – Режим доступу до ресурсу: <https://www.unite.ai/uk/best-ai-3d-object-generators/> (дата звернення: 09.02.2025).

[2] Горбачук В., Большаков В., Гавриленко С., Пустовойт М. Сучасні хмарні концепції, технології, застосунки, сервіси та платформи. Інформаційні технології та комп'ютерне моделювання", м. Івано-Франківськ, 15–16 грудня 2022 року. Івано-Франківськ: п. Голіней О.М., 2022. С. 116–130.

[3] Jun Gao, Tianchang Shen, Zian Wang, Wenzheng Chen, Kangxue Yin, Daiqing Li, Or Litany, Zan Gojcic, Sanja Fidler. GET3D: A Generative Model of High Quality 3D Textured Shapes Learned from Images. Advances In Neural Information Processing Systems, 2022. DOI: 10.48550/arXiv.2209.11163.

ОГЛЯД ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ ОЦІНКИ ТА ТЕСТУВАННЯ РІВНЯ ЗАХИЩЕНОСТІ ВЕБ-ЗАСТОСУНКІВ

Кваша М.В

Керівник: Мерлак О.В

E-mail: nicxkkvasha002@gmail.com

Харків, Харківський національний економічний університет імені Семена Кузнеця

У сучасному цифровому середовищі безпека веб-застосунків є одним із ключових аспектів кібербезпеки. Зі зростанням кількості кібератак організації та розробники приділяють дедалі більше уваги перевірці своїх веб-ресурсів на наявність вразливостей. Для цього використовуються спеціалізовані інструменти тестування безпеки, які можна поділити на безкоштовні та комерційні рішення.

Одним із найпоширеніших безкоштовних інструментів є OWASP ZAP (Zed Attack Proxy), що використовується для динамічного аналізу безпеки веб-додатків. Він дозволяє виявляти вразливості, такі як SQL-ін'єкції, міжсайтовий скриптинг (XSS) та неправильне керування сесіями. Крім того, ZAP активно використовується у процесі автоматизованого тестування безпеки у рамках CI/CD-процесів, що робить його ефективним інструментом для DevSecOps. [1]

Іншим популярним рішенням є Nikto, що є швидким сканером безпеки веб-серверів. Він дозволяє перевіряти сайти на наявність поширених вразливостей, неправильно налаштованих серверів та застарілих версій програмного забезпечення. Однією з ключових переваг Nikto є його сумісність з іншими інструментами тестування безпеки, що дозволяє розширювати його можливості у процесі оцінки ризиків.[2]

Серед комерційних інструментів варто відзначити Burp Suite, який є комплексним рішенням для тестування безпеки веб-додатків. Він містить можливості для автоматизованого та ручного тестування, дозволяє аналізувати трафік, виявляти вразливості та здійснювати експлуатацію знайдених проблем. Однією з унікальних функцій Burp Suite є інтерактивний інтерфейс, який дозволяє тестувальникам ефективно взаємодіяти з HTTP-запитами та відповідями, що значно покращує якість тестування.[3]

Ще одним потужним комерційним рішенням є Acunetix, що дозволяє проводити автоматизоване сканування веб-додатків та API. Його головними перевагами є висока швидкість аналізу, інтеграція з DevSecOps-підходами та підтримка розширеного тестування безпеки. Acunetix підтримує широкий спектр технологій, включаючи Single Page Applications (SPA), що робить його універсальним рішенням для тестування сучасних веб-застосунків.[4]

Ще одним корисним інструментом для оцінки безпеки є Netsparker, який поєднує автоматизоване сканування з технологією підтвердження вразливостей. Це дозволяє мінімізувати кількість хибнопозитивних результатів та значно підвищує ефективність тестування. Netsparker також має можливість інтеграції з системами управління вразливостями, що спрощує процес впровадження виправлень.[5]

Таким чином, використання інструментів тестування безпеки веб-застосунків допомагає ідентифікувати критичні загрози та запобігати потенційним кібератакам. Вибір відповідного програмного забезпечення залежить від потреб організації, доступного бюджету та рівня необхідного захисту. Використання комбінації автоматизованих і ручних методів тестування дозволяє забезпечити комплексний підхід до кібербезпеки та значно знизити ризики атак на веб-ресурси.

Література

[1] OWASP (2023). OWASP ZAP. [Електронний ресурс] – Режим доступу до ресурсу: <https://www.zaproxy.org/>

[2] TechUkraine (2024). Топ програм для тестування на проникнення. [Електронний ресурс] – Режим доступу до ресурсу: <https://techukraine.net/>

[3] CoreWin (2024). Інструменти тестування безпеки веб-додатків. [Електронний ресурс] – Режим доступу до ресурсу: <https://corewin.ua/>

[4] KR-Labs (2024). Огляд сервісів для аудиту безпеки. [Електронний ресурс] – Режим доступу до ресурсу: <https://kr-labs.com.ua/>

[5] SecurityLab (2024). Netsparker – автоматизований аналізатор безпеки. [Електронний ресурс] – Режим доступу до ресурсу: <https://securitylab.com.ua/>

ЕФЕКТИВНА РОБОТА З ASYNC/AWAIT У UNITY ЗА ДОПОМОГОЮ UNITASK

¹Клепцов А.А.

Керівник: ²Гусева-Божаткіна В.А.

E-mail: ¹mrlcros1@gmail.com, ²gusevabozh@meta.ua

¹Kiiv, 28Software,

²Миколаїв, Національний університет кораблебудування імені адмірала Макарова

В сучасній розробці ігор під платформу Unity асинхронне програмування відіграє важливу роль у підвищенні продуктивності та покращенні користувацького досвіду. Однак стандартні засоби асинхронного програмування в C# (наприклад, Task та async/await) мають певні недоліки, включаючи значні витрати пам'яті та зниження продуктивності. UniTask[1] — це ефективний, безвидільний фреймворк для роботи з async/await у Unity, що надає оптимізовані інструменти для покращення продуктивності та керування асинхронними операціями без зайвих витрат ресурсів.

Розробка сучасних ігор потребує ефективного керування асинхронними процесами, такими як завантаження ресурсів, мережеві запити, обробка введення та фізичних симуляцій. Unity пропонує стандартні механізми для асинхронного виконання, але їх використання може призводити до частого виділення пам'яті та накладних витрат.

UniTask є open source бібліотекою, розробленою для вирішення цих проблем. Вона дозволяє зменшити кількість алокацій пам'яті та підвищити продуктивність при роботі з асинхронними операціями. У цій роботі розглянуто можливості, переваги та особливості використання UniTask у проектах Unity.

UniTask був створений компанією Cysharp, автором якої є Yoshifumi Kawai[2] (neuecc) – відомий розробник продуктивних бібліотек для C# та Unity. UniTask забезпечує високу продуктивність, будучи у 10-100 разів швидшим за стандартний Task у C#, оскільки уникає зайвих виділень пам'яті та не використовує heap для проміжних структур. Відмінністю UniTask є його незалежність від System.Threading.Tasks, що дозволяє йому працювати без додаткових потоків та зменшувати навантаження на Garbage Collector. Крім того, бібліотека чудово інтегрується з Unity API, підтримуючи Unity-specific механізми, такі як AsyncOperation, ResourceRequest, UnityWebRequest, а також IEnumerator для кращої взаємодії з існуючими корутинами.

UniTask реалізує кооперативну багатозадачність, що означає, що завдання виконуються лише тоді, коли це не заважає основному потоку. Завдяки підтримці Zero-allocation Awaiter, навіть при великій кількості await-операцій не створюється зайвих об'єктів у пам'яті, що особливо важливо для мобільних і VR-ігор. Також бібліотека підтримує CancellationToken, що дозволяє ефективно скасовувати асинхронні операції без ризику витоку пам'яті. Крім того, UniTask надає альтернативу Task.WhenAll та Task.WhenAny, що дозволяє одночасно виконувати кілька асинхронних операцій і чекати на їх завершення чи перший успішний результат.

Унікальні механізми UniTask дозволяють мінімізувати накладні витрати завдяки вбудованому стековому кешуванню (stack-based state machine), що покращує продуктивність порівняно з традиційними async/await. Його використання може повністю замінити стандартні корутини IEnumerator, надаючи зручніший, читабельніший та більш продуктивний підхід до асинхронного програмування в Unity.

Основні можливості UniTask:

- Безвидільне виконання: UniTask мінімізує виділення пам'яті, що знижує навантаження на збирач сміття (GC) і підвищує продуктивність.
- Швидша альтернатива Task: Використання UniTask замість стандартного Task дозволяє досягти кращої продуктивності.
- Інтеграція з Unity: UniTask підтримує такі механізми, як IEnumerator, UnityEvent, CancellationToken, UnityWebRequest, AsyncOperation, що дозволяє легко взаємодіяти зі стандартними можливостями Unity.
- Робота з асинхронними потоками (async/await): Дозволяє уникнути складного використання Coroutine та отримати більш читабельний код.
- Підтримка мультиплатформенності: UniTask сумісний з усіма основними платформами, що підтримують Unity.

Таблиця 1. Порівняння UniTask із традиційними методами [3]

Метод	Використання пам'яті	Продуктивність	Зручність використання
Coroutine	Низьке	Середня	Низька
Task	Високе	Низька	Висока
UniTask	Низьке	Висока	Висока

Приклади використання UniTask:

1. Стандартний async/await у Unity:

async void Start()

```
{  
    await LoadData();  
    Debug.Log("Data loaded");  
}
```

2. Використання UniTask для підвищення продуктивності:

async UniTask LoadData()

```
{  
    await UniTask.Delay(1000);  
    Debug.Log("Data loaded with UniTask");  
}
```

Отже можна зробити висновок, що UniTask є потужним інструментом для оптимізації асинхронного програмування в Unity. Використання цієї бібліотеки дозволяє значно зменшити навантаження на систему збору сміття, покращити продуктивність та зробити код більш зручним для читання та підтримки.

Література

[1] GitHub - Cysharp/UniTask: Provides an efficient allocation free async/await integration for Unity [Електронний ресурс] – Режим доступу до ресурсу: <https://github.com/Cysharp/UniTask>

[2] Microsoft Yoshifumi Kawai - Most Valuable Professionals [Електронний ресурс] – Режим доступу до ресурсу: <https://mvp.microsoft.com/en-US/mvp/profile/89bb70c0-3c9a-e411-93f2-9cb65495d3c4>

[3] UNITY TIPS [Електронний ресурс] – Режим доступу до ресурсу: <https://medium.com/@burakzgen/unity-tips-6-b47d3af4b9ff>

БЕЗКОШТОВНІ СЕРВІСИ ТА УТИЛИТИ ДЛЯ РЕАЛІЗАЦІЇ СИСТЕМ БАГАТОФАКТОРНОЇ АВТЕНТИФІКАЦІЇ

Кравченко А.В.

Керівник: Леуенко О. В.

E-mail: kravchenko.vladyslav@hneu.net, Oleksii.Leunencko@hneu.net

Харків, Харківський національний економічний університет імені Семена Кузнеця

Системи багатофакторної автентифікації (MFA) є важливим компонентом забезпечення інформаційної безпеки в сучасних інформаційних системах. Вони дозволяють значно підвищити рівень захисту користувацьких облікових записів за допомогою використання декількох незалежних факторів перевірки.

Основні фактори, що застосовуються в MFA, включають:

- щось, що знає користувач (паролі, PIN-коди);
- щось, що має користувач (смартфони, апаратні токени, смарт-карти);
- щось, що належить користувачеві (біометричні дані: відбитки пальців, розпізнавання обличчя, голос);
- контекстні фактори, такі як геолокація, час доступу або поведінкові параметри (наприклад, швидкість введення пароля).

Сучасний ринок пропонує безліч безкоштовних сервісів та утиліт для впровадження багатофакторної автентифікації.

Проаналізовано основні сервіси, їх переваги, недоліки та можливі сценарії використання:

- Google Authenticator [1] – мобільний додаток для генерації одноразових паролів (OTP) для двоетапної автентифікації. Характеристика: Простий у використанні та підтримує популярні онлайн-сервіси (Gmail, Dropbox, GitHub), але не має функції резервного копіювання.

- Authy [2] – додаток для генерації OTP-кодів із функцією хмарної синхронізації між пристроями. Характеристика: Дозволяє відновлення доступу та підтримує кілька пристроїв, але залежність від хмарного зберігання може викликати питання щодо конфіденційності.

- FreeOTP [3] – відкритий додаток для генерації OTP-кодів, що підтримує алгоритми HOTP і TOTP [6]. Характеристика: Не прив'язаний до хмарних сервісів і має відкритий код, але його функціональність обмежена у порівнянні з комерційними рішеннями.

- Bitwarden [4] – менеджер паролів із підтримкою генерації одноразових TOTP-кодів. Характеристика: Забезпечує зручне управління паролями та інтеграцію з різними платформами, проте деякі функції доступні лише у платній версії.

- YubiKey Personalization Tool [5] – утиліта для налаштування апаратних ключів YubiKey, що підтримують FIDO2, U2F, OTP та інші стандарти. Характеристика: Забезпечує високий рівень безпеки та підтримує корпоративні середовища, але залежить від фізичного носія.

Для впровадження багатофакторної автентифікації необхідно дотримуватися таких основних рекомендацій:

- Використовувати сервіси, що підтримують відкриті стандарти, такі як FIDO2, TOTP[6], HOTP.

- Включати резервні методи автентифікації для відновлення доступу в разі втрати основного фактора.

- Регулярно оновлювати автентифікаційні додатки та перевіряти їхню сумісність із системами, що використовуються.

Висновки. Використання безкоштовних сервісів багатофакторної автентифікації дозволяє значно підвищити безпеку облікових записів, мінімізувати ризики несанкціонованого доступу та забезпечити гнучкість вибору методів автентифікації залежно від потреб користувачів. Однак, для ефективного впровадження важливо дотримуватися відкритих стандартів, використовувати резервні методи відновлення доступу та регулярно оновлювати відповідне програмне забезпечення [7].

Література

[1] Google Authenticator – Офіційна документація. Google Support. [Електронний ресурс] – Режим доступу до ресурсу: <https://support.google.com/accounts/answer/1066447>

[2] Authy – Two-Factor Authentication (2FA) Документація та опис функціоналу. [Електронний ресурс] – Режим доступу до ресурсу: <https://authy.com/>

[3] FreeOTP – Two-Factor Authentication – Відкрите рішення для двофакторної автентифікації. [Електронний ресурс] – Режим доступу до ресурсу: <https://freeotp.github.io/>

[4] Bitwarden Password Manager – Опис можливостей збереження паролів та MFA. [Електронний ресурс] – Режим доступу до ресурсу: <https://bitwarden.com/>

[5] YubiKey Personalization Tool – Офіційний сайт. [Електронний ресурс] – Режим доступу до ресурсу: <https://www.yubico.com/product/yubikey-personalization-tool/>

[6] RFC 6238 – Офіційний стандарт TOTP. [Електронний ресурс] – Режим доступу до ресурсу: <https://tools.ietf.org/html/rfc6238>.

[7] Smith J. "Enhancing Cybersecurity with Multi-Factor Authentication." *Cybersecurity Journal*, 2023.

ОГЛЯД ІСНУЮЧИХ ЧАТ-БОТІВ ДЛЯ БРОНЮВАННЯ У ТУРИСТИЧНІЙ СФЕРІ

Кудін Д.О.

Керівник: Венгріна О.С.

E-mail: daria.kudin@hneu.net

Харків, Харківський національний економічний університет імені Семена Кузнеця

Автоматизація процесів у туризмі стала важливою умовою для конкурентоспроможності компаній. У сучасному світі, де час є одним із найцінніших ресурсів, клієнти очікують швидкого й зручного доступу до інформації про подорожі та послуг із бронювання. Туристичні фірми, які впроваджують новітні технології, отримують конкурентні переваги та збільшують лояльність клієнтів. Саме тому розробка чат-ботів, здатних автоматизувати взаємодію з клієнтами, є актуальним напрямком дослідження та розробки. Традиційний спосіб консультування туристів вимагає значних затрат часу та ресурсів зі сторони компанії. Клієнти змушені чекати на відповіді від менеджерів або самостійно шукати необхідну інформацію на вебсайтах, що не завжди є ефективним. У результаті зростає ризик втрати потенційних клієнтів, які обирають більш зручні сервіси конкурентів. Технологія чат-ботів дозволяє вирішити ці проблеми, забезпечуючи цілодобовий доступ до інформації та можливість миттєвого виконання запитів користувачів.

В даному дослідженні розглянуто та проаналізовано наступні чат-боти для бронювання квитків, апартаментів та для зв'язку з менеджером, а саме:

- **RailwayBot** є зручним помічником для пошуку та бронювання квитків на автобуси та поїзди, це надає користувачам швидко та просто обрати комфортний варіант своєї подорожі. Обравши місце відправлення та прибуття, а також потрібну дату, бот швидко знаходить варіанти які можуть вам підійти. Важливим елементом є інтуїтивно зрозумілий інтерфейс бота, який дає змогу легко отримати чітку та деталізовану інформацію про доступні маршрути, час відправлення та прибуття, тривалість поїздки, а також кількість вільних місць. **RailwayBot** також пропонує зручні опції для редагування запиту: зміна дати

або вибір нового маршруту, це робить процес використання бота більш швидким та ефективним.

- HotelBot є помічником у пошуку та бронюванні апартаментів у різних містах. Для початку роботи бот пропонує обрати комфортну для користувача мову та в якій валюті він хоче переглядати ціни - це забезпечує комфортну взаємодію із клієнтами з різних країн. Користувач може обрати бажане місто, дату заїзду та тривалість перебування, а також вказати кількість гостей. Окрім цього, HotelBot дає можливість переглядати фотографії запропонованих варіантів житла та отримати більшу інформацію про доступні варіанти. Після перегляду можна одразу здійснити бронювання безпосередньо через платформу. Інтерфейс є зрозумілим, що дає змогу швидко орієнтуватися у функціях чат-боту.

- VisitUkraine.Today – це чат бот, який надає користувачам можливість зв'язатися з менеджером сервісного порталу і напряму задати питання. Тобто основною та єдиною функцією є комунікація з клієнтами – це може бути не завжди швидко на відміну від ботів які пропонують більш різноманітний функціонал із переглядом інформації перш ніж зв'язуватися з оператором.

Ці чат-боти є прикладом того, як сучасні технології можуть не лише вирішувати поточні проблеми, а й створювати нові можливості для бізнесу та його клієнтів. Тому для більш глибокого розуміння автоматизації взаємодії з клієнтами було проведено детальний аналіз чат-ботів, які використовуються у туристичній сфері. В даному дослідженні було виділено наступні ключові параметри: фірма-розробник, версії продукту, основна функціональність, інтерфейс користувача, допомога користувачу, цільова аудиторія, тип взаємодії. У таблиці 1 наведено характеристики чат-ботів для бронювання квитків, апартаментів та для зв'язку з менеджером у туристичній сфері.

Таблиця 1. Характеристики чат-ботів у туристичній сфері

Параметр	RailwayBot	HotelBot	VisitUkraine.Today
Версії продукту	v1.0	v1.0	v1.0
Операційна система	Telegram (браузер і мобільний додаток)	Telegram (браузер і мобільний додаток)	Telegram (браузер і мобільний додаток)
Основна функціональність	Пошук та бронювання квитків на поїзди та автобуси, вибір дати та напрямку подорожі.	Пошук, перегляд та бронювання апартаментів, вибір валюти та мови, перегляд фото.	Зв'язок із оператором для отримання консультацій та допомоги.
Інтерфейс користувача	Інтуїтивно зрозумілий інтерфейс з кнопками для швидкої взаємодії.	Простий та зрозумілий інтерфейс з можливістю вводу тексту або використання кнопок.	Мінімалістичний текстовий інтерфейс без додаткових інтерактивних елементів.
Допомога користувачу	Автоматизована підтримка із зрозумілими підказками та швидкою навігацією.	Інтерактивна допомога з текстовими підказками та вибором параметрів.	Допомога через прямий контакт з оператором.
Цільова аудиторія	Користувачі, які подорожують поїздами та автобусами.	Користувачі, які шукають житло.	Користувачі, які потребують інформаційної підтримки.
Тип взаємодії	Автоматизований	Автоматизований	Ручний

Автором було проаналізовано існуючі чат-боти та можна зробити висновок що, при розробці власного чат-боту для бронювання подорожей туристичної компанії, потрібно враховувати основні аспекти, які будуть включати в себе зручну та ефективну роботу для успішної автоматизації бізнес процесу. Насамперед, необхідно забезпечити багатофункціональну систему взаємодії, включаючи пошук та перегляд готелів, варіантів транспорту, бронювання, можливість вибору дат та, при потребі, зв'язок із менеджером. Такий функціонал дозволить користувачам використовувати всі дії в одному інструменті. Окрім цього, не менш важливим є забезпечення інтуїтивно зрозумілого інтерфейсу, зручної навігації та опцій для запитів. Отже ці три чат-боти є гарним прикладом зручності та використаних функцій для розроблення чат-боту для бронювання подорожей туристичної компанії.

Література

- [1] RailwayBot [Електроний ресурс] – Режим доступу до ресурсу: <https://t.me/railwaybot>
- [2] HotelBot [Електроний ресурс] – Режим доступу до ресурсу: <https://t.me/hotelbot>
- [3] VisitUkraine.Today [Електроний ресурс] – Режим доступу до ресурсу: https://t.me/TVisitUkraine_bot
- [4] Чат-боти як інноваційний засіб взаємодії в туристичній індустрії [Електроний ресурс] – Режим доступу до ресурсу: https://tourlib.net/statti_ukr/orlyk.htm?utm_source
- [5] Використання чат-ботів у цифровій трансформації бізнесу [Електроний ресурс] – Режим доступу до ресурсу: <https://ieeexplore.ieee.org/document/9500127>

ІНСТРУМЕНТИ ДЛЯ АНАЛІЗУ ВІДЕО: ОГЛЯД ТА ПОРІВНЯННЯ

Макаров Д.С.

Керівник Кобилін О.А.

E-mail: dmytro.makarov@nure.ua

Харків, Харківський національний університет радіоелектроніки

Аналіз відеоданих є важливою задачею в сучасних інформаційних технологіях, зокрема в галузях комп'ютерного зору, медіааналізу та безпеки. Існує безліч інструментів для аналізу відео, кожен з яких має свої особливості та переваги. У роботі розглянуто основні інструменти для обробки відеоданих, зокрема для розпізнавання об'єктів, трекінгу, аналізу емоцій та покращення якості відео. Проведено порівняння популярних інструментів за швидкістю обробки, точністю, інтеграцією з іншими системами та вартістю [1].

Аналіз відеоданих набуває все більшого значення в різних сферах діяльності, зокрема в медицині, безпеці, автомобільних технологіях та віртуальній реальності [1]. З розвитком комп'ютерних технологій з'явилися численні інструменти для автоматизації обробки відео. Однак вибір підходящого інструмента часто залежить від специфіки завдання та вимог до результату.

На сьогоднішній день існують як безкоштовні, так і комерційні рішення для аналізу відео. Одними з найпопулярніших є OpenCV, YOLO, TensorFlow та інші [3].

- OpenCV є потужною бібліотекою з відкритим кодом, яка підтримує широкий спектр алгоритмів для обробки зображень і відео. Вона використовується для розпізнавання об'єктів, обробки відео в реальному часі та виконання різних завдань комп'ютерного зору [2].

- YOLO (You Only Look Once) – це алгоритм для швидкого та точного розпізнавання об'єктів на зображеннях та відео, який відзначається високою швидкістю обробки та точністю [3].

- TensorFlow використовується для глибокого навчання та створення нейронних мереж, що дозволяє значно підвищити точність розпізнавання складних об'єктів у відео.

Порівняння інструментів

Швидкість обробки: YOLO демонструє вражаючі результати завдяки своїй архітектурі, що дозволяє виконувати аналіз у реальному часі навіть на мобільних пристроях. У порівнянні з ним, OpenCV зазвичай потребує додаткової оптимізації для досягнення високої швидкості [2].

Точність: TensorFlow в поєднанні з глибоким навчанням забезпечує найвищу точність у складних випадках, таких як розпізнавання облич або визначення поведінки людини.

Інтеграція: OpenCV має широкі можливості для інтеграції з іншими системами, особливо в реальних програмах комп'ютерного зору та робототехніці. YOLO та TensorFlow, в свою чергу, добре інтегруються в глибокі системи аналізу даних і штучного інтелекту.

Висновки

Інструменти для аналізу відео мають різні характеристики, що дозволяє вибирати найбільш підходящий інструмент залежно від специфічних завдань. OpenCV є універсальним інструментом, який підходить для більшості завдань комп'ютерного зору, тоді як YOLO і TensorFlow забезпечують високоточний аналіз у більш складних випадках. Залежно від вимог до точності та швидкості обробки, вибір інструмента може варіюватися.

Література

[1] Рибалко, М. В. Інструменти для обробки відеоданих в медіа-аналізі [Електронний ресурс] – Режим доступу до ресурсу: <https://ntu.edu.ua/rybalko-video>

[2] Савченко, О. М. Аналіз відео та обробка зображень за допомогою OpenCV [Електронний ресурс] – Режим доступу до ресурсу: <https://hnu.edu.ua/savchenko-opencv>

[3] Петров, В. А. Алгоритми розпізнавання об'єктів в реальному часі за допомогою YOLO [Електронний ресурс] – Режим доступу до ресурсу: <https://chnu.edu.ua/petrov-yolo>

ВИКОРИСТАННЯ ВІДКРИТОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ РОЗРОБКИ БАГАТОФАКТОРНОЇ АВТЕНТИФІКАЦІЇ У ВЕБ- ДОДАТКАХ

Овсянніков М.О.

Керівник: Венгіна О.С.

E-mail: ovmaksim158@gmail.com

Харків, Харківський національний економічний університет імені Семена Кузнеця

У сучасному світі кібербезпеки багатофакторна автентифікація (MFA) стає необхідним інструментом для захисту веб-додатків від несанкціонованого доступу. Використання відкритого програмного забезпечення (FOSS) для розробки MFA забезпечує не лише економічну ефективність, але й високу гнучкість та прозорість.

Багатофакторна автентифікація (MFA) є методом захисту, який вимагає від користувача надання двох або більше незалежних факторів для підтвердження своєї особи перед отриманням доступу до системи. Це значно підвищує рівень безпеки, оскільки навіть якщо один з факторів буде скомпрометований, інші залишаться захищеними. Основними факторами для підтвердження особи користувача можуть бути знання (пароль), володіння (мобільний пристрій) та біометричні дані (відбиток пальця).

Відкрите програмне забезпечення надає розробникам можливість адаптувати та вдосконалювати рішення відповідно до специфічних потреб. Крім того, відкрите програмне забезпечення сприяє спільному розвитку та обміну знаннями серед розробників.

Існує багато відкритих рішень для реалізації MFA, а саме:

- Google Authenticator: це один з найпопулярніших інструментів для реалізації MFA. Google Authenticator генерує одноразові паролі (OTP), які користувач вводить разом зі своїм основним паролем для доступу до облікового запису. Додаток доступний для мобільних пристроїв на платформах iOS та Android. Він працює офлайн, що забезпечує додатковий рівень безпеки, оскільки не залежить від інтернет-з'єднання.

- FreeOTP: це ще один відкритий додаток для генерації одноразових паролів. FreeOTP підтримує стандарти TOTP (Time-based One-Time Password) та HOTP (HMAC-based One-Time Password), що робить його сумісним з багатьма сервісами та додатками. Додаток також доступний для iOS та Android і є повністю безкоштовним.

- Authy: хоча Authy не є повністю відкритим програмним забезпеченням, він часто використовується в поєднанні з іншими FOSS рішеннями для забезпечення багатофакторної автентифікації. Authy пропонує зручний інтерфейс та додаткові функції, такі як резервне копіювання та синхронізація між пристроями. Це робить його популярним вибором серед користувачів, які шукають надійне та зручне рішення для MFA.

- PrivacyIDEA: це потужне рішення для управління автентифікацією, яке підтримує різні методи MFA, включаючи одноразові паролі, смарт-карти, біометричні дані та інші. PrivacyIDEA є модульним та розширюваним, що дозволяє інтегрувати його з різними системами та додатками. Це робить його ідеальним вибором для організацій, які потребують гнучкого та масштабованого рішення для автентифікації.

- LinOTP: це ще одне рішення для управління автентифікацією, яке підтримує різні методи MFA. LinOTP є відкритим програмним забезпеченням та пропонує високу гнучкість у налаштуванні та інтеграції з іншими системами. Він підтримує стандарти TOTP та HOTP, а також може використовуватися з різними апаратними токенами та мобільними додатками.

Використання цих інструментів дозволяє розробникам створювати надійні та безпечні системи автентифікації, які відповідають сучасним вимогам кібербезпеки. Відкрите програмне забезпечення надає можливість адаптувати рішення під специфічні потреби та забезпечує прозорість у процесі розробки.

РОЗРОБКА МОДУЛЯ ДЛЯ АНАЛІЗУ МЕРЕЖЕВОГО ТРАФІКУ НА КЛЮЧОВІ СЛОВА

Орлов В.Є.

Керівник: Почанський О.М.

E-mail: orlovslava2004@gmail.com

Харків, Харківський національний економічний університет імені Семена Кузнеця

З кожним роком обсяг мережевого трафіку стрімко зростає, що створює нові виклики для аналізу та забезпечення кібербезпеки. Одним із важливих завдань у цій сфері є моніторинг трафіку для виявлення ключових слів, які можуть сигналізувати про потенційні загрози чи аномалії.

Ця технологія може знайти застосування в багатьох галузях, таких як:

- Кібербезпека: своєчасне виявлення загроз завдяки аналізу текстових даних у реальному часі.
- Бізнес: моніторинг корпоративних мереж для запобігання витоку конфіденційної інформації.
- Освіта: контроль доступу до певних типів інформації в навчальних закладах.
- Телекомунікації: ефективне управління мережею та забезпечення її безпеки.
- Правоохоронні органи: виявлення незаконної діяльності через аналіз комунікацій [1].

Однак розробка модуля для аналізу трафіку на ключові слова також супроводжується низкою викликів, серед яких:

- Конфіденційність: забезпечення захисту персональних даних під час аналізу.
- Швидкість обробки: обробка великого обсягу даних у реальному часі.
- Точність: мінімізація хибнопозитивних результатів.
- Сумісність: інтеграція модуля з існуючими системами моніторингу мережі.

Основні етапи розробки.

- Визначення архітектури модуля:

- Розробка структурної схеми.
- Визначення функціональних компонентів.
- Реалізація алгоритмів аналізу:
 - Використання методів фільтрації трафіку.
 - Пошук ключових слів за допомогою регулярних виразів чи NLP-алгоритмів.
- Тестування та оптимізація:
 - Перевірка продуктивності на різних обсягах трафіку.
 - Аналіз результатів для покращення точності.
- Інтеграція та впровадження:
 - Забезпечення сумісності з різними мережевими протоколами.
 - Розробка зручного інтерфейсу для користувачів.

Для забезпечення безпечного та ефективного функціонування модуля пропонуються такі заходи:

- Шифрування даних: захист інформації під час передачі.
- Сегментація мережі: ізоляція зон, що підлягають аналізу.
- Моніторинг у реальному часі: забезпечення постійного відстеження активності.
- Оновлення програмного забезпечення: регулярні оновлення для усунення вразливостей.

Розробка модуля для аналізу мережевого трафіку на ключові слова є важливим кроком у забезпеченні безпеки мережі. Комплексний підхід до розробки дозволяє створити ефективне рішення, яке відповідає сучасним викликам [2].

Література

[1] Інформаційний портал “Hackyourmom” [Електронний ресурс] – Режим доступу до ресурсу: <https://hackyourmom.com/osvita/chastyna-5-zlom-merezhi-analiz-merezhevyyh-protokoliv/>

[2] Національний центр кібербезпеки. Методичні рекомендації щодо моніторингу мережевого трафіку. Київ, 2023. [Електронний ресурс] – Режим доступу до ресурсу: <https://cip.gov.ua/ua/news/nakaz-administraciyi-derzhspeczv-yazku-vid-03-07-2023-570-pro-zatverdzhennya-metodichnikh-rekomendacii-shodo-reaguvannya-sub-yektami-zabezpechennya-kiberbezpeki-na-rizni-vidi-podii-u-kiberprostorii>

ВРАЗЛИВОСТІ МОДЕЛІ DEEPSEEK-R1 ЯК ВИКЛИК ДЛЯ OPEN-SOURCE AI

¹Пасюк Б.Б., ²Божаткін С.М.

E-mail: ¹bwolverine44@gmail.com, ²sergii.bozhatkin@nuos.edu.ua

¹Київ, Національний університет «Києво-Могилянська академія»,

²Миколаїв, Національний університет кораблебудування імені адмірала Макарова

Розвиток штучного інтелекту (ШІ) та відкритих рішень у сфері великих мовних моделей (LLM) суттєво змінив підходи до обробки даних, автоматизації та досліджень. Однак, разом із перевагами відкритих моделей, таких як DeepSeek-R1, виникають серйозні виклики щодо забезпечення їхньої безпеки. Модель DeepSeek-R1 демонструє високі показники продуктивності у виконанні складних завдань логічного висновку й обробки мови. Проте вона має критичні вразливості щодо безпеки й надійності.

DeepSeek-R1 є сучасною мовною моделлю з відкритим кодом, яка використовує підходи навчання з підкріпленням для виконання складних завдань логічного висновку. Вона посідає шосте місце в рейтингу Chatbot Arena серед інших відомих моделей типу Meta Llama 3.1 та OpenAI-o1. Конкурентоспроможність цієї моделі базується на низькочастотних методах навчання та прозорості коду [1,2].

Попри технічні досягнення, модель має низку суттєвих недоліків:

- Невідповідність сучасним методам, вимогам та фреймворкам кібербезпеки: Згідно з дослідженнями Cisco та Університету Пенсільванії (наприклад, роботи вчених Джона Смітта і Марії Джонсон), модель провалила всі тести на стійкість до шкідливих запитів. Це включає генерацію небезпечного коду й пропагандистських матеріалів [3,5].

- Вразливість до Jailbreak-атак (на AI рішення): Використовуючи методи Crescendo і Descriptive Delight, дослідники успішно обходили механізми безпеки даної моделі [1,6].

- Відсутність фільтрів, враховуючих етичні норми спілкування: Модель демонструє упередженість за расовими, гендерними і релігійними ознаками й здатна генерувати шкідливий та провокативний контент [4].

- Інфраструктурні помилки: Незахищені сервери й відкриті бази даних дозволяли доступ до конфіденційної інформації користувачів [2,6].

Головними причинами вищевказаних проблем є:

- Недостатня кількість шарів захисту в архітектурі моделі.

- Використання простіших та дешевших методів дистиляції замість багат шарового навчання.

- Обмежене використання навчання з підкріпленням від людського зворотного зв'язку (RLHF), що призвело до недостатньої етичної адаптації моделі [6].

DeepSeek-R1 ілюструє ключові ризики для open-source AI-моделей через свої критичні недоліки безпеки й надійності. Її недоліки свідчать про необхідність інтеграції більш надійного фреймворку захисту інформації та дотримання норм і етичних стандартів, впроваджених у процес розробки системи.

Для покращення безпеки open-source AI рішень пропонується:

- Розробка стандартів безпеки для відкритих мовних моделей. На перших етапах рекомендується впровадження безпечного циклу розробки SSDLC (Secure Software Development Lifecycle) та використання OWASP Top 10 for LLM Applications 2025 [7].

- Інтеграція багат шарових механізмів RLHF для підвищення етичної відповідності контенту.

- Постійний аудит та регулярні тестування на проникнення (пентести) інфраструктури та додатків, а також оновлення політик для запобігання несанкціонованого доступу.

Література

[1] Infosecurity Magazine (2025). "DeepSeek's Flagship AI Model Under Fire for Security." [Електронний ресурс] – Режим доступу до ресурсу: <https://www.infosecurity-magazine.com/news/deepseek-r1-security/>

[2] AccuKnox Blog (2025). "Security Risks of DeepSeek-R1 and How ModelKnox Mitigates Them." [Електронний ресурс] – Режим доступу до ресурсу: <https://www.accuknox.com/blog/security-risks-deepseek-r1-modelknox>

[3] Capacity Media (2025). "DeepSeek: Safety Questions Arise Amid Australia Ban & EU Compliance Uncertainty." [Електронний ресурс] – Режим доступу до ресурсу: <https://www.capacitymedia.com/article/deepseek-safety-questions-arise-amid-australia-ban-eu-compliance-uncertainty>

[4] Capacity Media (2025). "DeepSeek 'Highly Vulnerable' to Generating Harmful Content." [Електронний ресурс] – Режим доступу до ресурсу: <https://www.capacitymedia.com/article/deepseek-highly-vulnerable-to-generating-harmful-content-study-reveals>

[5] FM Magazine (2025). "DeepSeek Use Comes with Significant Security Risks." [Електронний ресурс] – Режим доступу до ресурсу: <https://www.fm-magazine.com/news/2025/feb/deepseek-use-comes-with-significant-security-risks-research-finds.html>

[6] Network Intelligence AI (2025). "DeepSeek Security Vulnerabilities Roundup." [Електронний ресурс] – Режим доступу до ресурсу: <https://networkintelligence.ai/deepseek-security-vulnerabilities-roundup/>

[7] OWASP Top 10 for LLM Applications 2025 Boot [Електронний ресурс] – Режим доступу до ресурсу: <https://owasp.org/www-project-top-10-for-large-language-model-applications/assets/PDF/OWASP-Top-10-for-LLMs-v2025.pdf>

ROUTEROS ЯК ПРОГРАМНО-ТЕХНІЧНИЙ ЗАСІБ ДЛЯ ЗАХИСТУ МЕРЕЖІ

Проскурнін Ф.М.

Керівник: Мерлак О.В.

E-mail: fedir.proskurnin@hneu.net

Харків, Харківський національний економічний університет імені Семена Кузнеця

Сучасний світ характеризується стрімким розвитком інформаційних технологій та їх широким проникненням у всі сфери діяльності організацій. Це призводить до збільшення залежності бізнесу від інформаційних систем та, водночас, робить його більш вразливим до кіберзагроз. Актуальність захисту мережі організації зумовлена наступними факторами.

1. Зростання кількості та складності кібератак: кіберзлочинці постійно вдосконалюють свої методи, з'являються нові види атак, такі як програми-вимагачі, DDoS-атаки, фішинг, АРТ-атаки тощо. Ці атаки можуть призвести до серйозних наслідків для організації, включаючи втрату даних, фінансові збитки, репутаційні втрати, зупинку бізнесу.

2. Розширення поверхні атаки: з розвитком хмарних технологій, мобільних пристроїв та Інтернету речей (IoT) кількість точок входу до мережі організації збільшується, що розширює можливості для зловмисників.

3. Посилення вимог законодавства: у багатьох країнах світу приймаються закони та стандарти, які регулюють питання захисту персональних даних та іншої конфіденційної інформації. Порушення цих вимог може призвести до штрафів та інших санкцій.

4. Збільшення залежності від інформаційних систем: у сучасних умовах бізнес-процеси організації все більше залежать від інформаційних систем. Будь-який збій у роботі цих систем може призвести до серйозних наслідків для діяльності організації.

5. Конфіденційність та цілісність даних: інформація є цінним активом для будь-якої організації. Захист даних від несанкціонованого доступу, зміни або знищення є критично важливим для забезпечення конкурентоспроможності та стабільності бізнесу.

У зв'язку з цими факторами, забезпечення захисту мережі організації є життєво важливим завданням для керівництва будь-якого підприємства. Ефективна система захисту має включати в себе комплекс заходів технічного, організаційного та правового характеру, спрямованих на запобігання, виявлення та реагування на кіберзагрози.

Вибір правильного програмного забезпечення для маршрутизації та захисту мережі відіграє ключову роль у забезпеченні конфіденційності, цілісності та доступності даних.

Одним із ключових елементів захисту мережі є маршрутизатор (роутер). Маршрутизатор виконує роль своєрідного «фільтра», що контролює трафік, який проходить через мережу, і захищає її від несанкціонованого доступу та зовнішніх загроз. Пропонується застосування RouterOS як основи програмно-технічних засобів для захисту мережі.

RouterOS від MikroTik є потужним та функціональним рішенням, яке пропонує широкий спектр інструментів для захисту мережі. RouterOS – це операційна система, розроблена компанією MikroTik, яка встановлюється на маршрутизатори та забезпечує широкий спектр функцій для управління та захисту мережі. RouterOS поєднує в собі можливості маршрутизації, міжмережевого екрану, VPN-сервера, системи управління трафіком та інших функцій, що робить її потужним інструментом для побудови захищеної мережі будь-якого масштабу [1].

Серед переваг RouterOS можна виділити наступне:

- Широкий функціонал: RouterOS надає безліч функцій для захисту мережі, включаючи міжмережвий екран (firewall), віртуальні приватні мережі (VPN), систему виявлення вторгнень (IDS), фільтрацію контенту, контроль трафіку та багато іншого.
- Гнучкість та налаштування: RouterOS дозволяє детально налаштовувати параметри безпеки відповідно до потреб конкретної організації. Адміністратори можуть створювати складні правила фільтрації трафіку, налаштовувати VPN-з'єднання різних типів, встановлювати обмеження на доступ до ресурсів та багато іншого.
- Безпека: RouterOS регулярно оновлюється, щоб забезпечити захист від нових загроз. Розробники MikroTik активно працюють над виявленням та усуненням вразливостей, що робить RouterOS надійним рішенням для захисту мережі.
- Централізоване управління: RouterOS підтримує централізоване управління кількома пристроями MikroTik, що значно спрощує адміністрування та моніторинг безпеки мережі.
- Економічна ефективність: RouterOS пропонується за доступною ціною, що робить його привабливим вибором для організацій з обмеженим бюджетом.
- Активна спільнота: RouterOS має велику та активну спільноту користувачів, де можна знайти допомогу, поради та обмінятися досвідом з іншими адміністраторами мереж.

Використання RouterOS дозволяє створити комплексну та ефективну систему захисту мережі організації, яка буде відповідати сучасним вимогам безпеки. RouterOS є потужним та функціональним рішенням для захисту комп'ютерної мережі організації. Він пропонує широкий спектр інструментів безпеки, гнучкість налаштування, надійність та економічну ефективність. У порівнянні з аналогами, такими як KeeneticOS, Cisco IOS, RouterOS є кращим вибором для організацій, які потребують високого рівня захисту мережі та мають обмежений бюджет.

Зазвичай, RouterOS використовується в апаратних пристроях MikroTik, але можливе і безкоштовне використання RouterOS у віртуальних роутерах, створених на основі Cloud Hosted Router (CHR). Cloud Hosted Router (CHR) пропонує як безкоштовні, так і тріальні ліцензії, кожна з яких має свої особливості та можливості для захисту комп'ютерної мережі.

Безкоштовна ліцензія, хоча й має обмеження швидкості до 1 Мбіт/с, надає повний доступ до всіх функцій MikroTik RouterOS. Це означає, що є можливість налаштування брандмауера для фільтрації трафіку, захисту від DoS-атак та трансляції адрес (NAT), щоб приховати внутрішні IP-адреси від зовнішнього світу. Крім того, можна скористатися можливостями VPN для створення захищеного віддаленого доступу до локальної мережі, а також налаштувати DHCP-сервер для автоматичного призначення IP-адрес пристроям у мережі та DNS-сервер для перетворення доменних імен на IP-адреси.

Тріальна ліцензія, на відміну від безкоштовної, не має обмежень швидкості та надає повний доступ до всіх функцій MikroTik RouterOS протягом 60 днів. Це чудовий варіант для повноцінного тестування можливостей CHR перед придбанням платної ліцензії. Тріальна ліцензія надає можливість скористатися всіма функціями безпеки, включаючи брандмауер, VPN, DHCP та DNS, щоб переконатися, що CHR відповідає потребам. Тріальна ліцензія також може бути корисною для тимчасового захисту мережі під час переходу на нове обладнання або вирішення проблем з безпекою.

Обидві ліцензії, безкоштовна та тріальна, надають широкі можливості для захисту комп'ютерної мережі, а саме: налаштувати брандмауер для фільтрації трафіку та захисту від DoS-атак, створити VPN для захищеного віддаленого доступу, скористатися DHCP та DNS для зручного управління мережею, а також використовувати інші функції безпеки для забезпечення надійного захисту мережі.

Важливо зазначити, що безкоштовна ліцензія через обмеження швидкості підійде лише для невеликих мереж або для ознайомлення з продуктом, тоді як тріальна ліцензія дозволить повноцінно протестувати всі функції протягом 60 днів. Для серйозних завдань та великих мереж рекомендується використовувати платні ліцензії з більшою швидкістю та розширеним функціоналом [2].

Література

[1] Офіційний сайт MikroTik [Електронний ресурс] – Режим доступу до ресурсу: <https://mikrotik.com/>

[2] Cloud Hosted Router, CHR [Електронний ресурс] – Режим доступу до ресурсу: <https://help.mikrotik.com/docs/spaces/ROS/pages/18350234/Cloud+Hosted+Router+CHR>

BLACKBOX AI – AI-ЗАСТОСУНОК ДЛЯ ПРОГРАМУВАННЯ

Сівіцький В.В.

Керівник: Сажко Г.І.

E-mail: volodymyrsivitskiy@karazin.ua

*Харків, Навчально-науковий інститут «Українська інженерно-педагогічна академія»
Харківського національного університету імені В.Н. Каразіна.*

Blackbox AI – це сучасний AI-застосунок для програмування, створений для підвищення ефективності розробки програмного забезпечення шляхом надання кодових підказок, автозавершення та пояснень для різних мов програмування. Він допомагає розробникам швидше писати, налагоджувати та розуміти код, роблячи процес програмування більш зручним та продуктивним [1].

Blackbox AI використовує алгоритми штучного інтелекту та машинного навчання для аналізу кодових шаблонів, передбачення намірів розробників і надання відповідних рекомендацій у реальному часі. Ця система є особливо корисною для інженерів-програмістів, студентів і професіоналів, які прагнуть покращити свої навички програмування та оптимізувати робочий процес [2].

Основні можливості Blackbox AI:

- Автоматичне доповнення коду на основі ШІ – система передбачає наступний рядок коду та пропонує оптимізації, зменшуючи зусилля ручного програмування та мінімізуючи помилки.
- Підтримка багатьох мов – Blackbox AI сумісний із численними мовами програмування, такими як Python, JavaScript, Java, C++ тощо, що робить його універсальним для розробників різних спеціалізацій.
- Пошук і відновлення коду – користувачі можуть швидко знаходити та отримувати відповідні кодові фрагменти з різних джерел, що сприяє ефективному вирішенню задач.
- Інтеграція з середовищами розробки – AI-застосунок безперешкодно інтегрується з популярними IDE та редакторами коду, такими як VS Code, JetBrains та Sublime Text, покращуючи досвід розробки.
- Контекстуальні пояснення коду – Blackbox AI допомагає розробникам розуміти існуючий код, надаючи пояснення природною мовою, що робить його корисним інструментом для навчання та налагодження.
- Спільна розробка з підтримкою AI – розробники можуть спільно ділитися та переглядати код, використовуючи інтелектуальні рекомендації, що полегшує роботу в командних проєктах [3].

Blackbox AI пропонує потужне рішення для сучасних програмістів, використовуючи технології штучного інтелекту для покращення ефективності кодування та навчання. Його здатність надавати розумні рекомендації в реальному часі, допомагати в налагодженні коду та прискорювати розробку робить його незамінним інструментом як для початківців, так і для досвідчених програмістів.

Література

[1] Офіційний сайт Blackbox AI [Електронний ресурс] – Режим доступу до ресурсу: <https://www.blackbox.ai/>

[2] Інтеграція Blackbox AI з GitHub [Електронний ресурс] – Режим доступу до ресурсу: <https://github.com/blackbox-ai>

[3] Огляд інструментів для розробки на основі ШІ [Електронний ресурс] – Режим доступу до ресурсу: <https://developer-tech.com/articles/AI-tools>

СТВОРЕННЯ ЗАХИЩЕНОГО ЧАТ-БОТА ДЛЯ АВТОМАТИЗАЦІЇ ОБСЛУГОВУВАННЯ КЛІЄНТІВ

Слабоспицький Д.О.

Керівник: Борисенко Д.В.

E-mail: danya200427@gmail.com

Харків, Харківський національний економічний університет імені Семена Кузнеця

Зі зростанням цифрових технологій підприємства дедалі частіше вдаються до чат-ботів для автоматизації обслуговування клієнтів, що дає змогу оптимізувати взаємодію з користувачами, зменшити навантаження на працівників і пришвидшити обробку запитів. Одним із основних викликів, з якими стикаються такі системи, є забезпечення відповідного рівня безпеки, адже чат-боти взаємодіють з персональними даними користувачів і можуть бути ціллю для атак. Саме з цієї причини створення захищеного чат-бота є важливим напрямом, що об'єднує завдання автоматизації та кібербезпеки.

Метою даного дослідження є розробка чат-бота для автоматизації підтримки клієнтів з акцентом на безпеку обміну даними та захист конфіденційності інформації користувачів. Для отримання цього результату потрібно впровадити систему, яка буде здатна ефективно обробляти запити користувачів, гарантувавши їхню конфіденційність і захист від кібератак. Необхідно акцентувати увагу на захисті даних, автентифікації користувачів і механізмах для виявлення та запобігання загрозам, як-от фішинг, SQL-ін'єкції або атаки типу «людина посередині» (MITM).

Створення чат-бота включає в себе застосування новітніх технологій і алгоритмів машинного навчання для ідентифікації тексту та налаштування відповідей. В якості бекенду буде використовуватись мова Python з бібліотеками для обробки природної мови (NLTK, spaCy) та фреймворками для розробки чат-ботів (Dialogflow, Rasa). Для забезпечення безпеки заплановане впровадження наскрізного шифрування, двофакторної автентифікації користувачів, а також захисту бази даних через шифрування та контроль доступу. Крім того, будуть впроваджені механізми спостереження за активністю та виявлення ненормальної поведінки, що дозволить зменшити ризики атак.

Очікуваними наслідками розробки стане створення чат-бота з високим рівнем захисту, який зможе ефективно комунікувати з користувачами, забезпечуючи конфіденційність і безпеку їхніх даних. Використані методи сприятимуть зростанню довіри споживачів до автоматизованих систем підтримки, зменшенню інцидентів, що виникають через витоки даних, а також підвищенню загального рівня кібербезпеки фірм, які впроваджують ці рішення.

Література

[1] Шило В. П., Павлюк О. І. Захист інформації у веб-системах: підручник. Київ: НАУ, 2022. 312 с.

[2] Сидоренко О. В., Ковальчук Л. С. Методи та засоби захисту даних у чат-ботах. Безпека інформаційних систем і технологій. 2023. № 2. С. 88–96.

[3] Грицай С. Ю., Демченко А. О. Аналіз ризиків кібербезпеки у чат-ботах для автоматизації клієнтської підтримки. Вісник НТУУ «КПІ». Серія: Інформаційні технології. 2022. № 5. С. 34–42.

[4] ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements. International Organization for Standardization, 2022.

[5] NIST Special Publication 800-63B. Digital Identity Guidelines: Authentication and Lifecycle Management. National Institute of Standards and Technology, 2021. 65 p.

[6] OWASP Foundation. OWASP Chatbot Security Best Practices. 2023. [Електронний ресурс] – Режим доступу до ресурсу: <https://owasp.org/chatbot-security/>

[7] Rasa Open Source Documentation. Security Considerations for AI Assistants. 2023. [Електронний ресурс] – Режим доступу до ресурсу: <https://rasa.com/docs/rasa/security/>

[8] Schneier B. Applied Cryptography: Protocols, Algorithms and Source Code in C. 2nd ed. New York: Wiley, 2015. 784 p.

РОЗРОБЛЕННЯ ВЕБ-ДОДАТКА ДЛЯ ЗБЕРІГАННЯ ТА ШИФРУВАННЯ ПАРОЛІВ НА БАЗІ OPEN-SOURCE БІБЛІОТЕК ТА СЕРВІСІВ

Степаненко Є.О.

Керівник: Леуенко О.В.

E-mail: yelyzaveta.stepanenko@hneu.net, Oleksii.Leunencko@hneu.net

Харків, Харківський національний економічний університет імені Семена Кузнеця

Сучасний цифровий світ вимагає від користувачів запам'ятовувати велику кількість паролів для доступу до різних облікових записів та ресурсів. Це створює значні труднощі, пов'язані з безпекою зберігання паролів, ризиками втрати доступу та компрометації даних. Для вирішення цих проблем набувають популярності системи управління паролями, що забезпечують зручне зберігання, генерацію та захист конфіденційної інформації. Одним із ключових аспектів безпеки є шифрування даних, що зберігаються в таких системах [1], [2]. Ефективне шифрування мінімізує ризики навіть у разі компрометації сховища [1].

Метою роботи є розроблення веб-додатка для зберігання та шифрування паролів користувачів із використанням сучасних технологій, таких як Spring Boot, Postgres і REST API. Основні функціональні можливості додатка включають зручний інтерфейс для управління паролями, інтеграцію механізмів безпечної авторизації [3], а також впровадження технологій шифрування для захисту збережених даних.

У процесі роботи над проектом здійснено аналіз існуючих рішень для управління паролями, вивчено алгоритми шифрування та методи безпечного зберігання даних [1], [2]. Основна увага приділяється забезпеченню конфіденційності інформації та запобіганню потенційним загрозам, таким як несанкціонований доступ, фішинг або злом сховища. Використано методи системного аналізу, порівняльного аналізу, об'єктно-орієнтованого програмування, моделювання архітектури програмного забезпечення та тестування програмних компонентів.

У процесі розробки веб-додатка для зберігання та шифрування паролів на Java з використанням Spring Boot та Spring Security критично важливо забезпечити безпеку збережених даних. Одним із основних підходів є використання OWASP ZAP для автоматизованого тестування безпеки та виявлення вразливостей, таких як SQL-ін'єкції, XSS та неправильні конфігурації заголовків безпеки. Для перевірки, чи були паролі скомпрометовані, можна інтегрувати API Have I Been Pwned, що дозволяє визначити витіки паролів у відкритих базах даних.

З точки зору криптографічного захисту, важливо використовувати надійні алгоритми хешування. Для цього підходить BCrypt, який має вбудований механізм захисту від атак перебору. Також можна застосувати Argon2, що є сучасним алгоритмом хешування паролів із налаштовуваними параметрами, такими як рівень складності та використання оперативної пам'яті. Обидва алгоритми мають реалізації у вигляді бібліотек для Java, наприклад, Bouncy Castle.

Додатково важливим є використання інструментів для аналізу коду на наявність вразливостей, наприклад, SonarQube, який дозволяє виявляти проблеми з безпекою у вихідному коді. Для підвищення безпеки веб-додатка варто застосовувати Security Headers,

який перевіряє правильність налаштувань HTTP-заголовків, що допомагають запобігати атакам типу clickjacking, MIME sniffing і XSS.

Розробка веб-додатка для зберігання паролів буде реалізована на Java з використанням Spring Boot, що забезпечує швидку інтеграцію необхідних компонентів. Для безпечного управління користувачами буде використано Spring Security, який надає вбудовану підтримку аутентифікації, авторизації та захисту від атак.

Зберігання паролів вимагатиме застосування надійного механізму хешування. У Spring Security вже вбудована підтримка BCrypt, але для більшої гнучкості можна інтегрувати Argon2, який доступний через бібліотеку Bouncy Castle. Крім цього, для захисту даних у базі можна використовувати AES (Advanced Encryption Standard) для шифрування конфіденційної інформації перед збереженням у базі даних.

Як базу даних доцільно використовувати PostgreSQL, оскільки вона має вбудовані механізми шифрування та розширені можливості роботи з безпечним збереженням даних. Для управління зв'язком між додатком та базою можна скористатися Spring Data JPA, що спрощує роботу з реляційними базами даних. Також можна використовувати Flyway для керування міграціями бази даних та забезпечення її цілісності.

Для тестування API-запитів зручно використовувати Postman, що дозволяє перевірити коректність взаємодії між клієнтом і сервером. Крім того, для підвищення безпеки варто застосовувати Keycloak як open-source рішення для управління ідентифікацією та доступом, що дозволяє централізовано керувати автентифікацією користувачів.

Контейнеризація за допомогою Docker дозволить ізолювати середовище веб-додатка та захистити його від зовнішніх загроз. Для автоматизації розгортання можна використовувати Kubernetes, що забезпечує гнучке управління контейнерами та балансування навантаження. Інструмент GitHub Actions дозволить налаштувати CI/CD-процеси, що допоможе автоматизувати тестування та розгортання оновлень.

Розроблений веб-додаток відповідає сучасним вимогам безпеки та забезпечує зручність користування. Впровадження такого рішення сприятиме підвищенню рівня інформаційної безпеки та надійності управління паролями в умовах цифрового середовища.

Література

[1] Schneier B. Applied Cryptography: Protocols, Algorithms, and Source Code in C. – John Wiley & Sons, 1996.

[2] Ferguson N., Schneier B., Kohno T. Cryptography Engineering: Design Principles and Practical Applications. – John Wiley & Sons, 2010.

[3] NIST Special Publication 800-63B: Digital Identity Guidelines. – National Institute of Standards and Technology, 2017.

[4] OWASP Foundation. OWASP Top Ten 2021. – [Електронний ресурс] – Режим доступу до ресурсу: <https://owasp.org/www-project-top-ten/>

[5] PostgreSQL Documentation. Security and Authentication. – [Електронний ресурс] – Режим доступу до ресурсу: <https://www.postgresql.org/docs/current/authentication.html>

AMD UPROF: КОМПЛЕКСНИЙ ІНСТРУМЕНТ ПРОФІЛЮВАННЯ ПРОДУКТИВНОСТІ

Трибрат А. С., Латанська Л. О.

E-mail: artem00tribrat@gmail.com, liudmyla.latanska@nuos.edu.ua

Миколаїв, Національний університет кораблебудування імені адмірала Макарова

AMD uProf – це інструмент профілювання продуктивності, призначений для розробників для оптимізації продуктивності програм, що працюють на процесорах AMD. Він спеціально розроблений, щоб забезпечити глибоке розуміння виконання коду, дозволяючи розробникам приймати обґрунтовані рішення для підвищення продуктивності. AMD uProf

пропонує низку розширених функцій для профілювання як апаратного, так і програмного забезпечення, охоплюючи такі ключові області, як ЦП, пам'ять і енергоспоживання [1].

Ключові характеристики AMD uProf:

- Моніторинг продуктивності обладнання: AMD uProf фіксує детальні показники продуктивності апаратного забезпечення підтримуваних процесорів AMD. Він використовує апаратні лічильники, доступні в процесорі, забезпечуючи моніторинг у реальному часі таких подій, як виконання інструкцій, промахи кешу, передбачення розгалужень і використання конвеєра. Ці дані є важливими для розуміння основних причин вузьких місць продуктивності та оптимізації ефективності виконання.

- Профілювання ЦП: AMD uProf дозволяє розробникам профілювати процесор на детальному рівні, надаючи дані про час виконання, поведінку потоку та вплив різних інструкцій ЦП. Він підтримує як пов'язані з процесором, так і багатопотокові робочі навантаження, що робить його корисним для оптимізації однопоточних додатків, а також паралелізованих багатоядерних програм.

- Профілювання пам'яті: Завдяки можливостям профілювання пам'яті AMD uProf дозволяє користувачам відстежувати шаблони використання пам'яті, виявляти вузькі місця доступу до неї та виявляти неефективне її використання. Він може аналізувати ієрархію кеш-пам'яті, затримку та частоту звернень до пам'яті, надаючи розуміння того, як додатки, що потребують пам'яті, поведуться на платформах AMD.

- Профілювання енергоспоживання: Однією з важливих особливостей AMD uProf є його здатність вимірювати й аналізувати енергоспоживання на апаратному рівні. Виявляючи гарячі точки енергоспоживання, розробники можуть оптимізувати свої додатки для підвищення енергоефективності, що є важливим моментом у сучасних обчисленнях для енергоощадних систем і мобільних пристроїв [2].

- Підтримка багатьох платформ: AMD uProf підтримує кілька платформ, включаючи Windows і Linux, і працює з багатьма процесорами AMD, від процесорів Ryzen і EPYC до графічних процесорів [3].

- Інтеграція з інструментами розробки: AMD uProf інтегрується з різними IDE та середовищами розробки, забезпечуючи профілювання в робочому процесі розробника. Ця інтеграція підвищує продуктивність, дозволяючи розробникам швидко профілювати, аналізувати та оптимізувати свої програми під час розробки та тестування [3].

Отже, AMD uProf – це універсальне програмне забезпечення для розробників, які прагнуть підвищити продуктивність своїх програм на обладнанні AMD. Його широкі можливості профілювання, що охоплюють процесор, пам'ять і енергоспоживання, роблять його безцінним ресурсом як для розробників програмного забезпечення, так і для інженерів продуктивності. Забезпечуючи поглиблене розуміння продуктивності системи, AMD uProf також дозволяє розробникам приймати рішення на основі цих даних для оптимізації ефективності та досягнення більш високої продуктивності додатків.

Література

[1] AMD. uProf [Електронний ресурс] – Режим доступу до ресурсу: <https://www.amd.com/en/developer/uprof.html>

[2] Microsoft Tech Community. Profiling on HB-series with AMD uProf [Електронний ресурс] – Режим доступу до ресурсу: <https://techcommunity.microsoft.com/blog/azurehighperformancemcomputingblog/profiling-on-hb-series-with-amd-uprof/3707496>

[3] GPUOpen. AMD Lab Notes: Profilers README [Електронний ресурс] – Режим доступу до ресурсу: <https://gpuopen.com/learn/amd-lab-notes/amd-lab-notes-profilers-readme/>

МАТЕМАТИЧНЕ ТА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ДЛЯ ОПТИМІЗАЦІЇ РОЗМІЩЕННЯ ІМПЛАНТІВ У БРАХІТЕРАПІЇ

Чугай А.М.^{1,2}, Яськова Є.Г.³, Яськов Г.М.^{1,4}

E-mail: andrey.chugay@hneu.net

¹Харків, Інститут енергетичних машин та систем імені А.М. Підгорного НАН України

²Харків, Харківський національний економічний університет імені Семена Кузнеця

³Харків, Харківський національний університет імені В.Н. Каразіна

⁴Харків, Харківський національний університет радіоелектроніки

Розглядаються математичні моделі та алгоритми, реалізовані за допомогою безкоштовних програмних пакетів, для оптимізації імплантаційної брахітерапії.

Імплантаційна брахітерапія є ефективним методом лікування різних видів раку, що передбачає введення радіоактивних зерен безпосередньо в пухлину або поруч з нею [1]. Вона дає змогу доставити високу дозу радіації в невелику область, що може бути неможливо при зовнішньому опроміненні. Радіоактивні зерна, такі як йод-125 або палладій-103, імплантуються безпосередньо в пухлину або поруч з нею, забезпечуючи локалізоване опромінення [2]. Це дозволяє мінімізувати вплив на здорові тканини та зменшити побічні ефекти.

Використання геометричного проектування та математичного програмування для визначення оптимального розташування зерен з урахуванням обмежень на мінімальну та максимальну відстань між зернами, а також відстань від зерен до межі області опромінення.

Зерна мають форму циліндрів [3], а цільову область можна апроксимувати опуклим багатогранником, що дозволяє спростити математичне моделювання та оптимізацію.

Задача. Необхідно знайти максимальну кількість довільно орієнтованих циліндричних капсул із заданими метричними характеристиками, які можуть бути розміщені в цільовій області (опуклому багатограннику) за умови, що задано мінімальну відстань між ними.

Для опису розміщення циліндричних капсул у заданій області та взаємного розташування цих капсул використовується метод Ф-функцій Стояна [4]. Він дозволяє розглядати геометричні обмеження для довільно орієнтованих об'єктів. Використовуються нормалізовані Ф-функції, які визначають відстань між об'єктами. Цю задачу можна описати як задачу змішаного цілочислового програмування – Identical Item Packing Problem [5].

Алгоритм для розв'язання задачі ґрунтується на методі блочної оптимізації [6]. Задачу розбивають на підзадачі. На кожному кроці додається лише одна капсула. Для отримання пакування застосовується метод гомотетичних перетворень із коефіцієнтом гомотетії як незалежною змінною. Початковому розміщенню відповідає нульовий коефіцієнт гомотетії, тобто усі циліндри вироджені в точку. Розв'язуємо задачу максимізації коефіцієнта гомотетії, за умови розміщення циліндрів в цільовій області і розташуванні циліндрів на заданій мінімально допустимій відстані. Якщо коефіцієнт гомотетії в результаті розв'язання задачі дорівнює одиниці, то маємо пакування заданих циліндрів.

Для розв'язання задач нелінійного програмування використовується безкоштовний солвер IPOPT [7], який ґрунтується на методі внутрішньої точки. Графічна візуалізація здійснюється за допомогою OpenGL API [8].

Література

[1] Song M., Zhou X., Hou R. et al. CT-guided radioactive 125I seeds brachytherapy for lung oligometastases from colorectal cancer: initial results. BMC Cancer. 2024. Vol. 24, No. 265. <https://doi.org/10.1186/s12885-024-12013-2>.

[2] Wan Q., Tan L., Tang X., Wang W., Su Y., Wu Z., Ke M., Chen Z. The clinical value of iodine-125 seed implantation in the treatment of iodine-refractory differentiated thyroid carcinoma. Frontiers in Endocrinology, 2024. Vol. 15. <https://doi.org/10.3389/fendo.2024.1327766>.

[3] Abtahi M., et al. A Dosimetric evaluation of a high dose rate cobalt-60 brachytherapy source using shielded, single and multi-channel cylinder applicators for gynecological cancers. *Medical Dosimetry*. 2022. Vol. 47(4). P. 318–324.

[4] Stoian Y.H., Chuhai A.M. Methodology to Solve Optimal Placement Problems for 3D Objects. *Journal of Mechanical Engineering – Problemy Mashynobuduvannia*, 2020. Vol. 23(2). P. 60-71. <https://doi.org/10.15407/pmach2020.02.060>

[5] Wäscher G., Haußner H., Schumann H. An improved typology of cutting and packing problems. *European Journal of Operational Research*. 2007. 183(3), 1109-1130. <https://doi.org/10.1016/j.ejor.2005.12.047>.

[6] Yaskov G., Chugay A. Packing equal spheres by means of the block coordinate descent method. *Proc. of the Third International Workshop on Computer Modeling and Intelligent Systems (CMIS-2020), CEUR Workshop Proceedings*, 2020. P. 156–168.

[7] Wächter A., Biegler L.T. On the implementation of an interior-point filter line-search algorithm for large-scale nonlinear programming. *Mathematical Programming*, 2006. Vol. 106(1). P. 25–57. <https://doi.org/10.1007/s10107-004-0559-y>.

[8] OpenGL API Documentation Overview [Електронний ресурс] – Режим доступу до ресурсу: <https://www.opengl.org/Documentation/Documentation.html>

АНАЛІЗ ЯКОСТІ ПРОГРАМНОГО КОДУ PHP ЗА ДОПОМОГОЮ PHPMETRICS

Шутко І.С.

E-mail: ishutko@gmail.com

Миколаїв, Національний університет кораблебудування імені адмірала Макарова

Аналіз коду є важливим етапом у процесі розробки програмного забезпечення, що дозволяє оцінити його якість, складність та підтримуваність. У даній роботі розглядається використання інструменту phpMetrics для оцінювання метрик програмного коду PHP. Проведено аналіз якості коду на основі різних проєктів, що розміщені у відкритих сховищах GitHub, та зроблено висновки щодо ефективності застосування phpMetrics у процесі розробки. Окрему увагу приділено метрикам, що були використані у попередніх дослідженнях, зокрема в статті про оцінювання кількості рядків коду веб-застосунків на основі фреймворку Codeigniter.

Ключові слова: phpMetrics, аналіз коду, метрики якості, підтримуваність, складність коду, PHP, Codeigniter.

Аналіз якості програмного забезпечення є ключовим фактором забезпечення його надійності, ефективності та масштабованості. У мові PHP широко застосовуються статичні аналізатори коду, що дозволяють розробникам своєчасно виявляти проблеми та покращувати архітектуру застосунків. Одним із таких інструментів є phpMetrics, який здійснює комплексний аналіз коду, генерує звіти та надає статистичні дані про програмний продукт.

Метою дослідження є оцінка ефективності використання phpMetrics для аналізу коду PHP-проєктів та визначення його можливостей у виявленні потенційних проблем у кодї. Дослідження також передбачає аналіз ключових метрик, які були застосовані у попередній роботі щодо оцінки якості веб-застосунків на основі Codeigniter.

Для проведення дослідження використовувалися такі підходи:

- Вибірка PHP-проєктів із відкритих репозиторіїв GitHub.
- Аналіз отриманих метрик якості коду за допомогою phpMetrics.
- Порівняння отриманих даних з реальними проблемами, виявленими у кодї.
- Оцінка метрик, що були використані у попередній статті, зокрема:
 - Кількість класів – впливає на складність застосунку.
 - Середня кількість методів на клас – показник рівня модульності коду.
 - Метрика DIT (Depth of Inheritance Tree) – відображає глибину наслідування.

- Використання відстані Махаланобіса – для аналізу відхилень значень метрик та виявлення аномальних компонентів коду.

Основні метрики phpMetrics:

- Cyclomatic Complexity (CCN) – визначає складність функцій.
- Maintainability Index (MI) – оцінює підтримуваність коду.
- Afferent & Efferent Coupling (Ca & Ce) – характеризує взаємозв'язки між класами.
- Depth of Inheritance Tree (DIT) – показує рівень наслідування класів.
- Code Duplication – визначає рівень дублювання коду.

Висновки. Інструмент phpMetrics є потужним засобом для аналізу коду PHP-застосунків. Він дозволяє швидко оцінити якість коду, виявити потенційні проблеми та сприяти покращенню архітектури програмного забезпечення. Використання phpMetrics у процесі розробки дозволяє значно знизити технічний борг і покращити підтримуваність застосунків.

РОЗРОБКА ТА ВИКОРИСТАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ ВИЯВЛЕННЯ АНОМАЛІЙ У МЕРЕЖЕВОМУ ТРАФІКУ ЗА ДОПОМОГОЮ CNN

Ярмоленко В.С.

Керівник: Шаповалова О.О.

E-mail: veronika.yarmolenko@hneu.net, olena.shapovalova@hneu.net

Харків, Харківський національний економічний університет імені Семена Кузнеця

В умовах зростаючої загрози кібератак, ефективного виявлення аномалій у мережевому трафіку є важливим завданням для забезпечення кібербезпеки. Використання методів глибокого навчання, зокрема згорткових нейронних мереж (CNN), відкриває нові можливості у сфері автоматизованого моніторингу та аналізу мережевих потоків. Дослідження спрямоване на розробку програмного забезпечення для виявлення аномального трафіку за допомогою CNN, що дозволяє підвищити точність і швидкість реагування на потенційні загрози.

Актуальні проблеми, які вирішуються в межах даного дослідження:

- Збільшення складності атак, включаючи DDoS, SQL-ін'єкції, маніпуляції з DNS-запитами та експлуатацію вразливостей протоколів;
- Необхідність зменшення рівня хибнопозитивних спрацьовувань у класичних методах виявлення аномалій;
- Використання великих обсягів даних, що ускладнює аналіз трафіку традиційними методами;
- Оптимізація продуктивності системи виявлення для роботи в реальному часі.
- Методологія дослідження включає:
- Збір та обробку датасетів мережевого трафіку з реальними та симульованими аномаліями;
- Попередню обробку даних для перетворення трафіку у формат, придатний для аналізу згортковими нейронними мережами;
- Розробку архітектури CNN для автоматичного виявлення аномального трафіку;
- Навчання та тестування моделі з використанням відкритих та спеціалізованих наборів даних, таких як CICIDS2017, UNSW-NB15;
- Оцінку ефективності та порівняння запропонованого підходу з традиційними методами виявлення аномалій.

Для реалізації та тестування програмного забезпечення можна використовувати наступні інструменти:

- TensorFlow та Keras – для розробки та навчання згорткових нейронних мереж;
- Wireshark – для аналізу мережевого трафіку та збору даних;

- Snort – як система виявлення вторгнень (IDS) для порівняння методів виявлення аномалій;
- ELK Stack (Elasticsearch, Logstash, Kibana) – для візуалізації та аналізу великих обсягів мережевого трафіку;
- Scapy – для генерації тестового трафіку та емуляції аномальних мережевих ситуацій;
- PyTorch – як альтернативний фреймворк для експериментального навчання моделей.

Очікувані результати:

- Визначення оптимальної архітектури CNN для аналізу мережевого трафіку;
- Підвищення точності та швидкості виявлення аномалій у порівнянні з існуючими методами;
- Розробка програмного рішення, що дозволяє інтегрувати модель у системи моніторингу мережі;
- Надання рекомендацій щодо подальшого вдосконалення методів виявлення аномального трафіку.

Загалом, використання згорткових нейронних мереж у сфері кібербезпеки відкриває перспективи для автоматизації аналізу трафіку та покращення рівня захисту інформаційних систем. В рамках дослідження буде запропоновано ефективний підхід до виявлення аномалій у мережевому трафіку, що дозволить знизити ризики атак та забезпечити стабільність функціонування інформаційної інфраструктури.

Література

- [1] The Zeek Network Security Monitor. [Електронний ресурс] – Режим доступу до ресурсу: <https://zeek.org/>
- [2] CICIDS2017 Dataset. [Електронний ресурс] – Режим доступу до ресурсу: <https://www.unb.ca/cic/datasets/ids-2017.html>
- [3] Wireshark Network Protocol Analyzer. [Електронний ресурс] – Режим доступу до ресурсу: <https://www.wireshark.org/>
- [4] TensorFlow: Large-Scale Machine Learning on Heterogeneous Systems. [Електронний ресурс] – Режим доступу до ресурсу: <https://www.tensorflow.org/>
- [5] Scapy: Packet Manipulation for Python. [Електронний ресурс] – Режим доступу до ресурсу: <https://scapy.net/>
- [6] Nmap: The Network Mapper. [Електронний ресурс] – Режим доступу до ресурсу: <https://nmap.org/>

СЕКЦІЯ 3

COMPARISON OF RANDOM FOREST REGRESSION AND POLYNOMIAL REGRESSION ANALYSIS FOR CODE METRICS

Bryzghalov M.V., Kaminsky S.S., Makarova L.M.
*E-mail: 2001bruzga2001@gmail.com, marvis.kaminskyi@gmail.com,
lidia.makarova@nuos.edu.ua*
Mykolaiv, Admiral Makarov National University of Shipbuilding

Traditional regression techniques, like polynomial regression [1], have been widely used in software metrics analysis due to their simplicity. However, software metrics often exhibit complex, non-linear relationships, making methods like Random Forest regression more suitable. This study compares polynomial regression and Random Forest in terms of predictive accuracy and robustness, with a focus on predicting Lines of Code (LOC) using software metrics such as Number of Classes (NC), Number of Methods (NM), and Depth of Inheritance Tree (DIT).

The effectiveness of Random Forest Regression [2] was compared to Polynomial and Linear Regression for analyzing software metrics. Unlike linear regression, which assumes a simple linear relationship between dependent and independent variables, Random Forest Regression uses an ensemble of decision trees to aggregate predictions, enhancing accuracy and robustness. This model is well-suited for capturing non-linear relationships and reducing overfitting by averaging predictions across multiple trees. Given the complexity of software metrics, where dependencies are often non-linear, Random Forest is expected to provide a more accurate and reliable analysis.

The dataset used for comparison includes key software metrics such as Number of Classes (NC), Number of Methods (NM), and Depth of Inheritance Tree (DIT), with the Lines of Code (LOC) as the dependent variable. The data was taken from a previous article that described a mathematical model for estimating the size of software applications using 2D graphics engines [3]. All three models were assessed based on R-squared (R^2) values, Mean Magnitude of Relative Error (*MMRE*), *PRED*(0.25) and a 5-fold cross-validation [4] approach for robust performance estimation.

The analysis was conducted using Python, leveraging libraries such as scikit-learn [5] for regression modeling, evaluation, and cross-validation, pandas for data manipulation, and numpy for numerical operations. scikit-learn's implementations were used for both polynomial regression (via *PolynomialFeatures* and *LinearRegression*) and Random Forest regression (*RandomForestRegressor*) to compare performance across different metrics.

Models were evaluated using R-squared (R^2), Mean Magnitude of Relative Error (*MMRE*), *PRED*(0.25), and 5-fold cross-validation. R^2 measures how much variance in the dependent variable can be explained by the independent variables, with higher values indicating better fit. *MMRE* calculates the average relative error between predicted and actual values, with lower values indicating more accurate predictions. *PRED*(0.25) indicates the percentage of predictions within 25% of the actual value, with higher values reflecting better accuracy.

Mean Squared Error (*MSE*) is used to measure prediction accuracy. In cross-validation, scikit-learn [6] reports negative *MSE* to fit the framework of maximizing scores. Cross-validation is a technique used to assess a model's performance by dividing the dataset into multiple subsets, training the model on some subsets while testing it on others, and averaging the results to ensure robustness. A more negative *MSE* indicates higher error, while a less negative value corresponds to better performance. By negating *MSE*, we ensure that the model with the lowest error has the highest (least negative) score.

Model's evaluation metrics are presented in the table 1.

The analysis reveals that Random Forest Regression outperforms Polynomial Regression in terms of predictive accuracy and robustness, particularly with lower *MMRE* and higher *PRED*(0.25) values. However, when considering cross-validation performance, Linear Regression exhibits a slightly better result with the least negative CV Mean Score, indicating a better balance between error and variance for the given dataset. Random Forest still demonstrates superior performance in

capturing non-linear relationships, as indicated by its higher R^2 score and more accurate predictions in terms of error metrics like *MMRE* and *PRED*. The choice between models depends on the trade-off between prediction accuracy and interpretability, as well as computational constraints.

Table 1. Model's Evaluation Metrics

Metrics	R^2	MMRE	<i>PRED</i> (0.25)	CV Mean Score
Linear Regression	0.93	0.63	0.44	$57.07 * 10^6$
Polynomial Regression	0.96	0.40	0.45	$240.15 * 10^6$
Random Forest Regression	0.96	0.12	0.88	$71.71 * 10^6$

Despite its strong performance, Random Forest isn't always ideal [7]. It demands high computational resources, lacks interpretability, and may be unnecessary for small, linear datasets where linear regression suffices.

The analysis demonstrates that Random Forest Regression is a powerful tool for predicting the Lines of Code based on software metrics. We were comparing Random Forest to Polynomial Regression, specifically predicting Lines of Code (LOC) using metrics such as Number of Classes (NC), Number of Methods (NM), and Depth of Inheritance Tree (DIT). The results show that Random Forest provides significantly better predictive accuracy compared to Polynomial Regression in Python implementation. In the future, Random Forest could be compared to models with normalizing transformations, such as logarithmic, Box-Cox or Johnson transformations, to further assess the impact on predictive accuracy and model robustness.

References

- [1] Polynomial Regression. [Electronic resource] – Resource access mode: <https://medium.com/analytics-vidhya/understanding-polynomial-regression-5ac25b970e18>
- [2] Understanding Random Forest Algorithm With Examples. [Electronic resource] – Resource access mode: <https://www.analyticsvidhya.com/blog/2021/06/understanding-random-forest/>
- [3] Камінський С.С., Бризгалов М.В., Макарова Л.М. Математична модель для оцінювання розміру програмних застосунків, що використовують 2D графічні рушії. *Матеріали V Всеукраїнської науково-практичної інтернет конференції “Інформаційні технології: моделі, алгоритми, системи (ITMAS – 2024)”*. (30-31 жовтня 2024 р. , м. Миколаїв). Миколаїв, НУК імені адмірала Макарова, 2024. С. 69–70.
- [4] A Gentle Introduction to k-fold Cross-Validation. [Electronic resource] – Resource access mode: <https://machinelearningmastery.com/k-fold-cross-validation/> (retrieved: 01.02.2025 p.).
- [5] scikit-learn Machine Learning in Python. [Electronic resource] – Resource access mode: <https://scikit-learn.org/stable/index.html> (retrieved: 01.02.2025 p.).
- [6] Cross-validation: evaluating estimator performance. [Electronic resource] – Resource access mode: https://scikit-learn.org/stable/modules/cross_validation.html (retrieved: 01.02.2025 p.).
- [7] Can't Decide Between a Linear Regression or a Random Forest? [Electronic resource] – Resource access mode: <https://medium.com/artificialis/cant-decide-between-a-linear-regression-or-a-random-forest-here-let-me-help-ab941b94da4c> (retrieved: 01.02.2025 p.).

CLLOUDCOMPARE – FREE SOFTWARE FOR POINT CLOUD PROCESSING

Toots R.

E-mail: robtoots88@gmail.com

Kharkiv, Simon Kuznets Kharkiv National University of Economics

CloudCompare is powerful open-source software for processing point clouds, widely used in scientific and applied research. The software was initially developed by Daniel Girardeau-Montaut as part of his PhD research at Telecom ParisTech [1]. Since then, a community of contributors and researchers have continuously developed it. CloudCompare allows users to analyze, compare, and visualize large volumes of 3D data obtained through laser scanning and photogrammetry.

Key Capabilities of CloudCompare [2]:

- Loading and processing point clouds – supports major file formats (LAS, PLY, E57, XYZ, etc.).
- Filtering and editing – tools for noise removal, smoothing, and alignment of point clouds.
- Registration and comparison – powerful tools for comparing two-point clouds, detecting changes, and registering scans.
- Segmentation and clustering – enable users to extract specific objects or regions within a point cloud.
- Generation of digital terrain models (DTM/DSM) – creation of topographic models based on point clouds.
- Geometric analysis – computation of curvature, surface normals, and other geometric properties.
- Visualization and rendering – allow users to configure colors, textures, and overlay additional data.

CloudCompare provides an API for programmatic interaction, which enables users to automate workflows and extend their functionality. One of the most notable features is the Python wrapper CloudComPy, which allows users to load point clouds, process data using built-in CloudCompare functions, and export results [3]. CloudComPy provides direct access to point cloud data as numpy arrays and supports advanced operations such as curvature computation and point cloud filtering.

Example usage of CloudComPy for point cloud processing:

```
import cloudComPy as cc
cc.initCC()

# Load a point cloud
cloud = cc.loadPointCloud("myCloud.xyz")
print("cloud name: %s" % cloud.getName())
# Compute curvature as a scalar field
res = cc.computeCurvature(cc.CurvatureType.GAUSSIAN_CURV, 0.05, [cloud])
sfCurv = cloud.getScalarField(cloud.getNumberOfScalarFields() - 1)
cloud.setCurrentOutScalarField(sfCurv.getIndex())
# Filter points based on scalar field values
filteredCloud = cc.filterBySFValue(0.01, sfCurv.getMax(), cloud)
# Save the filtered point cloud
cc.SavePointCloud(filteredCloud, "filteredCloud.bin")
```

Additionally, CloudCompare includes the CCCoreLib C++ library, which provides low-level tools for working with point clouds, including data structures and core algorithms [4]. This enables developers to create custom applications and plugins tailored to specific requirements.

Why These Capabilities Matter? Point cloud data is increasingly used in fields such as geodesy, architecture, archaeology, and engineering. CloudCompare provides an efficient and

accessible alternative to commercial software solutions, offering high performance and an extensive feature set for processing and analyzing 3D data. Its open-source nature ensures continuous improvements and adaptation to emerging needs in the scientific and professional community.

References

[1] CloudCompare Official Website [Electronic resource] – Resource access mode: <https://www.danielgm.net/cc/>

[2] CloudCompareWiki [Electronic resource] – Resource access mode: <https://www.cloudcompare.org/doc/wiki/index.php>

[3] CloudComPy GitHub Repository [Electronic resource] – Resource access mode: <https://github.com/CloudCompare/CloudComPy>

[4] CCCoreLib GitHub Repository [Electronic resource] – Resource access mode: <https://github.com/CloudCompare/CCCoreLib>

ШТУЧНИЙ ІНТЕЛЕКТУАЛЬНИЙ КАПІТАЛ ЯК НОВИЙ ВИД РЕСУРСІВ НЕМАТЕРІАЛЬНОГО ПОХОДЖЕННЯ

Андрейчіков О.О.

Керівник: Старкова О.В.

E-mail: andreychikov.oleksandr@hneu.net

Харків, Харківський національний економічний університет імені Семена Кузнеця

Інтелектуальний капітал (ІК) традиційно асоціюється з людськими знаннями, досвідом, інноваційними ідеями, системою комунікаційних зв'язків, системою управління та іншими ресурсами нематеріального походження (РНП). Проте з появою та широким провадженням в роботу сучасних компаній штучного інтелекту (ШІ) з'явився новий клас (вид) ресурсів, які за походженням є результатом діяльності ШІ, наприклад, згенеровані ШІ ідеї або рекомендовані рішення, а за природою є елементами нематеріальними та неосяжними, що розширює межі уявлень та знань про інтелектуальний капітал та вимагає окремого дослідження цього феномену, розуміння його впливу на бізнес, економіку, науку та суспільство загалом як в рамках задач загального дослідження ШІ, так і в рамках дослідження ІК.

Саме тому метою даної роботи є аналіз результатів діяльності штучного інтелекту, зокрема його впливу на інтелектуальний капітал, організаційну ефективність, інноваційну діяльність та його впливу на ринок інтелектуальної праці. У роботі представлено міждисциплінарний підхід до вивчення цієї теми, що поєднує системологічний, економічний та соціологічний аналіз, що дозволяє системно поглянути на роль і місце штучного інтелекту в сучасній екосистемі нематеріальних активів.

Перше, що треба визначити в рамках даного дослідження – це мету, роль та місце штучного інтелекту в рамках його застосування у бізнес діяльності. Як зазначено в роботі [1], за своєю суттю штучний інтелект – це здатність машини або комп'ютерної системи виконувати завдання, для яких зазвичай потрібен людський інтелект. Іншими словами – це означає, що головною задачею ШІ є посилення або заміщення людського інтелекту, що мовою бізнесу в перспективі означає скорочення витрат на утримання великих команд та пов'язаних з цим різних видатків. Так згідно IBM Global AI Adoption Index 2022 [2] 77% підприємств вже інтегрують ШІ у свою діяльність або активно вивчають можливості його впровадження.

Говорячи про роль і місце штучного інтелекту, треба зазначити, що взаємодія з ним зазвичай відбувається через певні застосунки (ChatGPT, Siri, Grammarly тощо), які по суті є прикладним програмним забезпеченням, що і визначає роль і місце штучного інтелекту, бо застосунки на базі ШІ створені саме для виконання різних практичних задач: генерації текстів, зображень, розпізнання образів тощо.

Наступним важливим напрямком дослідження будь-яких систем та явищ є аналіз результатів їхньої діяльності (прояву), що дозволяє розкрити сутність та визначити цінність системи. В даному випадку, як вже частково зазначено, мова йде про широкий перелік кінцевих продуктів: від генерації конкретних типів файлів за заданими параметрами (графічні, аудіо, текстові та інші) до певних видів робіт/послуг (відповіді на питання, консультивання у чатах, управління обладнанням, автоматизована торгівля тощо). Умовно дані кінцеві продукти можна розділити на декілька основних груп за їх функціональним призначенням, що відповідає і основним напрямам ділової активності:

- Інформаційні та аналітичні продукти, в яких ШІ проявляє себе як когнітивна система здатна до обробки, інтерпретації та створення нових знань. Прикладом кінцевих продуктів можуть бути аналітичні звіти, прогностичні моделі, персоналізовані рекомендації, що мають високу економічну та управлінську цінність, бізнес-інсайти отримані з великих даних тощо.

- Персоналізовані сервіси та взаємодія, де ШІ проявляє себе як інструмент підвищення якості життя та ефективності комунікації між людиною і технологіями. До прикладів кінцевих продуктів можна віднести розумні асистенти на кшталт Alexa і Siri, які персоналізують взаємодію користувачів із цифровими платформами, різні рекомендаційні системи, які допомагають, наприклад, Netflix і Spotify створювати новий користувацький досвід для персоналізованого підбору контенту та економити сотні мільйонів доларів за рахунок використання машинного навчання.

- Автономні системи та пристрої, які демонструють цінність ШІ як адаптивної, автономної системи, що оптимізує складні процеси та підвищує їх ефективність. Прикладами можуть бути рішення для автономного транспорту, які вже використовуються у службах таксі та доставки дронами по всьому світу, роботизовані помічники у аеропортах та різних сервісних центрах, системи для автоматизації виробничих процесів, обслуговування клієнтів та надання медичних послуг. Так у звіті [3] Всесвітнього економічного форуму (ВЕФ) за 2025 рік зазначено, що рішення подібного класу вже мають реальні провадження у таких сферах і галузях як сільське господарство, гірничодобувна промисловість, нафтогазовий сектор, логістика тощо. Крім того, до 2035 року 75% транспортних засобів буде оснащено технологіями на базі штучного інтелекту.

- Генеративні продукти, в яких ШІ виступає творцем контенту, розширюючи межі традиційної творчості. У якості прикладів можна назвати результати діяльності GPT-подібних агентів при створенні маркетингових текстів, реклами, звітів, сценаріїв, що можуть мати комерційну та наукову цінність тощо. Так згідно глобального опитування McKinsey [4] щодо ШІ у травні 2024 року 65% респондентів повідомили, що їхні організації регулярно використовують генеративний ШІ, що майже вдвічі більше, ніж у попередньому опитуванні всього десять місяців тому.

Враховуючи викладене, можна зробити висновок, що інтеграція штучного інтелекту в роботу різних компаній покриває велику кількість бізнес потреб, створює нові можливості для розвитку бізнес моделей та створення інноваційних продуктів. Однак, разом із можливостями для власників капіталу та бізнесу ШІ створює ризики для найманих працівників і ринку інтелектуальної праці загалом. Згідно з дослідженням ВЕФ [5] проведеного у 2025 році 41% роботодавців мають намір скоротити чисельність своїх співробітників, оскільки ШІ автоматизує певну кількість задач та бізнес-процесів, а найбільше від впровадження ШІ постраждають інтелектуальні працівники.

Таким чином можна зробити висновок, що по мірі того, як штучний інтелект стає все більш потужним і повсюдним, необхідно забезпечити його відповідальний розвиток і використання, вирішуючи питання упередженості, конфіденційності та прозорості. Саме тому, подальші дослідження мають бути спрямовані на виявлення оптимальних механізмів використання ШІ в бізнесі, економіці, освіті та суспільному управлінні з урахуванням потенційних ризиків та викликів. Окремого дослідження потребує і класифікація

інтелектуального капіталу, а саме її розширення та/або уточнення з урахуванням появи нових елементів в її структурі.

Література

[1] Artificial intelligence: What it is, how it works and why it matters. [Електронний ресурс] – Режим доступу до ресурсу: <https://www.iso.org/artificial-intelligence>

[2] IBM Global AI Adoption Index 2022. [Електронний ресурс] – Режим доступу до ресурсу: <https://www.ibm.com/downloads/documents/us-en/107a02e94a48f5c1>

[3] How we bring AI into the physical world with autonomous systems. [Електронний ресурс] – Режим доступу до ресурсу: <https://www.weforum.org/stories/2025/01/ai-and-autonomous-systems>

[4] The state of AI in early 2024: Gen AI adoption spikes and starts to generate value. [Електронний ресурс] – Режим доступу до ресурсу: <https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai>

[5] Future of Jobs Report 2025. [Електронний ресурс] – Режим доступу до ресурсу: https://reports.weforum.org/docs/WEF_Future_of_Jobs_Report_2025.pdf

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ПІДТРИМКИ ПРОСУВАННЯ ПОДАЛЬШИХ ПОКУПОК

Артамошин Є.В., Льовкін В.М.

E-mail: vliovkin@gmail.com

Запоріжжя, Національний університет «Запорізька політехніка»

В сучасному світі велике місце займає торгівля як така, та певні засоби, що супроводжують процес купівлі-продажу з різних напрямків. Для забезпечення приємного та зручного досвіду покупок важливо надавати покупцю набір інструментів, які б полегшили йому цей процес. Один з таких інструментів – порадишник покупок, який на основі придбаних в минулому та цікавих для покупця товарів, створює перелік інших товарів, які б були корисні та актуальні для останнього. Подібний програмний продукт може розроблюватись з використанням різних підходів, таких як машинне навчання. Використання простих підходів при цьому сприяє швидкості, а значить більш високій практичній придатності таких засобів для реального використання.

Ідея, взята за основу в даній роботі полягає в вираховуванні індексу подібності одного товару до іншого, при цьому встановлюючи значення «1» для випадків максимальної подібності, а «0» – для випадків повної несхожості, за допомогою косинусної подібності. Головна перевага даного методу перед більш складними методами – це швидкість та передбачуваність. В умовах обмежених обчислювальних ресурсів або бюджету даний метод найбільш чіткий і надійний. Точність порад в основному залежить від кількості та якості характеристик для порівняння товару. Найпростіші варіанти – це вартість та категорія товару.

Алгоритм, покладений в основу визначення порад подальших покупок у програмі, має наступну послідовність дій:

- отримання даних про товари, які користувач вже придбав та на які часто звертає увагу;
- обробка даних про товари з ціллю виокремити з них значення характеристик для порівняння;
- для кожного товару з першого етапу вирахувати подібність з товарами, що наявні в каталозі магазину, утворивши тим самим матрицю подібності;
- вибір з матриці ряду товарів з найбільшим коефіцієнтом подібності. Категоріальні дані обов'язково потрібно перетворити на числовий ряд для подальшої роботи з ними.

Програмне забезпечення розроблювалось з використанням мови програмування Python, яка є високорівневою та орієнтованою на ефективне та швидке вирішення

різноманітних завдань з мінімальною необхідністю описувати складні алгоритми, завдяки наявності великого числа пакетів, написаних та безкоштовно розповсюджуваних іншими розробниками. У підсумку, для створення застосунку використано: пакет pandas для зручної обробки табличних даних у форматі DataFrame [1], пакет scikit-learn, який містить функцію для розрахунку косинусної подібності [2].

Алгоритм програми в процесі роботи циклічний. Він постійно очікує нові дані для пошуку подібних товарів з каталогу. Як і зазначено вище, програма перетворює вхідні дані в зручний табличний формат DataFrame, при цьому перетворюючи категоріальні дані на числовий ряд і виконуючи розрахунок подібності, утворюючи відповідну матрицю з якої вибирається певного розміру ряд перших за коефіцієнтом товарів, які в свою чергу відображаються користувачу. Для роботи з великими об'ємами даних запропоновано оптимізаційне рішення, яке полягає в попередній додатковій класифікації куплених товарів.

Література

[1] Pandas documentation [Електронний ресурс] – Режим доступу до ресурсу: <https://pandas.pydata.org/docs/index.html>

[2] sklearn API [Електронний ресурс] – Режим доступу до ресурсу: <https://pandas.pydata.org/docs/index.html>

ПРИСТРІЙ ДЛЯ ВИМІРЮВАННЯ ТЕМПЕРАТУРИ ПОВІТРЯ СКЛАДСЬКОГО ПРИМІЩЕННЯ ТА КОНТРОЛЮ УМОВ ДЛЯ ЗБЕРІГАННЯ ПРОДУКЦІЇ НА БАЗІ ARDUINO

Барда М. О.

Керівник: Крайник Я. М.

E-mail: Mukolabarda777@gmail.com

Миколаїв, Чорноморський національний університет імені Петра Могили

У сучасних умовах автоматизації логістичних процесів важливим аспектом збереження якості продукції є контроль температурного режиму на складах. Від дотримання оптимальних кліматичних умов залежить якість та термін придатності товарів, особливо чутливих до перепадів температури, таких як медикаменти, продукти харчування, хімічні реагенти тощо.

Актуальність аналізу параметрів навколишнього середовища в складських приміщеннях зумовлена необхідністю запобігання псуванню продукції. Контроль температури та своєчасне реагування на критичні відхилення дозволяють знизити фінансові втрати та покращити якість зберігання.

Метою роботи є створення пристрою для вимірювання температури та контролю умов зберігання продукції на базі мікроконтролера Arduino Pro Mini [1].

Arduino Pro Mini – це компактний мікроконтролер, що забезпечує енергоефективну роботу та простоту у використанні. Він взаємодіє з датчиком температури DS18B20 [2], модулем GSM SIM800L для передачі повідомлень про критичні температури, OLED-дисплеєм 128×64 для відображення даних та кнопкою для керування системою.

Пристрій має наступний функціонал:

- вимірювання температури повітря за допомогою датчика DS18B20;
- передача повідомлень через GSM-модуль SIM800L у разі виявлення критичних відхилень;
- візуалізація поточних параметрів на OLED-дисплеї;
- автономне живлення від літій-іонних акумуляторів 18650 з можливістю підзарядки через модуль TP4056 ;
- підвищення напруги до 5V через перетворювач MT3608 для стабільної роботи електронних компонентів;
- керування системою за допомогою кнопки.

Для живлення використовується акумуляторний блок із захисною платою TP4056. Напруга 3.7V підвищується до 5V за допомогою підсилювача MT3608, що дозволяє коректно працювати всім компонентам системи. Дані з датчика температури обробляються мікроконтролером Arduino, а у разі перевищення допустимого діапазону температура передається користувачеві через SMS або дзвінок за допомогою GSM-модуля SIM800L. На рисунку 1 представлена схема пристрою.

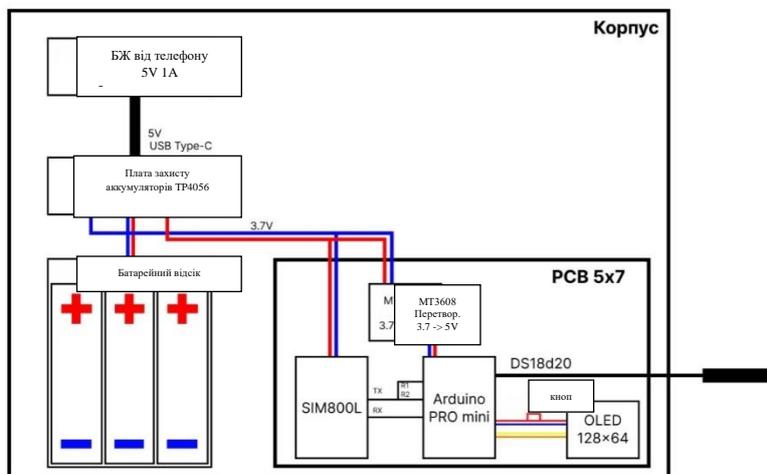


Рисунок 1 – Прототип пристрою

Для оцінки ефективності даного рішення було проведено аналіз наявних систем контролю клімату у складських приміщеннях. Аналіз показав, що більшість комерційних пристроїв мають високу вартість та складну інтеграцію в існуючі системи автоматизації (табл. 1). Запропонований пристрій на базі Arduino є більш доступним, його можна налаштувати під специфічні потреби користувача, а також він забезпечує автономну роботу за рахунок акумуляторного живлення.

Таблиця 1 – Основні характеристики систем моніторингу: Arduino та комерційні аналоги

Характеристика	Пристрій на Arduino	Комерційні системи моніторингу
Вартість	Низька ($\approx 20-50\$$)	Висока (від 200\$ і більше)
Гнучкість налаштувань	Висока (можна змінювати код)	Обмежена (залежить від виробника)
Тип живлення	Акумулятор 18650, 3.7V	Мережеве або акумуляторне
Можливість автономної роботи	Так (заряджається від USB)	Так, але залежить від моделі
Зв'язок	GSM (SMS, дзвінки)	GSM, Wi-Fi, LoRa
Датчик температури	DS18B20 ($\pm 0.5^\circ\text{C}$)	Прецизійні сенсори ($\pm 0.2^\circ\text{C}$)
Візуалізація даних	OLED 128x64	LCD-дисплеї, веб-інтерфейс
Простота встановлення	Висока (компактний розмір)	Середня (потрібні монтажні роботи)
Можливість розширення	Так (можна додати датчики)	Обмежена (залежить від моделі)

Таким чином, пристрій на базі Arduino є більш доступним та гнучким у налаштуванні, що дозволяє адаптувати його під різні умови експлуатації. Він підходить для невеликих складів та приватних господарств, де немає необхідності в складних промислових системах. У той час як комерційні рішення забезпечують вищу точність вимірювання та можливість підключення до централізованих систем контролю клімату, вони значно дорожчі та менш гнучкі у конфігурації.

Завдяки автономному живленню та GSM-зв'язку, пристрій здатний працювати навіть у віддалених місцях, де немає стабільного Wi-Fi або дротового підключення.

Література

[1] Borwankar J., Pandit S., Patel V., Nirmal J. H. IOT-Based Smart Warehouse Monitoring System. SSRN, 2023. DOI: 10.2139/ssrn.4461490/.

[2] Rahman R., Hashim U., Ahmad S. IoT based temperature and humidity monitoring framework. Bulletin of Electrical Engineering and Informatics, 2020. Vol. 9, No. 1. DOI:10.11591/eei.v9i1.1557.

ВИКОРИСТАННЯ LORAWAN ТА МАШИННОГО НАВЧАННЯ ДЛЯ АВТОМАТИЗАЦІЇ РОБОТИ РОЮ ДРОНІВ

Басов Д.Є., Пузирьов С.В.

E-mail: danila.9khan@gmail.com, sergii.puzarov@gmail.com

Миколаїв, Чорноморський національний університет імені Петра Могили

Безпілотні апарати (дрони) є тою технологією, що за останні декілька років набуває все більшої популярності та широкого використання. На даний момент в Україні їх застосування обмежується лише сферою національної оборони, але незабаром буде актуальним питання їх активного та ефективного цивільного застосування.

Збільшення ефективності роботи дронів здійснюється декількома шляхами. Перший спосіб полягає у об'єднанні дронів у систему, що називається «роєм». Дрони у рої діють скоординовано, обмінюючись даними між собою. Рої бувають централізовані та децентралізовані. У централізованому типі рою один дрон чи зовнішній комп'ютер відповідальний за координацію та планування дій. У випадку децентралізованого рою кожен дрон може зв'язуватися з іншим та приймати рішення самостійно. Децентралізований підхід до керування роєм дронів дозволяє використання автоматичних операцій та зменшує навантаження на комунікаційну складову.

Другий спосіб полягає у застосуванні штучного інтелекту. Найбільш ефективно штучний інтелект використовується для таких задач: детектування та відслідковування об'єктів, автономна навігація, планування шляху, координація дронів у рою, аналіз відео та зображень, кібербезпека [1].

Хоча і штучний інтелект, і ройова поведінка є популярними темами наукових досліджень, гібридних досліджень на даний момент досить мало. Малочисельними є і комерційні рішення. Прикладом такого рішення є комерційний рій дронів американського виробництва TealDrones 4-Ship, але інтеграція штучного інтелекту лише планується та дальність передачі даних лише 3-5 км [2].

Технологією, що може забезпечити більшу дальність передачі даних, є LoRaWAN. Це протокол бездротового зв'язку, заснований на технології радіочастотної модуляції LoRa. Особливостями LoRaWAN є велика дальність сигналу (до 5 км у урбанізованій місцевості та до 15 км – у сільській), низьке енергоспоживання, підвищена стійкість до завад, але невелика пропускна здатність (від 0,3 до 50 Кбіт/с) [3]. Останній факт робить малозручним передачу медіафайлів за допомогою LoRaWAN, але якщо делегувати аналіз відеопотоку нейронній мережі, буде достатньо передавати лише дані про детектований об'єкт.

Саме тому було запропоновано апаратно-програмний комплекс, який використовує нейронну мережу для детектування об'єктів та технологію LoRaWAN для комунікації.

Носієм запропонованого апаратно-програмного комплексу є рій дронів з елементами децентралізованого типу керування. Сам рій дронів в цілому є однорідною P2P-мережею, де в якості рівноправних P2P-вузлів виступають групи дронів. У свою чергу, кожна група представляє собою приватну мережу на базі протоколу LoRaWAN (рис. 1).

Вибір саме такої архітектури робить усю систему гнучкою, універсальною та більш захищеною. Так як, по-перше, P2P мережа верхнього рівня (тобто на рівні всього рою дронів) може бути будь якою в залежності від поставлених практичних завдань. А по-друге, наявність приватної мережі усередині груп дронів забезпечує їх ізоляцію.

Для реалізації елементів архітектури LoRaWAN (вузлів, шлюзів та мережевого серверу та серверу додатків) дрони у рої були поділені на дрони-вузли та керуючі дрони. Перші реалізують лише вузли мережі LoRaWAN, а останні – всі інші елементи архітектури LoRaWAN. Таким чином, керуючі дрони є центральним елементом у групах дронів. Вони обслуговують приватну мережу LoRaWAN і саме вони представляють свою групу у P2P-мережі верхнього рівня. Така система також зберігає стійкість до втрат, адже у випадку втрати чи виходу з ладу керуючого дрона дрони вузли, що належать до мережі його групи, перейдуть до мережі іншої.

Кожен дрон аналізує відеопотік з власної камери за допомогою нейронної мережі. При успішному детектуванні об'єкта, дані про нього зберігаються на локальному сховищі та передаються далі, разом з координатами дрона. Далі, дані рухаються по мережі LoRaWAN через шлюз до сервера додатків. Користувач взаємодіє з даними за допомогою підключеного до сервера клієнтського застосунку та відправляє команди назад за таким же шляхом.

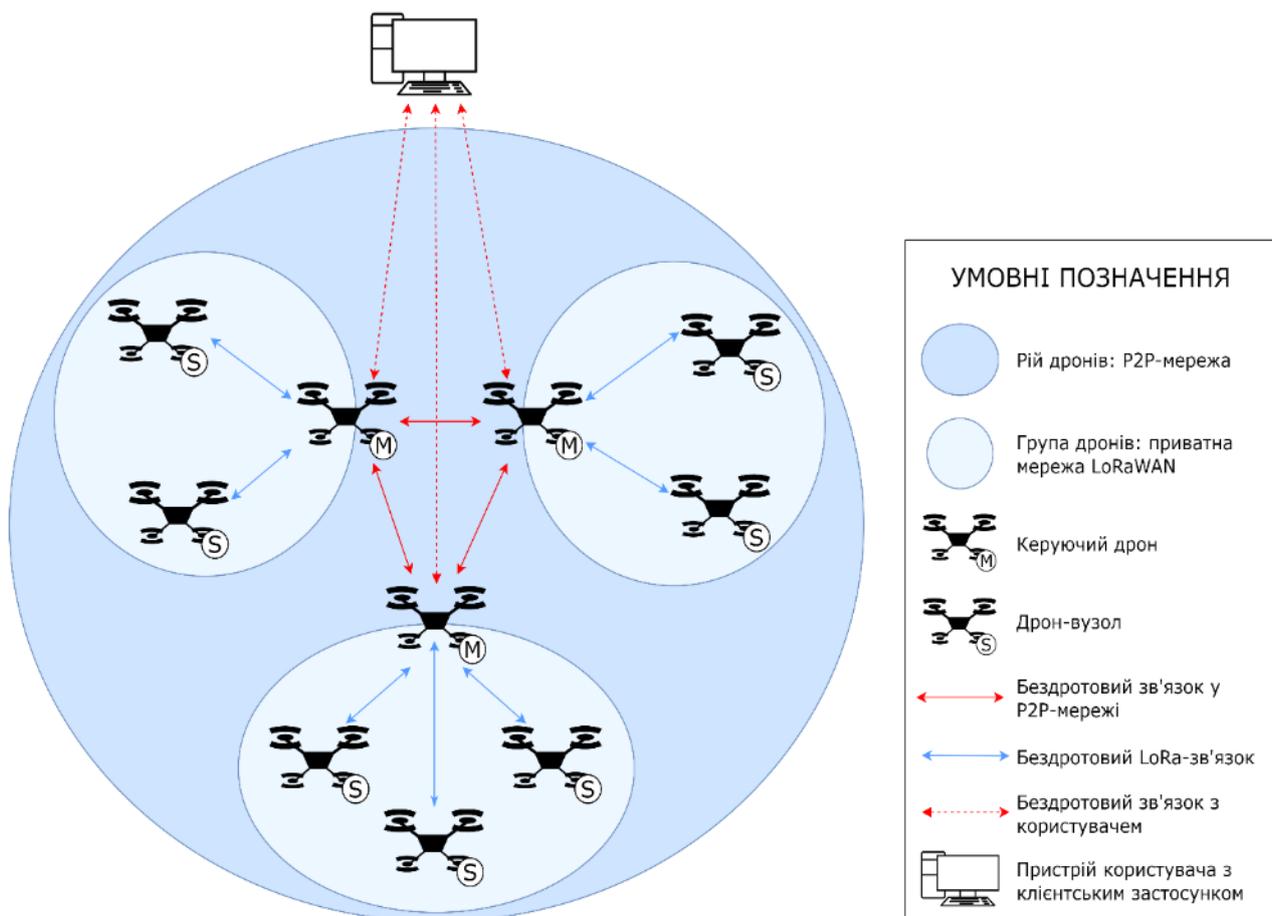


Рисунок 1 – Схема архітектури мережі запропонованого апаратно-програмного комплексу

Для апаратної реалізації основних компонентів було запропоновано використовувати одноплатний комп'ютер (наприклад, NVIDIA Jetson Nano), достатньо потужний для

підтримки роботи штучної мережі та мережевих застосунків, сумісну з ним камеру, а також: для дрона-вузла – LoRa-трансивер та GPS-модуль, а для керуючого дрона – LoRa-концентратор.

Запропонований апаратно-програмний комплекс може бути використаний для виконання задач у сферах, де потрібен автоматичний візуальний аналіз на великих площах та відстанях, а саме: у аграрній сфері, сфері охорони природи, під час пошуково-рятувальних операціях, наукових дослідженнях та інших видах моніторингу.

Література

[1] Telli K., Kraa O., Himeur Y., Ouamane A., Boumehraz M., Atalla S., Mansoor W. A Comprehensive Review of Recent Research Trends on Unmanned Aerial Vehicles (UAVs). 2023. Systems. Vol. 11. DOI: <https://doi.org/10.3390/systems11080400>.

[2] Athena AI announcement for Teal 2. [Електронний ресурс] – Режим доступу до ресурсу: https://tealdrones.com/press_releases/red-cat-and-athena-ai-announce-breakthrough-artificial-intelligence-and-computer-vision-capabilities-for-teal-2-military-grade-drone.

[3] LoRa® and LoRaWAN®: A Technical Overview. Semtech LoRa. [Електронний ресурс] – Режим доступу до ресурсу: https://www.katykoenen.com/wp-content/uploads/2024/07/LoRa_and_LoRaWAN-A_Tech_Overview-Downloadable.pdf.

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ДЛЯ АНАЛІЗУ ВІДГУКІВ ПРО МУЗИЧНИЙ КОЛЕКТИВ

Гордієнко А.В., Льовкін В.М.

E-mail: vliovkin@gmail.com

Запоріжжя, Національний університет «Запорізька політехніка»

Сучасні інструменти аналізу текстових даних стають більш актуальнішими в умовах широкого використання соціальних мереж для обміну думками, оцінки подій та формування громадської думки. Одним із широковідомих, але і важливих завдань у цій сфері є автоматичне визначення настрою текстових повідомлень, що дозволяє оцінювати популярність певного суб'єкта, ідентифікувати проблемні аспекти та формувати висновки на основі великих обсягів даних. Варіантом специфікації даного завдання є визначення настрою відгуків про музичний колектив, коли виконується дослідження думок, які висловили користувачі в соціальній мережі.

Розроблене у даній роботі програмне забезпечення виконує аналіз стрічки для визначення настрою відгуків про заданий музичний колектив. Його функціональність дозволяє ідентифікувати повідомлення як позитивні, негативні або нейтральні, підраховувати загальну кількість знайдених у соціальній мережі відгуків, а також кількість відгуків кожного виду. Користувач отримує можливість переглянути відгуки відповідно до обраної категорії.

Для реалізації програмного забезпечення було обрано мову програмування Python, що забезпечує широкий спектр інструментів для роботи з текстовими даними. Основу алгоритму складає використання засобів:

- NLTK (Natural Language Toolkit) – бібліотека для обробки природної мови, яка надає готові інструменти для токенизації тексту, видалення стоп-слів та аналізу настроїв;
- SentimentIntensityAnalyzer — модуль для визначення полярності тексту за шкалою від негативного до позитивного настрою.

Розроблене у підсумку програмне забезпечення передбачає наступні етапи для роботи:

- попередня обробка тексту: включає видалення стоп-слів, розділових знаків і токенизацію тексту;
- аналіз настроїв: відгуки класифікуються як позитивні, негативні або нейтральні на основі значення compound (зведеного індексу полярності);

- агрегація результатів: підраховуються загальна кількість відгуків і кількість відгуків кожного типу;
- інтерактивний перегляд: користувач може вибрати, які відгуки переглянути (позитивні або негативні).

Для роботи була використана модель *SentimentIntensityAnalyzer*, яка працює за моделлю *VADER*. Ця модель призначена для аналізу емоційної забарвленості текстів, що містять як формальні, так і неформальні висловлювання, включно з емоційними словами, аббревіатурами та емодзі. Модель використовує словник, в якому попередньо закладені оцінки для багатьох слів та фраз, що визначають позитивну чи негативну тональність. При цьому потрібно враховувати і обмеженість наявних засобів, адже дана модель не здатна враховувати сарказм або контекст. Зважаючи на швидкість роботи, модель цілком придатна для базового застосування в межах загального аналізу наявних відгуків.

Література

[1] Natural Language Toolkit documentation [Електронний ресурс] – Режим доступу до ресурсу: <https://www.nltk.org/>

[2] *SentimentIntensityAnalyzer* documentation [Електронний ресурс] – Режим доступу до ресурсу: <https://www.nltk.org/api/nltk.sentiment.SentimentIntensityAnalyzer.html?highlight=sentimentintensity>

ІІІ-МЕНЕДЖМЕНТ ЯК НОВА ПАРАДИГМА УПРАВЛІННЯ НА ОСНОВІ ШТУЧНОГО ІНТЕЛЕКТУ

Єль Мутахід А.Р.

Керівник: Щербина Н.В.

E-mail: elmutam@gmail.com

*Харків, Комунальний заклад "Харківський ліцей №11 імені Данила Дідики
Харківської міської ради"*

На сучасному етапі розвитку людства зміни в технологічному прогресі відбуваються дуже швидко, що обумовлює потребу адаптації до цих змін. Одним з ключових напрямів розвитку сучасних технологій є штучний інтелект (ШІ), який поступово бере на себе виконання все більшої кількості різноманітних функцій. У цьому контексті ШІ відіграє роль ключового рушія трансформацій та інновацій, змінюючи підходи до управління, виробничих процесів, обслуговування клієнтів, стратегічного планування та інших бізнес задач. На цьому тлі формується й нова управлінська парадигма ШІ-менеджменту, яка поєднує людський інтелект та досягнення в сфері штучного інтелекту в єдину синергійну систему.

Сутність ШІ-менеджменту в загальному вигляді можна визначити як систему управління, що інтегрує штучний інтелект для автоматизації, аналізу, прогнозування, підтримки прийняття рішень, координації, контролю та інших управлінських потреб. Особливо це актуально з ростом об'ємів даних та кількості різних комунікацій, які виникають у повсякденній роботі менеджерів різного спрямування. Основна мета такої взаємодії людини та штучного інтелекту полягає у досягненні більшої ефективності, гнучкості та адаптивності управлінських процесів. Ключовим аспектом цієї парадигми є баланс між людськими управлінськими компетенціями та можливостями ШІ.

Вже зараз можна побачити як змінюються підходи до організації праці, де сучасні компанії переходять до більш адаптивних і гнучких моделей. Використання ШІ в бізнесі відкриває значні переваги для власників капіталу, зокрема шляхом оптимізації витрат на персонал і спрощення управління. Застосування штучного інтелекту дозволяє автоматизувувати рутинні та аналітичні процеси, замінюючи велику кількість працівників ефективними алгоритмами. Це дає змогу підтримувати невеликий штат співробітників, зосереджених на стратегічних завданнях, що в свою чергу скорочує витрати на заробітну плату, соціальні гарантії та офісне утримання. Легка керованість невеликою командою

сприяє швидшому прийняттю рішень, гнучкості в адаптації до змін ринку та мінімізації операційних ризиків, що робить бізнес більш прибутковим та стійким.

Впровадження різних інструментів ШІ відбувається практично у всіх напрямках роботи сучасних менеджерів, починаючи з набору команд, коли попередній розгляд резюме та погодження часу інтерв'ю відбувається за допомогою інструментів на базі ШІ (HireVue, DevSkiller TalentScore, Harver та інші), які за заданими параметрами проводять фільтрацію та відбір найбільш релевантних резюме, погоджують час інтерв'ю, а потім його ще й самі і проводять, що зараз дуже активно використовується в роботі багатьох китайських банків [1]. В свою чергу потенційні кандидати також використовують потенціал та можливості ШІ для створення своїх резюме та відповідей на питання під час інтерв'ю, що врешті призводить до ситуації, коли одні ШІ створюють резюме, а інші їх перевіряють, зводячи роль людини у процесі рекрутингу до мінімуму. Наслідки подібної практики ще прийде вивчати і досліджувати вже найближчим часом.

Наступним великим напрямом впровадження ШІ є автоматизація багатьох рутинних повсякденних обов'язків менеджерів. До них можна віднести такі види функціональних задач як листування з клієнтами, відповіді на їх типові питання у чатах, консультування клієнтів, ведення протоколу зустрічей та підготовка різних артефактів за результатами їх проведення, до яких можна віднести наступні: транскрипція відеоконференцій, створення списку задач та строків їх виконання, призначення відповідальних, формалізація та опис ідей, створення самого протоколу зустрічей за встановлених зразком та багато інших, що вже досить якісно можуть робити такі ШІ сервіси як Zoom, Fellow, Notta та інші. Враховуючи велику кількість подібних рутинних задач, їх автоматизація за допомогою ШІ інструментів допомагає менеджерам суттєво спростувати процеси комунікацій, об'єднуючи електронну пошту, повідомлення з месенджерів, соціальних мереж, SMS та календарів в єдиний інтерфейс, що знижує когнітивне навантаження на них, знімаючи з менеджерів необхідність перемикатися між численними платформами чи витрачати час на аналіз формулювань, а навпроти зосередитися на управлінні командами, аналізі даних чи прийнятті рішень, не переймаючись про втрату важливих повідомлень.

Аналітика даних також відіграє критично важливу роль в роботі менеджерів, бо вони в своїй роботі мають справу з бюджетами, з великою кількістю відгуків клієнтів у соціальних мережах, з прогнозуванням продаж, що вже в багатьох випадках автоматизовано, але при інтеграції в ці процеси штучного інтелекту відбувається значне прискорення в роботі менеджерів, що робить управлінські рішення більш якісними та адаптивними.

Одним з багатьох прикладів ШІ інструментів, котрі допомагають зняти навантаження із найскладніших аспектів роботи сучасного менеджера в напрямі моніторингу та аналізу даних, можна назвати Amplitude AI [2] – сервісу, який використовується для аналізу поведінки користувачів та формування прогнозів щодо розвитку продукту. Ця система безперервно збирає дані з різноманітних джерел, аналізує їх у реальному часі й виявляє відхилення у поведінці користувачів. У випадку змін ШІ надсилає сповіщення, дозволяючи менеджеру оперативно реагувати. Також система може відповідати на запитання менеджера та візуалізувати дані у вигляді діаграм чи графіків, а також робити висновки та прогнози.

Не буде повним аналіз інструментів та засобів штучного інтелекту без згадки й про ChatGPT та його аналогів. Інструменти подібного класу буквально за кілька років були впровадженні в роботу не лише менеджерів, а й фахівців таких напрямків як копірайтинг, програмування, маркетинг та інших. Рішення на базі генеративних моделей штучного інтелекту зараз вже широко використовуються менеджерами для створення текстів, маркетингових матеріалів, листів та різних документів. Однак при більш просунутому рівні використання потенціалу цього інструментарію можна отримати значно більший ефект. Зокрема, ChatGPT може бути ефективно застосований для проведення мозкових штурмів спільно зі штучним інтелектом задля генерування ідей, спрямованих, наприклад, для покращення продукту чи розроблення нових функцій.

Враховуючи викладене, можна зробити висновок, що інтеграція штучного інтелекту у сферу менеджменту стає ключовим чинником трансформації сучасних підходів до управління. Використання інноваційних платформ, дозволяє менеджерам оптимізувати рутинні процеси, автоматизувати складні аналітичні завдання та забезпечувати ефективне управління інформацією. Завдяки ШІ, менеджери можуть швидше приймати рішення, краще розуміти потреби клієнтів, прогнозувати їхню поведінку та адаптуватися до змін. Ці інструменти зменшують навантаження на менеджерів, звільняючи час для стратегічних напрямів роботи і водночас знижують витрати на операційну діяльність. Ті організації, які найкраще адаптуються до цих змін в управлінській парадигмі нового покоління та зможуть інтегрувати технології штучного інтелекту в роботу свого менеджменту отримають значні стратегічні переваги за рахунок можливості оптимізації роботи команд, удосконалення користувацького досвіду і підвищення якості ухвалених рішень. Адже у сучасному світі з високою конкуренцією у всіх сферах бізнесу стає критично важливим бути гнучким та вміти використовувати новітні технології.

Література

[1] China banks use AI in recruitment, drawing mixed views from easing anxiety to trapping candidates [Електронний ресурс] – Режим доступу до ресурсу: <https://www.scmp.com/news/people-culture/trending-china/article/3290763/china-banks-use-ai-recruitment-drawing-mixed-views-easing-anxiety-trapping-candidates>

[2] Build Great Digital Products & Experiences [Електронний ресурс] – Режим доступу до ресурсу: <https://amplitude.com>

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ОПТИМІЗАЦІЇ СКЛАДУ ФУТБОЛЬНОЇ КОМАНДИ НА ОСНОВІ ПРОГНОЗУВАННЯ РЕЗУЛЬТАТИВНОСТІ ГРАВЦІВ

Коваленко В.П., Льовкін В.М.

E-mail: vliovkin@gmail.com

Запоріжжя, Національний університет «Запорізька політехніка»

В сучасному футбольному середовищі важливу роль відіграє ефективне формування команди, здатної досягти найкращих результатів. Основною задачею є об'єктивне оцінювання потенціалу гравців на основі їхньої статистики, з урахуванням вимог до складу команди. Для цього потрібні програмні рішення, які можуть поєднувати методи машинного навчання та оптимізаційні алгоритми. У даній роботі представлено програмне забезпечення, яке дозволяє оптимізувати склад футбольної команди, прогножуючи результати гравців на основі їхніх статистичних даних. Програма враховує різні позиції гравців. В основі рішення лежать такі алгоритми: Random Forest для прогнозування результативності гравців та лінійне програмування для оптимізації складу команди.

Програма розроблена мовою програмування Python. Робота програми починається із завантаження статистичних даних гравців із CSV-файлу за допомогою бібліотеки pandas [1]. У даних створюється нова цільова змінна, яка враховує голи, результативні передачі, хвилини гри, матчі без пропущених голів та позицію гравців. Ця змінна використовується як ціль для моделі машинного навчання.

Для прогнозування результативності гравців використовується модель RandomForestRegressor з бібліотеки scikit-learn [2]. Алгоритм Random Forest є ансамблевим методом машинного навчання, що базується на використанні множини дерев рішень. Основна ідея полягає у тому, що кожне дерево у моделі створюється на основі випадкової підмножини даних та характеристик, виділення яких загалом і є важливим завданням в межах описаної задачі. Остаточний результат формується шляхом усереднення прогнозів, отриманих від усіх дерев, які наявні у ансамблі. Це дозволяє алгоритму уникати перенавчання, бути стійким до шуму в даних та ефективно працювати зі складними

взаємозв'язками у даних, що посилює необхідність його застосування для розв'язання цієї задачі. Навчання моделі відбувається на основі навчального набору даних, які створюються за допомогою функції `train_test_split` з бібліотеки `scikit-learn`.

Після прогнозування результативності модель додає розраховані значення до початкового набору даних у вигляді нової ознаки. Оптимізація складу команди здійснюється за допомогою методу лінійного програмування з використанням функції `linprog` з бібліотеки `scipy` в частині підпаketу `optimize` [3]. Було враховано обмеження на кількість гравців за позиціями (1 воротар, 4 захисники, 4 півзахисники, 2 нападники). У результаті визначається оптимальний склад команди, максимізуючи результативність у рамках заданих обмежень.

Основні переваги розробки включають точність прогнозів, забезпечену використанням алгоритму `Random Forest`, гнучкість у зміні параметрів вибору команди, а також оптимальність у формуванні складу. Запропоноване програмне забезпечення демонструє можливості ефективного застосування машинного навчання та оптимізаційних методів у футбольному аналізі. Використання цієї розробки дозволяє автоматизувати процес прийняття рішень при формуванні складу команди, враховуючи як індивідуальну результативність гравців, так і загальні обмеження.

Література

[1] Pandas documentation [Електронний ресурс] – Режим доступу до ресурсу: <https://pandas.pydata.org/docs/index.html>

[2] sklearn API [Електронний ресурс] – Режим доступу до ресурсу: <https://scikit-learn.org/stable/modules/classes.html>

[3] SciPy documentation [Електронний ресурс] – Режим доступу до ресурсу: <https://docs.scipy.org/doc/scipy/>

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ РЕКОМЕНДУВАННЯ МУЗИЧНИХ КОМПОЗИЦІЙ НА ОСНОВІ ІНТЕРЕСІВ КОРИСТУВАЧА

Коганті К. К., Льовкін В. М.

E-mail: vliovkin@gmail.com

Запоріжжя, Національний університет «Запорізька політехніка»

У сучасному цифровому середовищі, активною частиною якого є музика, можливість персоналізувати списки відтворення музики для користувачів стала важливою функцією для потокових платформ. Зважаючи на велику кількість доступних пісень, створення рекомендацій на основі вподобань користувачів є одночасно складним і важливим завданням. Розробка програмного забезпечення, що має підтримувати цей процес, не лише покращує користувацький досвід, але й сприяє глибшій взаємодії з платформою.

У цій роботі описано створення програмного додатку, призначеного для рекомендування музичних композицій користувачам на основі їхніх інтересів. Додаток використовує дані з платформи `Spotify` для отримання списків відтворення, аналізу музичних композицій та генерування персоналізованих рекомендацій за допомогою машинного навчання. Метод, реалізований у програмі для підтримки рекомендування музичних композицій, працює в декілька етапів: отримання списків відтворення музичних композицій, завантаження музичних композицій, виділення аудіо-характеристик, навчання рекомендаційної моделі та генерування рекомендацій на основі обраних користувачем музичних композицій. Користувачі можуть взаємодіяти з програмою, вибираючи списки відтворення музичних композицій, переглядаючи музичні композиції та отримуючи індивідуальні пропозиції щодо схожої музики. Музичні композиції з обраного списку відтворення завантажуються разом з їхніми звуковими характеристиками, такими як танцювальність, енергійність та валентність. В основі використовується метод `k`-найближчих сусідів (`Nearest Neighbors`) для навчання моделі рекомендацій на основі витягнутих

характеристик музичних композицій. На основі музичної композиції, обраної користувачем, навчена модель пропонує схожі музичні композиції зі списків прослуховування.

Для реалізації використано бібліотеки scikit-learn для реалізації методу Nearest Neighbors [1], Spotipy [2] для взаємодії з API сервісу Spotify для отримання списків відтворення музичних композицій, музичних композицій та аудіо-функцій, а також Pandas для маніпуляцій з даними та попередньої обробки. Модель Nearest Neighbors визначає схожі музичні композиції, аналізуючи числові характеристики звуку, такі як темп, енергійність і танцювальність. Цей підхід ефективний для пошуку подібності у багатовимірних даних.

Основні функції розробленого програмного забезпечення включають пошук списків відтворення музичних композицій і музичних композицій, вилучення аудіо-даних і створення рекомендацій. Функція `get_featured_playlists` витягує популярні списки відтворення музичних композицій, `get_tracks_from_playlist` витягує музичні композиції з вказаного списку відтворення, а `get_audio_features` витягує числові характеристики музичних композицій. Функція `train_model` навчає модель на основі методу k-найближчих сусідів на основі ознак музичних композицій, а `recommend_tracks` генерує рекомендації для вибраної музичної композиції, визначаючи її найближчих сусідів у просторі ознак.

Розроблене програмне забезпечення дозволяє користувачам відкривати для себе нову музику відповідно до своїх уподобань, досліджувати музичні композиції зі схожими звуковими характеристиками та покращувати свій досвід прослуховування, створюючи унікальні списки відтворення музичних композицій.

Література

[1] Nearest Neighbors – scikit-learn [Електронний ресурс] – Режим доступу до ресурсу: <https://scikit-learn.org/stable/modules/neighbors.html>

[2] Spotipy Library for Python [Електронний ресурс] – Режим доступу до ресурсу: <https://spotipy.readthedocs.io>

АНАЛІЗ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ УПРАВЛІННЯ ІТ-ПРОЄКТАМИ

Назаров Д.Л., Слісаренко М.В.

E-mail: unrealist@ukr.net, slisarenko.mykola@hneu.net

Харків, Харківський національний економічний університет імені Семена Кузнеця

Єдиною галуззю народного господарства, яка навіть під час пандемії Ковід 19 та військового стану демонструє приріст обсягів діяльності та прибутку, є ІТ-галузь. Динамізм, мобільність та еластичність до різких змін зовнішнього середовища ІТ-галузі забезпечується специфікою діяльності ІТ-компаній та їх здатністю проваджувати свою діяльність децентралізовано у часі та просторі. Така децентралізація виконання ІТ-проектів стає можливою, в першу чергу, за допомогою використання сучасних інформаційно-комунікаційних технологій. За наявності ефективного менеджменту, наступною умовою та запорукою успішного виконання ІТ-проекту є використання досконалого програмного забезпечення для управління проектом, яке охоплює усі стадії проекту, забезпечує усі види взаємодії учасників, спільну роботу над проектом, планування робіт та часу на їх виконання, дотримання плану та вимог замовника тощо.

Аналіз складу команди ІТ-проекту, комплексу завдань (робіт), який виконує кожен з учасників проекту, видів взаємодія учасників ІТ-проекту під час його виконання дозволив визначити критерії аналізу програмного забезпечення для управління та забезпечення ІТ-проектів, а саме: функціонал: має надавати необхідні функції для управління проектами, такі як планування, розподіл завдань, відстеження прогресу, управління ресурсами, облік часу виконання завдань та робіт, комунікація (внутрішній месенджер, додавання коментарів до завдань) та звітність (наявність якісної технічної підтримки та документації); ширина функціоналу та масштабованість: має забезпечувати монопроектні рішення, чи управління

портфелями проєктів, а також здатність підтримувати масштабування проєктів і команд; гнучкість налаштувань та забезпечення гнучких моделей розробки: має бути гнучкою та дозволяти налаштовувати робочий процес, адаптувати інструменти до потреб конкретного проєкту, а також забезпечувати розробку продуктів за гнучкими моделями типу Agile, Scrum, Kanban тощо; інтегрованість: має інтегруватися з іншими інструментами, які використовуються в компанії, наприклад, з інструментами Atlassian Group, Microsoft (Teams, Outlook і Power BI), Slack і Google Calendar тощо; безпечне використання: має забезпечувати безпеку даних проєкту; зручність використання: інтерфейс програми має бути інтуїтивно зрозумілим і зручним для усіх користувачів (учасників проєкту); ціна: вартість програми повинна відповідати бюджету проєкту та компанії. Аналіз найбільш поширених програм для управління ІТ-проєктами за виділеними критеріями наведено у табл.1.

Таблиця 1 – Характеристика програмного забезпечення для управління ІТ-проєктами

Назва програмного забезпечення	Функціональність	Ширина функціоналу та масштабованість	Гнучкість налаштувань та підтримка моделей розробки	Інтегрованість	Безпека	Зручність використання	Ціна: вартість
1	2	3	4	5	6	7	8
Jira	Розширена підтримка Agile та DevOps, інтегровані інструменти для управління беклогом, спринтами та моніторингу виконання завдань	Висока масштабованість, адаптація до великих проєктів, підтримка великих команд та інтеграція з корпоративними системами	Підтримує Waterfall, Agile, Scrum, Kanban, інтеграція з CI/CD-процесами	Глибока інтеграція з Confluence, Bitbucket, Bamboo та іншими DevOps-інструментами	Відповідає стандартам ISO 27001, GDPR, підтримує двофакторну автентифікацію	Складний інтерфейс, потребує навчання	\$7 за користувача/місяць (план Standard), розширені функції у планах Premium та Enterprise
Asana	Орієнтоване на командне управління проєктами, підтримує Kanban та Scrum, дозволяє структурувати завдання та відстежувати їх прогрес	Середня масштабованість, підходить для команд середнього розміру, інтеграція з хмарами	Гнучкі налаштування з можливістю адаптації до Scrum та Kanban	Підтримка понад 100 інтеграцій, включаючи Slack, Google Drive, Zoom	Шифрування даних, контроль доступу, відповідає SOC 2	Інтуїтивно зрозумілий, легке навчання	Безкоштовно для команд до 15 осіб, преміум-плани від \$10 за користувача/місяць
Trello	Візуалізація робочих процесів через Kanban-дошки, ефективне управління малими та середніми проєктами	Обмежена масштабованість, орієнтована на малі проєкти та окремі команди	Обмежена можливість налаштувань, в основному орієнтована на Kanban	Інтеграція через API та сторонні плагіни	Базові засоби захисту, відповідність GDPR	Дуже простий, швидкий у використанні	Безкоштовна базова версія, преміум-плани від \$5 за користувача/місяць
Microsoft Project	Комплексна система управління портфелями проєктів, розширена підтримка Gantt-діаграм, фінансове планування, аналіз продуктивності ресурсів	Максимальна масштабованість, ефективне управління великими портфелями проєктів, інтеграція з ERP-системами	Глибока кастомізація робочих процесів, підтримка критичних шляхів, адаптація до різних методологій	Глибока інтеграція з Microsoft 365, SharePoint, Teams	Корпоративні механізми захисту, відповідність ISO, SOC, HIPAA	Складний, потребує професійного налаштування	Від \$10 за користувача/місяць, корпоративні плани з розширеними можливостями

1	2	3	4	5	6	7	8
Basecamp	Інструмент для колаборативного управління проєктами, орієнтований на малий та середній бізнес, підтримує централизоване спілкування та управління завданнями	Підтримує середню кількість користувачів, інтегрується з основними сервісами для командної роботи	Підтримує класичне управління проєктами з елементами гнучких методологій	Обмежена інтеграція з популярними сервісами (Google Workspace, Dropbox)	Стандартне шифрування, контроль доступу	Збалансований між функціональністю та простотою	\$15 за користувача/місяць, фіксований план \$299/місяць для необмеженої кількості користувачів
ClickUp	Гнучка система управління завданнями з багатовимірним представленням даних, включає вбудовані автоматизовані робочі процеси, інтеграції	Гнучка масштабованість, підтримує розширення функціоналу через інтеграції та API	Розширені можливості налаштування, підтримка індивідуальних робочих процесів	Розширена інтеграція через API та Zapier	Розширені налаштування безпеки, інтеграція з SIEM	Сучасний UX, зручний інтерфейс	Безкоштовна базова версія, преміум-плани від \$7 за користувача/місяць
monday.com	Модульне середовище для адаптивного управління робочими процесами, підтримує персоналізовані шаблони та потужні інструменти аналітики	Висока масштабованість завдяки модульній архітектурі, підходить для середніх та великих команд	Адаптивні моделі управління, підтримка власних автоматизованих робочих процесів	Висока інтеграція через відкритий API, підтримка Power Automate	Відповідає PCI DSS, розширена автентифікація	Гнучкий інтерфейс, підтримка кастомізації	Плани від €9 за користувача/місяць, корпоративні пакети
Teamwork	Спеціалізоване ПЗ для командної роботи, включає відстеження часових витрат, фінансове планування та звіти по навантаженню ресурсів	Гнучка архітектура, що дозволяє розширювати функціонал залежно від потреб проєкту	Гнучкі можливості налаштування, інтеграція з фінансовими системами	Інтеграція з інструментами фінансового та ресурсного планування	Вбудовані механізми захисту та контроль ризиків	Простий у використанні з базовими знаннями	Плани від \$10.99 за користувача/місяць, гнучка цінова політика
Smartsheet	Інноваційна платформа управління проєктами на основі електронних таблиць, підтримує автоматизовані процеси прийняття рішень	Підтримує середній та великий бізнес, інтегрується з іншими інструментами для обробки великих БД	Динамічне налаштування процесів управління проєктами, що дозволяє швидко адаптуватися до змін	Підтримка інтеграції з BI-аналітикою та платформами даних	Контроль доступу на рівні завдань, SOC 2	Зрозумілий інтерфейс, швидке навчання	Плани від \$9 за користувача/місяць, корпоративні рішення
SpiraPlan	Інструмент для управління життєвим циклом проєкту з підтримкою інтеграцій з DevOps, комплексний підхід до відстеження продуктивності	Максимальна масштабованість для управління комплексним і програмами та інженерними проєктами	Підтримка комплексних робочих процесів для IT-розробки	Глибока інтеграція з DevOps-екосистемами	Корпоративна безпека, відповідність NIST, ISO	Орієнтований на професіоналів	Ціноутворення залежить від рівня підтримки та масштабів використання

1	2	3	4	5	6	7	8
Notion	Мультифункціональна платформа для управління знаннями та організаційного управління проектами, що поєднує функції управління завданнями, документування, баз даних та командної співпраці	Висока масштабованість; підтримує персоналізовані робочі простори, інтегрується з API для кастомізованого розширення функцій.	Гнучка конфігурація структури даних, підтримує Kanban-дошки, календарі, БД та інші інструменти структурованого управління процесами	Інтегрується з Google Drive, Slack, Zapier, а також має API для розширених можливостей автоматизації	Відповідає стандартам SOC 2, підтримує розширене управління доступами, шифрування даних	Інтуїтивно зрозумілий інтерфейс; підтримує кастомізацію відповідно до специфічних організаційних вимог	Безкоштовна версія для індивідуального використання, плани для команд починаються від \$10 за користувача на місяць

Наведений в табл. 1 перелік програм не є вичерпним. Вибір інструменту залежить від потреб і розміру команди, а також від вимог ІТ-проєкту: якщо проєкт невеликий та короткотривалий – не обов'язково обирати складне і вартісне програмне забезпечення, яке найбільш поширене. У такому випадку можна обійтися простішими програмами, використання яких забезпечить простіше та швидше управління проєктом.

Литература

- [1] Jira [Електроний ресурс] – Режим доступу до ресурсу: <https://www.atlassian.com/software/jira>
- [2] Asana [Електроний ресурс] – Режим доступу до ресурсу: <https://asana.com/>
- [3] Trello [Електроний ресурс] – Режим доступу до ресурсу: <https://trello.com/>
- [4] Microsoft Project [Електроний ресурс] – Режим доступу до ресурсу: <https://www.microsoft.com/uk-ua/microsoft-365/project/project-management-software>
- [5] Basecamp [Електроний ресурс] – Режим доступу до ресурсу: <https://basecamp.com/>
- [6] ClickUp [Електроний ресурс] – Режим доступу до ресурсу: <https://clickup.com/>
- [7] Monday.com [Електроний ресурс] – Режим доступу до ресурсу: <https://monday.com/>
- [8] Teamwork [Електроний ресурс] – Режим доступу до ресурсу: <https://www.teamwork.com/>
- [9] Smartsheet [Електроний ресурс] – Режим доступу до ресурсу: <https://www.smartsheet.com/>
- [10] SpiraPlan [Електроний ресурс] – Режим доступу до ресурсу: <https://www.inflectra.com/Products/SpiraPlan/Highlights.aspx>
- [11] Notion [Електроний ресурс] – Режим доступу до ресурсу: <https://www.notion.com/>

СТВОРЕННЯ ГЕОІНФОРМАЦІЙНОЇ СИСТЕМИ ДЛЯ ПРОЄКТІВ ВІДНОВЛЕННЯ

Осауленко І. А.

E-mail: iger372@meta.ua

Черкаси, Черкаський національний університет імені Богдана Хмельницького

Розроблена Міністерством цифрової трансформації України Стратегія розвитку сфери відкритих даних є черговою важливою віхою в напрямку удосконалення системи електронного урядування і водночас покликана відіграти непересічну роль в процесі планування післявоєнного відновлення. Серед актуальних завдань створення детальних реєстрів знищеного і пошкодженого майна, наявних об'єктів житлової нерухомості для розміщення внутрішньо переміщених осіб, вільних земельних ділянок для ведення бізнесу.

Зазначена інформація необхідна для обґрунтованого прийняття управлінських рішень як на загальнодержавному рівні, так і на рівні окремих регіонів і громад. Крім того, розвиток

відкритих даних сприятиме покращенню взаємодії громадян з державними органами, може спростити деякі процедури, наприклад, отримання допомоги і компенсацій особами, постраждалими внаслідок бойових дій, стимулюватиме ділову активність, інноваційні процеси і створення нових робочих місць, а також допомагатиме шукачам вакансій краще зорієнтуватись на ринку праці.

Ще один важливий аспект пов'язаний з тим, що проекти відновлення потребуватимуть великих обсягів зовнішнього фінансування, а однією з ключових вимог міжнародних донорів та інвесторів є прозорість використання коштів та інших ресурсів, що зумовлює необхідність відповідних можливостей для моніторингу.

Водночас слід розуміти, що для ефективного використання відкриті дані повинні бути попередньо зібрані і підготовлені, а також подані у зручній для користувачів формі [1].

Для представлення різноманітних просторових даних, у тому числі при плануванні розвитку територій, впродовж останніх років вже майже повсюдно стали використовуватись геоінформаційні системи (ГІС). Оскільки використання комерційних продуктів вимагає додаткових витрат, що не для всіх суб'єктів є прийнятним, доцільно звернути увагу на вільно розповсюджені системи з відкритим кодом, серед яких напевне найвідомішою є QGIS.

Ця система має велику кількість переваг, в числі яких кросплатформенність, можливість інтеграції з іншим популярним відкритим інструментом OpenStreetMap та імпорту даних із різних СУБД, широкий функціонал, робота з растровими і векторними шарами, доступний великий набір плагінів і можливість створення власних на мові програмування Python для вирішення вузькоспеціалізованих завдань [2].

За рахунок отримання даних від інформаційної системи управління проектами, яка використовується, наприклад, регіональним проектним офісом, ГІС може детально відобразити просторову структуру проекту, що сприятиме кращому розумінню специфіки проектів з кількома локаціями і складною логістикою. Також можлива візуалізація стейкхолдерів і меж територій, на які проект справлятиме той чи інший вплив (економічний, екологічний, соціальний, безпековий тощо).

Звісно, можуть бути додані шари, які відображатимуть поточний стан виконання проектів в розрізі дотримання графіків виконання робіт і використання ресурсів, передбачені фільтри за територіальною, галузевою чи іншими ознаками.

Ще один аспект, який заслуговує на увагу, це підбір команди проекту шляхом розміщення в ГІС інформації про вакансії і відповідні кваліфікаційні вимоги.

Література

[1] Стратегія розвитку сфери великих даних (Проект). [Електронний ресурс] – Режим доступу до ресурсу: <https://thedigital.gov.ua/storage/uploads/files/2.%20Стратегія.pdf>.

[2] Hoptsi D., Siedov A., Anopriienko T., Khainus D., Yaremko D. Advantages of using QGIS to solve spatial planning tasks. Baltic surveying: International Scientific Journal. Volume 18. Poland : Lithuania, 2023. - С. 50-56.

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ АВТОМАТИЗОВАНОГО ВИЗНАЧЕННЯ АКОРДІВ У АУДІОФАЙЛАХ

Панченко Є.О., Льовкін В.М.

E-mail: vliovkin@gmail.com

Запоріжжя, Національний університет «Запорізька політехніка»

Музика є складовою культури та стала неодмінною майже у всіх аспектах людського життя, а тому розвиток технологій аналізу аудіо є важливою задачею. Відповідно програма, що опрацьовує аудіофайли для автоматичного визначення акордів, актуальна для підтримки галузі. Використання цієї програми можливе для використання як у навчанні музикантів, так у роботі над інструментами для композиторів та навіть в інтерактивних музичних додатках. Оскільки обсяги цифрової музичної інформації продовжують зростати, підвищується

необхідність ефективного та точного розпізнавання акордів існуючим програмним забезпеченням.

У цій роботі розроблено програмне забезпечення, яке дозволяє автоматично визначати акорди в аудіофайлах формату WAV. Для реалізації використано сучасні методи обробки сигналів та машинного навчання. Спочатку аудіофайл завантажується за допомогою бібліотеки librosa, з нього витягуються мелкепстральні коефіцієнти, які виступають основними ознаками для подальшого аналізу [1]. Додатково для аналізу нотного запису використовуються файли формату MusicXML, які опрацьовуються за допомогою бібліотеки music21, з метою отримання акордів у вигляді їхніх інтервальних представлень.

Для створення програмного забезпечення було використано мову програмування Python, яка є високорівневою, інтерпретованою та об'єктно-орієнтованою мовою, що забезпечує зручність розробки завдяки своїй гнучкості та багатій екосистемі бібліотек. У розробці застосунку були використані такі ключові бібліотеки окрім librosa. Бібліотека music21, що дозволяє працювати з нотними записами у форматі MusicXML, забезпечуючи доступ до гармонійної структури композицій та акордів [2]. Бібліотека sklearn (Scikit-learn), яка використовувалась для навчання моделі машинного навчання RandomForestClassifier, що дозволяє ефективно класифікувати акорди на основі екстрагованих ознак [3].

Робота програми над автоматизованим визначенням акордів у аудіофайлах відбувається за наступними етапами:

- на початковому етапі завантажується аудіофайл формату WAV за допомогою функції librosa.load, далі з аудіосигналу екстрагуються мелкепстральні коефіцієнти;
- з нотного запису у форматі MusicXML витягуються акорди за допомогою бібліотеки music21, парсинг XML-файлу здійснюється функцією converter.parse;
- навчання моделі RandomForestClassifier починається з підготовки навчальної вибірки: ознаки з аудіо-файлів та відповідні акорди з нотного запису поєднуються у дві окремі множини: X (вектор ознак) та Y (мітки акордів);
- для прогнозування акорду використовується функція predict_chord, яка приймає на вхід навчений класифікатор та новий аудіофайл, здійснюється прогноз акорду за допомогою методу predict;
- завершальним етапом є перетворення числових інтервальних представлень акордів у нотації (наприклад, "C", "D#") за допомогою функції, яка співставляє інтервали із назвами нот.

Література

[1] McFee, B., Raffel, C., Liang, D., et al. (2015). "librosa: Audio and Music Signal Analysis in Python" [Електронний ресурс] – Режим доступу до ресурсу: https://www.researchgate.net/publication/328777063_librosa_Audio_and_Music_Signal_Analysis_in_Python

[2] Cuthbert, M. S., & Ariza, C. (2010). "music21: A Toolkit for Computer-Aided Musicology and Symbolic Music Data" [Електронний ресурс] – Режим доступу до ресурсу: <https://archives.ismir.net/ismir2010/paper/000108.pdf>

[3] Pedregosa, F., et al. (2011). "Scikit-learn: Machine Learning in Python" [Електронний ресурс] – Режим доступу до ресурсу: <https://www.jmlr.org/papers/volume12/pedregosa11a/pedregosa11a.pdf>

СИСТЕМА ВИЗНАЧЕННЯ НОТ НА ОСНОВІ ЧАСТОТИ ЗВУКОВИХ КОЛИВАНЬ

Петров А. Р.

Керівник: Обухова К. О.

E-mail: miray7772@gmail.com

Миколаїв, Чорноморський національний університет імені Петра Могили

У світі музики та акустики визначення нот на основі частоти звукових коливань стало невід'ємною частиною сучасних технологій. Ця технологія широко використовується для автоматичного налаштування музичних інструментів, аналізу звукових записів, а також в навчальних програмах для музикантів. Вона дозволяє забезпечити високу точність та швидкість розпізнавання нот, що є надзвичайно важливим в умовах реального часу, наприклад, під час живих виступів або при використанні музичних інструментів.

З розвитком цифрових технологій та аудіообробки, застосування систем визначення нот стало доступним не лише професіоналам, але й аматорам та студентам музичних навчальних закладів. Тому дослідження цієї технології має велике практичне значення для музичної індустрії, а також для розвитку нових методів у музичному навчанні та аудіообробці.

Метою цієї роботи є розробка апаратно-програмного комплексу для визначення нот на основі частоти звукових коливань, що дозволяє забезпечити точне і швидке розпізнавання музичних нот в реальному часі. Для цього необхідно дослідити та застосувати сучасні методи аналізу частотних характеристик звуку, вивчити основні технології для розробки таких систем та визначити апаратні компоненти, які будуть використовуватися при створенні комплексу.

Для реалізації системи планується використати швидке перетворення Фур'є (FFT) – алгоритм, який розкладає звуковий сигнал на частотні складові, що дозволяє визначити його частоту (рис. 1).

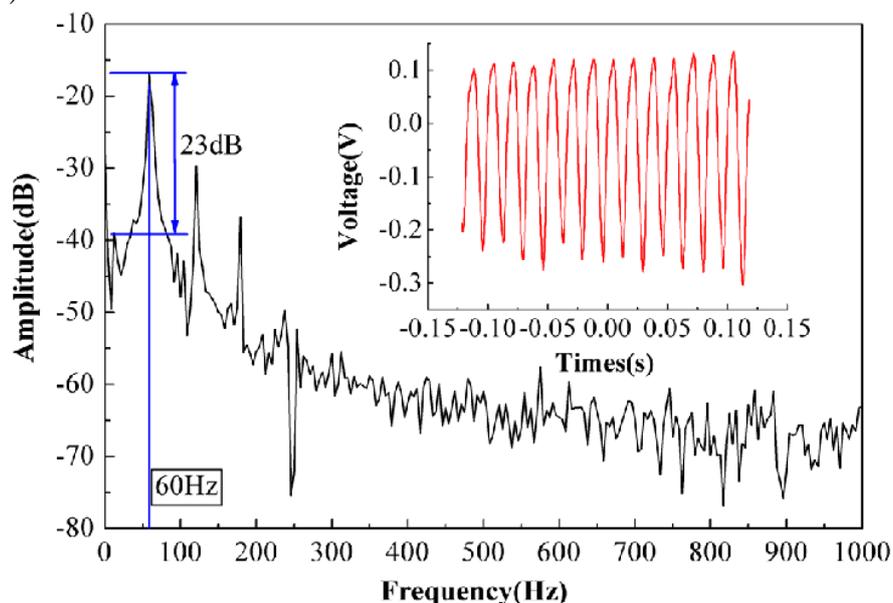


Рисунок 1 – Спектр у часовій та частотній області [1]

FFT використовується для перетворення часового аудіосигналу в частотне представлення. Математичною основою FFT є перетворення Фур'є, яке розкладає функцію часу (сигнал) на складові частоти [2]:

$$X(f) = \int_{-\infty}^{\infty} x(t)e^{-j2\pi ft} dt$$

де $X(f)$ – представлення в частотній області;

f – частота;

t – час;

$e^{-j2\pi ft}$ – комплексна експоненціальна функція.

Алгоритм швидкого перетворення Фур'є ефективно обчислює це перетворення для дискретних сигналів, що робить його можливим для обробки навіть у застосунках реального часу. У процесі роботи системи також буде використано акустичний спектр, який являє собою сукупність частот звукових хвиль, аналіз яких допоможе досягти максимальної точності при розпізнаванні нот (рис. 2) [3].

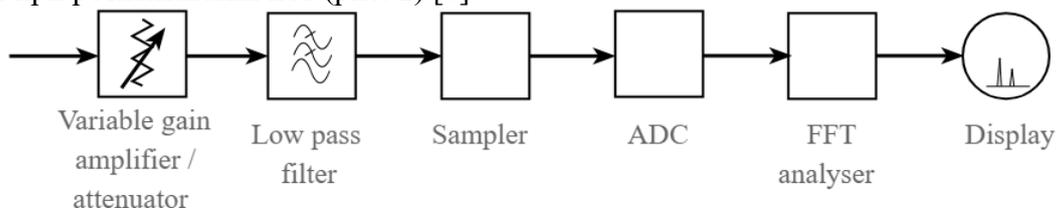


Рисунок 2 – Блок-схема аналізатора спектру FFT

Основою пристрою буде система розпізнавання звуку, яка вимірюватиме частоту звукових коливань і визначатиме відповідні музичні ноти. Основним елементом є мікрофонний модуль, що буде записувати звук та перетворювати його на електричний сигнал. Важливо, щоб мікрофон мав високу чутливість і мінімальні спотворення, оскільки точність визначення частоти залежить від якості вхідного сигналу. Для обробки звуку потрібен мікроконтролер – плата Arduino, що дозволить виконувати розрахунки для визначення частоти та ноти. Крім того, буде використано дисплей, для відображення нот, що відповідають частоті.

Алгоритм роботи системи визначення нот на основі частоти звукових коливань включає наступні кроки:

- мікрофонний модуль вловлює звукові коливання та перетворює їх на цифровий сигнал;
- цей сигнал обробляється плата Arduino, що реалізує алгоритм FFT, для виділення основної частоти;
- отримана частота порівнюється з базою даних музичних нот;
- на дисплеї виводиться точна нота, що відповідає цій частоті, разом з її значенням.

Використання Arduino, мікрофонного модуля, дисплея та алгоритму FFT у цій системі допоможе забезпечити розпізнавання звуків у режимі реального часу. Завдяки простоті та універсальності такої пристрій може знайти широке застосування. Система допоможе як музикантам, так і тим, хто просто цікавиться музикою. Вона стане в пригоді для поглиблення розуміння нотної системи та правильного налаштування музичних інструментів. Також система сприятиме вивченню основ музики та допоможе краще розрізняти ноти на слух.

Література

[1] Liu Yu., Ni W., Yang L., Huang S., Liu H., Sun Yi., Xia R., Yao Y., Yan, L., Luo, Yi., Xu Zh., Xu G., Sun Q., Tang X., Shum P. Real-time spectral interferometry enables ultrafast acoustic detection. *Applied Physics Letters*, 2023. Vol. 123, Is. 21. DOI: 10.1063/5.0178453.

[2] Ahmad M. Deep Learning 101: Lesson 23: The Basics of Audio Signal Processing with FFT. [Електронний ресурс] – Режим доступу до ресурсу: <https://munebsa.medium.com/deep-learning-101-lesson-23-the-basics-of-audio-signal-processing-with-fft-ffef65689c1d#:~:text=In%20audio%20processing%2C%20FFT%20is,signal%20into%20its%20frequency%20components> (Last accessed: 10.02.2025).

[3] Poole I. FFT Spectrum Analyzer. [Електронний ресурс] – Режим доступу до ресурсу: <https://www.electronics-notes.com/articles/test-methods/spectrum-analyzer/fft-fast-fourier-transform-spectrum-analyser.php> (Last accessed: 10.02.2025).

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ПРИ ВИВЧЕННІ ДИСЦИПЛІНИ «ПРОТИПОЖЕЖНЕ ВОДОПОСТАЧАННЯ»

Петухова О.А., Білаш Є.А., Швед А.В.

E-mail: voda1970@gmail.com

Черкаси, Національний університет цивільного захисту України

Дисципліна “Противопожежне водопостачання” є професійним обов'язковим освітнім компонентом підготовки бакалаврів з галузі знань К «Безпека та оборона» за спеціальністю К8 «Пожежна безпека» за освітньо-професійною програмою «Пожежна безпека». Протягом останніх чотирьох років виникали труднощі у освітньому процесі багатьох вишів України: спочатку Covid, зараз війна. Але підготовка якісних фахівців завжди була і залишається основною задачею освіти. Для досягнення цього використовуються різні форми та методи навчання, заохочення всіх учасників освітнього процесу до покращення викладання та засвоєння навчального матеріалу, відпрацювання практичних навичок, що може забезпечити використання інформаційних технологій (ІТ).

В Національному університеті цивільного захисту України використання ІТ почали здійснювати задовго до того, як в цьому стала гостра необхідність [1-3]. Тому деякій досвід вже мали і викладацький склад і методичні працівники, і цей досвід поглиблюється та продовжує з успіхом втілюватися в освітній процес. У зв'язку з необхідністю більшість занять переводити в режим онлайн навчання, потреба у розширенні кола використання сучасних онлайн методів та способів значно зростає. Проведення лекцій на доступних платформах ZOOM та MEET вже не викликає труднощів та добре сприймається всіма учасниками освітнього процесу. Але є питання, пов'язані з іншими етапами планування та реалізації одержання знань та навичок.

На думку авторів, основні складові використання ІТ у вищі можна представити наступними групами:

- складання розкладу занять,
- заняття,
- спостереження за успішністю та відвідуванням занять,
- формування бази результатів навчання.

Найбільша кількість учасників освітнього процесу приймають участь саме у другій групі – заняттях. Правильна та раціональна організація реалізації проведення занять безпосередньо впливає і на якість освітнього процесу і на ефективність, що є одним з показників його успішності.

На фоні відповідної якісної організації методичної складової занять, важливим є якісне відпрацювання кожного їх етапу. Так, на початку онлайн заняття, як правило, здійснюється перевірка присутності здобувачів вищої освіти. Для цього можливо зробити особисту перевірку, але при значній кількості здобувачів у групі, це займає багато часу. Можливо зробити скрін екрану та після заняття заповнити відповідний журнал, але це також потребує додаткового часу. В НУЦЗ України використовується програмний комплекс "Автоматизована система управління навчальним закладом" (info@mkr.org.ua), що являє собою безліч пов'язаних між собою програм, які забезпечують управління вишем в єдиному інформаційному просторі. Комплекс включає модулі, що працюють в середовищі Windows (навчальний модуль, деканат, абітурієнт, методичний відділ, відділ кадрів та ін.) та WEB портал (відображення розкладу занять, успішності, навчальних планів, нарахувань оплат за гуртожиток, контроль оплат за навчання та гуртожиток, тестування здобувачів вищої освіти, їх запис на вивчення вибіркового дисциплін тощо). Вся інформація зберігається в одній спільній базі даних. Саме за допомогою цього програмного комплексу з легкістю та дуже швидко здійснюється реєстрація здобувачів вищої освіти на заняттях, при цьому спосіб реєстрації викладач може обрати за власним розсудом - або саме викладач здійснює реєстрацію, або реалізується самореєстрація (з передбаченим механізмом виключення недобросовісності на цьому етапі).

На цьому робота з комплексом протягом заняття не завершується - в комплексі є журнал групи, який формується відповідно до списку групи, дисципліни, її тематичного плану та розкладу занять. Протягом заняття, або після нього, викладач може виставити оцінки, відмітити перескладання або, при відсутності здобувача на занятті, відпрацювання за відповідними заняттями. Кожному здобувачу доступна ця інформація з особистого кабінету, що є зручним та забезпечує відповідний рівень конфіденційності.

Наступним кроком заняття, а також додатковим способом перевірки та активності здобувачів, включаючи попередні заняття, є перевірка ступеня засвоєння знань за темою. Для цього успішно та ефективно використовується тестування. При викладанні дисципліни “Протипожежне водопостачання” використовуються гугл-класи, в яких викладаються теоретичні матеріали занять, завдання для самостійної роботи, методичні матеріали для їх виконання, а також розміщуються тести, створені за допомогою гугл-форм. Зазвичай для проходження тестів здобувачам вищої освіти надається час близько 10 хвилин, після цього проводиться аналіз результатів з демонстрацією відповідей (за згодою здобувача) або з знаходженням та обґрунтуванням правильних варіантів.

При проведенні лекцій активно використовуються презентації PowerPoint або WPS Presentation, які відображають структуру заняття, дозволяють звернути увагу на основні поняття, визначення, формули, включають в себе фото-, відеоматеріал. Презентація розміщується у гугл-класі. Тобто, за умовою наявності бажання, здобувачеві надається можливість розібратись у запропонованій темі безпосередньо протягом заняття, або самостійно.

Практичні заняття, які передбачають відпрацювання практичних навичок, дистанційно проводити дуже складно. Для того, щоб досягти успіхів і в цьому питанні, при вивченні дисципліни “Протипожежне водопостачання” використовуються навчально-тестові симулятори (програмні комплекси, що поєднують навчання за відповідною темою, містять відеодемонстрацію вправ, мають завдання для виконання здобувачами вищої освіти, реалізують оцінювання правильності дій на кожному етапі роботи), програмні комплекси для проведення розрахункових лабораторних робіт (лабораторна робота з розрахунку внутрішнього протипожежного водопроводу та дослідження впливу змін характеристик складових пожежних кран-комплектів на їх кількість), а також є досвід проведення тестових контрольних робіт з розв'язання задач за темою “Випробування на водовіддачу водопровідних мереж” (розроблений пакет на 10 варіантів, де кожний складається з п'яти задач).

Використання доступних ІТ дозволяє готувати та проводити лекції та практичні заняття з “Протипожежного водопостачання” так, щоб кожна тема була доступна до розуміння здобувачам вищої освіти, а також формувала у них навички та поняття, що дозволить їм зайняти достойне місце у ланках ДСНС України, або в будь-якій іншій сфері праці.

Література

[1] Петухова О.А., Горносталь С.А. Features of distance learning in the study of special disciplines // Інформаційні технології: Наука, техніка, технологія, освіта, здоров'я (MicroCAD-2021): матеріали ХХІХ міжн. наук.-практ. конф. – НТУ «ХПІ», Харків, 2021. – С. 273.

[2] Петухова О.А., Добринська В.Є., Кулеш Д.П. Способи підвищення ефективності навчання з наукового напрямку цивільна безпека // Безпека людини у сучасних умовах: матеріали ІХ Міжнародної науково-методичної конференції, Міжнародної наукової конференції EAS – Харків: НТУ «ХПІ», 2022. (<http://repositsc.nuczu.edu.ua/handle/123456789/16422>)

[3] Петухова О.А. Шляхи інтеграції професійної освітньої компоненти до європейського освітнього простору. // Методологія сучасних наукових досліджень: матеріали Ювілейної ХХ Міжнародної науково-практичної конференції. – Харків: ХНПУ імені Г.С. Сковороди, 2024. – С. 88-91 <http://repositsc.nuczu.edu.ua/handle/123456789/19904>

ПРОГРАМНІ ЗАСОБИ ДЛЯ СТАТИЧНОГО АНАЛІЗУ КОДУ НА KOTLIN

Приходько С.Б., Кольцов А.В.

E-mail: sergiy.prykhodko@nuos.edu.ua, andrew.koltsov@gmail.com

Миколаїв, Національний університет кораблебудування імені адмірала Макарова

У сучасному процесі розробки програмного забезпечення статичний аналіз коду відіграє важливу роль у ранньому виявленні дефектів, порушень стандартів та потенційних вразливостей. Такий аналіз дозволяє виявляти проблеми ще до етапу виконання програми, що знижує витрати на їх виправлення та допомагає підтримувати високу якість коду. Крім того, збір архітектурних метрик, таких як метрики з набору СК [1], дає можливість об'єктивно оцінювати складність, якість та розмір не лише окремих компонентів системи, а й на рівні програмного забезпечення в цілому, за рахунок застосування математичних моделей про що свідчать численні дослідження на цю тему [2-4].

Сучасні інструменти, такі як Detekt, SonarQube, Semgrep, Android Lint та PMD, надають можливості для статичного аналізу коду на Kotlin. Detekt орієнтований на пошук помилок, аналіз складності та дотримання кодстайлу, але не забезпечує повного збору СК-метрик. SonarQube, разом із плагіном SonarKotlin, пропонує широкий спектр показників якості коду, але його архітектурний аналіз обмежений: багато метрик, наприклад, успадкування та зв'язність (coupling), не розраховуються «з коробки». Semgrep зосереджений на пошуку вразливостей та типових помилок, Android Lint орієнтований на Android-розробку, а PMD, хоча й підтримує Kotlin, не охоплює повний спектр СК-метрик. На відміну від них, CodeMR (<https://www.codemr.co.uk/>) виділяється здатністю збирати повний набір СК-метрик.

Переваги CodeMR полягають у спеціалізованому підході до збору СК-метрик та інтеграції з популярними IDE, такими як IntelliJ IDEA, Android Studio та Eclipse. Це робить архітектурний аналіз зручним для розробників, особливо у великих проектах. Недоліком є необхідність оформлення підписки, хоча доступний 7-денний пробний період.

Як і будь-які інструменти статичного аналізу, CodeMR має обмеження. Навіть за наявності повного набору метрик можливі хибні спрацьовування або складнощі в інтерпретації даних. Правильне налаштування та адаптація інструменту залишаються ключовими для отримання коректних результатів.

Таким чином, сучасні засоби статичного аналізу, такі як Detekt, SonarQube, Semgrep, Android Lint та PMD, надають широкі можливості для виявлення дефектів та покращення якості коду. Однак, якщо мета – отримати комплексний набір архітектурних метрик СК, CodeMR є унікальним рішенням для глибокого аналізу структури та складності системи.

Література

[1] Chidamber, S., & Kemerer, C. (1994). A metrics suite for object oriented design. *IEEE Transactions on Software Engineering*, 20 (6), 476–493. (<https://doi.org/10.1109/32.295895>)

[2] Prykhodko, S. B., Prykhodko, N. V., & Koltsov, A. V. (2024). A nonlinear regression model for early LOC estimation of open-source Kotlin-based applications. *Radio Electronics Computer Science Control*, 1, 85. (<https://doi.org/10.15588/1607-3274-2024-1-8>)

[3] Prykhodko, S., & Prykhodko, N. (2022). A technique for detecting software quality based on the confidence and prediction intervals of nonlinear regression for RFC metric. *2021 IEEE 16th International Conference on Computer Sciences and Information Technologies (CSIT)*, 499–502. (<https://doi.org/10.1109/csit56902.2022.10000532>)

[4] Prykhodko, S., Prykhodko, N., & Smykodub, T. (2022). A joint statistical estimation of the RFC and CBO metrics for Open-Source applications developed in Java. *2021 IEEE 16th International Conference on Computer Sciences and Information Technologies (CSIT)*, 442–445. (<https://doi.org/10.1109/csit56902.2022.10000457>)

РОЗРОБКА СИСТЕМИ АУТЕНТИФІКАЦІЇ З ВИКОРИСТАННЯМ БІОМЕТРІЇ ЗА ДОПОМОГОЮ ARDUINO

Пудла М.С

Керівник: Лимаренко В.В.

E-mail: mashapudla2004@gmail.com

Харків, Харківський національний економічний університет імені Семена Кузнеця

Аутентифікація — це процес визначення, чи є людина тим, за кого себе видає. Іншими словами, аутентифікацією підтверджується справжність особистості, на підставі чого їй надається право доступу та користування закритим ресурсом або об'єктом. Прогресивним методом підтвердження ідентичності стала біометрична аутентифікація, тобто аналіз біологічних показників людини, при якому проводиться зіставлення унікальних фізичних характеристик тіла, з тими, що попередньо введені в аналітичний пристрій.

Для порівняльного аналізу, завчасно створюється еталонна модель біометричних характеристик розпорядників ресурсу, яка вводиться в базу електронно-аналітичного пристрою (ЕАП). В якості таких показників використовуються: відбитки пальців або долонь, малюнок райдужної оболонки очей, особливості вух або тембр голосу. На об'єктах з суворим режимом доступу використовується поєднання кількох характеристик, та навіть формула ДНК.

Таким чином, з'являються два набори біометричних показників: один попередньо встановлений в ЕАП власником ресурсу, а другий знаходиться у пред'явника. Процедура біометричної аутентифікації проводиться в три етапи: спочатку електронно-аналітичний пристрій зчитує пред'явлену біометричну інформацію, потім обробляє отриманий сигнал, після чого проводить порівняння зі зразком з бази даних. Якщо показники збігаються, то електронно-аналітичний пристрій визнає пред'явника власником, з правом доступу до об'єкта або користування ресурсом.

У даній роботі розглядається розробка системи аутентифікації з використанням біометрії на основі платформи Arduino. Основна мета дослідження – створення ефективної, доступної та надійної системи ідентифікації користувачів, яка може бути використана в різних сферах, таких як контроль доступу до приміщень, захист персональних даних або управління пристроями.

Дослідження охоплює аналіз існуючих біометричних технологій, вибір оптимальних сенсорів та компонентів для реалізації системи, а також розробку програмного забезпечення для обробки біометричних даних і прийняття рішень щодо автентифікації користувачів. Особлива увага приділяється питанню безпеки та точності системи, а також можливостям інтеграції її з іншими рішеннями.

Результатом роботи стане створення прототипу біометричної системи аутентифікації, яка продемонструє можливість використання доступних технологій на базі Arduino для підвищення рівня безпеки в різних сферах діяльності.

Література

[1] Worldvision. Переваги та недоліки біометричної системи аутентифікації. [Електронний ресурс] – Режим доступу до ресурсу: https://worldvision.com.ua/preimushchestva-i-nedostatki-biometricheskoy-sistemy-autentifikatsii/?srsltid=AfmBOoom6CEU30Sjf_ocssEx4AwzkN5xw1VD704yA7ZKCZQnHdZxXWOU

[2] Nixj. [Електронний ресурс] – Режим доступу до ресурсу: <https://nixj.ua/vidi-biometrichno-autentifikac>

BLENDER – ПОТУЖНИЙ ІНСТРУМЕНТ ДЛЯ АРХІТЕКТУРНОЇ ВІЗУАЛІЗАЦІЇ

Свинаренко М.С.

E-mail: svynarenko.maksym@ksada.org

Харків, Харківська державна академія дизайну і мистецтва

Архітектурна візуалізація є критично важливою складовою процесу проектування в архітектурі, оскільки вона дозволяє архітекторам і дизайнерам доносити свої ідеї до клієнтів, інвесторів та до широкої аудиторії. Сучасні програмні інструменти для 3D моделювання та візуалізації повинні не тільки забезпечувати високу якість зображення, але й бути доступними і зручними у використанні. Blender – безкоштовна програма з відкритим кодом – здобула популярність як універсальний засіб для архітектурної візуалізації [1].

Основи Blender

Blender був створений у 1995 році і отримав статус відкритого програмного забезпечення у 2002 році. Це потужний інструмент, що включає до себе модуль для моделювання, рендерингу, анімації, скульптингу, текстурювання та багато іншого. Програмне забезпечення підтримує різні платформи, включаючи Windows, macOS та Linux.

Можливості для архітектурної візуалізації [2].

- **Моделювання.** Blender пропонує різні інструменти для створення 3D моделей, такі як полігональне моделювання, NURBS, скульптинг і процедурне моделювання. Це дозволяє архітекторам точно відтворювати складні форми і структури будівель, інтер'єрів та ландшафтів.

- **Матеріали та текстурювання.** Blender забезпечує розвинуту систему роботи з матеріалами, яка дозволяє користувачам створювати детальні текстури та матеріали, що відповідають реальним. Вбудований редактор матеріалів забезпечує велике розмаїття налаштувань, що робить зображення максимально реалістичними.

- **Рендеринг.** Blender підтримує два основні рендерери: Cycles та Eevee. Cycles — це рендерер на основі фізичного моделювання, який забезпечує високоякісну фотореалістичну візуалізацію. Eevee, у свою чергу, є рендерером у реальному часі, що дозволяє швидко отримувати зображення з високою якістю, але з меншою деталізацією.

- **Анімація.** Blender має вражаючі можливості для анімації. Це дозволяє створювати динамічні презентовані матеріали. Анімаційні тури по проекту, що включають зміну перспективи і динамічні елементи, значно покращують сприйняття проекту.

- **Додатки та плагіни.** Спільнота Blender активно розробляє різноманітні аддони, що розширюють функціональність програми. Це включає плагіни для професійного архітектурного моделювання, візуалізації та рендерингу, які можуть значно спростити робочий процес.

Blender, як інструмент для архітектурної візуалізації, має багато переваг, які можуть суттєво спростити робочі процеси, підвищити якість кінцевого продукту та зробити процес проектування більш ефективним [3]:

- **Безкоштовність та відкритий код.** Blender є безкоштовним програмним забезпеченням, що означає, що будь-хто може завантажити, використовувати та модифікувати його безкоштовно. Це відкриває доступ до потужних інструментів навіть для тих, хто працює в умовах обмеженого бюджету, таких як студенти, стартапи або малий бізнес.

- **Гнучкість та модульність.** Blender надає користувачу величезну гнучкість завдяки модульній архітектурі, що дозволяє налаштовувати інтерфейс та робочий процес відповідно до індивідуальних потреб. Це допомагає архітекторам створювати специфічні робочі середовища, які відповідають їхнім стилям роботи.

- Потужні інструменти для анімації. Blender забезпечує широкі можливості для анімації, включаючи скелетну анімацію, прийоми постановки та візуальні ефекти. Це дозволяє створювати оглядові анімації і презентації проектів, що робить їх більш інтерактивними і привертаячими увагу.

- Інтеграція з іншими інструментами. Blender підтримує безліч форматів файлів, таких як FBX, OBJ, STL, Collada тощо, що дозволяє безперешкодно імплементувати його у вже наявні робочі процеси. Це також дає змогу архітекторам комбінувати Blender з іншими програмними забезпеченнями, що використовуються на ринку.

- Велика спільнота та ресурси. Blender має активну спільноту користувачів, яка забезпечує підтримку, обмін знаннями та ресурсами. Це включає форуми, навчальні відео, документацію та онлайн-курси, які можуть допомогти новачкам швидше освоїти програму.

- Регулярні оновлення та поліпшення. Blender регулярно отримує оновлення, які включають нові функції, виправлення помилок та вдосконалення. Це свідчить про активний розвиток програмного забезпечення та відповідь на потреби користувачів. Таким чином, стабільність і розвиток програми забезпечують тривалий термін служби інвестицій у навчання та користування Blender.

- Унікальні функції, як додаткові вкладки. Blender забезпечує користувачам доступ до унікальних функцій, таких як Grease Pencil для малюнків та 2D анімації безпосередньо в 3D просторі. Це дозволяє архітекторам використовувати графічні елементи для ілюстрації своїх ідей на етапах планування та презентації.

- Універсальність. Blender застосовується не лише в архітектурі, а й у різних сферах, таких як анімація, ігрова індустрія, VFX, продуктова візуалізація тощо. Це робить його універсальним інструментом для фахівців з різних галузей, що підвищує цінність навичок роботи з Blender на ринку праці.

Недоліки:

- Крива навчання. Перехід на Blender може бути складним для новачків, особливо тим, хто звик до інших програм.

- Обмежена технічна підтримка. Як продукт з відкритим кодом, Blender не має централізованої технічної підтримки, що може бути проблемою для деяких користувачів.

- Вимоги до системи. Для плавної роботи з великими проектами та високоякісним рендерингом Blender вимагає досить потужного комп'ютера. Недостатні системні ресурси можуть спричинити гальмування та проблеми з продуктивністю, особливо під час обробки складних сцен.

Висновок. Blender стає все більш важливим інструментом у сфері архітектурної візуалізації. Його потужні можливості моделювання, рендерингу й анімації разом із доступністю роблять його чудовим вибором як для професіоналів, так і для студентів. Підвищення якості візуалізацій за допомогою Blender може суттєво поліпшити комунікацію між архітекторами та клієнтами, а також сприяти реалізації більш складних та амбітних проектів.

У майбутньому можна очікувати подальшого розвитку Blender і інтеграції нових технологій, таких як віртуальна та доповнена реальність, що ще більше підвищить його цінність у сфері архітектурної візуалізації.

Література

[1] Wikipedia. Blender [Електронний ресурс] – Режим доступу до ресурсу: <https://uk.wikipedia.org/wiki/Blender>

[2] Go-mother. Blender [Електронний ресурс] – Режим доступу до ресурсу: <https://go-mother.com/2023/05/21/blender-3d/>

[3] Infodlapolaka. Blender [Електронний ресурс] – Режим доступу до ресурсу: <https://infodlapolaka.pl/uk/blender-від-безкоштовного-програмного-забезпечення-до-професійного-інструменту-для-створення-тривимірних-світів/>

РОЗРОБКА ПОШУКОВОЇ СИСТЕМИ ДЛЯ РІЗНИХ ГАЛУЗЕЙ ЗНАНЬ

Сімак А.В., Льовкін В.М.

E-mail: vliovkin@gmail.com

Запоріжжя, Національний університет «Запорізька політехніка»

У сучасному цифровому світі, де інформаційні потоки зростають експоненційно, ефективний пошук інформації стає критично важливим. Особливо це актуально для спеціалізованих галузей знань, де користувачам необхідно швидко знаходити релевантні дані серед величезної кількості джерел. Традиційні пошукові системи часто не здатні забезпечити необхідну точність та релевантність результатів у таких контекстах, що підкреслює потребу у розробці спеціалізованих рішень.

Метою цієї роботи є розробка пошукової системи, яка дозволяє виконувати пошук у визначених галузях знань з урахуванням параметрів, таких як тема запиту, мова та локалізація пошуку. Система спочатку перевіряє, чи належить запит до однієї з заданих галузей, і лише у випадку відповідності виконує пошук. Це забезпечує високу релевантність результатів та ефективність використання ресурсів.

Для реалізації цього завдання використовуються різні методи обробки та аналізу даних. Основним методом оцінювання релевантності є TF-IDF [1], який дозволяє визначити значущість кожного слова у контексті конкретного документа. Крім того, для оцінки подібності між запитом та документами застосовується косинусна подібність, яка обчислює кут між векторами запиту та документів у багатовимірному просторі.

Метод роботи пошукової системи складається з кількох етапів.

Перший етап включає збір даних з обраних вебресурсів, парсинг контенту з обраних вебсайтів за допомогою власного скрипта, збереження його у структурованому форматі та створення індексу.

На другому етапі система перевіряє запит користувача на відповідність заданим критеріям: перевіряє наявність ключових слів теми, визначає мову запиту за допомогою бібліотеки langdetect [2] та перевіряє локалізацію за допомогою аналізу доменів сайтів.

Якщо запит відповідає всім умовам, система переходить до етапу пошуку з подальшим ранжуванням результатів за релевантністю. Завдяки використанню TF-IDF та косинусної подібності система забезпечує високу точність пошуку та релевантність результатів, що відповідають інтересам користувача. Крім того система підтримує багатомовні запити та локалізацію, що робить її універсальною для використання у різних регіонах та мовних середовищах, тому користувач отримує найрелевантніші результати на першій сторінці, що значно підвищує ефективність пошуку.

У практичному застосуванні система може використовуватись для пошуку інформації у спеціалізованих ресурсах, таких як наукові бази даних, технічні форуми чи освітні платформи. Наприклад, користувач, зацікавлений у темі «машинного навчання», може швидко знайти найбільш релевантні статті та матеріали з відповідних джерел, що економить час та підвищує продуктивність роботи.

Таким чином, розроблена пошукова система забезпечує ефективний та точний пошук у визначених галузях знань, враховуючи специфічні параметри запиту користувача. Використання сучасних методів аналізу даних та машинного навчання гарантує високу якість результатів та задоволення потреб користувачів у швидкому та релевантному доступі до інформації.

Література

[1] Understanding TF-IDF (Term Frequency-Inverse Document Frequency) [Електронний ресурс] – Режим доступу до ресурсу: <https://www.geeksforgeeks.org/understanding-tf-idf-term-frequency-inverse-document-frequency/>

[2] Langdetect Documentation [Електронний ресурс] – Режим доступу до ресурсу: <https://pypi.org/project/langdetect/>

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ АНАЛІЗУ ІНФОРМАЦІЙНОГО ВМІСТУ НА ВИЯВЛЕННЯ РЕКЛАМНОГО КОНТЕНТУ

Степанов І.А., Льовкін В.М.

E-mail: vliovkin@gmail.com

Запоріжжя, Національний університет «Запорізька політехніка»

У сучасному інформаційному середовищі, переповненому контентом, для користувачів стає критично важливим визначати рекламні матеріали в інтернет-ресурсах. Величезна кількість вебсайтів публікує як новини, так і рекламні статті, що ускладнює для читача можливість відрізнити корисний контент від промоційного. З огляду на ці виклики, розробка програмного забезпечення для автоматичного розпізнавання реклами в текстах є актуальною і важливою задачею, яка може допомогти користувачам краще орієнтуватися в інформаційних потоках.

У роботі розроблено програмне забезпечення, яке за допомогою засобів машинного навчання аналізує текстовий контент вебсайтів або новинних статей і визначає наявність рекламного характеру. Метод, що використовується в програмі, передбачає декілька етапів: попередню обробку тексту, перетворення тексту у векторні представлення, навчання моделі та класифікацію контенту на рекламний і нерекламний. Користувач може або ввести текст для аналізу, або вказати URL-адресу, з якої програма автоматично зчитує текст та проводить аналіз. Рекламний текст, як правило, має певні характерні ознаки – це використання вигідних пропозицій, акційних термінів таких, як «знижки», «ексклюзивно», «найкраща ціна» та інших маркетингових прийомів. Нерекламний контент орієнтований на інформування, а не на стимулювання до покупки, що дозволяє відокремити його за стилем викладу.

Для створення програмного забезпечення використовувалась мова Python, а також бібліотеки scikit-learn, requests і BeautifulSoup. Клас TfidfVectorizer [1] із бібліотеки scikit-learn був використаний для векторизації тексту шляхом перетворення кожного документа у вектор, що відображає значущість кожного слова у тексті. Клас LogisticRegression [2] із пакету scikit-learn навчений класифікувати текст як рекламний або нерекламний, залежно від тренувальних даних. Для розв'язання задачі класифікації тексту на рекламний і нерекламний було застосовано клас LogisticRegression. Ця модель обрана з огляду на її ефективність для бінарної класифікації та інтерпретованість результатів. У випадку розпізнавання рекламного контенту LogisticRegression дозволяє на основі навчальних даних визначити, до якої з двох категорій – рекламний або нерекламний контент – належить текст. Модель LogisticRegression [2] навчається на векторизованих даних. Під час навчання LogisticRegression оптимізує параметри, щоб мінімізувати функцію втрат, зокрема log loss, що дозволяє отримати більш точні ймовірності для класифікації.

Для реалізації алгоритму були створені такі основні функції: завантаження сторінки, використовуючи бібліотеку BeautifulSoup [3] для отримання тексту, виконання очистки та нормалізації тексту за допомогою модуля corpus пакету NLTK [4], прийом тексту як вхідних даних, обробка тексту за допомогою класу TfidfVectorizer, передача у модель та повертання результату класифікації, надавання користувачу можливості введення тексту або URL для аналізу, а також виведення результату.

Література

[1] Using TF-IDF Vectorization for Text Processing [Електронний ресурс] – Режим доступу до ресурсу: https://scikit-learn.org/stable/modules/feature_extraction.html

[2] Logistic Regression Classifier in Scikit-learn [Електронний ресурс] – Режим доступу до ресурсу: https://scikit-learn.org/stable/modules/linear_model.html

[3] BeautifulSoup Documentation for Web Scraping [Електронний ресурс] – Режим доступу до ресурсу: <https://www.crummy.com/software/BeautifulSoup/bs4/doc>

[4] Natural Language Toolkit (NLTK) for Text Preprocessing [Електронний ресурс] – Режим доступу до ресурсу: <https://www.nltk.org>

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ДЛЯ АВТОМАТИЗОВАНОГО ВИЗНАЧЕННЯ ЖАНРІВ КІНОСТРІЧОК

Федишен С.В., Льовкін В.М.

E-mail: vliovkin@gmail.com

Запоріжжя, Національний університет «Запорізька політехніка»

У сучасних умовах поширення процесів автоматизації обробки текстових даних важливим завданням є створення програмних засобів, які можуть ефективно класифікувати текстову інформацію. Однією з важливих задач на практиці, яку можна віднести до цієї сфери, є автоматизоване визначення жанру кінострічки на основі її синопсису. Це питання актуальне для розробки рекомендаційних систем, а також для перевірки коректності класифікації жанрів, обраних користувачами. Тоді результат такої роботи може бути вхідними даними для наступних етапів роботи, а може використовуватися і як самостійна інформація для підтримки роботи відповідної системи.

Для вирішення сформульованої задачі в роботі було використано підхід багатоміткової класифікації тексту, що дозволяє кожний фільм співвіднести одразу з декількома жанрами одночасно. Запропонований метод вирішення задачі базується на векторизації текстових даних із застосуванням міри TF-IDF, а також на використанні моделі логістичної регресії з підходом OneVsRestClassifier для визначення жанрів.

Відповідний метод, покладений в основу визначення жанру кінострічки, має наступну послідовність етапів: обробка та підготовка даних, що включає отримання інформації про кінострічки з відповідного сервісу (фактично було при розробленні програми використано сервіс IMDb через бібліотеку Cinemagoer), видалення записів із відсутньою або неповною інформацією, а також фільтрацію рідкісних жанрів; перетворення текстових даних у векторне представлення (фактично під час реалізації за допомогою TfidfVectorizer з пакету scikit-learn) для створення числових векторів із тексту синопсисів; навчання моделі логістичної регресії для багатоміткової класифікації на основі навчального набору даних; оцінка точності моделі за метриками precision, recall і F1-score; визначення жанрів, яке здійснюється за допомогою навченої моделі для нового тексту синопсису кінострічки.

Програмне забезпечення розроблено з використанням мови програмування Python, яка є високорівневою, багатofункціональною та має широкий набір бібліотек, що спрощують роботу з текстовими даними та алгоритмами машинного навчання. У рамках роботи застосовувалися такі бібліотеки: pandas – для зручного оброблення табличних даних, роботи з даними типу DataFrame і підготовки набору даних до подальшого аналізу [1], scikit-learn – для векторизації текстів за допомогою TfidfVectorizer, а також для створення і навчання моделі багатоміткової класифікації [2], Cinemagoer – для автоматизованого отримання даних із бази сервісу IMDb, що дозволяє зручно збирати метайнформацію про фільми, їхні жанри та синопсиси [3].

Робота програми в частині даного методу починається збором даних із IMDb за допомогою бібліотеки Cinemagoer, які зберігаються у DataFrame. Тексти синопсисів перетворюються у числові вектори через TfidfVectorizer, після чого дані розділяються на навчальний і тестовий набори. Модель OneVsRestClassifier з логістичною регресією навчається на навчальних даних, а її точність оцінюється за метриками precision, recall і F1-score. Навчена модель визначає жанри для нових описів кінострічок.

Література

[1] Pandas documentation [Електронний ресурс] – Режим доступу до ресурсу: <https://pandas.pydata.org/docs/index.html>

[2] sklearn API [Електронний ресурс] – Режим доступу до ресурсу: <https://scikit-learn.org/stable/modules/classes.html>

[3] Cinemagoer documentation [Електронний ресурс] – Режим доступу до ресурсу: <https://cinemagoer.github.io/>

3D MODELING APP – БЕЗКОШТОВНІ ІНСТРУМЕНТИ ДЛЯ МОДЕЛЮВАННЯ НА ТЕЛЕФОНІ

Чайка А.В.

Керівник: Сажко Г.І.

E-mail: wowalinachaika@gmail.com

*Харків, Навчально-науковий інститут «Українська інженерно-педагогічна академія»
Харківського національного університету імені В.Н. Каразіна*

Актуальність: у сучасному світі, де технології розвиваються неймовірними темпами, 3D-моделювання стає важливим інструментом у багатьох сферах, включаючи: дизайн, архітектуру, розробку відеоігор, віртуальну реальність тощо. Хоча існує багато професійних інструментів для моделювання, безкоштовні мобільні додатки роблять 3D-моделювання набагато простішим для широкого кола користувачів. Це важливо для студентів, аматорів і навіть професіоналів, яким потрібен швидкий доступ до інструментів моделювання за допомогою телефону або планшета.

Програми для 3D-моделювання на мобільних пристроях, як-от 3D MODELING APP, дозволяють створювати об'єкти, зберігати їх та експортувати в різні формати. Завдяки безкоштовним інструментам, такі додатки стають доступними для широкого кола користувачів, від студентів до професіоналів.

Безкоштовні додатки дозволяють створювати складні 3D-моделі за допомогою простих у використанні інтерфейсів та інструментів, які можуть значно покращити навчання та творчість. Оскільки мобільні пристрої стають не лише засобом комунікації, а й важливим інструментом для цифрового дизайну, вивчення безкоштовних інструментів 3D-моделювання допоможе розвивати креативні індустрії та освіту.

Постановка проблеми: незважаючи на стрімкий розвиток інструментів для 3D-моделювання, багато професійних програм є досить дорогими або складними в освоєнні, що робить їх недоступними для широкого кола користувачів. Однак на ринку також з'являються безкоштовні мобільні додатки, які дозволяють створювати 3D-моделі без дорогого комп'ютера чи спеціалізованого обладнання. Важливо розуміти, наскільки ефективні ці інструменти, які їхні функції та як їх можна використовувати для різних цілей.

Метою цього дослідження є оцінка ефективності безкоштовних мобільних додатків для 3D-моделювання, функціональні можливості для 3D-моделювання на мобільних пристроях, зокрема додатка 3D MODELING APP, а також їх здатність задовольняти потреби користувачів з різним рівнем підготовки. Основними аспектами, які будуть розглянуті, є:

- Функціональність: аналіз інструментів у 3D MODELING APP, доступних у безкоштовних мобільних додатках для 3D-моделювання.
- Зручність використання: оцінка інтерфейсу, навчання та процесу створення 3D-моделі.
- Продуктивність і ресурси: аналіз того, наскільки ефективно ці програми працюють на мобільних пристроях і який їхній вплив на ресурси телефону.
- Обмеження та переваги: вивчення обмежень, з якими можна зіткнутися під час використання додатку, та їхніх переваг порівняно з більш професійним програмним забезпеченням для 3D-моделювання.

Результат дослідження: 3D MODELING APP - додаток 3D-моделювання, який дозволяє легко створювати 3D-моделі, об'єкти, графіку мистецтва, картини, створювати 3D-персонажів та проектувати 3D-ігри на ходу за допомогою жестів на мобільному телефоні чи планшеті [1].

Додаток 3D MODELING APP є потужним інструментом для створення 3D моделей, доступним для широкого кола користувачів, від новачків до досвідчених професіоналів. Його основні можливості включають:

- Інтерфейс: додаток має інтуїтивно зрозумілий інтерфейс, який дозволяє швидко освоїти роботу з ним навіть тим, хто тільки починає працювати в галузі 3D-моделювання.
- Функціональність: користувачі можуть створювати складні 3D об'єкти за допомогою базових інструментів (створення геометричних фігур, виділення, злиття, розтягування тощо).
- Ресурсозбереження: додаток оптимізований для роботи на мобільних пристроях з низькими ресурсами, забезпечуючи високий рівень продуктивності навіть на старіших моделях телефонів.
- Експорт: підтримуються різні формати для експорту моделей, такі як .obj, .stl та .fbx, що дає змогу використовувати створені моделі в інших програмах або для 3D-друку.
- Додаток також надає користувачам різні інструменти для редагування текстур, освітлення та анімації, що дозволяє створювати високоякісні моделі для різних цілей: від дизайну до ігор.

Кажучи про можливості, 3D MODELING APP має інтуїтивно зрозумілий та користувацький інтерфейс, який дозволяє швидко освоїти основні функції навіть новачкам у сфері 3D-моделювання. Після запуску програми користувачі потрапляють на головний екран, де відразу доступні базові інструменти для створення 3D об'єктів, а також панелі для налаштування властивостей об'єкта (розміри, форма, текстури тощо).

Програма має кілька модулів:

- Моделювання: для створення та редагування об'єктів.
- Матеріали та текстури: для надання поверхням об'єктів різноманітних текстур та кольорів.
- Анімація: для створення базових анімацій моделей.

Оцінка зручності використання показала, що додаток пропонує прості інструменти, але в той же час не обмежує користувачів у можливостях для створення складних моделей. Це дозволяє як новачкам, так і досвідченим користувачам швидко отримувати бажані результати.

Додаток надає основні інструменти для 3D моделювання, які включають:

- Створення геометричних форм (сфери, куби, циліндри, піраміди та інші примітиви).
- Операції з об'єктами (переміщення, масштабування, повороти, об'єднання, розділення, видалення частин моделей).
- Редагування вершин: можливість змінювати форму об'єктів на рівні точок для отримання складніших форм.
- Текстури: додавання і налаштування текстур для створення більш реалістичних або абстрактних поверхонь [2].

Також, програма добре оптимізована для роботи на мобільних пристроях середнього та низького класу. Програму було протестовано на кількох пристроях з різними характеристиками, і в усіх випадках вона продовжувала працювати без серйозних проблем з продуктивністю. Більш складні моделі можуть вимагати більше ресурсів, але програма надає корисні опції для зменшення складності моделі під час її створення. Це дозволяє забезпечити гарну продуктивність при одночасному використанні інших додатків на мобільному пристрої.

Однією з ключових переваг додатка є можливість експортувати 3D моделі в різні формати, що забезпечує їх подальше використання в інших програмах. Формати, підтримувані додатком, включають:

- .obj: популярний формат для 3D моделей, що зберігає геометрію та текстури.
- .fbx: формат, що дозволяє зберігати анімацію і більш складні 3D сцени.
- .stl: формат, використовуваний для 3D друку.

Це дозволяє користувачам не тільки створювати моделі для візуалізації, але й готувати їх до реального виготовлення через 3D принтери. Така гнучкість важлива для професіоналів у галузі дизайну, архітектури та розробки ігор [3].

Згідно з відгуками користувачів, додаток має позитивну репутацію завдяки своїй зручності, доступності і можливості працювати з моделями на ходу. Користувачі відзначають, що цей додаток є чудовим стартом для тих, хто хоче спробувати себе в 3D-моделюванні, не вимагаючи великих інвестицій у програмне забезпечення або потужні комп'ютери. Однак деякі користувачі зауважують, що для створення дуже складних моделей додаток може бути недостатньо потужним, і вони рекомендують використовувати додатки для комп'ютерів або професійне програмне забезпечення для роботи з великими проєктами.

Кажучи про сильні сторони, то додаток має наступні переваги: безкоштовний доступ до основних функцій; простота у використанні, що дозволяє новачкам швидко освоїти інструменти 3D моделювання; гнучкість експорту моделей в різні формати; стабільна робота на мобільних пристроях середнього класу.

Але також є і наступні обмеження: обмежена кількість складних функцій для висококваліфікованих професіоналів; для більш складних, або великих моделей можуть знадобитися більш потужні інструменти; відсутність розширеної підтримки для 3D анімацій, або роботи з великими сценами.

Отже, Додаток 3D MODELING APP є потужним і доступним інструментом для створення 3D моделей, який поєднує зручний інтерфейс, функціональність і оптимізацію під мобільні пристрої. Це ідеальний інструмент для студентів, початківців, а також для професіоналів, які потребують швидкого та простого рішення для створення 3D контенту без необхідності використання дорогих програм.

Рекомендації та висновки: додаток 3D MODELING APP є простим та ефективним інструментом для створення 3D моделей на мобільних пристроях. Він підходить як для новачків, так і для більш досвідчених користувачів, завдяки інтуїтивно зрозумілому інтерфейсу та інструментам для моделювання, текстурювання і експорту моделей у формати .obj, .fbx та .stl. Програма забезпечує хорошу продуктивність на пристроях середнього класу, що робить її доступною для широкого кола користувачів.

Проте для складніших проєктів або роботи з великими моделями може бути необхідним використання більш потужного програмного забезпечення на комп'ютерах, таких як Blender або Autodesk Maya. Тим не менш, для базових проєктів та 3D друку додаток є цілком підходящим варіантом.

Рекомендується використовувати 3D MODELING APP для створення базових та середніх за складністю 3D моделей, особливо початківцям у 3D моделюванні. Для складніших проєктів доцільно звертатися до професійного ПЗ з розширеними функціями. Регулярне оновлення додатку допоможе підтримувати стабільність і ефективність роботи.

Література

[1] 3D Modeling App: Sculpt & Draw. [Електронний ресурс] – Режим доступу до ресурсу: <https://play.google.com/store/apps/details?id=com.inforcegames.app3dmodelling&hl=uk>

[2] 3D Modeling App. [Електронний ресурс] – Режим доступу до ресурсу: <https://3d-modeling-app.en.uptodown.com/android>

[3] How to use 3D modeling app | full tutorial | model from scratch on phone | all tools and function. [Електронний ресурс] – Режим доступу до ресурсу: https://youtu.be/WneM2OgDaUI?si=1Ync26yy1hsT_bDI

ОГЛЯД ФРЕЙМВОРКУ KIVU З ТОЧКИ ЗОРУ РОЗРОБКИ МОБІЛЬНИХ ЗАСТОСУНКІВ

Штаба В.Г., Макарова Л.М.

E-mail: shtaba09@gmail.com, lidiia.makarova@nuos.edu.ua

Миколаїв, Національний університет кораблебудування імені адмірала Макарова

У світі кросплатформової розробки для мобільних платформ сьогодні домінують два фреймворки – Xamarin і React Native. Xamarin утримує позиції, оскільки знаходиться під крилом Microsoft і активно просувається компанією. React Native є розробкою не менш впливового Facebook.

Фреймворк Kivu – це мультиплатформний фреймворк з відкритим вихідним кодом для розробки застосунків мовою Python. Починаючи з версії 1.7.2, він поширюється за ліцензією MIT; попередні версії використовували ліцензію LGPL 3. Фреймворк Kivu застосовується для створення складних багатофункціональних мобільних та десктопних застосунків з підтримкою муьтитач або природного користувацького інтерфейсу. Фреймворк працює на всіх поширених платформах: Windows, Linux, macOS, iOS, Android та Raspberry Pi.

Використання фреймворку Kivu з мовою програмування Python для розробки мобільних застосунків має свої переваги та недоліки. Простота та читабельність коду, кросплатформність і велика кількість бібліотек роблять Python чудовим вибором для новачків і швидкого прототипування. Однак продуктивність, обмежена підтримка нативних функцій та розмір застосунків можуть стати серйозними перешкодами.

Використання фреймворку Kivu надає більш швидшу розробку, лаконічніший код, можливість миттєвих змін та їх відстеження в реальному часі. Це майже ідеальний кросплатформний фреймворк – більше 90% коду, написаного один раз, буде працювати на всіх підтримуваних платформах. Для порівняння: у випадку з Xamarin лише 60% коду можна повторно використовувати, хоча розробники заявляють про 80%. Фреймворк Kivu – зрілий фреймворк, що розвивається з 2011 року. Він навіть старший за React Native (2015 рік) і є ровесником Xamarin (2011 рік) [1].

Для перевірки на практиці було розроблено тестовий застосунок для платформ Android та iOS. Застосунок являє собою набір звичайних сторінок з інформацією про пристрій, ліцензійною сторінкою, чатом та головним меню і екраном привітання. Реалізація за допомогою фреймворку Kivu виявилась доволі простою, оскільки більшість функціоналу будувалась на віджетах та готових бібліотеках Kivu. Як виявилось, Kivu дуже адаптивний і його графічні елементи однаково добре відображаються на Android та iOS, проте він потребує створення окремих форм для платформ, щоб враховувати їх особливості, також сам фреймворк спрощує доступ до не нативних функцій пристрою, що полегшує роботу розробника. Це є перевагою, адже рендеринг інтерфейсу та обробка подій не залежать від особливостей платформи: не потрібно використовувати нативні API для керування цими процесами, що дозволяє додатку безперешкодно працювати практично на будь-якій платформі. Уся графіка відображається за допомогою нативних викликів OpenGL та SDL2 на GPU, що забезпечує надзвичайно швидке візуальне відтворення меню, кнопок та інших елементів інтерфейсу, включаючи як 2D, так і 3D графіку.

Перевагами розробки мобільних застосунків з використанням фреймворку Kivu є наступні.

Оскільки основою розробки є мова програмування Python, темпи розробки застосунків значно перевищують ті, що можна досягти за допомогою інших мов програмування чи фреймворків. До того ж, величезна кількість готових бібліотек Python доступна для використання у проєктах.

Завдяки тому, що фреймворк Kivu для відтворення графіки спирається на OpenGL та GPU, а також використовує власні віджети, швидкість рендерингу інтерфейсу залишається

на високому рівні. Це дозволяє повністю уникнути проблем, які часто виникають в інших фреймворках, де для реалізації окремих елементів інтерфейсу доводиться вдаватися до нативних компонентів.

Можна також використовувати сторонні бібліотеки у своїх проєктах, якщо мова йде про Android. Все це дозволяє повністю контролювати всі події, що відбуваються на екрані: дотик, мультитач, свайп, стиснення та інші. Оскільки ці функції є невід'ємною частиною фреймворку Kivu, розробнику не доведеться звертатись до нативного коду для їх реалізації.

Використання нативних можливостей обмежується лише тими випадками, коли потрібен доступ до специфічних функцій платформи, таких, яких не може бути в посправжньому кросплатформовому фреймворку, наприклад, робота з камерою.

Хоча фреймворк Kivu має багато переваг, існують і деякі недоліки, які також варто враховувати при його використанні для розробки мобільних застосунків.

Швидкість "холодного старту". Перший запуск програми може бути досить тривалим через необхідність розгортання всіх бібліотек. Наступні запуски відбуваються швидше, але все ж можуть бути повільнішими порівняно з нативними застосунками, залежно від навантаження на процесор мобільного пристрою.

Робота зі списками. Виведення списків великого розміру може бути неефективним. Наприклад, для списків з елементами змінної висоти, як-от цитати з різною кількістю тексту, відображення більше десяти елементів одночасно, це може зайняти 10-15 секунд, що буде вимагати реалізації підвантаження елементів під час прокрутки списку.

Обмеження на розмір тексту. Відображення тексту, що перевищує 6500 символів (приблизно 3,5 сторінки друкованого тексту), може призвести до появи чорного екрану. Це можна вирішити шляхом розбиття тексту на менші частини з подальшим об'єднанням, але такий підхід виглядає як тимчасове рішення.

Варто зазначити, що деякі з цих проблем можуть бути вирішені або пом'якшені за допомогою оптимізації коду та використання відповідних віджетів. Наприклад, для ефективної роботи зі списками можна використовувати віджет RecycleView, який дозволяє швидко обробляти великі списки.

Незважаючи на вказані недоліки, фреймворк Kivu залишається потужним інструментом для кросплатформової розробки мобільних застосунків, особливо коли потрібна швидка розробка та використання можливостей мови програмування Python.

Література

[1] Kivu – фреймворк для крос-платформної розробки №1. [Електронний ресурс] – Режим доступу до ресурсу: <https://habr.com/articles/418839/> (дата звернення 25.01.2025).

[2] Ключові переваги розробки мобільного застосунку на Python. [Електронний ресурс] – Режим доступу до ресурсу: <https://wezom.com.ua/blog/sozdanie-mobilnogo-prilozhenija-na-python> (дата звернення 25.01.2025).

**Матеріали XVI-ої Міжнародної науково-практичної конференції
«FREE AND OPEN SOURCE SOFTWARE»**

Харківський національний економічний університет імені Семена Кузнеця

Відповідальний за випуск: Старкова О.В.

Редактор: Міхєєв І.А.

Затверджено засіданням кафедри кібербезпеки та інформаційних технологій
ХНЕУ імені С. Кузнеця
протокол № 12 від «27» лютого 2025 р.

Видавець і виготовлювач – ХНЕУ імені С. Кузнеця, 61166, м. Харків, просп.
Науки, 9-А
Свідоцтво про внесення суб'єкта видавничої справи до Державного реєстру
ДК № 4853 від 20.02.2015 р.