EUROPEAN CONFERENCE

# Conference Proceedings

I International Science Conference
«New ways of creating scientific ideas for implementation»

September 18 – 20, 2023

Varna, Bulgaria

# NEW WAYS OF CREATING SCIENTIFIC IDEAS FOR IMPLEMENTATION

Abstracts of I International Scientific and Practical Conference

Varna, Bulgaria
(September 18-20, 2023)

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

**Стебаєв Дмитро,**
магістрант кафедри інформатики
Харківський національний університет радіоелектроніки,

За результатами дослідження «алмазної моделі» щодо врахування визначення зв'язку між мотивацією при здійсненні хакером кібератаки були виділені основні тези [1-10]:

– 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 мотивацію: розроблена модель машинного навчання, в даному випадку «Логістична регресія», демонструє високу точність у передбаченні мотивації хакера на основі аналізу характеристик кібератак;

– 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.

Підкреслено важливість та потенціал стратегій захисту щодо врахування визначення зв'язку між мотивацією при здійсненні хакером кібератаки.

«Діамантова модель» – це структура, яка використовується в кібербезпеці для розуміння й аналізу кіберзагроз і атак. Він зосереджений на чотирьох ключових компонентах: супротивник, інфраструктура, можливості та жертва. Коли справа доходить до дослідження мотивації хакерів, які здійснюють кібератаки в рамках

цієї системи, ми можемо використовувати комбінацію методів, щоб отримати уявлення про їхню мотивацію.

Ось декілька методів дослідження та підходів, які ми можемо розглянути:

– Open Source Intelligence (OSINT): збирайте 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: досліджуйте темну мережу та підпільні форуми, щоб зібрати інформацію про мотиви, тактику, методи та процедури кіберзлочинців. Це може дати цінну інформацію про кримінальне підпілля;

– аналіз поведінки: вивчайте поведінку суб'єктів загрози та аналізуйте шаблони їхніх минулих атак. Шукайте підказки в їхніх діях, наприклад, вибір цілей, методи атаки та викрадання даних;

– психологічне профілювання: співпрацюйте 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: проведіть 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 вивчіть конкретні кібератаки та учасників загроз, щоб зрозуміти їхню мотивацію. Проаналізуйте цілі, час і методи, які використовуються в цих атаках;

– статистичний аналіз [11-14]: збирайте та аналізуйте 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: аналізуйте 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: використовуйте методи машинного навчання для аналізу великих обсягів текстових даних із різних джерел [15-18], таких як соціальні медіа, щоб виявити моделі та настрої, пов'язані з мотивацією хакера;

– співпраця з правоохоронними органами: співпрацюйте 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: занурте дослідників у культуру хакерів, фізично або через онлайн-взаємодії, щоб отримати глибоке розуміння їхніх мотивацій, цінностей і переконань;

– етичное хакерство та Red Teaming: проводьте етичні хакерські вправи та об'єднуйтеся в червону команду для імітації кібератак. Проаналізуйте мотиви та

прийоми, які використовує червона команда, щоб зрозуміти мислення кіберзловмисників;

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

Усі ці аспекти підкреслюють важливість дбайливого та обачного підходу до збору та підготовки даних для дослідження «алмазної моделі» щодо врахування визначення зв'язку між мотивацією при здійсненні хакером кібератаки .

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.

**Список літератури:**

1. 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.

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

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

4. 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.

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

6. Терейковський, І. А. (2015). *Нейромережеві моделі, методи і засоби оцінювання параметрів безпеки інтернет-орієнтованих інформаційних систем* (Doctoral dissertation).

7. Барабаш, О. В. (2020). Моделі кібератак в системі інформаційної безпеки підприємства на основі використання фріланс-ресурсу.

8. Іванченко, О. В. (2019). Теоретико-множинна модель кібератаки системи корпоративного управління. *Mathematical Problems of Technical Mechanics and Applied Mathematics-2019*, 65.

9. Казакова, Н. Ф., Фразе-Фразенко, О. О., & Щербина, Ю. В. (2019). Способи моделювання кібератак у сучасному кіберпросторі. *Тези доповідей*, 12.

10. Зозуля, А. А., Стопакевич, О. А., & Стопакевич, А. О. (2021). Система моделювання кібератаки підміною OPC-сервера при комп'ютерному управлінні технологічними установками. *Informatics & Mathematical Methods in Simulation*, *11*(3).

11. Гороховатський В., Творошенко І., Сидоренко Д. (2021) Класифікація зображень із використанням кластерного подання, Міжнародний науковий симпозіум «Інтелектуальні рішення-С». Обчислювальний інтелект (результати, проблеми, перспективи). Теорія прийняття рішень: праці міжн. наук. симпозіуму (Вересень 29, 2021). Київ – Ужгород, С. 44-45.

12. Кучеренко, Е. И., & Творошенко, И. С. (2010). Прикладные аспекты моделирования нечетких процессов в сложных системах. *Збірник наукових праць Харківського університету Повітряних сил*, (1), С. 127-131.

13. Gorokhovatskyi V., Gadetska S., Ponomarenko R. (2020) Recognition of Visual Objects Based on Statistical Distributions for Blocks of Structural Description of Image. Proc. of the XV Int. Scientific Conference “Intellectual Systems of Decision Making and Problems of Computational Intelligence” (ISDMCI’2019), Ukraine, May 21–25, 2019, pp. 501-512.

14. Tvoroshenko, I., & Zarivchatskyi, R. (2020). Analysis of existing methods for searching object in the video stream.

15. Gorokhovatskyi, V., Peredrii, O., Tvoroshenko, I., & Markov, T. (2023). Матриця відстаней для множини компонентів структурного опису як інструмент для створення класифікатора зображень, *Advanced Information Systems*, 7(1), С. 5-13.

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

17. Gorokhovatskyi, V., Tvoroshenko, I., Kobylin, O., & 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.

18. Pomazan, V., Tvoroshenko, I., & 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.