Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет Інформаційно-аналітичних технологій та менеджменту
(повна назва)
Кафедра Інформатики
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти другий (магістерський)

ДОСЛІДЖЕННЯ «АЛМАЗНОЇ МОДЕЛІ» ЩОДО ВРАХУВАННЯ ВИЗНАЧЕННЯ ЗВ'ЯЗКУ МІЖ МОТИВАЦІЄЮ ПРИ ЗДІЙСНЕННІ ХАКЕРОМ КІБЕРАТАКИ
(тема)

Виконав:
студент 2 курсу, групи ІНФм-22-3
Стебаєв Д.І.
(прізвище, ініціали)

Спеціальності 122 Комп'ютерні науки
(код і повна назва спеціальності)

Тип програми освітньо-професійна

Освітня програма Інформатика
(повна назва освітньої програми)

Керівник проф. Кузьомін О. Я.
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри _____ Кобилін О.А.
(підпис) (прізвище, ініціали)

2024 р.

Харківський національний університет радіоелектроніки

Факультет Інформаційно-аналітичних технологій та менеджменту
(повна назва)

Кафедра Інформатики
(повна назва)

Рівень вищої освіти другий (магістерський)

Спеціальність 122 Комп'ютерні науки
(код і повна назва)

Тип програми освітньо-професійна

Освітня програма Інформатика
(повна назва освітньої програми)

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
«____»_____ 2024 р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

студентові Стебаєву Дмитру Ігоровичу
(прізвище, ім'я, по батькові)

1. Тема роботи Дослідження «алмазної моделі» щодо врахування визначення зв'язку між мотивацією при здійсненні хакером кібератаки

затверджена наказом по університету від 3 листопада 2023 року № 1280Ст

2. Термін подання студентом роботи до екзаменаційної комісії 25 грудня 2023 р.

3. Вихідні дані до роботи науково-методична та науково-технічна література, матеріаликонференцій, дані інтернет-мережі, бібліотека OpenCV, мова програмування Python, середовище розроблення Notebook.

4. Перелік питань, що потрібно опрацювати в роботі

1. Огляд методів дослідження «алмазної моделі».
2. Комп'ютерна модель щодо врахування визначення зв'язку між мотивацією при здійсненні хакером кібератаки.
3. Протестувати розроблений застосунок та провести аналіз результатів.
4. Виявити перспективи подальшої роботи.

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (п.5 включається до завдання за рішенням випускової кафедри) Актуальність дослідження, об'єкт та мета дослідження, постановка задачі дослідження, вихідні дані дослідження, етапи розроблення, результат тестування, висновки, перспективи подальших досліджень, апробація результатів роботи.

6. Консультанти розділів роботи (п.6 включається до завдання за наявності консультантів згідно з наказом, зазначеним у п.1)

Найменування розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		підпис	дата

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Терміни виконання етапів роботи	Примітка
1	Отримання завдання на кваліфікаційну роботу	03.11.2023	
2	Аналіз завдання, підбір літератури	03.11.23-05.11.23	
3	Аналіз літератури з досліджуваної проблеми	06.11.23-09.11.23	
4	Аналіз методів дослідження «алмазної моделі».	10.11.23-21.11.23	
5	Розробка методу «алмазної моделі».	22.12.23-01.12.23	
6	Програмна реалізація	02.12.23-08.12.23	
7	Оформлення пояснювальної записки	09.12.23-10.12.23	
8	Перевірка на плагіат	11.12.2023	
9	Рецензування	15.12.2023	
10	Підготовка презентації та доповіді	17.12.2023	
11	Занесення роботи в електронний архів	25.12.2023	
12	Попередній захист кваліфікаційної роботи	04.01.2024	

Дата видачі завдання 3 листопада 2023 р.

Студент _____
(підпис)

Керівник роботи _____ проф. Кузьомін О. Я.
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ/ABSTRACT

Пояснювальна записка до кваліфікаційної роботи: 61 с., 1 табл., 55 джерел.

АЛМАЗНА МОДЕЛЬ, МОТИВАЦІЯ ХАКЕРА, КІБЕРАТАКА, ІНФОРМАЦІЙНА БЕЗПЕКА, МАШИННЕ НАВЧАННЯ.

Об’єктом дослідження роботи є методи протидії хакерським кібератакам, а предметом дослідження — ефективність використання «алмазної моделі» для прогнозування хакерської кібератаки.

Метою дослідження є всебічно дослідити та зрозуміти «алмазну модель» та перевірити, чи покращує її використання захист програм від потенційних кібератак.

Використано методи числового моделювання та аналітичного обґрунтування. Проведено дослідження та аналіз методів «алмазної моделі».

Досліджено методи «Open Source Intelligence (OSINT)», «Аналіз Dark Web», «Аналіз поведінки», «Статистичний аналіз», «Машинне навчання та обробка природної мови (NLP)», «Перехресні посилання на джерела даних», та інші. Розроблено алгоритм «алмазної моделі».

У результаті дослідження здійснена програмна реалізація системи для розпізнавання хакерських кібератак з використанням «алмазної моделі».

DIAMOND MODEL, HACKER MOTIVATION, CYBER ATTACK, INFORMATION SECURITY, MACHINE LEARNING.

The research object of the work is the methods of countering hacker cyberattacks, and the subject of research is the effectiveness of using the "diamond model" for predicting hacker cyberattacks. The purpose of the study is to comprehensively investigate and understand the "diamond pattern" and see if its use improves the protection of applications against potential cyber attacks.

Numerical modeling and analytical reasoning methods were used. The research and analysis of the "diamond model" methods was carried out.

The methods of "Open Source Intelligence (OSINT)", "Dark Web Analysis", "Behavior Analysis", "Statistical Analysis", "Machine Learning and Natural Language Processing (NLP)", "Cross-references to data sources" and others were studied. The "Diamond Model" algorithm was developed.

As a result of the research, a software implementation of the system for recognizing hacker cyberattacks using the "diamond model" was carried out.

ЗМІСТ

Перелік умовних позначень, символів, одиниць, скорочень і термінів.....7
Вступ.....8
1 Огляд основних методів «алмазної моделі» щодо врахування визначення зв’язку між мотивацією при здійсненні хакером кібератаки.....11
1.1 Основні тези дослідження «алмазної моделі».....11
1.2 Основні методи дослідження «алмазної моделі».....14
1.3 Аналіз літературних джерел.....16
1.4 Постановка задачі дослідження.....20
2 Алмазна модель. Дослідження методів 22
2.1 Open Source Intelligence (OSINT).....22
2.2 Dark Web Analysis.....23
2.3 Behavioral Analysis.....24
2.4 Psychological Profiling.....25
2.5 Interviews and Surveys.....26
2.6 Case Studies.....28
2.7 Statistical Analysis.....29
2.8 Content Analysis.....30
2.9 Machine Learning and Natural Language Processing (NLP).....32
2.10 Collaboration with Law Enforcement.....33
2.11 Ethnographic Research.....34
2.12 Ethical Hacking and Red Teaming.....36
2.13 Cross-Referencing Data Sources.....37
2.14 Переваги та недоліки розглянутих методів.....38
3 Комп’ютерна модель щодо врахування визначення зв’язку між мотивацією при здійсненні хакером кібератаки.....44
3.1 Обґрунтування вибору середовища програмної реалізації.....44
3.2 Програмна реалізація.....47
3.3 Інструкція користувача.....50

3.4 Тестування та аналіз розробленої моделі.....51
Висновки.....53
Перелік джерел посилання.....56

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

NMT – Neural Machine Translation (нейронний машинний переклад)

ШІ – штучний інтелект

NLP – Natural Language Processing (обробка природної мови)

ВСТУП

Тема дослідження «алмазної моделі» щодо врахування визначення зв’язку між мотивацією при здійсненні хакером кібератаки належить до області кібербезпеки та кіберкриміналістики. Ця тема є надзвичайно актуальною та важливою у сучасному світі, оскільки інформаційні системи і технології стали неотдільною частиною нашого життя і функціонування суспільства в цілому. Наприклад, енергосистема України потребує захисту від російських кібератак [1], що підтверджує актуальність даної роботи навіть для повсякденного життя простих громадян.

Зростання кількості та складності кібератак свідчить про те, що хакери виявляють новий рівень професіоналізму та спеціалізації у своїх діях. Важливо розуміти, що стоїть за цими атаками, які мотиви спонукають кіберзлочинців до вчинення незаконних дій у кіберпросторі. Мотивація може бути різною, від фінансової вигоди та політичних мотивів до простої бажання завдати шкоду.

Дослідження мотивації при здійсненні хакерських атак є ключовим завданням для розробників заходів з кібербезпеки, правоохоронних органів та організацій, що працюють у цій галузі. Розуміння мотивації допоможе покращити заходи захисту, вчасно розпізнавати та відповідати на загрози, а також ефективно взаємодіяти з іншими галузями наукових та практичних досліджень. Актуальність цієї теми обумовлена різким зростанням кіберзлочинності та її впливом на сучасне суспільство, економіку та політику.

Дослідження мотивації хакерів та використання «алмазної моделі» може мати важливий вплив на різні сфери життя [2–7]:

– кібербезпека. Розуміння мотивації хакерів допомагає розробити більш ефективні стратегії кібербезпеки та захисту інформації [8];

– боротьба з кіберзлочинністю: здійснення аналізу мотивації може сприяти виявленню та припиненню кіберзлочинності;

– промислова безпека. Застосування алмазної моделі для аналізу мотивації може допомогти виявити загрози для промислових об’єктів та запобігти можливим атакам;

– кіберполітика. Розуміння мотивації хакерів має важливе значення для формулювання кіберполітики та міжнародних стандартів;

– приватність та захист даних. Дослідження може сприяти покращенню захисту особистих даних та приватності в інтернеті;

– економіка. Кібератаки можуть мати серйозний вплив на економіку, тому розуміння мотивації хакерів є важливим для попередження фінансових втрат [9, 10];

– суспільство та політика. Аналіз мотивації хакерів може мати вплив на громадську думку та політичні рішення щодо кібербезпеки та кіберзахисту;

– дослідження і розвиток. Збільшення розуміння мотивації хакерів сприяє розвитку нових методів та технологій для протидії кіберзагрозам;

– глобальна безпека. Забезпечення кібербезпеки є однією з глобальних проблем, і дослідження мотивації хакерів важливе для забезпечення стабільності та безпеки у світі;

– освіта та навчання. Розуміння мотивації хакерів може бути використане для розвитку освітніх програм та навчання про кібербезпеку та кіберзахист [11–21].

Усі ці сфери життя відчувають вплив кіберзагроз, і дослідження мотивації хакерів є ключовим для подолання цих викликів та покращення загального рівня кібербезпеки.

Метою даного дослідження є всебічно дослідити та зрозуміти «алмазну модель» та перевірити, чи покращує її використання захист програм від потенційних кібератак.

До досягнення визначеної мети були поставлені наступні завдання:

- проаналізувати існуючи літературні джерела, в яких описана «алмазна модель» та методи аналізу кібератак, в яких вона використовується;
- проаналізувати методи збору даних, які використовуються при застосуванні «алмазної моделі»;
- розробити комп’ютерну модель, яка передбачає хакерську атаку, без використання «алмазної моделі»;
- розробити комп’ютерну модель, яка передбачає хакерську атаку, з використанням «алмазної моделі»;
- порівняти якість комп’ютерних моделей з використанням «алмазної моделі» та без її використання.

Об’єктом дослідження роботи є методи протидії хакерським кібератакам, а предметом дослідження — ефективність використання «алмазної моделі» для прогнозування хакерської кібератаки.

Наукова новизна отриманих результатів полягає у тому, що ця робота дозволяє оцінити ефективність використання «алмазної моделі» у застосунках протидії кібератакам, чого не було зроблено в інших дослідженнях.

Таким чином, отримані результати мають безпосереднє практичне значення при використанні їх для створення застосунків, які спрямовані на протидію хакерським кібератакам, тому що допомагають підвищити якість таких систем.

1 ОГЛЯД ОСНОВНИХ МЕТОДІВ «АЛМАЗНОЇ МОДЕЛІ» ЩОДО ВРАХУВАННЯ ВИЗНАЧЕННЯ ЗВ’ЯЗКУ МІЖ МОТИВАЦІЄЮ ПРИ ЗДІЙСНЕННІ ХАКЕРОМ КІБЕРАТАКИ

1.1 Основні тези дослідження «алмазної моделі»

Кібератаки можуть мати широкий спектр наслідків, оскільки їхні впливи можуть виявлятися в різних сферах, включаючи технічні, економічні та соціальні аспекти. Ось кілька ключових проблем і наслідків, які можуть виникнути внаслідок кібератак:

– втрата конфіденційності: кібератаки можуть призвести до витоку конфіденційної інформації, такої як особисті дані користувачів, фінансові документи, або бізнес-таємниці;

– пошкодження репутації: успішні кібератаки можуть порушити репутацію організацій або навіть держав. Публічне виявлення недостатньої кібербезпеки може призвести до втрати довіри;

– втрата доступу до ресурсів: атаки можуть вплинути на доступність інформації або послуг, що може суттєво вплинути на продуктивність та функціонування організацій;

– економічні збитки: кібератаки призводять до великих економічних збитків через витрати на відновлення, втрату прибутку та погіршення інвестицій;

– загроза національній безпеці: спрямовані кібератаки можуть бути засобом гібридної війни, загрожуючи національній безпеці.

Від куди надходить кіберзагроза:

– кіберзлочинці: злочинці та кібергрупи можуть атакувати з метою виправдання фінансових вигід або просто задля власної задоволеності;

– кібершпигуни: держави часто використовують кібершпигунство для отримання конфіденційної інформації з інших країн;

– хактивісти: групи або окремі особи можуть вчиняти атаки як форму протесту або вираження певних політичних переконань;

– інсайдери: зловживання доступом внутрішніх осіб організації може призвести до витоку конфіденційної інформації.

Втрати від атак у різних сферах:

– бізнес: великі економічні втрати, втрата клієнтів і репутації;

– охорона здоров’я: загроза для життя пацієнтів через атаки на медичні системи;

– фінанси: витрати на відновлення та компенсації клієнтам;

– енергетика: загроза для енергетичних систем і можливість відключення;

– виробництво: зупинка виробництва та втрати через атаки на індустріальні системи;

– громадська безпека: загроза для критичних інфраструктурних систем.

Зрозуміння цих аспектів дозволяє розробляти ефективні стратегії кібербезпеки та попереджати можливі наслідки кібератак.

За результатами дослідження «алмазної моделі» щодо врахування визначення зв’язку між мотивацією при здійсненні хакером кібератаки були виділені основні тези [12, 14]:

– мотивація визначає характер атаки: дослідження підтверджує, що мотивація хакера має важливий вплив на характеристики та методи кібератаки. Різні мотивації призводять до різних цілей та стратегій атаки;

– модель машинного навчання ефективно передбачає атаку: розроблена модель машинного навчання, в даному випадку «Випадковий ліс», яка демонструє високу точність у передбаченні хакерскої атаки використовуючи алмазну модель;

– застосунок для кібербезпеки: результати дослідження вказують на важливість врахування мотивації при аналізі кібератак для покращення систем кібербезпеки та передбачення потенційних загроз;

– спрямованість на майбутнє дослідження: дослідження відкриває шлях для подальших досліджень, включаючи розширення моделей для врахування більш широкого спектру мотивацій та розгляду аспектів етики та правових аспектів у цій області;

– значення аналізу мотивації: аналіз мотивації хакера є важливим елементом в сфері кібербезпеки, оскільки дозволяє краще розуміти та передбачати дії зловмисників та реагувати на них з більшою ефективністю;

– співпраця з іншими галузями: дослідження вказує на необхідність співпраці з експертами з психології, кримінальної поведінки та інших галузей для більш глибокого розуміння мотивації хакера;

– можливість покращення кібербезпеки: врахування мотивації при розробці стратегій захисту може допомогти підвищити рівень кібербезпеки і захистити інформаційні активи від кіберзагроз.

Ці тези підкреслюють важливість та потенціал стратегій захисту щодо врахування визначення зв’язку між мотивацією при здійсненні хакером кібератаки.

Головною метою є створення комплексного методу, який дозволить аналізувати та розуміти мотивацію, що підштовхує кіберзлочинців до вчинення атак у кіберпросторі.

Напрямок дослідження методів формування моделі спрямовані на вивчення та аналіз сучасних методів у галузі врахування визначення зв’язку між мотивацією при здійсненні хакером кібератаки.

Дослідження базується на інтеграції різних підходів та методів. Цей інтердисциплінарний підхід дозволяє створити комплексну та досить точну модель мотивації хакерів, що є важливим для розробки ефективних заходів з кібербезпеки та протидії кібератакам.

1.2 Основні методи дослідження «алмазної моделі»

«Алмазна модель» — це структура, яка використовується в кібербезпеці для розуміння й аналізу кіберзагроз і атак. Вона зосереджена на чотирьох ключових компонентах: супротивник, інфраструктура, можливості та жертва. Коли справа доходить до дослідження мотивації хакерів, які здійснюють кібератаки в рамках цієї системи, використовуються комбінації методів, щоб отримати уявлення про їхню мотивацію. Ось декілька методів дослідження та підходів, які розглянути у кваліфікаційній роботі:

– Open Source Intelligence (OSINT). Збирає загальнодоступну інформацію з вебсайтів, соціальних мереж, форумів та інших онлайн-джерел, щоб зрозуміти мотивацію відомих суб’єктів загрози. Проаналізуйте їх онлайн-діяльність, комунікацію та приналежність;

– аналіз Dark Web. Досліджує темну мережу та підпільні форуми, щоб зібрати інформацію про мотиви, тактику, методи та процедури кіберзлочинців (TTP). Це може дати цінну інформацію про кримінальне підпілля;

– аналіз поведінки. Вивчає поведінку суб’єктів загрози та аналізує шаблони їхніх минулих атак. Шукає підказки в їхніх діях, наприклад вибір цілей, методи атаки та викрадання даних;

– психологічне профілювання. Співпрацює з психологами або експертами з поведінки для розробки профілів суб’єктів загрози на основі наявних даних. Це може включати аналіз мови, стилю спілкування та психологічних рис, які виявляють у своїй діяльності в Інтернеті;

– інтерв’ю та опитування. Проводить інтерв’ю чи опитування з особами, які мають внутрішні знання про хакерські спільноти або були залучені до кіберзлочинної діяльності. Це може надати інформацію про мотивацію з перших вуст;

– приклади. Детально вивчає конкретні кібератаки та учасників загроз, щоб зрозуміти їхню мотивацію. Аналізує цілі, час і методи, які використовуються в цих атаках;

– статистичний аналіз. Збирає та аналізує дані про кібератаки, включаючи такі атрибути, як тип атаки, цільові галузі та географічне розташування. Статистичні методи можуть допомогти визначити тенденції та кореляції, пов’язані з мотиваціями;

– аналіз вмісту. Аналізує письмові матеріали, такі як записки про викуп чи маніфести хакерів, залишені суб’єктами загрози під час або після кібератак. Це може пролити світло на їхні мотиви та цілі;

– машинне навчання та обробка природної мови (NLP). Використовує методи машинного навчання та НЛП для аналізу великих обсягів текстових даних із різних джерел, таких як соціальні медіа, щоб виявити моделі та настрої, пов’язані з мотивацією хакера;

– співпраця з правоохоронними органами. Співпрацює з правоохоронними органами, де це можливо, для збору розвідувальних даних про суб’єктів загрози та їхні мотиви. Правоохоронні органи можуть мати доступ до секретної інформації та досвід у цій сфері;

– етнографічні дослідження. занурює дослідників у культуру хакерів, фізично або через онлайн-взаємодії, щоб отримати глибоке розуміння їхніх мотивацій, цінностей і переконань;

– етичне хакерство та Red Teaming. Проводить етичні хакерські вправи та об’єднує в червону команду для імітації кібератак. Аналізує мотиви та прийоми, які використовує червона команда, щоб зрозуміти мислення кіберзловмисників;

– перехресні посилання на джерела даних. Об’єднає дані з багатьох джерел і методів для перехресних посилань і перевірки висновків про мотивацію хакера. Це може допомогти скласти більш повну картину.

1.3 Аналіз літературних джерел

У джерелах [2, 3] досліджено, як застосовується штучний інтелект у медицині. Його використання серйозно поліпшує якість діагнозів, пришвидшує процеси та зменшує вплив людського фактору.

Джерело [4] пояснює специфіку використання комп’ютерного моделювання, яке застосовується у мобільних пристроях охорони. Це допомагає значно підвищити рівень безпеки та зменшити витрати на експлуатацію системи вцілому.

Дослідження [5] застосування штучного інтелекту під час роботи з кримінальними елементами допомагає виявити закономірності поведінки злочинців і робить спробу передбачити ще не скоєні злочини.

Джерело [8] досліджує моделювання повторюваних понять у незбалансованих потоках даних, що є важливим чисельним методом, який широко застосовується у інших задачах машинного навчання.

У джерелі [11] досліджено, як проблеми інформаційної безпеки обумовлюють дослідження уразливостей, моделей кібератак, які складаються з чотирьох груп: моделі кібератак на стандартне програмне забезпечення і пропрієтарні застосунки; моделей кібератак на конфігурацію сервера, рівень виправлень сервера та моделей кібератак на мережеву інфраструктуру.

У джерелі [12] представлено моделі кібератак мережного та хостового типу, які на відміну від відомих, враховують не тільки особливості їх поведінки, але й архітектурні особливості, що дозволить створити базу поведінок атак мережного та хостового типу для їх використання в процесі виявлення атак. Запропоновані принципи складають основу для розробки моделей опису здійснення кібератак на комп’ютерні системи і діляться на класи: моделі теоретико-множинного опису кібератак; моделі теоретико-множинного опису шкідливого програмного забезпечення мережного типу; моделі теоретико-множинного опису шкідливого програмного забезпечення хостового типу.

У джерелі [13] досліджено, що в найближчому майбутньому не виключається поява нових потенційно небезпечних кібератак, що в свою чергу може призвести до погіршення їх виявлення й нейтралізації та, як наслідок, негативно вплинути на рівень захищеності інформаційних та інформаційно-телекомунікаційних систем критичної інформаційної інфраструктури. Виходячи із зазначеного у статті вирішується актуальної задачі виявлення та нейтралізації потенційно небезпечних кібератак яка зводиться до розроблення диференціально-ігрової моделі їх шаблону.

У джерелі [14] запропоновано концептуальні засади впровадження організаційно – технічної моделі кіберзахисту. Зокрема, визначені її місія, мета, призначення та цілі. Вперше визначені сили та засоби кіберзахисту. Розглянуто архітектуру організаційно-технічної моделі кіберзахисту, яка являє собою структуровану систему, яка складається з трьох інфраструктур кіберзахисту, а саме: організаційно-керуючу інфраструктуру кіберзахисту, як сукупність суб’єктів забезпечення кібербезпеки, що формують та/або реалізують державну політику у сфері кібербезпеки; технологічну інфраструктуру кіберзахисту, як сукупність сил та засобів кіберзахисту, а також інфраструктури, що забезпечує функціонування сил кіберзахисту, інформаційно-комунікаційних мереж та їх ресурсів, що використовуються в інтересах сил кіберзахисту та базисну інфраструктуру кіберзахисту, як сукупність об’єктів критичної інформаційної інфраструктури, критичних активів, комунікаційних і технологічних систем підприємств.

У джерелі [15] проаналізовано уразливості, проблеми безпеки та моделі атак, які притаманні на підприємстві. Як різновид кібератак, існують таргетовані кібератаки APT (Advanced Persistent Threat – «Розвинена стійка загроза»), які відрізняються цілеспрямованістю від масових хакерських атак - коли одночасно атакується велике число цілей. Взагалі усі види кібератак можна класифікувати за чотирма групами відповідно до мережевої інфраструктури, рівня виправлень, конфігурації сервера і стандартного програмного забезпечення.

Джерело [16] присвячена вирішенню науково-прикладної проблеми, що полягає у створенні комплексної методології розробки широкодоступних ефективних нейромережевих засобів оцінки параметрів безпеки Інтернет-орієнтованих інформаційних систем, які за рахунок теоретично обґрунтованого вибору характеристик, дозволяють оперативно розпізнавати нові види кібератак при обмежених обчислювальних ресурсах та варіативності умов застосування. На основі створеної методології побудовано нейромережеву систему оцінки параметрів безпеки, яка в порівнянні з аналогами дозволяє зменшити похибку класифікації, верифікувати отримані результати і забезпечити оперативну адаптацію до умов застосування та нових типів кібератак. З використанням запропонованих рішень розроблено засоби розпізнавання шкідливого програмного забезпечення, спаму, витоків текстової інформації та мережевих кібератак.

У джерелах [16, 17] досліджено стратегічні пріоритети системи інформаційної безпеки підприємства, що залучає фріланс-ресурс, а також досліджено систему кібербезпеки підприємства у контексті аналізу кіберризику підприємства з детермінацією його послідовних етапів. Доведено, що сучасний підхід ризик-менеджменту підприємства складається з наступних послідовних етапів: передбачення кількості можливих кібератак, проведення статистично-аналітичної оцінки кібератак, здійснення вчасної ідентифікації, здійснення розробки плану дій та превентивних заходів щодо усунення ідентичних кібератак, реалізація системи контролю та внесення модернізованих підходів аудиту кібератак на підприємстві.

У джерелі [18] проаналізовано проблемі удосконалення якості транспортно-логістичних процесів на основі розвитку процесного підходу в діяльності організації та застосування методів для статистичного управління якістю процесів. Сформовано двофазну модель для обґрунтування ефективних заходів управління якістю транспортно-логістичних процесів підприємства.

Джерело [19] досліджує особливість сучасних технологій роботи з великими даними є відсутність усталеної математичної теорії, що визначає процедури пошуку і оброблення інформації і через це розробники пропонують на ринку програмні продукти, які мають велику кількість уразливостей. Це дозволяє зловмисникам будувати складні алгоритми атак, що можуть досягати своєї мети різними способами, в залежності від ситуації в кіберпросторі.

У джерелі [20] викрито можливість нової кібератаки на робочі станції керування технологічними установками промислових процесів. Сенс кібератаки полягає в тому, що по мережі, яка зв’язує технологічні станції, робиться підміна OPC-сервера, після чого технологічна установка зловмисником переводиться в аварійний стан таким чином, щоб оператор, спостерігаючи за технологічним процесом за допомогою SCADA-системи не міг помітити розбалансування процесу.

У джерелах [21–27] обговорюється основні операційні процедури аналізу за допомогою машинного навчання, підсумовується останні застосування алгоритмів машинного навчання в кількох зрілих галузях та обговорюється вдосконалення, необхідні для широкого застосування.

Джерела [28–35] надають опис технології прийняття рішень в інформаційних системах, методи інтелектуального аналізу та оброблення даних, аналіз багатовимірних даних. Розглядаються особливості та перспективи використання інструментів штучного інтелекту (ШІ) в галузі письмового перекладу та навчанні перекладу у закладах вищої освіти (ЗВО) України. Відповідно до результатів наукових розвідок світових та українських дослідників застосування ШІ в перекладацькій діяльності ще не набуло значного поширення, не зважаючи на стрімкий розвиток цього інструменту за останні 10 років. Окрім того, актуальним залишається питання підвищення технічної компетентності українських перекладачів.

У джерелах [37–43] розкрито цілі та завдання злочинних посягань хакерів з використанням шпигунського та шкідливого програмного

забезпечення. Деталізовано особливості кібератак, які проводять хакери та кіберзлочинці. Висвітлено технічний аспект виявлення, блокування та протидії масштабному застосуванню шпигунського та шкідливого програмного забезпечення у мережах в умовах кібервійни. Узагальнено загрози та ризики використання штучного інтелекту під час кібератак. Наведено приклади новітніх розробок щодо впровадження шпигунського та шкідливого програмного забезпечення. Висвітлено людський фактор припинення злочинної діяльності хакерів, який передбачає їх фізичне затримання, арешт зловмисників та їх кримінальне переслідування. Охарактеризовані зміст та напрями кіберсуперництва в умовах кібервійни. Визначено перспективи та надано прогноз очікуваної злочинної діяльності російських хакерів та кіберзловмисників у 2023 році. Запропоновано пріоритети щодо боротьби із наслідками поширення шкідливого та шпигунського програмного забезпечення в умовах кібервійни.

1.4 Постановка задачі дослідження

Метою роботи є всебічно дослідити та зрозуміти «алмазну модель» та перевірити, чи покращує її використання захист програм від потенційних кібератак.

До досягнення визначеної мети були поставлені наступні завдання:

– проаналізувати існуючи літературні джерела, в яких описана «алмазна модель» та методи аналізу кібератак, в яких вона використовується;

– проаналізувати методи збору даних, які використовуються при застосуванні «алмазної моделі»;

– розробити комп’ютерну модель, яка передбачає хакерську атаку, без використання «алмазної моделі»;

– розробити комп’ютерну модель, яка передбачає хакерську атаку, з використанням «алмазної моделі»;

– порівняти якість комп’ютерних моделей з використанням «алмазної моделі» та без її використання.

Об’єктом дослідження роботи є методи протидії хакерським кібератакам, а предметом дослідження – ефективність використання «алмазної моделі» для прогнозування хакерської кібератаки.

Наукова новизна отриманих результатів полягає у тому, що ця робота дозволяє оцінити ефективність використання «алмазної моделі» у застосунках протидії кібератакам, чого не було зроблено в інших дослідженнях.

Таким чином, отримані результати мають безпосереднє практичне значення при використанні їх для створення застосунків, які спрямовані на протидію хакерським кібератакам, тому що допомагають підвищити якість таких систем.

2 АЛМАЗНА МОДЕЛЬ. ДОСЛІДЖЕННЯ МЕТОДІВ.

2.1 Open Source Intelligence (OSINT)

Дослідження методу «Open Source Intelligence (OSINT)» в контексті побудови «алмазної моделі» мотивації хакерів є важливим елементом нашого дослідження. «OSINT» полягає у зборі та аналізі інформації з відкритих джерел, таких як вебсайти, соціальні медіа, форуми, блоги, інтернет-джерела новин та багато інших [21].

Метод «OSINT» може бути використаний для наступних цілей у контексті «алмазної моделі»:

– збір інформації про загрози. Однією з головних мет дослідження є визначення, які загрози існують у кіберпросторі. «OSINT» може бути використаний для моніторингу активності потенційних загроз та для збору інформації про їхні дії;

– аналіз профілів індивідів та груп. Важливо розуміти, хто стоїть за кібератаками. «OSINT» дозволяє аналізувати профілі та активність індивідів та груп у кіберпросторі;

– спостереження за змінами в мережі. За допомогою «OSINT» можна виявляти зміни в мережі, що можуть свідчити про зміну мотивації або плани кіберзлочинців;

– пошук ознак перед кібератакою. «OSINT» дозволяє шукати ознаки планування або підготовки кібератаки, такі як пошуки вразливостей, обговорення методів атак та інші;

– моніторинг ринку кіберзлочинності. Дослідження ринку кіберзлочинності через «OSINT» може надати інформацію про те, які послуги або інструменти пропонуються на чорному ринку та їхню цінову динаміку;

– виявлення трендів і патернів. Аналіз «OSINT» може допомогти виявити тренди та патерни в кіберзлочинності, що може бути корисним для прогнозування майбутніх атак.

2.2 Dark Web Analysis

Дослідження методу «Dark Web Analysis» є надзвичайно важливим, оскільки саме на підпільних ресурсах та форумах часто відбувається обговорення та обмін інформацією про кібератаки та злочинні дії в кіберпросторі. Нижче подані способи, які можуть бути застосовані для дослідження методу «Dark Web Analysis» у контексті побудови моделі мотивації хакерів [22]:

– збір інформації про кіберзлочинців. Аналіз «Dark Web» може допомогти ідентифікувати основних акторів та групи, які здійснюють кібератаки. Це дозволяє дізнатися, хто саме здійснює ці атаки і які їхні мотиваційні фактори;

– моніторинг обговорень та планування. На підпільних форумах часто обговорюються плани та підготовка кібератак. «Dark Web Analysis» може виявити такі обговорення та надати інформацію про можливі мотиваційні фактори за ними;

– збір статистичних даних. «Dark Web» може бути джерелом статистичних даних про типи атак, їхню частоту, мети та інші параметри. Ця інформація може бути використана для аналізу мотиваційних тенденцій;

– вивчення інструментів та ресурсів. Аналіз «Dark Web» дозволяє вивчати інструменти та ресурси, що пропонуються для проведення кібератак. Це може вказувати на мотиваційні фактори, такі як фінансова вигода або політичні мотиви;

– вивчення психологічних аспектів. Аналіз обговорень на підпільних форумах може розкрити психологічні аспекти мотивації кіберзлочинців, такі як задоволення від ризику, анонімність, або бажання завдати шкоду;

– спостереження за трендами та новими загрозами. Вивчення «Dark Web» дозволяє бути в курсі нових трендів та еволюції загроз у кіберпросторі.

2.3 Behavioral Analysis

Дослідження методу «Behavioral Analysis» (аналіз поведінки) у контексті побудови «алмазної моделі» мотивації хакерів є важливим елементом нашого дослідження. Цей метод дозволяє аналізувати вчинки та звички кіберзлочинців для розуміння їхньої мотивації та цілей. Нижче наведено способи, які можуть бути застосовані для дослідження методу «Behavioral Analysis» у контексті побудови моделі мотивації хакерів [23]:

– збір та аналіз історії дій. Аналіз історії дій кіберзлочинців дозволяє виявити патерни та звички у їхньому поведінці. Наприклад, чи є певні типи атак, які вони виконують регулярно, і які об’єкти вони обирають для атак;

– профілювання та класифікація. За допомогою «Behavioral Analysis» можна профілювати кіберзлочинців на основі їхньої поведінки та класифікувати їх за різними категоріями, такими як хакери-активісти, кіберзлочинці-професіонали, або хактивісти з політичними мотивами;

– аналіз вразливостей та об’єктів атак. Шляхом аналізу поведінки можна визначити, на які типи об’єктів чи вразливостей звертають увагу кіберзлочинці. Це може вказувати на їхню мотивацію та цілі;

– моніторинг змін у поведінці. Аналіз змін у поведінці кіберзлочинців може допомогти виявити зміни у їхній мотивації або планах. Наприклад, перехід від виконання атак на фінансові установи до політично мотивованих атак;

– психологічний аналіз. Застосування психологічних методів для розуміння мотивації кіберзлочинців та їхньої особистості;

– аналіз структури та організації груп. Якщо кіберзлочинці діють у групах, то «Behavioral Analysis» може допомогти розкрити ієрархію та ролі у цих групах, що може вказувати на їхню мотивацію та цілі;

– спостереження за динамікою поведінки. Аналіз зміни поведінки кіберзлочинців з часом може виявити нові мотиваційні фактори або зміни у їхніх стратегіях.

Дослідження «Behavioral Analysis» дозволить отримати глибше розуміння мотивації хакерів та покращити «алмазну модель» для більш точного аналізу мотиваційних факторів у кіберкримінальних діях.

2.4 Psychological Profiling

Дослідження методу «Psychological Profiling» (психологічного профілювання) у контексті побудови «алмазної моделі» дозволяє розкрити психологічні аспекти мотивації кіберзлочинців та зрозуміти їхні ментальні та особистісні характеристики. Нижче наведено способи, які можуть бути застосовані для дослідження методу «Psychological Profiling» у контексті побудови моделі мотивації хакерів [24]:

– аналіз особистісних рис. За допомогою «Psychological Profiling» можна вивчати особистісні риси кіберзлочинців, такі як агресивність, нахмуреність, нахиленість до ризику, емоційна стійкість та інші фактори, які можуть впливати на їхню мотивацію;

– психологічні мотиви. Дослідження психологічних мотивів, таких як задоволення від ризику, бажання контролю, пошук визнання або задоволення від завдання шкоди, може допомогти розкрити, що стоїть за мотивацією кіберзлочинців;

– аналіз соціальної динаміки. «Psychological Profiling» може допомогти виявити, як соціальна динаміка, така як груповий тиск, впливає на мотивацію кіберзлочинців;

– профіль способів діяльності. Розкриття та аналіз способів діяльності кіберзлочинців може вказати на їхні психологічні мотиви. Наприклад, хакери, які використовують соціальну інженерію для атак, можуть мати інші мотивації, ніж ті, хто спеціалізується на викраденні даних;

– аналіз психологічного впливу. Вивчення того, які фактори психологічного впливу, такі як пропаганда, маніпуляція чи інші методи, використовуються для маніпулювання кіберзлочинцями та спонукають їх до певних дій;

– порівняльний аналіз. Порівнювати психологічні характеристики різних кіберзлочинців та груп може розкрити спільні або відмінні мотиваційні фактори;

– застосування методів психологічного профілювання. Застосування спеціалізованих методів та інструментів для аналізу психологічного профілю може допомогти отримати глибше розуміння мотивації.

2.5 Interviews and Surveys

Дослідження [25] методу «Interviews and Surveys» (інтерв’ю та опитування) у контексті побудови «алмазної моделі» мотивації хакерів надає цінну інформацію з першоджерела, яка допоможе розкрити їхні мотиваційні фактори та цілі. Нижче наведено способи, які можуть бути застосовані для дослідження методу «Interviews and Surveys» у контексті побудови моделі мотивації хакерів:

– проведення структурованих інтерв’ю. Спеціалізовані інтерв’ю з хакерами або експертами у цій області можуть допомогти виявити їхні мотивації, досвід та погляди на свою діяльність;

– опитування кіберзлочинців. За умови анонімності можна провести опитування кіберзлочинців, щоб дізнатися, що саме спонукає їх до кіберкримінальних дій та які їхні цілі;

– опитування потенційних жертв атак. Опитування компаній або інших потенційних жертв кібератак може надати інформацію про те, які типи атак їх вразливості, а також їхню перспективу на мотивацію кіберзлочинців;

– аналіз демографічних даних. Зібрані дані про демографічні характеристики кіберзлочинців (вік, стать, освіта тощо) можуть допомогти визначити зв’язок між цими характеристиками та мотивацією;

– оцінка психологічних аспектів. Питання, спрямовані на оцінку психологічних станів, таких як ступінь агресивності, емоційна стійкість та інші, можуть розкрити психологічні фактори мотивації;

– зіставлення відповідей із вчинками. Порівняння відповідей кіберзлочинців або експертів з їхніми реальними діями може допомогти зрозуміти, наскільки інформація, надана у відповідях, відповідає реальному стану справ;

– аналіз мотиваційних патернів. Інтерв’ю та опитування можуть допомогти визначити патерни та спільні мотиваційні фактори серед різних кіберзлочинців;

– кваліативний та кількісний аналіз відповідей. Комбінація кваліативного та кількісного аналізу може надати більш об’єктивну картину мотивації.

Дослідження методу «Interviews and Surveys» дозволить отримати унікальну інсайтову інформацію про мотивацію хакерів та підтвердити або вдосконалити «алмазну модель» для більш точного аналізу мотиваційних факторів у кіберкримінальних діях.

2.6 Case Studies

Дослідження методу «Case Studies» (вивчення окремих випадків) у контексті побудови «алмазної моделі» мотивації хакерів може бути дуже цінним, оскільки воно дозволяє глибоко аналізувати конкретні ситуації та історії кібератак. Нижче наведено способи, які можуть бути застосовані для дослідження методу «Case Studies» у контексті побудови моделі мотивації хакерів:

– вибір репрезентативних кейсів. Обираючи різноманітні та репрезентативні кейси кібератак, можна вивчити різні мотиваційні фактори та обставини;

– аналіз технічних аспектів. Вивчення технічних деталей атак, використаних у кейсах, може вказати на конкретні мотивації, такі як здобуток фінансової вигоди, репутаційний шкідливий вплив або інші;

– аналіз потенційних жертв та їхніх характеристик. Вивчення, кому спрямовані атаки, може допомогти зрозуміти мотивацію кіберзлочинців. Наприклад, атаки на фінансові установи можуть бути мотивовані фінансовим здобутком;

– аналіз наслідків та цілей атак. Вивчення наслідків атак та досягнених цілей може розкрити мотиваційні фактори. Наприклад, атака, яка призвела до втрати важливих даних, може мати мотивацію в шантажі або відновленні даних;

– аналіз способів виконання атак. Розгляд використаних методів та інструментів може вказати на технічні знання та мотивацію кіберзлочинців;

– оцінка впливу та реакції на атаку. Аналіз впливу атаки на потерпілих і їхню реакцію може допомогти зрозуміти, які мотиваційні фактори відіграли роль у вчинку кіберзлочинців;

– порівняльний аналіз кейсів. Порівнювати різні кейси може допомогти виявити спільні мотиваційні фактори та визначити патерни;

– виявлення трендів та еволюції атак. Аналіз кейсів на різних етапах розвитку кіберзлочинності може допомогти виявити зміни в мотиваційних факторах та методах атак.

Дослідження методу «Case Studies» дозволить отримати глибше розуміння мотивації кіберзлочинців на основі конкретних випадків та допоможе покращити «алмазну модель» для аналізу мотиваційних факторів у кіберкримінальних діях.

2.7 Statistical Analysis

Дослідження методу «Statistical Analysis» (статистичний аналіз) у контексті побудови «алмазної моделі» мотивації хакерів може надати об’єктивну та кількісну інформацію про зв’язок між різними факторами та мотивацією. Нижче наведено переваги та недоліки використання статистичного аналізу в цьому контексті [26].

Переваги статистичного аналізу:

– об’єктивність. Статистичний аналіз базується на об’єктивних даних, що дозволяє уникнути суб’єктивного впливу дослідника;

– кількісні дані. Статистичний аналіз дозволяє обробляти кількісні дані, такі як статистика атак, демографічні характеристики кіберзлочинців, обсяги збитків і т. д.;

– виявлення кореляцій. Аналіз даних може розкрити кореляції між різними факторами та мотивацією, що допомагає встановити зв’язки;

– тренди і патерни. Статистичний аналіз дозволяє виявляти тренди та патерни в злочинності та мотивації кіберзлочинців на основі історичних даних;

– моделювання. За допомогою статистичного моделювання можна розробити прогнози щодо мотивації та поведінки кіберзлочинців.

Недоліки статистичного аналізу:

– спрощення реальності. Статистичний аналіз може спрощувати складну реальність, ігноруючи багато важливих факторів;

– кореляція не означає причинно-наслідковий зв’язок. Виявлення кореляції між факторами та мотивацією не означає автоматично наявність причинно-наслідкового зв’язку;

– неспроможність врахувати контекст. Статистичний аналіз може не враховувати контекстуальні особливості окремих ситуацій;

– залежність від якості даних. Результати статистичного аналізу залежать від якості та достовірності вхідних даних;

– потребує великої кількості даних. Для проведення статистичного аналізу може знадобитися велика кількість даних, особливо для дослідження рідкісних подій.

Загалом, статистичний аналіз може бути корисним інструментом у дослідженні мотивації кіберзлочинців, але він повинен використовуватися разом з іншими методами та з урахуванням їхніх переваг та обмежень для отримання більш повного розуміння даної проблеми.

2.8 Content Analysis

Метод «Content Analysis» (аналіз вмісту) може бути важливим інструментом для вивчення текстової інформації, такої як текстові повідомлення, статті, форуми та інше. Нижче наведено переваги та недоліки використання методу «Content Analysis».

Переваги методу Content Analysis:

– аналіз тексту. Метод «Content Analysis» дозволяє аналізувати текстову інформацію, що може включати в себе заяви, заголовки, коментарі та інше, для виявлення вказівок на мотивацію;

– знаходження ключових слів і фраз. Вибірковий аналіз тексту може виявити ключові слова і фрази, пов’язані з мотивацією, такі як «фінансовий злочин», «ідеологічний мотив» тощо;

– визначення тем і тематичних груп. Content Analysis може допомогти визначити загальні теми та тематичні групи, пов’язані з кібератаками та мотивацією;

– моніторинг змін в часі. Аналіз текстової інформації дозволяє відслідковувати зміни в мотивації та поведінці кіберзлочинців з плином часу.

Недоліки методу Content Analysis:

– суб’єктивність інтерпретації. Аналіз тексту може бути суб’єктивним і залежить від інтерпретації дослідника. Різні дослідники можуть приходити до різних висновків;

– не всі дані є доступними. Деяка текстова інформація може бути недоступною або зашифрованою, що обмежує можливості аналізу;

– часова та ресурсна інтенсивність. Аналіз великих обсягів тексту вимагає багато часу та ресурсів;

– обмеженість на наявних даних. Метод «Content Analysis» обмежений наявністю текстових даних і не може застосовуватися до інших видів інформації, таких як аудіо чи відео;

– використання великої вибірки. Для надійних результатів потрібна велика вибірка текстової інформації.

Усупереч недолікам, метод «Content Analysis» може допомогти зрозуміти, які теми та тематичні групи пов’язані з мотивацією кіберзлочинців, і виявити ключові слова та фрази, які можуть вказувати на мотиваційні фактори. При правильному використанні цей метод може бути корисним доповненням до інших аналітичних підходів у дослідженні мотивації кіберзлочинців.

2.9 Machine Learning and Natural Language Processing (NLP)

Метод «Machine Learning and Natural Language Processing (NLP)» (машинне навчання та обробка природної мови) є важливим, оскільки цей підхід дозволяє аналізувати великі обсяги текстової інформації та автоматично виявляти зв’язки та закономірності. Нижче наведено переваги та недоліки використання методу «Machine Learning and NLP» [27, 28].

Переваги методу Machine Learning та NLP:

– автоматизація. Машинне навчання та NLP дозволяють автоматизувати аналіз великих обсягів текстової інформації, що зекономлює час та ресурси;

– виявлення патернів. Моделі машинного навчання можуть виявляти складні патерни та зв’язки у тексті, які можуть залишитися непоміченими для людини;

– аналіз сентименту. За допомогою NLP можна визначити сентимент текстів, що допомагає розуміти настрій та емоції авторів;

– класифікація текстів. Машинне навчання дозволяє класифікувати текстову інформацію за категоріями, що спрощує обробку та аналіз;

– прогнозування поведінки. Моделі машинного навчання можуть використовуватися для прогнозування майбутньої поведінки кіберзлочинців на основі їхнього текстового сліду в мережі.

Недоліки методу Machine Learning та NLP:

– потребує великої кількості даних. Моделі машинного навчання вимагають великої кількості позитивних та негативних прикладів для навчання, що може бути складним у випадку рідкісних подій;

– потребує експертного знання. Використання машинного навчання та NLP вимагає експертного знання в області обробки природної мови та вибору відповідних функцій для аналізу;

– залежність від якості даних. Результати аналізу залежать від якості вхідних даних, а нечистоти або некоректність можуть призвести до неточностей;

– інтерпретація результатів. Деякі моделі машинного навчання можуть бути чорними ящиками, і їхні рішення можуть бути складно зрозуміти;

– конфіденційність інформації. Аналіз текстів може порушувати конфіденційність особистої інформації авторів.

Враховуючи ці переваги та недоліки, метод «Machine Learning and NLP» може бути потужним інструментом для дослідження мотивації кіберзлочинців, але вимагає обережного підходу та співпраці з фахівцями у галузі для досягнення найкращих результатів.

2.10 Collaboration with Law Enforcement

Дослідження методу «Collaboration with Law Enforcement» (співпраця з правоохоронними органами) у контексті побудови «алмазної моделі» мотивації хакерів є важливим, оскільки цей підхід передбачає співпрацю з офіційними структурами для отримання інформації та ресурсів. Нижче наведено переваги та недоліки використання методу «Collaboration with Law Enforcement» [29].

Переваги методу Collaboration with Law Enforcement:

– доступ до ресурсів та інформації. Співпраця з правоохоронними органами може надати доступ до спеціалізованих ресурсів та інформації, яка може бути недоступною публічно;

– законність та легітимність. Робота з правоохоронними органами гарантує законність та легітимність отриманих даних та інформації;

– експертна підтримка. Спеціалісти правоохоронних органів можуть надати експертну підтримку у проведенні досліджень та аналізі мотивації кіберзлочинців;

– можливість взаємодії з іншими дослідниками. Співпраця з правоохоронними органами може включати взаємодію з іншими дослідниками та експертами у галузі кібербезпеки.

Недоліки методу Collaboration with Law Enforcement:

– конфіденційність даних. Робота з правоохоронними органами може потенційно порушити конфіденційність особистих даних індивідів;

– обмеженість в доступі. Співпраця з правоохоронними органами може обмежувати доступ до певних джерел інформації та даних;

– інтереси та обмеження правоохоронців. Правоохоронні органи можуть мати свої власні інтереси та обмеження, які можуть вплинути на хід дослідження;

– часовий фактор. Співпраця з правоохоронними органами може займати багато часу і вимагати великих зусиль;

– етичні питання. Існують етичні питання, пов’язані зі співпрацею з правоохоронними органами, особливо коли йдеться про роботу з конфіденційною інформацією.

Співпраця з правоохоронними органами може бути корисною у дослідженні мотивації хакерів, але вимагає обережного врахування переваг та недоліків, а також дотримання законодавства та етичних стандартів у процесі роботи.

2.11 Ethnographic Research

Метод [30] «Ethnographic Research» (етнографічні дослідження) у контексті побудови «алмазної моделі» мотивації хакерів може бути цікавим інструментом для розуміння соціокультурних та психологічних аспектів

кібератак. Нижче наведено переваги та недоліки використання методу «Ethnographic Research».

Переваги методу Ethnographic Research:

– глибоке розуміння контексту. Етнографічні дослідження дозволяють дослідникам глибше розуміти соціокультурний та організаційний контекст, у якому діють хакери;

– спостереження в реальному часі. Дослідження проводяться в реальному часі, що дозволяє отримувати актуальну інформацію про поведінку та мотивацію хакерів;

– участь у спільнотах. Дослідники можуть взяти участь у кіберспільнотах та спілкуватися з хакерами, що дозволяє збирати інформацію з перших вуст;

– подолання зміщення спостерігача. Етнографічні дослідження допомагають подолати зміщення спостерігача, оскільки дослідники стають частиною досліджуваного середовища.

Недоліки методу Ethnographic Research:

– часово- і ресурсозатратність. Етнографічні дослідження можуть бути дуже часо та ресурсозатратними, оскільки вони вимагають тривалого перебування в специфічних середовищах;

– обмежена репрезентативність. Зібрана інформація може бути обмеженою в репрезентативності, оскільки дослідникам доступно обмежене коло хакерів;

– етичні питання. Взаємодія з кіберзлочинцями може порушувати етичні норми та правила законодавства;

– суб’єктивність спостережень. Результати етнографічних досліджень можуть бути суб’єктивними і залежати від інтерпретації дослідника;

– ризик безпеки. Робота з хакерами може створювати ризик для безпеки дослідника та його даних.

Ураховуючи ці переваги та недоліки, етнографічні дослідження можуть бути корисним доповненням до інших методів дослідження мотивації

хакерів. Вони дозволяють отримати глибше розуміння соціокультурних та психологічних аспектів, але вимагають обережного планування та уважної уваги до етичних та безпекових аспектів.

2.12 Ethical Hacking and Red Teaming

Метод «Ethical Hacking and Red Teaming» (етичне хакерство та Red Teaming) у контексті побудови «алмазної моделі» мотивації хакерів може бути корисним, оскільки цей метод передбачає активну імітацію атак та виявлення слабких місць у системах безпеки. Нижче наведено переваги та недоліки використання методу «Ethical Hacking and Red Teaming» [31].

Переваги методу Ethical Hacking and Red Teaming:

– пошук вразливостей. Цей метод дозволяє ідентифікувати потенційні вразливості в інформаційних системах та застосунках шляхом активних тестів;

– підвищення рівня безпеки. Результати етичного хакерства і Red Teaming можуть бути використані для підвищення рівня безпеки та усунення ідентифікованих проблем;

– реалістичність атак. Даний метод дозволяє відтворювати реалістичні сценарії атак, що допомагає зрозуміти, яким чином хакери можуть діяти;

– оцінка захищеності. Етичне хакерство та Red Teaming дозволяють проводити оцінку загальної захищеності системи.

Недоліки методу Ethical Hacking and Red Teaming:

– вартість і складність. Цей метод може бути дорогим та складним у реалізації, оскільки вимагає висококваліфікованих спеціалістів та спеціалізованого обладнання;

– потенційні ризики. Проведення етичного хакерства може мати непередбачувані наслідки, які можуть вплинути на роботу інформаційних систем;

– легітимність та правові аспекти. Проведення тестів на проникнення може суперечити законодавству та стандартам безпеки, і тому вимагає відповідних легітимних дозволів;

– обмежена спроможність виявлення всіх загроз. Навіть після проведення тестів на проникнення, можуть залишитися приховані вразливості, які не були виявлені;

– потенційна дестабілізація системи. Використання цього методу може викликати дестабілізацію інформаційної системи або мережі.

Ураховуючи ці переваги та недоліки, етичне хакерство та Red Teaming можуть бути ефективними інструментами для оцінки та підвищення рівня кібербезпеки, але вимагають обережного планування, дотримання правових аспектів і великої уваги до безпеки та етики під час виконання.

2.13 Cross-Referencing Data Sources

Метод «Cross-Referencing Data Sources» (перехресне посилання на джерела даних) у контексті побудови «алмазної моделі» мотивації хакерів може бути корисним для збору та аналізу інформації з різних джерел. Нижче наведено переваги та недоліки використання цього методу [18–20].

Переваги методу Cross-Referencing Data Sources:

– підвищена достовірність. Перехресне посилання на джерела даних дозволяє перевірити і підтвердити інформацію з різних джерел, що сприяє підвищенню її достовірності;

– збільшена повнота даних. Цей метод дозволяє отримати більше повної інформації, оскільки дані можуть бути зібрані з різних джерел;

– виявлення зв’язків. Перехресне посилання на джерела даних дозволяє виявляти зв’язки та патерни між різними елементами інформації;

– підвищення точності аналізу. Цей метод допомагає підвищити точність аналізу даних завдяки перевірці та узгодженню інформації з різних джерел;

Недоліки методу Cross-Referencing Data Sources:

– спрощена аналітика. Збільшення обсягу даних може призвести до ускладнення аналізу та ускладнення виявлення істотних патернів;

– запити до джерел даних. Здійснення запитів до різних джерел даних може бути часо- та ресурсозатратним процесом;

– приватність і безпека. Збільшення доступу до даних з різних джерел може порушувати питання приватності та безпеки;

– недоступність даних. У деяких випадках може виявитися, що не всі дані доступні для перехресного посилання або їх неможливо підтвердити.

Ураховуючи ці переваги та недоліки, перехресне посилання на джерела даних може бути корисним методом для побудови «алмазної моделі» мотивації хакерів, але вимагає уважного планування, аналізу та обережного використання для досягнення найкращих результатів.

2.14 Переваги та недоліки розглянутих методів

Нейронні мережі та глибоке навчання в сфері кібербезпеки мають свої досягнення:

– виявлення загроз: нейронні мережі здатні аналізувати величезний обсяг даних для виявлення аномалій та ідентифікації підозрілих активностей, що полегшує виявлення кіберзагроз;

– прогнозування вразливостей: глибоке навчання дозволяє створювати моделі, які можуть прогнозувати можливі вразливості та слабкі місця в кіберзахисті;

– автоматизація відгуку на інциденти: системи на базі глибокого навчання дозволяють автоматизувати виявлення та реагування на кіберінциденти, прискорюючи процес реагування на загрози;

– розпізнавання образів: нейронні мережі успішно використовуються для розпізнавання образів та ідентифікації зловмисного програмного забезпечення на основі виявлених сигнатур.

Недоліки:

– необхідність великої кількості даних: глибоке навчання ефективне лише при наявності великої кількості навчальних даних, що може бути обмеженням в кібербезпеці, де дані можуть бути обмежені або цінні;

– вразливість до атак: моделі глибокого навчання можуть бути піддані атакам, таким як атаки з введенням або атаки на перенавчання, що створює ризик для точності результатів;

– висока вимогливість до обчислювальних ресурсів: нейронні мережі, особливо глибокі, вимагають значних обчислювальних ресурсів, що може бути високою вартістю для організацій;

– труднощі інтерпретації результатів: глибокі моделі навчання є чорним ящиком, і їхні рішення можуть бути важко інтерпретувати, що ускладнює розуміння причин кібератак;

– нестабільність: глибоке навчання може бути чутливим до шуму в даних, що може впливати на стабільність та надійність моделей.

Загалом, нейронні мережі та глибоке навчання є потужними інструментами в сфері кібербезпеки, але їхній успіх залежить від правильного використання та усунення недоліків.

Коротко, позитивні і негативні моменти даних методів вказані в таблиці 2.1.

Таблиця 2.1 Позитивні і негативні моменти методів

Метод	**Позитив**	**Негатив**
1	**2**	**3**
Open Source Intelligence (OSINT)	- Доступність і відкритість даних - Швидкість і ефективність - Попередження кібератак	- Обмеженість джерел - Неспецифічність даних - Небезпека неправильного розуміння
Аналіз Dark Web	- Доступ до конфіденційної інформації - Виявлення потенційних загроз - Додатковий контекст	- Ілегальність та етика - Ризик безпеки - Обмежений доступ
Аналіз поведінки	- Дієва інформація - Виявлення відхилень - Засіб раннього попередження	- Приватність та права - Ложнопозитиви - Обмеженість інформації - Потенційна недостатня точність
Психологічне профілювання	- Глибше розуміння мотивації - Передбачення дій - Раннє виявлення загроз - Персоналізований підхід	- Етичні питання - Недостатня точність - Важкість отримання даних - Ризик стереотипів
Інтерв’ю та опитування	- Прямий доступ до інформації - Виявлення внутрішніх мотивів - Додатковий контекст для аналізу	- Достовірність інформації - Важкість доступу до хакерів - Можливий ризик - Обмежена об’єктивність

Продовження таблиці 2.1

1	2	3
Приклади	- Конкретність і ілюстрація - Навчання та усвідомлення - Підтвердження гіпотез - Різноманітність сценаріїв	- Обмеженість універсальності - Неоднозначність та інтерпретація - Відсутність повної інформації - Залежність від джерел
Статистичний аналіз	- Об’єктивність - Глибинне розуміння - Підтвердження гіпотез - Корисна інформація для прийняття рішень	- Обмежена точність - Залежність від якості даних - Непередбачуваність людського фактору
Аналіз вмісту	- Збільшення обсягу даних - Виявлення глибинних зв’язків - Різноманітність джерел інформації	- Необхідність обробки великих обсягів інформації - Можливість неточностей - Необхідність експертної інтерпретації
Машинне навчання та обробка природної мови (NLP)	- Автоматизація аналізу - Пошук ключових слів - Виявлення відхилень і аномалій - Аналіз в реальному часі	- Необхідність великої кількості даних - Обмеження мовних моделей - Проблеми з конфіденційністю даних

Продовження таблиці 2.1

1	2	3
Співпраця з правоохоронними органами	- Доступ до ресурсів і повноважень - Правовий аспект - Кримінальне переслідування - Спільна робота з іншими організаціями	- Питання конфіденційності даних - Часові обмеження - Складність ідентифікації злочинців
Етнографічні дослідження	- Глибоке розуміння мотивації - Контекстуальний підхід - Інсайти для заходів з кібербезпеки - Індивідуалізація підходу	- Час та витрати - Ризик безпеки - Суб’єктивність досліджень
Етичне хакерство та Red Teaming	- Виявлення слабких місць - Тестування кібербезпеки - Симуляція кібератак - Попередження інцидентів	- Витрати на ресурси - Ризик помилок - Можливість незаконного доступу -Обмежена покриття загроз
Перехресні посилання на джерела даних	- Збагачення даними - Підтвердження інформації - Ширший аналіз - Розкриття нових зв’язків	- Час та зусилля - Неоднорідність даних - Питання конфіденційності - Спеціалізована експертиза

Усі ці аспекти підкреслюють важливість дбайливого та обачного підходу до збору та підготовки даних для великомовних моделей для перекладу.

Дослідити мотивацію хакерів складно через таємний і часто анонімний характер діяльності кіберзлочинців. Етичні та юридичні міркування мають першочергове значення в таких дослідженнях, і співпраця з відповідними органами чи організаціями має важливе значення для забезпечення дотримання законів і етичних стандартів. Крім того, сфера досліджень кібербезпеки постійно розвивається, тому вкрай важливо бути в курсі останніх методологій і технологій.

3 КОМП’ЮТЕРНА МОДЕЛЬ ЩОДО ВРАХУВАННЯ ВИЗНАЧЕННЯ ЗВ’ЯЗКУ МІЖ МОТИВАЦІЄЮ ПРИ ЗДІЙСНЕННІ ХАКЕРОМ КІБЕРАТАКИ

3.1 Обґрунтування вибору середовища програмної реалізації

Для дослідження методів створення «алмазної моделі» мотивації хакерів та програмної реалізації цього дослідження важливо вибрати підходяще середовище програмування, яке відповідає завданням та об’єктивам дослідження. Для цього використовувалися підходи, описані у [44]. Ось обґрунтування вибору середовища програмної реалізації:

– Python як універсальна мова програмування. Python є однією з найпоширеніших та універсальних мов програмування. Він має широкий спектр бібліотек для обробки та аналізу даних, що дозволить здійснити комплексний аналіз мотивації хакерів;

– бібліотеки для машинного навчання та обробки природної мови. Python має добре розвинені бібліотеки, такі як scikit-learn, TensorFlow, та NLTK, які дозволяють виконувати аналіз текстової інформації та застосовувати методи машинного навчання;

– зручність та швидкість розробки: Python відомий своєю зручністю та швидкістю розробки завдяки чіткому синтаксису та багатофункціональності;

– велика спільнота та документація: Python має велику та активну спільноту розробників, а також багато документації та ресурсів для вивчення;

– підтримка даних форматів: Python легко обробляє різні формати даних, включаючи тексти, JSON, XML, CSV та інші;

– можливість візуалізації даних: в середовищі Python є багато бібліотек для створення графіків і візуалізації даних, що сприяє кращому розумінню результатів дослідження;

– можливість інтеграції з іншими мовами та інструментами: Python може бути легко інтегрований з іншими мовами програмування та інструментами, що розширює можливості дослідження.

Зважаючи на ці переваги, використання Python в якості середовища програмної реалізації дослідження «алмазної моделі» мотивації хакерів є обґрунтованим та ефективним вибором. Воно дозволить здійснити аналіз та моделювання мотивації хакерів з використанням широкого спектру інструментів та бібліотек, що підвищить якість та результативність дослідження.

Під час дослідження мотивації хакерів та побудови «алмазної моделі» виникли проблеми з обчислювальними ресурсами, особливо при роботі з великим обсягом даних та складними обчисленнями. Ось деякі з проблем:

– обмежені обчислювальні ресурси. Недостатні обчислювальні ресурси можуть призвести до затримок у проведенні аналізу та моделювання, що може ускладнити вчасну реакцію на кіберзагрози;

– пам’ять і зберігання даних. Обробка великого обсягу даних може вимагати великої кількості оперативної пам’яті та місця для зберігання. Недостатня пам’ять може призвести до зниження продуктивності;

– час обчислень. Деякі алгоритми та методи машинного навчання можуть бути дуже часомісткими. Недостатні обчислювальні ресурси можуть затримати дослідження;

– складність обчислень. Складність аналізу та моделювання мотивації хакерів може вимагати великої обчислювальної потужності та високошвидкісних комп’ютерів;

– обмежені можливості візуалізацією Візуалізація результатів дослідження може бути важкою без потужного обчислювального обладнання та відповідних інструментів;

– витрати на обчислювальні ресурси. Придбання та підтримка обчислювальних ресурсів може вимагати значних витрат.

Для подолання цих проблем використовуються наступні стратегії:

– хмарні обчислювальні ресурси. Використання хмарних сервісів, які дозволяють масштабувати обчислювальні ресурси в залежності від потреб дослідження;

– оптимізація алгоритмів. Вибір та оптимізація алгоритмів для оптимального використання обчислювальних ресурсів;

– використання спеціалізованих обчислювальних ресурсів. Використання графічних процесорів (GPU) або спеціалізованих обчислювальних установок для обробки даних;

– розподіл обчислень. Розподіл завдань на кілька обчислювальних вузлів або серверів для прискорення обчислень;

– моніторинг та управління ресурсами. Постійний моніторинг та управління використанням обчислювальних ресурсів для ефективного використання.

Забезпечення достатніх обчислювальних ресурсів є важливим аспектом дослідження «алмазної моделі» мотивації хакерів та допоможе досягти кращих результатів та зрозуміти цей важливий аспект кібербезпеки.

Розробка «алмазної моделі» є складним дослідницьким проєктом, який складається з кількох етапів. Нижче надано загальний огляд цих кроків разом із деякими прикладами коду Python. Слід зазначити, що це спрощена демонстрація, і створення повноцінної дослідницької системи потребуватиме більш глибокої роботи та, можливо, групи дослідників та інженерів.

У рамках кваліфікаційної роботи були розроблені такі кроки:

– збір і підготовка даних;

– «алмазна модель» поведінки хакера та кіберзагроз;

– навчання;

– оцінювання;

– тонка настройка та оптимізація;

– розгортання.

3.2 Програмна реалізація

Цей скрипт використовує бібліотеки `pandas`, `numpy`, та `scikit-learn` для оцінки ефективності класифікаційної моделі машинного навчання на основі вхідних даних. Використовуються дані з датасету Attacked [45]. Скрипт реалізований наступним чином:

– імпортується необхідні бібліотеки, такі як `pandas`, `numpy`, `os`, `train_test_split` для розділення даних на навчальні та тестові набори, `RandomForestClassifier` для побудови моделі випадкового лісу та `accuracy_score` для оцінки точності моделі.

```
import pandas as pd
import numpy as np
import os
from sklearn.model_selection import train_test_split
from sklearn.ensemble import RandomForestClassifier
from sklearn.metrics import accuracy_score
```

– визначується початкове значення `seed` для генератора випадкових чисел, щоб результати були відтворюваними.

```
seed = 879
```

– визначується функція `evaluate_model`, яка приймає навчальні та тестові дані, побудовує модель випадкового лісу, здійснює передбачення на тестових даних та обчислює точність моделі.

```
def evaluate_model(x_train, x_test, y_train, y_test):
    # Train a machine learning model
```

model = RandomForestClassifier(n_estimators=100, random_state=seed)

model.fit(x_train, y_train)

 # Make predictions on the test data

y_pred = model.predict(x_test)

 # Evaluate the model

accuracy = accuracy_score(y_test, y_pred)

return accuracy

– визначується функція `apply_diamond_model`, яка застосовує кодування одного гарячого вектора (one-hot encoding) до вхідних даних, яке зазвичай використовується для опрацювання категоріальних змінних.

def apply_diamond_model(x):

 # Apply one hot encoding

return pd.get_dummies(x, columns=['Port'])

– головна функція `main` виконує наступні дії: завантажує дані з CSV-файлу 'attack.csv'.

data_filename = os.path.dirname(os.path.realpath(__file__)) + '/../data/attack.csv'

data = pd.read_csv(data_filename)

– виконує попередню обробку даних, видаляючи рядки з відсутніми значеннями в колонці 'FlowPackets'.

data = data[np.isfinite(data['FlowPackets'])]

– розділяє дані на набори ознак (x) та міток (y).

```
# Split the data into features (x) and labels (y)
x = data.drop('attack', axis=1)
y = data['attack']
```

– розділяє дані на навчальні та тестові набори, де 80% даних використовуються для навчання та 20% для тестування.

```
# Calculate accuracy
x_train, x_test, y_train, y_test = train_test_split(x, y, test_size=0.2, random_state=seed)
general_score = evaluate_model(x_train, x_test, y_train, y_test)
```

– обчислює загальний показник точності моделі на навчальних та тестових даних, застосовує «алмазну модель» (функцію `apply_diamond_model`) до даних та обчислює точність моделі на цих даних.

```
# Calculate accuracy using diamond model
x_train, x_test, y_train, y_test = train_test_split(apply_diamond_model(x), y, test_size=0.2, random_state=seed)
diamond_model_score = evaluate_model(x_train, x_test, y_train, y_test)
```

– виводить результати точності для загальної моделі та «алмазної моделі».

```
print(f'General score:\t\t{general_score}')
print(f'Diamond model score:\t{diamond_model_score}')
```

– востаннє, код виконує головну функцію `main`, якщо файл запускається напряму (не імпортується в інший скрипт).

```
if __name__ == '__main__':
    main()
```

Важливо враховувати, що для коректної роботи цього скрипта необхідно мати відповідний CSV-файл «attack.csv» у вказаному розташуванні і встановлені всі необхідні бібліотеки (pandas, numpy, scikit-learn). Цей скрипт використовує RandomForestClassifier для побудови моделі машинного навчання і оцінки її точності з використанням тестового набору даних.

3.3 Інструкція користувача

Щоб запустити представлений застосунок, треба налаштувати середовище, встановити необхідні пакети та запустити скрипт. Для цього треба виконати наступні кроки:

```
## Вимоги
- python 3,8+

## Встановлення
> python3 -m venv venv
> source venv/bin/activate
> pip install -r requirements.txt

## Використання
> source venv/bin/activate
> python main.py
```

3.4 Тестування та аналіз розробленої моделі

Даний скрипт виконує аналіз результатів моделювання та порівнює точність двох моделей: загальної моделі та «алмазної моделі». Ось кілька ключових моментів аналізу результатів виконання цього скрипту:

– оцінка точності моделей. Скрипт використовує класифікатор «Випадкового лісу» (Random Forest) для побудови моделей на основі навчальних даних та обчислює точність цих моделей на тестових даних. Точність є показником ефективності моделі, вимірюється від 0 до 1, де 1 означає ідеальну модель;

– порівняння результатів. Скрипт порівнює точність загальної моделі (без «алмазної» обробки даних) та точність «алмазної моделі»;

– виведення результатів. Результати обчислення точності для обох моделей виводяться на екрані. Це дозволяє користувачу побачити, наскільки ефективно «алмазна модель» впливає на точність моделі;

– порівняння з попередніми результатами. Якщо точність «алмазної моделі» виявляється вищою, ніж точність загальної моделі, це може свідчити про корисність використання «алмазної» обробки даних;

Загалом, аналіз результатів цього скрипта допомагає визначити, наскільки ефективно використовувати «алмазну» обробку даних в контексті моделювання та як ця обробка може покращити точність моделі.

Після виконання скрипта отримано результати (лістинг 3.1).

Лістинг 3.1 Результати виконання скрипту:

```
General score:      0.6124260355029586
Diamond model score: 0.6260355029585799
```

У цьому прикладі, результати показують, що точність «алмазної моделі» (0,63) є вищою, ніж точність загальної моделі (0,61). Це свідчить про те, що використання «алмазної» обробки даних покращило ефективність моделі.

Аналіз результатів включає в себе наступні кроки:

– порівняння точності: перший крок - це порівняти точність двох моделей. У цьому прикладі «алмазна модель» має вищу точність, що є позитивним сигналом.

– порівняння зі стандартами: точність сама по собі може бути непрозорою. Тому важливо порівняти її зі стандартами або попередніми результатами. Якщо точність вища, ніж минулі результати, це може свідчити про поліпшення.

У наведеному прикладі, згідно з аналізом результатів, видно, що використання «алмазної» обробки даних допомагає покращити точність моделі, і це може бути корисним для подальших досліджень та застосувань в області машинного навчання та аналізу даних.

ВИСНОВКИ

У рамках кваліфікаційної роботи за результатами дослідження «алмазної моделі» щодо врахування визначення зв’язку між мотивацією при здійсненні хакером кібератаки можуть бути наступними:

– зв’язок між мотивацією і характеристиками кібератаки: дослідження підтвердило існування зв’язку між мотивацією хакера та характеристиками кібератаки. Різні типи мотивації можуть впливати на обрані цілі, методи та масштаб атаки;

– модель передбачення хакерскої атаки: розроблена модель машинного навчання (у цьому випадку «Випадковий ліс») яка може ефективно передбачати хакерску атаку на основі характеристик мережевого трафіку. Модель показала, що використання алмазної моделі покращує точність моделі;

– важливість аналізу мотивації в кібербезпеці: дослідження підкреслило важливість аналізу мотивації хакера для зрозуміння і передбачення кібератак. Розроблена модель може бути корисним інструментом для кібербезпеки та виявлення потенційно небезпечних атак;

– потенційні застосування: результати дослідження можуть бути використані в сфері кібербезпеки для покращення реагування на кібератаки, виявлення аномалій та розробки систем захисту;

– подальші дослідження: дослідження підкреслює важливість подальших досліджень у цій області, зокрема, розширення моделей для врахування більш широкого спектру мотивацій та більш складних методів передбачення.

Загалом, дослідження «алмазної моделі» в контексті врахування мотивації при здійсненні кібератаки дало цінні висновки та відкрило нові можливості для поліпшення кібербезпеки та виявлення потенційно небезпечних активностей в цій сфері [46-54].

Під результатами дослідження «алмазної моделі» щодо врахування зв’язку між мотивацією при здійсненні хакером кібератаки можна виділити декілька подальших перспектив та напрямків для подальших досліджень:

– розширення моделі: перспективою є розширення моделі для врахування більш широкого спектру мотивацій, включаючи соціальні, геополітичні та економічні аспекти. Розробка більш складних моделей машинного навчання, які враховують ці різні мотивації, може покращити передбачення кібератак;

– використання глибинного навчання: використання глибинного навчання та нейронних мереж може покращити точність передбачення мотивації хакера. Глибинне навчання дозволяє автоматично виділяти складні закономірності у великих обсягах даних;

– інтеграція з системами кібербезпеки: розробка інтегрованих систем, які враховують мотивацію хакера при прийнятті рішень з кібербезпеки, може допомогти автоматично реагувати на потенційно небезпечні атаки та захищати інформаційні ресурси;

– вивчення еволюції мотивацій: дослідження того, як змінюються мотивації хакерів з часом, може допомогти передбачити майбутні кіберзагрози та реагувати на них заздалегідь;

– врахування контексту: розгляд можливостей врахування контексту атаки, такого як географічне розташування, типи жертв і глобальні події, що можуть впливати на мотивацію хакера;

– співпраця з іншими галузями: співпраця зі спеціалістами у сферах психології, кримінальної поведінки та кібербезпеки може допомогти глибше розуміти мотивацію хакера та розробити більш точні моделі.

Загалом, розробка та дослідження «алмазної моделі» щодо мотивації при здійсненні хакером кібератаки є лише початком широкої галузі досліджень у сфері кібербезпеки. Подальший розвиток цього напрямку може покращити нашу здатність передбачати та захищати від кіберзагроз.

Результати дослідження апробовано у вигляді тез доповідей під час I Міжнародної науково-практичної конференції «NEW WAYS OF CREATING SCIENTIFIC IDEAS FOR IMPLEMENTATION» [36], та статті у студентському науковому журналі «UNIVERSUM» [55].

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Forbes Ukraine – Російські хакери координують дії з військовими та посилюють атаки напередодні зими. Як Україна протистоїть кібератакам на енергосистему. URL: https://forbes.ua/company/rosiyski-khakeri-koordinuyut-dii-z-viyskovimi-ta-posilyuyut-ataki-naperedodni-zimi-yak-ukraina-protistoit-kiberatakam-na-energosistemu-08112023-17242 (дата звернення 26.11.2023).

2. Прокіпець, В., & Кузьомін, О. (2022). МЕТОДИ АНАЛІЗУ ЗОБРАЖЕНЬ ЛЕГЕНІВ ДЛЯ ДИАГНОСТУВАННЯ COVID. *Grail of Science*, (14-15), 356-361.

3. Шустрова, А. Є., & Кузьомін, О. Я. (2023). Спільний автокодер із порогом виявлення аномалії суглоба на виробничих лініях.

4. Мєдєнцев, Д. В., & Кузьомін, О. Я. (2023). *Розробка пристрою з GSM сигналізацією* (Doctoral dissertation).

5. Berkovskyi, D., & Kuzomin, O. (2023). CREATION OF INTELLIGENT SYSTEMS FOR ANALYZING SUPERMARKET VISITORS TO IDENTIFY CRIMINAL ELEMENTS. *Collection of scientific papers «SCIENTIA»*, (May 5, 2023; Sydney, Australia), 113-118.

6. Uchqun o‘g‘li, B. S., Kuzomin, O., & Lyashenko, V. (2023). Decision support procedures for decision making in a COVID condition.

7. Верколаб, Г. С. (2022). *Розробка та дослідження детектору маски для обличчя з OPENCV, KERAS/TENSORFLOW і глибоким навчання* (Doctoral dissertation).

8. Кузьомін О. Я. Моделювання повторюваних понять у незбалансованих потоках даних / С. Є. Холодов, Кузьомін О. Я. // Розвиток наукової думки постіндустріального суспільства: сучасний дискурс : матеріали III Міжнародної наукової конференції, 28 квітня 2023 р., Львів. — Вінниця : «Європейська наукова платформа», 2023. – С. 112-119.

9. Кузьомін, О. Я., Василенко, О. О., & СВИСТУНОВ, І. (2020). Розробка багатоагентних структур для вирішення проблем медичної системи діагностування. *Радіоелектроніка та інформатика*, *2*, 47-54.

10. Кузьомін, О. Я. (2008). *Методи, моделі та інформаційні технології моніторингу і ліквідації наслідків надзвичайних природних ситуацій* (Doctoral dissertation, ОЯ Кузьомін).

11. Галахов, Є. М., & Собчук, В. В. (2019). Розвиток моделей кібератак у площині інформаційної безпеки підприємства. *Науковий журнал «Телекомунікаційні та інформаційні технології». Київ, ДУТ*, (4), 65.

12. Лисенко, С. М. (2019). Моделі кібератак мережного та хостового типу.

13. Okhrimchuk, V. (2020). Узагальнена диференційно-ігрова модель шаблону потенційно небезпечної кібератаки. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, *4*(8), 113-123.

14. Потій, О. В., Семенченко, А. І., Бакалинський, О. О., & Мялковський, Д. В. (2021). Концептуальні засади впровадження організаційно-технічної моделі кіберзахисту України. *Захист інформації*, *23*(1), 47-59.

15. Барабаш, О. В., & Галахов, Є. М. (2019). Підхід до класифікації моделей кібератак у площині інформаційної безпеки підприємства. *ВВК 73*, 156.

16. БАРАБАШ, О. В. (2020). МОДЕЛІ КІБЕРАТАК В СИСТЕМІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА НА ОСНОВІ ВИКОРИСТАННЯ ФРІЛАНС-РЕСУРСУ.

17. Іванченко, О. В. (2019). ТЕОРЕТИКО-МНОЖИННА МОДЕЛЬ КІБЕРАТАКИ СИСТЕМИ КОРПОРАТИВНОГО УПРАВЛІННЯ. *Mathematical Problems of Technical Mechanics and Applied Mathematics-2019*, 65.

18. Казакова, Н. Ф., Фразе-Фразенко, О. О., & Щербина, Ю. В. (2019). СПОСОБИ МОДЕЛЮВАННЯ КІБЕРАТАК У СУЧАСНОМУ КІБЕРПРОСТОРІ. *Тези доповідей*, 12.

19. Зозуля, А. А., Стопакевич, О. А., & Стопакевич, А. О. (2021). СИСТЕМА МОДЕЛЮВАННЯ КІБЕРАТАКИ ПІДМІНОЮ ОРС-СЕРВЕРА ПРИ КОМП'ЮТЕРНОМУ УПРАВЛІННІ ТЕХНОЛОГІЧНИМИ УСТАНОВКАМИ. *Informatics & Mathematical Methods in Simulation*, *11*(3).

20. Запорожченко, М. М. (2023). МІСЦЕ OSINT В ЖИТТЄВОМУ ЦИКЛІ КІБЕРАТАКИ.

21. Kim, S. S., Hwang, K. S., Yang, J. Y., Chae, J. S., Kim, G. R., Kan, H., ... & Bae, M. A. (2020). Neurochemical and behavioral analysis by acute exposure to bisphenol A in zebrafish larvae model. *Chemosphere*, *239*, 124751.

22. Noecker Jr, J., Ryan, M., & Juola, P. (2013). Psychological profiling through textual analysis. *Literary and Linguistic Computing*, *28*(3), 382-387.

23. Shackleton, S., Bezerra, J. C., Cockburn, J., Reed, M. G., & Abu, R. (2021). Interviews and surveys. In *The Routledge Handbook of Research Methods for Social-Ecological Systems* (pp. 107-118). Routledge.

24. Ribelles, N., Jerez, J. M., Rodriguez-Brazzarola, P., Jimenez, B., Diaz-Redondo, T., Mesa, H., ... & Alba, E. (2021). Machine learning and natural language processing (NLP) approach to predict early progression to first-line treatment in real-world hormone receptor-positive (HR+)/HER2-negative advanced breast cancer patients. *European Journal of Cancer*, *144*, 224-231.

25. Wei, J., Chu, X., Sun, X. Y., Xu, K., Deng, H. X., Chen, J., ... & Lei, M. (2019). Machine learning in materials science. *InfoMat*, *1*(3), 338-358.

26. Hounmenou, C., & Toepp, S. (2023). Exploring private investigation agencies' experience of collaboration with law enforcement in Investigations of human trafficking cases. *Societies*, *13*(2), 44.

27. Hackett, A. (2017). Parents as researchers: collaborative ethnography with parents. *Qualitative research*, *17*(5), 481-497.

28. Творошенко, І. С. (2021). Технології прийняття рішень в інформаційних системах: навч. посібник. *Харків: ХНУРЕ*.

29. Гороховатський, В. О., & Творошенко, І. С. (2021). Методи інтелектуального аналізу та оброблення даних: навч. Посібник.

30. Гороховатський В.О., Творошенко І.С. (2022) Аналіз багатовимірних даних за описом у формі множини компонент: монографія. Харків: ХНУРЕ, 124 с.

31. Daradkeh, Y.I., Tvoroshenko, I., Gorokhovatskyi, V., Latiff, L.A., and Ahmad, N. (2021) Development of Effective Methods for Structural Image Recognition Using the Principles of Data Granulation and Apparatus of Fuzzy Logic, *IEEE Access*, 9, pp. 13417-13428.

32. Gorokhovatskyi, V.O., Tvoroshenko, I.S., and Peredrii O.O. (2020) Image classification method modification based on model of logic processing of bit description weights vector, *Telecommunications and Radio Engineering*, 79(1), pp. 59-69.

33. Tvoroshenko I., and Gorokhovatskyi V. (2022) The Application of Hybrid Intelligence Systems for Dynamic Data Analysis, *International Journal of Engineering and Information Systems*, 6(2), pp. 40–48

34. Daradkeh Y.I., Gorokhovatskyi V., Tvoroshenko I., and Al-Dhaifallah M. (2022) Classification of Images Based on a System of Hierarchical Features, *Computers, Materials & Continua*, 72(1), pp. 1785–1797.

35. Tvoroshenko, I., & Kukharchuk, V. (2021). Current state of development of applications for recognition of faces in the image and frames of video captures.

36. Стебаєв, Д. Дослідження «алмазної моделі» щодо врахування визначення зв'язку між мотивацією при здійсненні хакером кібератаки. In *The I International Scientific and Practical Conference «New ways of creating scientific ideas for implementation», September 18-20, 2023, Varna, Bulgaria. 285 p.* (p. 273).

37. Садомська, Б. (2021). Система кібербезпеки США: еволюція політичної стратегії від президентства Джорджа Буша до Джозефа Байдена.

38. Силаєва, Г. О. (2022). Кібертероризм як інструмент протистояння держав на міжнародній арені.

39. Музика, В. В. (2021). *Атрибуція кібератак проти об'єктів критичної інфраструктури: визначення основних проблем та шляхів їх вирішення* (Doctoral dissertation, Одеса).

40. Комаров, М. Ю. (2019). Огляд кібератак на об'єкти критичної інфраструктури. *Elektronnoe Modelirovanie*, *41*(6).

41. ПОЛЯКОВ, О. (2023). Сучасні тренди виявлення та протидії застосуванню шпигунських та шкідливих програм. *Інформація і право*, (2 (45)), 125-138.

42. Grycyshen, D., Malyshev, K., Nonik, V., & Molotai, V. (2023). Механізм забезпечення кібербезпеки правоохоронної системи. *Social Development and Security*, *13*(4), 18-34.

43. Гуцалюк, М. В. (2020). Шляхи посилення спроможностей правоохоронних та інших державних органів у сфері боротьби з кіберзлочинністю. *Інформація і право*, (3 (34)), 75-87.

44. Стебаєв Д.І. Апаратно-програмне забезпечення бездротової системи моніторингу електрофізичної установки: кваліфікаційна робота першого (бакалаврського) рівня вищої освіти: 6.050101 Комп'ютерні науки. Харків, 2013. 42 с. (с. 34).

45. Kaggle – Attacked dataset. URL: https://www.kaggle.com/datasets/vtu10547/attacked/data (дата звернення 01.11.2023).

46. Daradkeh Y.I., Gorokhovatskyi V., Tvoroshenko I., and Zeghid M. (2022) Tools for fast metric data search in structural methods for image classification, *IEEE Access*, 10, pp. 124738-124746.

47. Gorokhovatskyi V., Tvoroshenko I., Kobylin O., and Vlasenko N. (2023) Search for visual objects by request in the form of a cluster representation for the structural image description, *Advances in Electrical and Electronic Engineering*, 21(1), pp. 19-27.

48. Гороховатський В.О., Творошенко І.С., Чмутов Ю.В. (2022)

Застосування систем ортогональних функцій для формування простору ознак у методах класифікації зображень, *Сучасні інформаційні системи*, 6(3), с. 5-12.

49. Гороховатський В., Передрій О., Творошенко І., Марков Т. (2023) Матриця відстаней для множини компонентів структурного опису як інструмент для створення класифікатора зображень, *Сучасні інформаційні системи*, 7(1), С. 5-13.

50. Pomazan V., Tvoroshenko I., and Gorokhovatskyi V. (2023) Development of an application for recognizing emotions using convolutional neural networks, *International Journal of Academic Information Systems Research*, 7(7), pp. 25-36.

51. Pomazan V., Tvoroshenko I., and Gorokhovatskyi V. (2023) Handwritten character recognition models based on convolutional neural networks, *International Journal of Academic Engineering Research*, 7(9), pp. 64-72.

52. Tvoroshenko I., Gorokhovatskyi V., Kobylin O., and Tvoroshenko A. (2023) Application of deep learning methods for recognizing and classifying culinary dishes in images, *International Journal of Academic and Applied Research*, 7(9), pp. 57-70.

53. Gorokhovatskyi V., Tvoroshenko I. (2023) Identification of visual objects by the search request. *International scientific symposium «INTELLIGENT SOLUTIONS-S». Computational intelligence (results, problems and perspectives). Decision making theory: proceedings of the international symposium*, September 28, 2023, Kyiv-Uzhorod, Ukraine, pp. 25-27.

54. Yakovleva O., Kovač M., Ardasov V. & Yeremenko I. (2023). Study on adding functionality to the Zoom online conference system for monitoring the participant activities, *Public Administration and Regional Development*, 19(1), pp. 158-184.

55. Стебаєв, Д. (2023). Дослідження «алмазної моделі» щодо врахування визначення зв’язку між мотивацією при здійсненні хакером кібератаки. *UNIVERSUM*, (2), 75-84.