КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (29), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.29.893
УДК 004.056

Микитюк Артем В'ячеславович
доктор філософії, заступник завідувача кафедри
комп'ютерних наук та технологій штучного інтелекту в сфері кібербезпеки
Інститут спеціального зв'язку та захисту інформації
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського», Київ, Україна
ORCID ID: 0000-0002-8307-9978
mukuta8888@gmail.com

Горнійчук Іван Вікторович
доктор філософії, старший викладач кафедри
комп'ютерних наук та технологій штучного інтелекту в сфері кібербезпеки
Інститут спеціального зв'язку та захисту інформації
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського», Київ, Україна
ORCID ID: 0000-0001-6754-4764
horniychuk.ivan@gmail.com

Поліщук Вікторія Романівна
магістрант кафедри
комп'ютерних наук та технологій штучного інтелекту в сфері кібербезпеки
Інститут спеціального зв'язку та захисту інформації
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського», Київ, Україна
ORCID ID: 0009-0003-4596-1219
polisukv230@gmail.com

Бичковська Олександра Василівна
молодший науковий співробітник науково-дослідного центру
Інститут спеціального зв'язку та захисту інформації
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського», Київ, Україна
ORCID ID: 0009-0004-2896-0545
o.bychkovska@kpi.ua

ІНФОРМАЦІЙНА СИСТЕМА ЗБОРУ ТА АНАЛІЗУ ДАНИХ ПРО ДІЯЛЬНІСТЬ ХАКЕРСЬКИХ УГРУПОВАНЬ

Анотація. Сучасний світ із його зростаючою залежністю від інформаційних систем та технологій потребує надійного захисту від кібератак, що набуває особливої актуальності в умовах зростання активності хакерських угруповань. Атаки, спрямовані на державні та приватні організації, охоплюють не лише критичну інфраструктуру, а й викрадення конфіденційної інформації, фінансові махінації та дестабілізаційні дії у кіберпросторі. Зокрема, хакерські угруповання, використовуючи новітні техніки, інструменти та програмні засоби, становлять значну загрозу для інформаційної безпеки як окремих організацій, так і держав загалом. Вони діють приховано, швидко адаптуються до нових умов і мають високий рівень координації, що ускладнює процес виявлення та протидії. Це потребує зосередженого моніторингу, постійного аналізу їхньої діяльності, а також систематизації та накопичення отриманої інформації для створення єдиної бази знань про цю діяльність. Часто такі угруповання діють на міжнародному рівні, впливаючи на стабільність і безпеку в різних регіонах світу, зокрема в Україні. У статті розглянуто проблему відсутності комплексного інструменту для збирання, структурування й аналізу даних про хакерські угрупування, із можливістю фільтрації за типом угруповання, географією їхньої діяльності, часовими періодами активності, а також використовуваними техніками та інструментами. Окрему увагу приділено розробці інформаційної системи, яка не лише зберігає та

аналізує інформацію про діяльність хакерських угруповань, але й дозволяє фахівцям налаштовувати дані відповідно до локальних потреб. Реалізація такої системи вимагає використання сучасних підходів до збору, нормалізації та аналізу даних. Враховуючи динаміку змін у кіберпросторі, ефективне оброблення інформації про атакувальні операції потребує реалізації алгоритмів фільтрації, кластеризації та статистичного аналізу, що дозволяє автоматизовано ідентифікувати тенденції у використанні атакувальних технік. Відмінною рисою цієї системи є її адаптація до українського контексту, з урахуванням специфіки локального кіберпростору, мовних особливостей, типових сценаріїв атак та пріоритетів національної безпеки. Це у свою чергу сприяє підвищенню ефективності аналітичної роботи українських фахівців, зміцненню кібероборони та формуванню стійкої моделі реагування на кіберзагрози.

Ключові слова: інформаційна система; кібербезпека; хакерські угруповання; база знань; фільтрація даних; аналіз кіберзагроз.

ВСТУП

Зі зростанням складності кібератак та еволюцією методів атакувальних операцій виникає необхідність у високоефективних засобах обліку, аналізу та класифікації даних про хакерські угруповання. Сучасні атакувальні кампанії базуються на багаторівневих тактиках і техніках, що робить традиційні підходи до їх ідентифікації малоефективними. Для вирішення цієї проблеми доцільним є застосування інформаційної системи, яка агрегує, обробляє та візуалізує інформацію про хакерські угруповання, їхні техніки та тактики відповідно до структури MITRE ATT&CK. Реалізація такої системи вимагає використання сучасних підходів до збору, нормалізації та аналізу даних. Враховуючи динаміку змін у кіберпросторі, ефективне оброблення інформації про атакувальні операції потребує реалізації алгоритмів фільтрації, кластеризації та статистичного аналізу, що дозволяє автоматизовано ідентифікувати тенденції у використанні атакувальних технік. Існуючі системи аналітики хакерських угруповань або орієнтовані на закриті корпоративні рішення, або не враховують гнучкість налаштування фільтрації та обробки даних. Таким чином, постає завдання розробки інформаційної системи збору та аналізу даних про діяльність хакерських угруповань, яка забезпечуватиме: централізований облік атакувальних груп, структуризацію та фільтрацію технік атак, візуалізацію взаємозв’язків між угрупованнями та техніками.

Аналіз останніх досліджень і публікацій. Значні збитки від кібератак та діяльності хакерських угруповань підкреслюють актуальність проблеми кібербезпеки та необхідність моніторингу загроз. Так, численні випадки кібершпигунства, атак програмами-вимагачами, цільових зломів національної інфраструктури та поширення шкідливого програмного забезпечення вказують на еволюцію хакерських методів та зростаючу небезпеку для державних і приватних організацій. Серед них атаки таких угруповань, як UAC-0010, UAC-0028 та Sandworm, які діють за підтримки державних установ і здійснюють складні кібератаки на критичну інфраструктуру та інші важливі об’єкти. Аналіз останніх досліджень та публікацій у сфері кібербезпеки, таких як звіти Державної служби спеціального зв’язку та захисту інформації України та Ради національної безпеки і оборони України, допомагає висвітлити основні тенденції та ризики, що виникають в умовах розвитку кіберзагроз [1]–[3].

Хакерські угруповання постійно адаптуються до нових викликів і розробляють нові методи та інструменти для досягнення своїх цілей, що вимагає від організацій постійного вдосконалення засобів захисту і впровадження нових стандартів безпеки. Важливо розуміти, що сучасні кібератаки використовують не тільки технологічні, але й психологічні методи, що робить їх складнішими та небезпечнішими для бізнесу, урядів і суспільства в цілому.

Одним із найпоширеніших методів залишається фішинг — техніка, що полягає в обмані жертв через підроблені електронні листи, вебсайти або повідомлення, які виглядають легітимними. Наприклад, жертву можуть переконати в тому, що вона отримує повідомлення від свого банку або роботодавця, змушуючи завантажити шкідливий файл або надати особисті дані. Вплив фішингових атак посилюється через використання соціальних мереж, де хакери можуть збирати дані про жертву для подальшого таргетованого обману [4].

Кейлогери є ще одним небезпечним інструментом, оскільки вони здатні приховано записувати всі натискання клавіш на комп'ютері жертви. Це дозволяє хакерам отримати паролі, інформацію про кредитні картки, номери телефонів та іншу конфіденційну інформацію, що зберігається у текстовому форматі. Кейлогери можуть бути встановлені на пристрої через фішингові посилання або троянські програми і залишаються непоміченими в системі, що робить їх особливо небезпечними [4].

DDoS-атаки — методи, які стають особливо актуальними під час політичних і економічних криз. Вони створюють штучне навантаження на вебсервери, роблячи їх недоступними для користувачів. DDoS-атаки часто застосовуються як спосіб дестабілізації діяльності організацій та є частиною більш масштабних кампаній, спрямованих на порушення зв'язку або обслуговування важливих структур, таких як банківські системи або державні портали [4].

Ще однією небезпечною технікою є крадіжка файлів cookie, в яких зберігаються дані користувача для авторизації на різних вебсайтах. Крадіжка cookie дозволяє злочинцям використовувати ці файли для входу на захищені ресурси від імені жертви. Зловмисники можуть перенаправляти користувачів на фальшиві сторінки або впроваджувати шкідливі розширення браузера, які підмінюють автентифікацію [4].

Підробка бездротових точок доступу (WAP) дозволяє хакерам отримати доступ до даних, що передаються через мережу. Злочинці створюють фальшиві точки доступу Wi-Fi у громадських місцях, маскуючись під легітимні мережі. Підключившись до такої мережі, користувачі ризикують передати свої особисті дані, паролі та іншу конфіденційну інформацію хакерам [4].

Троянське програмне забезпечення також залишається популярним серед хакерів. Троянські програми виглядають як легітимні файли або додатки, але після інсталяції на пристрої починають виконувати шкідливі функції. Трояни можуть використовуватися для викрадення даних, моніторингу активності користувача або завантаження додаткового шкідливого ПЗ. Багато троянів створені для тривалого шпигунства за користувачами і збирання даних, що робить їх особливо небезпечними в корпоративних мережах [4].

Атаки грубою силою використовують автоматизовані програми для перебору можливих комбінацій паролів, доки не буде знайдено правильний. Цей метод є особливо ефективним проти слабких паролів і підкреслює важливість використання складних паролів і багатофакторної аутентифікації [4].

Соціальна інженерія є психологічною методикою, за допомогою якої зловмисники обманюють людей, змушуючи їх видати конфіденційну інформацію або виконати шкідливу дію. Використовуючи телефонні дзвінки, повідомлення у соціальних мережах чи навіть особисте спілкування, хакери маніпулюють довірою жертв і використовують їх для проникнення у захищені системи [4].

Складні APT-атаки (Advanced Persistent Threat) — це довготривалі та добре організовані кампанії, спрямовані на проникнення в мережу з метою викрадення конфіденційної інформації або шпигунства. Такі атаки характерні для угруповань, які мають значні фінансові ресурси та використовують висококваліфікованих фахівців.

APT-атаки є особливо небезпечними, оскільки їх важко виявити, і вони можуть залишатися в системі протягом тривалого часу [5].

BEC-атаки (Business Email Compromise) полягають у видаванні зловмисника за керівника або іншого працівника організації з метою обману співробітників і отримання доступу до конфіденційних даних або фінансових ресурсів. BEC-атаки націлені на довірливі відносини всередині організації і можуть призвести до значних фінансових втрат [5].

Окрім цього, хакери активно використовують різні спеціалізовані інструменти, серед яких [6]:

1. Інструменти для мережевого злому надають хакерам комплексні можливості для глибокого аналізу та картографування мережі, що є критично важливим для підготовки атак. З їхньою допомогою зловмисники можуть визначати основні компоненти мережі, аналізувати хост-системи, а також перевіряти налаштування DNS, що дозволяє отримати інформацію про структуру мережі та основні маршрути передачі даних. Деякі з цих інструментів також здатні перехоплювати пакети даних, завдяки чому хакери отримують можливість детально аналізувати трафік і моделювати можливі вектори атак. Такий підхід допомагає виявити слабкі місця мережевої інфраструктури, що можуть бути використані для проникнення в систему або спричинення збоїв у її роботі.

2. Інструменти для бездротового злому орієнтовані на аналіз бездротових мереж, що зазвичай є менш захищеними порівняно з дротовими мережами. Вони дозволяють зловмисникам перехоплювати трафік і аналізувати протоколи безпеки, особливо в громадських мережах Wi-Fi, де часто використовуються слабкі протоколи захисту, такі як WEP. Використовуючи їх, хакери можуть не тільки отримати доступ до мережевого трафіку, але й розшифровувати його, отримуючи конфіденційну інформацію. Це відкриває широкі можливості для вторгнення в захищені мережі, а також дозволяє зловмисникам перехоплювати чутливі дані, такі як особисті повідомлення, банківську інформацію та інші особисті дані користувачів.

3. Інструменти для злому паролів є важливими засобами в арсеналі хакерів і забезпечують різні способи для розкриття паролів. До основних методів відносяться атака методом перебору, коли автоматизована програма генерує усі можливі комбінації символів до отримання потрібного пароля; словникова атака, що використовує базу даних популярних паролів або словникових слів для прискорення процесу; а також атака з використанням райдужних таблиць, яка дозволяє значно зменшити час на розкриття пароля за рахунок використання заздалегідь обчислених хеш-значень. За допомогою цих них зловмисники можуть отримати доступ до захищених облікових записів, що відкриває можливість для подальшого проникнення в систему, отримання конфіденційних даних і доступу до важливих ресурсів.

4. Інструменти для оцінювання вразливостей використовуються для сканування мереж, програмного забезпечення та операційних систем з метою виявлення потенційних вразливостей. Вони дозволяють ідентифікувати слабкі місця, зокрема некоректно налаштовані програми, застарілі версії програмного забезпечення, невиправлені вразливості, помилки конфігурації та інші фактори, що можуть призвести до успішної атаки. Зловмисники часто застосовують їх до здійснення атак, щоб максимально використовувати знайдені слабкі місця і мати можливість втрутитися у функціонування системи до того, як захист буде посилений або проблеми усунуті.

Слід зазначити, що описані методи й інструменти становлять лише частину арсеналу кіберзлочинців. Щоб зменшити ризики, організаціям слід постійно вдосконалювати захист, впроваджувати сучасні методи аутентифікації, проводити тренінги з кібергігієни для співробітників і оновлювати свої системи безпеки. Усе це вимагає не тільки технічних

інструментів, але й розуміння психологічних факторів, що впливають на вразливість до кібератак.

Ці реалії визначають нагальну потребу в системах, здатних швидко адаптуватися до нових загроз і забезпечувати адекватний рівень захисту для користувачів з різних секторів, включаючи критичну інфраструктуру, охорону здоров'я, енергетику та державні установи.

Законодавчі зміни в Європейському Союзі, такі як Директива NIS2 та Закон про кіберстійкість, також вказують на потребу вдосконалення підходів до кіберзахисту. Директива NIS2 розширює вимоги до кібербезпеки, охоплюючи нові галузі, зокрема хмарні обчислення та цифрову інфраструктуру. Це свідчить про перехід до більш уніфікованої стратегії кібербезпеки, що охоплює широкий спектр секторів, зокрема охорону здоров'я, транспорт та енергетику, забезпечуючи при цьому захист критичної інфраструктури. На рівні окремих організацій це означає впровадження комплексних аудитів та розробку індивідуальних планів дій, спрямованих на усунення вразливостей [7].

Крім того, останні масштабні кібератаки на медичні та енергетичні компанії у США, наприклад, на UnitedHealth та Kaiser, підкреслили потребу у вдосконаленні захисних механізмів у цих галузях. Витоки даних мільйонів клієнтів та багатомільйонні збитки, які були завдані через такі атаки, вказують на важливість розробки та впровадження нових стандартів для забезпечення кібербезпеки в охороні здоров'я. Проте брак фінансування ключових організацій, таких як NIST, що займаються розробкою цих стандартів, ускладнює цей процес [8].

Для створення інформаційної системи було проведено аналіз існуючих програмних рішень з кібербезпеки, таких як MITRE ATT&CK, CAPEC, CWE, NVD, CVE та Recorded Future. Кожна з цих систем має свої особливості та обмеження. Наприклад:

- MITRE ATT&CK є важливою базою знань, що описує тактики, техніки та процедури хакерських угруповань на основі реальних випадків атак [9];
- CAPEC зосереджується на загальних шаблонах атак, корисних для тестування захищеності систем [10];
- CWE забезпечує класифікацію програмних помилок, які можуть призвести до вразливостей [11];
- NVD і CVE — відкриті бази даних, що містять інформацію про відомі вразливості. [12], [13];
- Recorded Future є інструментом для аналізу загроз у реальному часі, що використовує штучний інтелект і машинне навчання для обробки великих обсягів даних [14].

Таблиця 1

Порівняння існуючих програмних рішень з новою системою

Критерій	MITRE ATT&CK	CAPEC	CWE	NVD	CVE	Recorded Future
Розширена інформація	+	–	–	–	–	+
Додавання угруповань	–	–	–	–	–	–
Локалізація (українська)	–	–	–	–	–	–
Функція фільтрації	–	–	–	+	+	+
Моніторинг	–	–	–	–	–	+

Порівняння систем, що представлено в табл. 1 показало, що інформаційна система повинна поєднувати переваги існуючих рішень та додавати нові функціональні можливості, а саме:

- розширену інформацію про атаки;
- додавання нових хакерських угруповань;
- українську локалізацію;
- функції фільтрації та аналізу.

Це дозволить запропонованій системі бути особливо корисною для досліджень у галузі кібербезпеки в українському контексті, зокрема для аналітиків, які працюють над локальними та глобальними кіберзагрозами.

Метою статті є розробка інформаційної системи, що забезпечить фільтрацію даних за визначеними параметрами, аналіз технік та інструментів угруповань, а також покращення можливостей фахівців у протидії кіберзагрозам шляхом більш детального розуміння діяльності хакерських угруповань.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Для організації та систематизації технік атак в інформаційній системі збору та аналізу даних про діяльність хакерських угруповань використовується класифікація на основі MITRE ATT&CK. Цей підхід дозволяє групувати техніки за тактиками атак, що відображають основні етапи злому [15].

Структуризація базується на трирівневій ієрархії [15]:

- тактики (Tactics) — стратегічні цілі атаки;
- техніки (Techniques) — конкретні методи досягнення тактики;
- підтехніки (Sub-techniques) — варіації конкретних технік.

Ця модель дозволяє впорядковано аналізувати дії хакерських угруповань та створювати зв’язки між групами та їхніми техніками.

З метою структуризації технік атак у системі кожна техніка прив’язана до відповідної тактики MITRE ATT&CK. Це дозволяє категоризувати техніки за етапами атаки, що спрощує аналітичний підхід [15].

Ініціалізація доступу (Initial Access) — отримання первинного доступу до системи жертви [16]:

- T1566 — Фішинг (Spear Phishing Link, Attachment);
- T1190 — Експлуатація вразливостей вебдодатків (Exploit Public-Facing Application);
- T1078 — Використання скомпрометованих акаунтів (Valid Accounts);
- T1133 — Компрометація VPN або віддаленого доступу (External Remote Services).

Виконання (Execution) — запуск шкідливого коду в системі жертви [16]:

- T1059 — Командні оболонки (Command and Scripting Interpreter);
- T1204 — Запуск шкідливого файлу користувачем (User Execution);
- T1047 — Використання PowerShell;
- T1106 — Автоматизація виконання через API Windows.

Закріплення у системі (Persistence) — методи утримання доступу після компрометації [16]:

- T1543 — Запуск через системні служби (Create or Modify System Process);
- T1574 — DLL Hijacking;

– T1547 — Автозапуск через реєстр Windows (Registry Run Keys);
– T1136 — Створення прихованих акаунтів.

Ескалація привілеїв (Privilege Escalation) — отримання розширених прав у системі [16]:

– T1068 — Експлуатація уразливостей в ОС (Exploitation for Privilege Escalation);
– T1134 — Підміна токенів доступу (Token Impersonation);
– T1078 — Використання адміністративних облікових записів.

Обхід захисту (Defense Evasion) — приховування активності та уникнення виявлення [16]:

– T1497 — Виявлення пісочниць та віртуальних машин;
– T1202 — Безфайлові атаки;
– T1070 — Очищення логів (Indicator Removal on Host);
– T1036 — Маскування процесів та файлів.

Збір інформації (Collection) — методи збору чутливої інформації із системи жертви [16]:

– T1056 — Кейлогери (Input Capture);
– T1114 — Перехоплення електронної пошти (Email Collection);
– T1005 — Копіювання файлів користувача (Data from Local System);
– T1119 — Перехоплення скріншотів (Screen Capture).

Ексфільтрація даних (Exfiltration) — передача викрадених даних з системи [16]:

– T1041 — Передача даних через C2-канали (Exfiltration Over C2 Channel);
– T1567 — Використання хмарних сервісів;
– T1020 — Передача файлів через FTP або HTTP.

Командування та контроль (Command and Control) — збереження контролю над скомпрометованими системами [16]:

– T1572 — VPN-тунелювання (Protocol Tunneling);
– T1090 — Застосування проксі-серверів (Proxy Connection);
– T1001 — Шифрування C2-трафіку.

В інформаційній системі реалізовано математичний апарат для обробки та аналізу технік атак, що включає візуалізацію даних у форматі кругових діаграм і гістограм, а також механізм багатокритеріальної фільтрації для глибшого аналізу, приклади наведено на рис. 1 [17], [18].

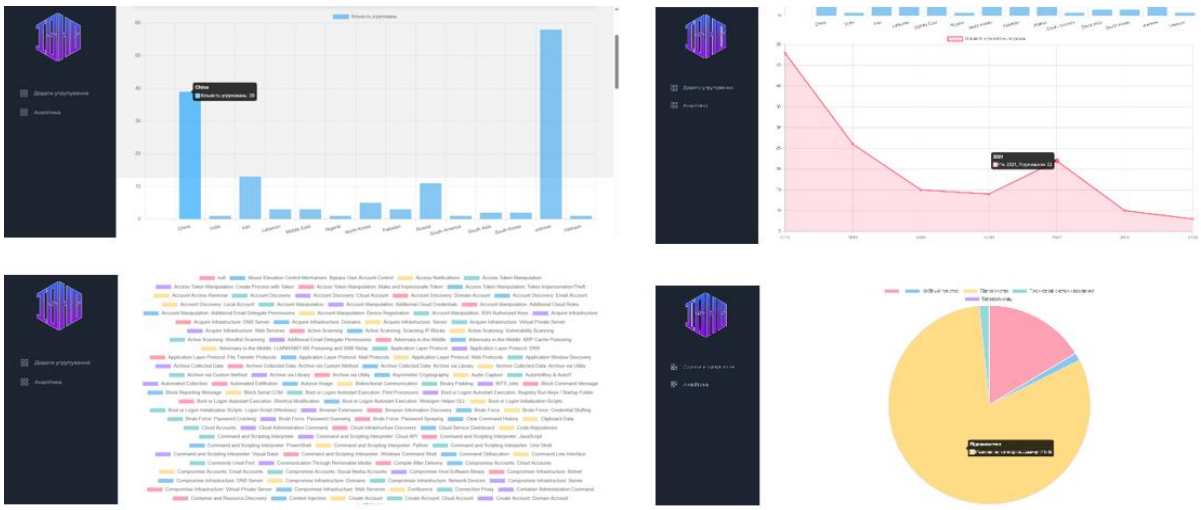

Рис. 1. Інтерфейс інформаційної системи збору та аналізу даних про діяльність хакерських угруповань

На основі даних про кількість застосувань кожної техніки будується ймовірнісний розподіл, що дозволяє визначити найбільш поширені техніки атак серед хакерських угруповань.

Ймовірнісний розподіл технік атак:

$$P(T_i) = \frac{T_i}{T}, \quad (1)$$

$P(T_i)$ — ймовірність використання техніки T_i;

T_i — кількість випадків застосування конкретної техніки у всіх зареєстрованих атаках;

T — загальна кількість технік.

Це дозволяє визначити, які техніки атак є найпоширенішими, а які зустрічаються рідше.

Даний підхід дозволяє отримати такі аналітичні висновки:

1. Виявлення критичних технік атак. Найбільш використовувані техніки можуть вказувати на основні методи атак, що застосовуються хакерськими угрупованнями. Наприклад, якщо техніка T1566 (Фішинг) має високий показник $P(T_i)$, це означає, що атаки через соціальну інженерію домінують у вибірці.
2. Порівняння популярності технік. Використання частотного розподілу дозволяє порівнювати частоту застосування різних методів атак. Наприклад, техніка T1078 (Valid Accounts — використання скомпрометованих акаунтів) може мати нижчий показник, ніж T1204 (User Execution — запуск шкідливого файлу користувачем), що може свідчити про більшу залежність атак від людського фактора.
3. Прогнозування майбутніх атак. Аналіз тенденцій у використанні технік допомагає прогнозувати можливі вектори атак, що дає змогу ефективніше будувати систему кіберзахисту. Наприклад, якщо певна техніка T1547 (Registry Run Keys — автозапуск через реєстр) зростає у частоті використання, то це може свідчити про зміну тактики угруповань.

Результати частотного аналізу технік атак мають практичне застосування в різних аспектах кібербезпеки:

1. Пріоритизація заходів захисту. Аналіз поширених технік дозволяє визначити, на які загрози слід звернути найбільшу увагу. Наприклад, якщо T1059 (Command and Scripting Interpreter — командні оболонки) має високий рівень використання, то слід посилити моніторинг та обмеження доступу до PowerShell, CMD та інших інтерпретаторів.
2. Автоматизований аналіз інцидентів. Знаючи ймовірності використання технік, можна автоматизувати аналіз логів та подій у SIEM-системах. Наприклад, частота спроб експлуатації вразливостей (T1190 — Exploit Public-Facing Application) може свідчити про масову сканувальну активність.
3. Оцінка ризиків для конкретних організацій. Якщо у певній галузі часто використовуються специфічні техніки атак, можна розробити індивідуальні сценарії захисту. Наприклад, у фінансовому секторі можуть бути

популярними T1078 (Valid Accounts) та T1041 (Exfiltration Over C2 Channel), що вимагає посиленого контролю доступу та моніторингу витоку даних.

Візуальне зображення у вигляді гістограм розподілу технік атак для хакерських угруповань дозволяє оцінити, які угруповання використовують більшу кількість атакувальних технік, а які мають вузьку спеціалізацію. Вона представляє дискретний розподіл частот для кількості технік, які використовуються різними хакерськими угрупованнями.

Нехай:

$G = \{G_1, G_2, ..., G_n\}$ — множина хакерських угруповань;

T — множина всіх можливих технік атак;

$f(G_i)$ — кількість технік, що використовує угруповання G_1.

Розподіл частот можна описати за допомогою емпіричної функції розподілу:

$$F(T) = \frac{1}{n} \sum_{i=1}^{n} f(G_i), \quad (2)$$

де:

$F(T)$ — середня кількість технік на одне угруповання;

$f(G_i)$ — кількість технік, що використовує конкретне угруповання;

n — загальна кількість угруповань у вибірці.

Ця формула дозволяє оцінити середню кількість технік атак, що застосовуються угрупованнями, та визначити загальні тенденції у використанні методів атак.

Даний аналіз дає змогу:

1. Визначити рівень складності атак угруповань:
   – якщо $F(T)$ є високим, це означає, що більшість угруповань використовують широкий набір технік, що ускладнює їхню ідентифікацію та нейтралізацію;
   – якщо $F(T)$ є низьким, це означає, що угруповання діють більш вузькоспрямовано (наприклад, спеціалізуються лише на вебатаках або фішингу).
2. Порівняти хакерські угруповання за рівнем їхньої загрози:
   – якщо $f(G_i)$ для конкретного угруповання G_i значно перевищує середнє значення $F(T)$, то це угруповання можна класифікувати як високоризиковане;
   – угруповання з малим значенням $f(G_i)$ можуть бути менш небезпечними або спеціалізованими на конкретних атаках.
3. Прогнозувати еволюцію загроз:
   – якщо середнє значення $F(T)$ зростає з часом, це може свідчити про універсалізацію атакуючих методів, що означає збільшення складності атак;
   – якщо значення стабільне, це означає, що угруповання дотримуються певних схем атак без суттєвих змін.

Для оцінки того, які саме домени (сфери застосування атак) є найбільш вразливими, та на які області слід звернути особливу увагу в рамках кіберзахисту, використовується кругова діаграма. Вона представляє відносні частки атак у різних доменах (категоріях).

В математичній моделі домени атак представлені множиною:

$$D = \{d_1, d_2, ..., d_m\}, \quad (3)$$

де:

D — множина всіх доменів атак (наприклад, підприємства, мобільні пристрої, промислові системи);

d_m — конкретний домен атаки.

Кожному домену відповідає кількість атак:

$N(d_i)$ — кількість атак, що сталися у домені;

N — загальна кількість атак у всіх доменах.

Для розрахунку відносної частки атак у кожному домені використовується формула:

$$P(d_i) = \frac{N(d_i)}{N}, \quad (4)$$

де:

$P(d_i)$ — ймовірність того, що атака належить до домену;

$N(d_i)$ — кількість атак у конкретному домені;

N — загальна кількість атак у всіх доменах.

Формула (4) дозволяє визначити відсоткову частку кожного домену в загальному обсязі атак.

Модель дозволяє розподілити та класифікувати атаки за сферами застосування:

1. Визначення домінуючих доменів атак:
   – якщо $P(d_i)$ для певного домену значно перевищує інші значення, це свідчить про цілеспрямованість атак у цій галузі;
   – наприклад, якщо підприємства (Business Sector) мають найвищу частку атак, це може вказувати на активне використання фішингових та мережевих атак у корпоративному середовищі.
2. Пріоритизація кіберзахисту:
   – домени з найбільшою часткою атак потребують підвищеного рівня захисту та моніторингу;
   – наприклад, якщо промислові системи (Industrial Control Systems, ICS) мають високий показник $P(d_i)$, то слід посилити заходи безпеки в цій галузі.
3. Оцінка тенденцій атак:
   – зіставлення значень $P(d_i)$ у різні періоди дозволяє виявити зміну пріоритетів атакуючих угруповань;
   – наприклад, якщо зростає частка атак на мобільні пристрої (Mobile Devices), це може свідчити про активізацію атак у мобільному середовищі (зловмисне ПЗ, перехоплення даних).

Фільтрація є ключовим етапом обробки даних у системі, що дозволяє користувачам швидко знаходити необхідну інформацію, відсіюючи нерелевантні записи. На основі розробленого інтерфейсу система використовує багатокритеріальну фільтрацію, де дані відбираються за кількома параметрами одночасно.

ISSN 2663 - 4023

Нехай:

$G = \{G_1, G_2, ..., G_n\}$ — множина всіх хакерських угруповань у базі знань;

$F = \{f_1, f_2, ..., f_n\}$ — множина активних фільтрів (наприклад, країна, рік, домен, особливості тощо);

$R(G)$ — це функція фільтрації, результатом якої є підмножина угруповань, які залишилися після фільтрації.

Фільтрація застосовується послідовно або комбінується за логікою «AND» (перетин множин) та «OR» (об'єднання множин), що можна описати рівнянням:

$$R(G) = \bigcap_{i=1}^{m} f_i(G), \tag{5}$$

де $f_i(G)$ — підмножина угруповань, що відповідає критерію f_i.

Якщо користувач обирає кілька значень у межах одного фільтра (наприклад, країна = Китай або Іран), застосовується логіка «OR»:

$$f_{країна}(G) = G_{Китай} \bigcup G_{Іран}, \tag{6}$$

Якщо ж обирається кілька фільтрів одночасно (наприклад, країна = Китай і рік = 2023), застосовується логіка «AND»:

$$R(G) = G_{Китай} \bigcap G_{2023}, \tag{7}$$

Система підтримує такі основні фільтри:

1. Фільтр за країною $f_{країна}$, відбирає угруповання, які належать до обраних країн:

$$f_{країна}(G) = \left\{ G_i \in G \middle| G_{i,країна} \in S_{країн} \right\}, \tag{8}$$

$S_{країн}$ — множина вибраних країн.

2. Фільтр за роком створення $f_{рік}(G)$, відбирає угруповання, створені у вибраному році або діапазоні років:

$$f_{рік}(G) = \left\{ G_i \in G \middle| G_{i,рік} \in S_{років} \right\}, \tag{9}$$

3. Фільтр за доменом діяльності $f_{домен}(G)$, відбирає угруповання, що спеціалізуються на конкретних типах атак (наприклад, підприємства, мобільні пристрої, промислові системи):

$$f_{домен}(G) = \left\{ G_i \in G \middle| G_{i,домен} \in S_{доменів} \right\}, \tag{10}$$

4. Фільтр за особливостями діяльності $f_{особливість}(G)$, відбирає угруповання, що мають певні атрибути (наприклад, використовують специфічне ПЗ, певні техніки атак або проводять кіберкампанії):

$$f_{особливість}(G) = \left\{ G_i \in G \middle| G_{i,особливість} \in S_{особливостей} \right\}, \tag{11}$$

При виборі кількох параметрів одночасно підсумкова множина результатів обчислюється через перетин множин:

$$R(G) = f_{країн}(G) \bigcap f_{рік}(G) \bigcap f_{домен}(G) \bigcap f_{особливість}(G). \tag{12}$$

Якщо користувач вказує кілька значень в одному фільтрі, то вони об'єднуються логічною операцією «OR», а всі фільтри між собою поєднуються через «AND».

Основну частину інформаційної системи реалізовано на Laravel як на надійному PHP-фреймворці, призначеному для розробки вебдодатків за архітектурною схемою «модель-представлення-контролер» (MVC).

Архітектура MVC [19]:

– модель — відповідає за логіку даних, що лежить в основі програми;
– представлення — це те, що користувач бачить і з чим взаємодіє в додатку;
– контролер — виступає в ролі ядра додатку і взаємодіє з моделлю та представленням.

На рис. 2 зображена архітектура інформаційної системи збору та аналізу даних про діяльність хакерських угруповань, що використовує Nginx, фреймворк Laravel MVC і зовнішнє джерело даних, таке як база знань MITRE ATT&CK [20].

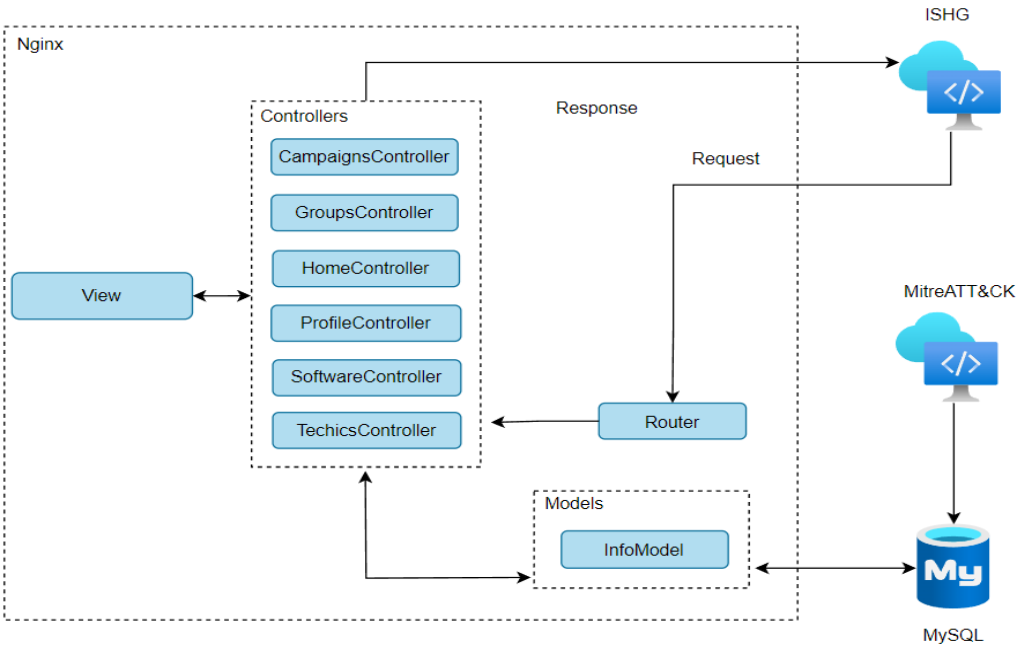

Рис. 2. Архітектура інформаційної системи збору та аналізу даних про діяльність хакерських угруповань

Ця архітектура побудована за такою логікою:

Дані з бази знань MITRE ATT&CK аналізуються та зберігаються в базі даних MySQL. Це передбачає отримання актуальної інформації про кіберзагрози та перетворення її в структурований формат, сумісний зі схемою бази даних інформаційної системи.

Запитами керує Nginx, який діє як вебсервер. Він спрямовує вхідні запити до відповідних контролерів у програмі Laravel.

Компонент маршрутизатора програми отримує ці запити та направляє їх до відповідного контролера на основі URL-адреси та типу запиту (GET або POST) [21].

Кожен «Controller» відповідає за обробку певних типів даних і операцій:

– CampaignsController — керує даними та діями, пов'язаними з кампаніями хакерських угруповань;

- GroupsController — керує операціями, пов’язаними з угрупованнями і їх описом;
- HomeController — керує взаємодією з інформаційною панеллю;
- ProfileController — працює з інформацією профілів угруповань;
- SoftwareController — контролює дані, пов’язані з програмним забезпеченням, такими як уразливості або інструменти, які використовують злочинні суб’єкти;
- TechicsController — керує тактиками, техніками та процедурами (TTP), які використовують хакерські угруповання.

Контролери взаємодіють з моделями (наприклад, InfoModel), щоб отримати, оновити або маніпулювати даними, що зберігаються в базі даних MySQL. Модель представляє структуру даних і логіку програми. Після обробки даних контролер надсилає результати назад до перегляду, який форматує та відображає інформацію для користувача.

Компонент представлення «View» використовує шаблони Blade (які використовуються в Laravel) для динамічного відтворення вебсторінок на основі даних, отриманих від контролерів. Це дає змогу користувачам взаємодіяти з інтерфейсом, який відображає дані.

Ця архітектура ефективно розділяє проблеми, дозволяючи керувати розробкою та обслуговуванням вебпрограми, з чіткими шляхами та відповідальністю за обробку даних, взаємодію з користувачем та зовнішню інтеграцію.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У статті розглянуто концепцію та реалізацію інформаційної системи, призначеної для збору та аналізу даних про діяльність хакерських угруповань. Запропоноване рішення базується на використанні сучасних інформаційних технологій, математичних методів та бази знань MITRE ATT&CK, що забезпечує ефективне опрацювання великих обсягів даних про кіберзагрози. Реалізована система дозволяє здійснювати багатофакторну фільтрацію інформації, аналіз тенденцій використання атакувальних технік, адаптацію під локальні потреби фахівців з кібербезпеки. Актуальність розробки зумовлена зростанням активності хакерських угруповань і необхідністю підвищення рівня захисту національного кіберпростору.

Подальші дослідження доцільно спрямувати на інтеграцію системи із зовнішніми джерелами кіберрозвідки та поглибленням функцій візуалізації даних для аналітиків.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Operational Center for Response to Cyber Incidents of the State Center for Cyber Defense of the SSSCIP. (2023). *Report on the work of the Vulnerability Detection and Response to Cyber Incidents and Cyberattacks System for 2023*. https://scpc.gov.ua/api/files/9c21855d-74da-45d1-90f9-5d4f6795996a
2. Operational Center for Response to Cyber Incidents of the State Center for Cyber Defense of the SSSCIP. (2024). *Report on the work of the Vulnerability Detection and Response to Cyber Incidents and Cyberattacks System for 2024*. https://scpc.gov.ua/api/files/72e13298-4d02-40bf-b436-46d927c88006
3. National Security and Defense Council of Ukraine. (2024). *Annual analytical review: Key events, trends, and challenges in cybersecurity in 2024*. https://www.rnbo.gov.ua/files/2024/NATIONAL_CYBER_SCC/20250109/Year%20in%20review_UKR_upd.pdf
4. Bernaldo, M. (2024, March 21). The 15 most common hacking techniques. *Ciberseguridad y servicios informáticos (soluciones IT) | ESED*. https://www.esedsl.com/en/blog/the-15-most-common-hacking-techniques

5. HackerOne. (n.d.). *What is hacking?* https://www.hackerone.com/knowledge-center/what-hacking-black-hat-white-hat-blue-hat-and-more
6. Hackr.io. (n.d.). *The best ethical hacking tools in 2025 | Full guide*. https://hackr.io/blog/best-hacking-tools
7. State Service for Special Communications and Information Protection of Ukraine. (n.d.). *EU Directive NIS2: What is it, for what needs was it developed and why is Ukraine implementing it*. https://cip.gov.ua/ua/news/direktiva-yes-nis2-sho-ce-take-dlya-yakikh-potreb-rozroblena-ta-dlya-chogo-ukrayina-yiyi-implementuye
8. National Security and Defense Council of Ukraine. (2024). *Cyber digest: Overview of events in the field of cybersecurity, April 2024*. https://www.rnbo.gov.ua/files/НКІЦК/Cyber%20digest_Apr_2024_UA.pdf
9. MITRE. (n.d.). *MITRE ATT&CK®*. https://attack.mitre.org/
10. MITRE. (n.d.). *CAPEC - Common Attack Pattern Enumeration and Classification (CAPEC™)*. https://capec.mitre.org
11. MITRE. (n.d.). *CWE - Common Weakness Enumeration*. https://cwe.mitre.org
12. National Institute of Standards and Technology. (n.d.). *NVD - General*. https://nvd.nist.gov/general
13. MITRE. (n.d.). *CVE - CVE*. https://cve.mitre.org
14. Recorded Future. (n.d.). *Advanced cyber threat intelligence*. https://www.recordedfuture.com
15. Cynet. (n.d.). *Quick guide to MITRE ATT&CK: Matrices, tactics, techniques & more*. https://www.cynet.com/network-attacks/quick-guide-to-mitre-attck-matrices-tactics-techniques-more/#heading-1
16. MITRE. (n.d.). *Techniques - Enterprise | MITRE ATT&CK®*. https://attack.mitre.org/techniques/enterprise
17. Polishchuk, V., Puchkov, O., Subach, I., Mykytiuk, A., & Onishchenko, V. (2024). *Certificate of registration of copyright for the work: Computer program "Information system for recording data on hacker groups 'ISHG'"* (Copyright certificate No. 129603). Ukrainian National Office of Intellectual Property and Innovation.
18. Polishchuk, V., Puchkov, O., Subach, I., Mykytiuk, A., & Onishchenko, V. (2025). *Certificate of registration of copyright for the work: Computer program "Analytical subsystem of the information system for accounting data on hacker groups 'AIS'"* (Copyright certificate No. 136635). Ukrainian National Office of Intellectual Property and Innovation.
19. Codecademy. (n.d.). *MVC architecture explained: Model, View, Controller*. https://www.codecademy.com/article/mvc
20. Polishchuk, V. R., & Mykytiuk, A. V. (2024). Information system for recording data on hacker groups. In *VII scientific and practical conference of cadets (students), postgraduates, doctoral candidates and young scientists "Current issues of the application of special information and communication systems"* (pp. 412–413). Igor Sikorsky Kyiv Polytechnic Institute.
21. CODE Magazine. (n.d.). *Dependency injection and service container in Laravel*. https://www.codemag.com/Article/2212041/Dependency-Injection-and-Service-Container-in-Laravel

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (29), 2025
ISSN 2663 - 4023

Artem Mykytiuk
PhD in Computer Science, Deputy Head of the Department of
Computer Science and Artificial Intelligence Technologies in Cybersecurity
Institute of Special Communications and Information Protection
National Technical University of Ukraine
"Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine
ORCID ID: 0000-0002-8307-9978
mukuta8888@gmail.com

Ivan Horniichuk
PhD in Computer Science, Senior Lecturer of the Department of
Computer Science and Artificial Intelligence Technologies in Cybersecurity
Institute of Special Communications and Information Protection
National Technical University of Ukraine
"Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine
ORCID ID: 0000-0001-6754-4764
horniychuk.ivan@gmail.com

Viktoriia Polishchuk
Master's cadet of the Department of
Computer Science and Artificial Intelligence Technologies in Cybersecurity
Institute of Special Communications and Information Protection
National Technical University of Ukraine
"Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine
ORCID ID: 0009-0003-4596-1219
polisukv230@gmail.com

Oleksandra Bychkovska
Junior Research Associate of the Research Center
Institute of Special Communications and Information Protection
National Technical University of Ukraine
"Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine
ORCID ID: 0009-0004-2896-0545
o.bychkovska@kpi.ua

INFORMATION SYSTEM FOR THE COLLECTION AND ANALYSIS OF DATA ON HACKER GROUP ACTIVITIES

Abstract. The modern world's growing dependence on information systems and technologies requires robust protection against cyberattacks. This has become particularly relevant amid the increasing activity of hacker groups. Attacks targeting state and private organizations encompass not only critical infrastructure but also the theft of confidential information, financial fraud, and destabilizing actions in cyberspace. In particular, hacker groups, using the latest techniques, tools, and software, pose a significant threat to the information security of individual organizations and entire states. They operate covertly, adapt quickly to new conditions, and have a high level of coordination, which complicates the detection and mitigation of their activities. This necessitates focused monitoring, continuous analysis of their activities, as well as the systematization and accumulation of the information obtained to create a unified knowledge base about their operations. Such groups often operate at an international level, affecting stability and security in various regions of the world, particularly in Ukraine. This article addresses the absence of a comprehensive tool for collecting, structuring, and analyzing data on hacker groups. This tool would enable filtering by group type, geography of activity, time periods of activity, as well as the techniques and tools used. Special attention is paid to the development of an information system that not only stores and analyzes information about the activities of hacker groups but also allows specialists to adapt data to local needs. The implementation of such a system requires the use of modern approaches to data collection, normalization, and analysis. Given the dynamic changes in cyberspace, the effective

processing of information about attack operations requires the implementation of algorithms for filtering, clustering, and statistical analysis, which allows for the automated identification of trends in the use of attack techniques. A distinctive feature of this system is its adaptation to the Ukrainian context, considering the specifics of the local cyberspace, linguistic features, typical attack scenarios, and national security priorities. This, in turn, contributes to increasing the effectiveness of the analytical work of Ukrainian specialists, strengthening cyber defense, and developing a resilient model for responding to cyber threats.

Keywords: information system; cybersecurity; hacker groups; knowledge base; data filtering; cyber threat analysis.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Operational Center for Response to Cyber Incidents of the State Center for Cyber Defense of the SSSCIP. (2023). *Report on the work of the Vulnerability Detection and Response to Cyber Incidents and Cyberattacks System for 2023*. https://scpc.gov.ua/api/files/9c21855d-74da-45d1-90f9-5d4f6795996a
2. Operational Center for Response to Cyber Incidents of the State Center for Cyber Defense of the SSSCIP. (2024). *Report on the work of the Vulnerability Detection and Response to Cyber Incidents and Cyberattacks System for 2024*. https://scpc.gov.ua/api/files/72e13298-4d02-40bf-b436-46d927c88006
3. National Security and Defense Council of Ukraine. (2024). *Annual analytical review: Key events, trends, and challenges in cybersecurity in 2024*. https://www.rnbo.gov.ua/files/2024/NATIONAL_CYBER_SCC/20250109/Year%20in%20review_UKR_upd.pdf
4. Bernaldo, M. (2024, March 21). The 15 most common hacking techniques. *Ciberseguridad y servicios informáticos (soluciones IT) | ESED*. https://www.esedsl.com/en/blog/the-15-most-common-hacking-techniques
5. HackerOne. (n.d.). *What is hacking?* https://www.hackerone.com/knowledge-center/what-hacking-black-hat-white-hat-blue-hat-and-more
6. Hackr.io. (n.d.). *The best ethical hacking tools in 2025 | Full guide*. https://hackr.io/blog/best-hacking-tools
7. State Service for Special Communications and Information Protection of Ukraine. (n.d.). *EU Directive NIS2: What is it, for what needs was it developed and why is Ukraine implementing it*. https://cip.gov.ua/ua/news/direktiva-yes-nis2-sho-ce-take-dlya-yakikh-potreb-rozroblena-ta-dlya-chogo-ukrayina-yiyi-implementuye
8. National Security and Defense Council of Ukraine. (2024). *Cyber digest: Overview of events in the field of cybersecurity, April 2024*. https://www.rnbo.gov.ua/files/НКІЦК/Cyber%20digest_Apr_2024_UA.pdf
9. MITRE. (n.d.). *MITRE ATT&CK®*. https://attack.mitre.org/
10. MITRE. (n.d.). *CAPEC - Common Attack Pattern Enumeration and Classification (CAPEC™)*. https://capec.mitre.org
11. MITRE. (n.d.). *CWE - Common Weakness Enumeration*. https://cwe.mitre.org
12. National Institute of Standards and Technology. (n.d.). *NVD - General*. https://nvd.nist.gov/general
13. MITRE. (n.d.). *CVE - CVE*. https://cve.mitre.org
14. Recorded Future. (n.d.). *Advanced cyber threat intelligence*. https://www.recordedfuture.com
15. Cynet. (n.d.). *Quick guide to MITRE ATT&CK: Matrices, tactics, techniques & more*. https://www.cynet.com/network-attacks/quick-guide-to-mitre-attck-matrices-tactics-techniques-more/#heading-1
16. MITRE. (n.d.). *Techniques - Enterprise | MITRE ATT&CK®*. https://attack.mitre.org/techniques/enterprise
17. Polishchuk, V., Puchkov, O., Subach, I., Mykytiuk, A., & Onishchenko, V. (2024). *Certificate of registration of copyright for the work: Computer program "Information system for recording data on hacker groups 'ISHG'"* (Copyright certificate No. 129603). Ukrainian National Office of Intellectual Property and Innovation.
18. Polishchuk, V., Puchkov, O., Subach, I., Mykytiuk, A., & Onishchenko, V. (2025). *Certificate of registration of copyright for the work: Computer program "Analytical subsystem of the information system for accounting data on hacker groups 'AIS'"* (Copyright certificate No. 136635). Ukrainian National Office of Intellectual Property and Innovation.

19. Codecademy. (n.d.). *MVC architecture explained: Model, View, Controller*. https://www.codecademy.com/article/mvc
20. Polishchuk, V. R., & Mykytiuk, A. V. (2024). Information system for recording data on hacker groups. In *VII scientific and practical conference of cadets (students), postgraduates, doctoral candidates and young scientists "Current issues of the application of special information and communication systems"* (pp. 412–413). Igor Sikorsky Kyiv Polytechnic Institute.
21. CODE Magazine. (n.d.). *Dependency injection and service container in Laravel*. https://www.codemag.com/Article/2212041/Dependency-Injection-and-Service-Container-in-Laravel