Розроблення методу дослідження кіберзлочинів за типом вірусів-вимагачів з використанням моделей штучного інтелекту в системі менеджменту інформаційної безпеки критичної інфраструктури

Development of a method for investigating cybercrimes by the type of ransomware using artificial intelligence models in the information security management system of critical infrastructure

Андрій Партика [A]
к.тех.н., старший викладач кафедри, e-mail: andrii.i.partyka@lpnu.ua, ORCID: 0000-0003-3037-8373

Олег Гарасимчук [A]
к.тех.н., доцент, доцент кафедри, e-mail: oleh.i.harasymchuk@lpnu.ua, ORCID: 0000-0002-8742-8872

Олена Нємкова [A]
д.тех.н., професор, професор кафедри, e-mail: olena.a.niemkova@lpnu.ua, ORCID: 0000-0003-0690-2657

Ярослав Совин [A]
к.тех.н., доцент, доцент кафедри, e-mail: yaroslav.r.sovyn@lpnu.ua, ORCID: 0000-0002-5023-8442

Валерій Дудикевич [A]
д.тех.н., професор, професор кафедри, e-mail: valerii.b.dudykevych@lpnu.ua, ORCID: 0000-0001-8827-9920

Andrii Partyka [A]
Candidate of Technical Sciences, e-mail: andrii.i.partyka@lpnu.ua, ORCID: 0000-0003-3037-8373

Oleh Harasymchuk [A]
Candidate of Technical Sciences, Associate Professor, e-mail: oleh.i.harasymchuk@lpnu.ua, ORCID: 0000-0003-3037-8373

Elena Nyemkova [A]
Dr of Technical Sciences, Professor, e-mail: olena.a.niemkova@lpnu.ua, ORCID: 0000-0003-0690-2657

Yaroslav Sovyn [A]
Candidate of Technical Sciences, Associate Professor, e-mail: yaroslav.r.sovyn@lpnu.ua, ORCID: 0000-0002-5023-8442

Valerii Dudykevych [A]
Dr of Technical Sciences, Professor, e-mail: valerii.b.dudykevych@lpnu.ua, ORCID: 0000-0001-8827-9920

[A] Національний університет "Львівська політехніка", м. Львів, Україна

[A] Lviv Polytechnic National University, Lviv, Ukraine

Received: April 10, 2024 | Revised: April 17, 2024 | Accepted: April 30, 2024

DOI: 10.33445/sds.2024.14.2.6

Мета роботи: розробка методу виявлення вірусів-вимагачів у системах менеджменту інформаційної безпеки критичної інфраструктури узгодженого зі стандартом ISO 27001:2022.
Метод: аналіз, синтез та моделювання.
Результати дослідження: дослідження виявило, що використання штучного інтелекту може покращити здатність систем безпеки критичної інфраструктури ідентифікувати та реагувати на атаки шифрувальників.
Теоретична цінність дослідження: Це дослідження розвиває існуючі теорії використання штучного інтелекту у кібербезпеці, демонструючи, як глибоке навчання може бути адаптоване для специфічних потреб кіберзахисту критичної інфраструктури. Воно також сприяє розвитку теорій управління кіберризиками, інтегруючи технології ШІ в стратегії безпеки.
Практична цінність дослідження: Дослідження надає практичні рекомендації для розробників політик та фахівців із кібербезпеки щодо інтеграції штучного інтелекту в системи управління безпекою. Це також вказує на потенційні точки вдосконалення у виявленні та реагуванні на інцидент інформаційної безпеки.
Майбутні дослідження: Дослідження ефективності роботи запропонованої моделі.
Тип статті: теоретичний.

Purpose: to develop a method for detecting ransomware in the information security management systems of critical infrastructure that is compliant with the ISO 27001:2022 standard.
Method: analysis, synthesis and modeling.
Findings: The study found that the use of artificial intelligence can significantly improve the ability of critical infrastructure security systems to identify and respond to encryption attacks.
Theoretical implications: This research improves existing theories of the use of artificial intelligence in cyber security, demonstrating how deep learning can be adapted for the specific needs of cyber defense of critical infrastructure. It also advances theories of cyber risk management by integrating AI technologies into security strategies.
Practical implications: The study provides practical recommendations for cybersecurity professionals regarding integrating artificial intelligence into security management systems. It also points to potential areas of improvement in incident detection and response.
Future research: Analysis of the effectiveness of the proposed model.
Paper type: theoretical.

Ключові слова: кіберзлочин, штучний інтелект, система управління інформаційною безпекою, ISO 27001, віруси-вимагачі.

Key words: Cybercrime, Artificial Intelligence, Information Security Management System, ISO 27001, ransomware.

Вступ

За останнє десятиліття кіберзлочинність значно зросла. Одним із ключових факторів є поширення онлайн-спільнот кіберзлочинців, де актори торгують продуктами та послугами, а також навчаються один в одного. Відповідно, розуміння роботи та поведінки цих спільнот становить великий інтерес, і вони досліджувалися в багатьох дисциплінах з різними, часто досить новими, підходами [1]. Зважаючи на дослідження публікацій проведених повідними компаніями, що надають послуги інформаційної безпеки CISCO та IBM система управління інформаційною безпекою критичної інфраструктури є пріоритетною ціллю кіберзлочинців. Інтеграція штучного інтелекту (AI) у систему управління інформаційною безпекою критичної інфраструктури (CIISMS) є значним кроком вперед у боротьбі з кіберзлочинами. Оскільки кіберзагрози стають дедалі складнішими та поширенням площі війни на кіберпростір, лише традиційних заходів безпеки вже недостатньо для захисту систем критичної інфраструктури, які лежать в основі найважливіших секторів нашого суспільства, зокрема енергетики, водопостачання, транспорту та охорони здоров'я [2]. Тому у даній статті розглядаються поточні дослідження, застосування та майбутні напрямки штучного інтелекту для покращення виявлення та запобігання кіберзлочинам у рамках CIISMS.

Алгоритми штучного інтелекту особливо ефективні в моніторингу мережевого трафіку та виявленні відхилень від норми, які можуть свідчити про кібератаку. Моделі машинного навчання навчаються на величезних наборах даних звичайного та зловмисного трафіку, щоб розрізняти доброякісні аномалії та справжні загрози [3]. Аналізуючи історичні дані, штучний інтелект може передбачати майбутні кіберзагрози, що дозволяє вживати проактивні заходи захисту. Цей підхід має вирішальне значення для захисту критично важливої інфраструктури, де навіть мінімальна недоступність може мати значні наслідки. Технології штучного інтелекту, включаючи машинне навчання (ML), обробку природної мови (NLP) і нейронні мережі, пропонують можливості для розпізнавання шаблонів, прогнозування потенційних загроз і автоматизації механізмів реагування. Їх впровадження в CIISMS зумовлене необхідністю попереджати, ідентифікувати та пом'якшувати кібератаки зі швидкістю та точністю, які далеко перевищують людські можливості.

Системи штучного інтелекту можуть також автоматично реагувати на раніше невідомі виявлені загрози, впроваджуючи швидкі стратегії реагування щоб запобігти або мінімізувати шкоду на відміну від традиційних SIEM, EDR чи антивірусів. Ця здатність необхідна для забезпечення безперервної роботи критично важливих служб. Також, системи дослідження кібератак на базі штучного інтелекту можуть аналізувати електронні листи та веб-вміст у режимі реального часу, виявляючи та блокуючи спроби поширення шкідливого ПЗ, які часто передують більш серйозним кібератакам на критичну інфраструктуру.

Теоретичні основи дослідження

У контексті зростання кіберзагроз і потреб захисту критичної інфраструктури було досягнуто значних успіхів у розробці методів розслідування кіберзлочинів, зокрема програм-вимагачів, за допомогою моделей штучного інтелекту. Для даного дослідження було проаналізовано наукові роботи, зосереджуючись на їхньому внеску у сфері кібербезпеки, керованої ШІ, для захисту критичної інфраструктури.

Дослідження Джека Хьюза описує спільноти кіберзлочинців, які мають вирішальне значення для розробки моделей штучного інтелекту, які передбачають і протидіють еволюції тактик програм-вимагачів [1]. Мануела Тваронавічене та Делла Каса аналізують модель управління кібербезпекою, розроблену спеціально для захисту критичної інфраструктури, пропонуючи заходи захисту інформації, які є важливими для інтеграції можливостей ШІ в існуючі системи управління безпекою [2]. Роботи Ікбала Саркера та Фенг Тао досліджують

ширше застосування штучного інтелекту в кібербезпеці, наголошуючи на прогнозній аналітиці та виявленні загроз, які покращують здатність системи ефективно обробляти інциденти програм-вимагачів [3, 4]. Дослідження Харуна Оз, Ахмета Аріса та інших "Опитування програм-вимагачів: еволюція, таксономія та рішення для захисту" аналізує програми-вимагачі, надаючи детальну систематику та різні механізми захисту, які дають змогу розробляти цільові рішення ШІ [5]. Емпіричні дані зі звіту Cybersecurity Ventures (2024) і статистика злочинності ФБР за 2022 рік підкреслюють складності у виявленні та частоти атак програм-вимагачів, вказуючи на потребу в моделях ШІ, які постійно оновлюються з урахуванням останніх даних і тенденцій [6, 7].

Крім того, Деепті Відярті та Амінанто у своїх наукових працях досліджують конкретні методології, такі як статичний аналіз зловмисного програмного забезпечення та пріоритезацію загроз на основі штучного інтелекту, які підвищують ефективність моделей штучного інтелекту в сценаріях загроз у реальному часі [8, 9]. Робота Апруцезе та Маркетті наголошують на необхідності, щоб системи ШІ були стійкими проти агресивних атак [10]. Дослідження "Глибоке навчання для виявлення вторгнень у кібербезпеку: підходи, набори даних і порівняльні дослідження" розглядає методи глибокого навчання для кібербезпеки, керуючи оптимальним вибором алгоритмів штучного інтелекту для виявлення програм-вимагачів і запобігання їм [11].

Вимоги, встановлені ISO/IEC 27001, і стратегії впровадження, описані Адріаном Фатурохманом визначають, що системи управління безпекою, розширені штучним інтелектом, не тільки зміцнюють захист від програм-вимагачів, але й узгоджуються з глобальною практикою безпеки, забезпечуючи комплексну структуру для управління кібербезпекою в критичних інфраструктурах [12, 13].

Постановка проблеми

Останнім часом кіберзлочини, особливо віруси-вимагачі, становлять серйозну загрозу для інформаційної безпеки організацій, зокрема у сфері критичної інфраструктури. Ці атаки можуть призвести до втрати важливих даних, фінансових збитків та навіть порушення функціонування життєво важливих служб. Стандарт ISO 27001:2022 встановлює вимоги до систем менеджменту інформаційної безпеки (СМІБ), які допомагають організаціям захистити свою інформацію. Втім, існуючі підходи до виявлення та запобігання кіберзлочинам часто не ефективні проти новітніх та швидко адаптуючись вірусів-вимагачів. Використання алгоритмів штучного інтелекту (ШІ) може запропонувати нові можливості для покращення захисту інформаційних систем у цьому контексті. Однак, дослідження, що вивчають застосування ШІ для боротьби з вірусами-вимагачами у відповідності до ISO 27001:2022, залишаються обмеженими. Тому дане дослідження зосереджено на розробці інноваційного методу використання алгоритмів ШІ для виявлення та нейтралізації вірусів-вимагачів, які загрожують інформаційній безпеці критично важливих інфраструктурних об'єктів та визначити відповідність методу вимогам міжнародного стандарту ISO 27001:2022.

Результати

1. Огляд можливостей алгоритмів ШІ для дослідження кіберзлочинів

Зростання частоти та якості кібератак стимулює кіберсистеми з підтримкою ШІ. Зростаюча кількість інцидентів масштабних кібератак у всьому світі привернула увагу організацій до необхідності захисту їхньої інформації. Мотивами цих кіберзлочинців є політична конкуренція, конкуренти пересуваються заради вигоди та шкоди імені інших, міжнародна крадіжка інформації та радикальні несвітські інтереси кластерів. Більшість кібератак здійснюються з метою отримання прибутку [4].

Провівши детальний огляд літератури про використання ШІ було сформовано у порівняльну таблицю 1. Дані для якої отримано з обширної сукупності джерел, включаючи академічну літературу, галузеві звіти, практичні приклади та думки експертів, щоб скласти схему застосування ШІ в розслідуваннях кіберзлочинів. Галузеві висновки, отримані зі звітів компаній з кібербезпеки та ринкових досліджень технологічних аналітиків, запропонували прагматичний погляд на ефективність та застосування моделей штучного інтелекту в реальних сценаріях. Цей багатогранний підхід забезпечив цілісний огляд особливостей моделей ШІ, що відобразив динамічну взаємодію технологій, застосування та ефективності моделей штучного інтелекту в сфері кібербезпеки.

Таблиця 1 – Огляд особливостей моделей Штучного Інтелекту

Моделі та їх особливості	Deep Learning Модель	Random Forest	Isolation Forest
Основне застосування	Комплексне розпізнавання образів	Класифікація та регресія	Виявлення аномалій
Сильні сторони	Висока точність у різних середовищах, багатих на дані	Висока точність і стійкість до переобладнання	Ефективне для виявлення аномалій без навчальних даних
Обмеження	Вимагає значних обчислювальних ресурсів	Може бути вимогливим до обчислювальних ресурсів	Може мати вищі показники помилкових спрацьовувань в деяких контекстах
Вимоги до даних	Підтримуються різні типи	Дані з мітками для навчання	Дані без міток або з мінімальною підготовкою
Обчислювальна інтенсивність	Високий	Від помірної до високої	Помірна
Адаптивність до нових загроз	Корисно для глибокого аналізу даних	Помірна	Висока
Використання у розслідуванні кіберзлочинів	Комплексне розпізнавання образів	Ефективна у класифікації та визначенні відхилень	Ефективна у виявленні прихованих аномалій

Розширена порівняльна таблиця містить детальний огляд кількох моделей штучного інтелекту, підкреслюючи їх застосування, переваги, обмеження та дає можливість оцінити їх використання у сфері розслідування кіберзлочинів. Моделі керованого навчання, зокрема Random Forest, відмінно справляються із завданнями, що вимагають класифікації та прогнозування, забезпечуючи високу точність під час навчання з великою кількістю позначених даних, хоча їм важко адаптуватися до нових загроз через їх залежність від попередньо позначених наборів даних. З іншого боку, неконтрольовані моделі, такі як Isolation Forest, здатні виявляти аномалії та нові шаблони без позначених даних, пропонуючи вирішальну перевагу у виявленні нових кіберзагроз, хоча й із тенденцією до більшої кількості помилкових спрацьовувань. Моделі глибокого навчання, включаючи виділяються в аналізі складних типів даних, таких як зображення та послідовна інформація, вимагаючи значної обчислювальної потужності та великих наборів даних, але забезпечуючи неперевершену глибину аналізу даних.

У сукупності ці моделі штучного інтелекту надають багатогранний набір інструментів для аналітиків безпеки, кожен зі своїми перевагами та обмеженнями, таким чином забезпечуючи комплексний підхід до виявлення, аналізу та пом'якшення кіберзагроз у інформаційних системах.

2. Характеристики програм-вимагачів

В останні роки програми-вимагачі були одними з найвідоміших зловмисних програм, спрямованих на кінцевих користувачів, уряди та бізнес-організації. Це стало дуже прибутковим бізнесом для кіберзлочинців із доходами в мільйони доларів і дуже серйозною загрозою для організацій із фінансовими збитками у мільярди доларів [5]. Атаки програм-вимагачів представляють собою форму кіберзлочинності, яка заслуговує на особливу увагу через вплив на окремих осіб, підприємства та критичну інфраструктуру. Хоча вони становлять незначну частку кіберзлочинів, їхні наслідки є непрогнозованими, що заслуговує на цілеспрямований аналіз і стратегію реагування.

По-перше, атаки програм-вимагачів непрогнозовані. Вони не лише відмовляють у доступі до критично важливих даних і систем, але й вимагають викуп за відновлення доступу, чинячи величезний тиск на жертву. Ця подвійна загроза доступності до даних та втрата коштів робить програми-вимагачі унікальним типом кіберзлочину. По-друге, фінансові наслідки пов'язані зі сплатою викупу, разом із простоєм і відновленням можуть бути не прийнятними для малого та середнього бізнесу. У звіті Cybersecurity Ventures 2023 прогнозується, що збитки від програм-вимагачів вартуватиме світу 20 млрд доларів до 2031 року [6] проти 20 млрд доларів у 2020 році, що свідчить про швидке зростання економічного впливу цієї кіберзлочинності. По-третє, атаки програм-вимагачів мають ширший суспільний вплив. Якщо атака націлена на критично важливу інфраструктуру, для прикладу служби охорони здоров'я, водоочисні споруди чи постачальників електроенергії, наслідки можуть виходити за рамки фінансових втрат і впливати на здоров'я та безпеку населення. Атака WannaCry у 2017 році, яка вразила понад 200 000 комп'ютерів у 150 країнах, у тому числі критично важливі сегменти Національної служби охорони здоров'я Великобританії, підкреслює потенціал широко-масштабної шкоди. Крім того зловмисники постійно вдосконалюють свої методи, щоб обійти заходи безпеки. Вони часто застосовують передові методи, як-от шифрування, для блокування файлів користувачів і вимагають викуп у крипто валютах, які важко відстежити, ускладнюючи роботу правоохоронних органів.

Хоча інциденти з програмами-вимагачами можуть становити близько 10% усіх кіберзлочинів – цифра, яка змінюється залежно від звітності та аналізу, – вони часто мають надмірну видимість і вплив. Наприклад, у Звіті ФБР про злочини в Інтернеті за 2022 рік висвітлено програмне забезпечення-вимагач як серйозну проблему, незважаючи на те, що інші форми кіберзлочинності трапляються частіше. Зосередження уваги на програмах-вимагачах виправдано їхньою здатністю швидко завдавати серйозної шкоди, фінансовими витратами та потенційною небезпекою для життя в разі зламу критичних систем [7]. Методи виявлення зловмисного програмного забезпечення на основі сигнатур, яким важко виявити програми-вимагачі нульового дня, не підходять для захисту файлів користувачів від атак, спричинених ризикованими невідомими програмами-вимагачами. Тому потрібен новий механізм захисту, спеціалізований на програмах-вимагачах, і цей механізм має зосереджуватися на специфічних для програм-вимагачів операціях, щоб відрізняти програми-вимагачі від інших типів шкідливих програм, а також безпечних файлів [8].

Програми-вимагачі, можуть бути виявлені через різні атрибути, які сигналізують про їх присутність і потенційне розгортання. Розуміння цих показників має вирішальне значення для раннього виявлення та запобігання атакам програм-вимагачів, які призначені для шифрування файлів жертв і вимагають викуп за ключі дешифрування. У цьому огляді висвітлюються ключові атрибути програм-вимагачів, які є індикаторами кіберінцидентів та можуть бути використані для виявлення кіберзлочинів:

– несподіване шифрування файлів: однією з характерних ознак атаки програм вимагачів є раптове та неавторизоване шифрування файлів. Жертви можуть виявити, що їхні документи, бази даних та інші важливі файли недоступні, часто замінені версіями з

незнайомими розширеннями або нотатками про викуп як імена файлів. Часто використовується AES 256 алгоритм шифрування файлів;

– незвичайна мережева активність: програми-вимагачі часто зв'язуються із зовнішніми серверами (C&C) для отримання інструкцій або надсилання ключів шифрування. Ця незвичайна мережева активність може бути раннім показником зламу, особливо якщо вона стосується відомих шкідливих IP-адрес або доменів [9];

– зміни файлової системи: атаки програм-вимагачів можуть призвести до помітних змін у структурі файлової системи. Це включає створення нових файлів (нотаток про викуп), зміну наявних розширень файлів і видалення тіньових копій або файлів резервних копій, щоб перешкодити спробам відновлення;

– втручання в програмне забезпечення безпеки: деякі складні варіанти програм-вимагачів намагаються вимкнути або обійти програмне забезпечення безпеки. Індикатори включають вимкнені антивірусні програми, вимкнені правила брандмауера або змінені параметри безпеки системи;

– збільшення активності процесора та диска: (CPU > 70% – 90%) процес шифрування вимагає значних обчислювальних ресурсів. Незрозумілий сплеск активності ЦП і диска може свідчити про те, що програми-вимагачі активно шифрують файли у фоновому режимі [9] ;

– підозрілі модифікації реєстру: програмне забезпечення-вимагач може вносити зміни в реєстр, щоб установити постійність, запустити процес шифрування під час завантаження або вимкнути функції відновлення. Відстеження неочікуваних або неавторизованих змін реєстру може допомогти виявити програми-вимагачі;

– незвичайні спроби входу: якщо програмне забезпечення-вимагач поширюється через мережу, у різних системах можуть бути незвичні спроби входу, оскільки програмне забезпечення-вимагач намагається отримати доступ до спільних мережевих ресурсів і зашифрувати їх;

– інструкції з розшифрування або примітки про викуп: нарешті, поява в системі інструкцій з розшифрування або приміток про викуп є остаточним показником атаки програм-вимагачів. Ці примітки часто містять інструкції щодо оплати викупу та можуть містити інші погрози чи попередження.

Раннє розпізнавання цих атрибутів може мати ключове значення для зменшення впливу атак програм-вимагачів. Організаціям і окремим особам слід навчитися розпізнавати ці ознаки та швидко реагувати, щоб стримати та усунути загрозу програм-вимагачів, зводячи до мінімуму втрату даних і час відновлення.

3. Порівняння можливостей виявлення програм-вимагачів алгоритмами ШІ

Щоб порівняти моделі штучного інтелекту для виявлення програм-вимагачів на основі визначених атрибутів, ми розглянемо кілька ключових аспектів: точність виявлення, здатність до навчання, адаптованість до нових штамів програм-вимагачів, вимоги до обчислювальних ресурсів і здатність виявляти певні атрибути програм-вимагачів визначені на основі проаналізованих досліджень [10-12]. Нижче наведено порівняння різних моделей ШІ, які зазвичай використовуються для виявлення програм-вимагачів (Табл. 2).

У цьому порівнянні кожна модель демонструє унікальні переваги за вказаними характеристиками. Random Forest відомий своєю високою точністю виявлення та надійністю в середовищах із багатим набором функцій, що робить його ідеальним для середовищ структурованих даних. Isolation Forest вирізняється адаптивністю, здатністю виявляти нові типи програм-вимагачів без попереднього знання.

Таблиця 2 – Огляд можливостей виявлення програм-вимагачів алгоритмами ШІ

Модель ШІ	Точність виявлення	Здатність до навчання	Адаптивність	Вимоги до ресурсів	Приклади використання
Deep Learning (Моделі Глибокого Навчання)	Висока для складних форм даних	Постійно вдосконалюється за допомогою нових даних	Висока у різних сценаріях	Дуже високі, значні обчислювальні ресурси	Ефективна для розпізнавання зображень
Isolation Forest (Ізоляційний Ліс)	Змінюється, може бути високою для виявлення аномалій	Може самонавчатись використовуючи немарковані дані	Висока, добре розпізнає нові закономірності	Від середніх до високих, залежно від складності даних	Моніторинг мережевого трафіку на незвичайні моделі
Random Forest (Випадковий Ліс)	Висока	Обмежується наданими даними	Можна оновлювати новими даними	Високі	Прогнозування подій безпеки в IT-інфраструктурі

Моделі глибокого навчання, зокрема CNN, забезпечують високу точність виявлення складних і нюансованих форм даних, але вимагають значних обчислювальних ресурсів. Вибір найкращої моделі штучного інтелекту для виявлення програм-вимагачів значною мірою залежить від конкретного випадку використання, доступних ресурсів, а також характеру даних і загроз.

4. Метод дослідження кіберзлочинів за типом вірусів-вимагачів використовуючи моделі Isolation Forest та Random Forest в системі менеджменту інформаційної безпеки критичної інфраструктури

Вибір найкращої моделі штучного інтелекту для виявлення програм-вимагачів у інформаційних системах системи управління інформаційною безпекою критичної інфраструктури (ISMS) передбачає вибір моделі, яка вирізняється точністю, адаптивністю та ефективністю в середовищах із високими ставками. Враховуючи специфічні вимоги критичної інфраструктури, яка вимагає високої надійності та здатності швидко адаптуватися до нових загроз, така модель, як Random Forest, може бути особливо ефективною завдяки своїй надійності та високій точності виявлення. Однак дуже важливо поєднати це з можливістю адаптації таких моделей, як Isolation Forest, для виявлення нових загроз, створюючи таким чином багатошарову стратегію захисту.

Нижче запропонований метод впровадження випадкового лісу (Random Forest) для виявлення програм-вимагачів у інформаційних системах:

Етап 1: Збір даних і попередня обробка. Необхідно зібрати історичні дані (X) про мережевий трафік, системні журнали, поведінку користувачів і відомі підписи програм-вимагачів. Попередньо обробити дані, щоб структурувати їх відповідно до машинного навчання, що включає нормалізацію, обробку відсутніх значень і вибір функцій для виділення атрибутів, що вказують на програмне забезпечення-вимагач, використовуючи формулу нормалізації:

$$x_i' = \frac{x_i - \mu}{\sigma},$$

де x_i – вектори представляють функції, отримані з мережевого трафіку, журналів і дій системи;

μ – середнє значення;

σ стандартне відхилення набору даних.

Етап 2: Навчання випадкового лісу: використовуючи історичні дані для навчання моделі випадкового лісу, потрібно зосередитись на розрізненні між діяльністю програм-вимагачів і звичайними операціями. Навчання моделі Random Forest за допомогою можна здійснювати за допомогою X_{train}, Y_{train}, де Y представляє мітки (наприклад, програми-вимагачі або доброякісні). Для кожного дерева t у лісі потрібно вибрати випадкові підмножини функцій і точок даних для побудови дерева:

$$t = build\_tree\left(X_{train}^{(t)}, Y_{train}^{(t)}\right)$$

Та останнім кроком навчання є агрегування результатів усіх дерев для визначення рішення Випадкового Лісу:

$$RF(X) = majority\_vote(\{t(X)\}_{t=1}^{T})$$

Етап 3: Навчання ізоляційного лісу (Isolation Forest). Необхідно навчити модель ізоляційного лісу для виявлення аномалій, які можуть свідчити про дії програм-вимагачів. Формула виявлення аномалій для Ізоляційного Лісу така:

$$IF(X) = \{is\_anomaly(x_i)\},$$

де *is*_anomaly (*x_i*) визначає, чи є *x_i* викидом на основі довжини шляху в ізольовані дерева.

Етап 4: Інтеграція з ізоляційним лісом для нових загроз. Необхідно доповнити модель Random Forest ізольованим лісом, щоб покращити здатність системи виявляти нові та невідомі варіанти програм-вимагачів. Якщо Random Forest забезпечує надійне виявлення на основі відомих шаблонів, Isolation Forest визначить аномалії, які можуть представляти нові загрози програм-вимагачів. Для даних у реальному часі x_realtime обчислюємо:

RF_score(x_realtime) = RF(x_realtime), щоб отримати оцінку ймовірності програм-вимагачів із Random Forest

IF_score(x_realtime) = IF(x_realtime) для визначення балів аномалій із Ізольяційного Лісу.

Визнаємо комбінований критерій виявлення:

$$D(x_{ratm}) = \alpha \cdot RF_{score}(x_{ratm}) + (1 - \alpha) \cdot IF_{score}(x_{ratm}),$$

де α є ваговим коефіцієнтом, що збалансовує дві моделі.

Етап 5: Моніторинг і виявлення в реальному часі. Необхідно розгорнути навчені моделі для моніторингу мережевого трафіку та дій системи в реальному часі. Моделі повинні аналізувати вхідні дані, щоб виявити потенційні індикатори програм-вимагачів, наприклад незвичну активність шифрування або мережевий зв'язок. Також пропонуємо створити протокол для негайного сповіщення та реагування на виявлення потенційної активності програм-вимагачів. Система повинна автоматизувати початкові заходи стримування, щоб обмежити поширення атаки та повідомити персонал служби безпеки для подальшого розслідування. Для цього можна задати наступну умову: якщо D(x_realtime) перевищує попередньо визначене порогове значення θ, потрібно ініціювати попередження та запустити протоколи відповіді.

Етап 6: Постійне навчання та оновлення. Необхідно регулярно оновлювати модель новими даними та аналізом загроз, щоб підтримувати її ефективність. Це включає перенавчання моделі Random Forest з новими сигнатурами програм-вимагачів та адаптацію моделі Isolation Forest до змін поведінки мережі.

Завдяки інтеграції Random Forest та Isolation Forest у ISMS критичної інфраструктури можна використовувати сильні сторони обох моделей для створення динамічного та

надійного захисту від програм-вимагачів, забезпечуючи як виявлення відомих загроз, так і виявлення нових, потенційно шкідливих дій. Проте існує потреба у проведені майбутніх досліджень для аналізу ефективності запропонованого методу.

5.Аналіз Відповідності Міжнародним Стандартам

Дане дослідження встановлює також відповідність запропонованого методу міжнародним стандартам для інтеграції у CIISMS. Описаний метод виявлення програм-вимагачів за допомогою алгоритмів штучного інтелекту в критичній інфраструктурі ISMS забезпечує відповідність контролям ISO 27001:2022 [12], встановлюючи системний підхід до управління інформаційною безпекою, що є одним із основних принципів стандарту ISO. Для оцінки відповідності було визначено контролі ISO 27001:2022, які можуть бути впроваджені використовуючи запропонований метод:

– управління активами: запропонований метод може ідентифікувати критично важливі дані та системи, які є важливими для діяльності організації, таким чином допомагаючи класифікувати та належно поводитися з активами відповідно до вимог ISO 27001:2022.

– контроль доступу: виявляючи спроби несанкціонованого доступу або аномалії в поведінці користувачів, моделі Random Forest та Isolation Forest можуть сприяти посиленню контролю доступу, що є ключовою вимогою стандарту ISO 27001:2022.

– безпека операцій: запропонований метод підвищує безпеку операцій, надаючи можливості моніторингу та виявлення в реальному часі, забезпечуючи захист засобів обробки інформації від будь-яких потенційних загроз кібербезпеці.

– безпека зв'язку. Аналізуючи мережевий трафік і журнали, метод ШІ допомагає визначити та зменшити ризики, пов'язані з передачею інформації, таким чином підтримуючи аспект безпеки ISO 27001:2022.

– придбання, розробка та обслуговування системи: розробка та інтеграція моделей штучного інтелекту в ISMS демонструють відповідність вимогам ISO 27001:2022 щодо придбання, розробки та обслуговування системи, гарантуючи, що інформаційна безпека є невід'ємною частиною життєвого циклу системи та можуть бути інтегровані у DevSecOps підхід [14].

– управління інцидентами інформаційної безпеки: запропонований метод, керований моделями Random Forest та Isolation Forest, забезпечує надійні механізми для виявлення інцидентів і реагування на них, що відповідає вимогам ISO 27001:2022 щодо своєчасного й ефективного управління інцидентами інформаційної безпеки.

Зважаючи на визначний вплив запропонованого методу на відповідність стандарту ISO 27001:2022 потрібно також вказати, що вказаний метод дослідження кіберзлочинів може бути використаний для покращення контролів інформаційної безпеки системи менеджменту інформаційної безпеки при перехресному впровадженні стандартів. У Таблиці 3 представлено зіставлення, яке показує, як можна інтегрувати метод виявлення програм-вимагачів на основі ШІ та продемонструвати відповідність цим трьом критичним стандартам кібербезпеки.

Таблиця 3 – Відповідність фреймворкам кібербезпеки

Аспект відповідності	ISO 27001:2022	NIST CSF	CIS Critical Controls
Ідентифікувати та захистити	Управління активами Класифікація інформації	Управління активами Контроль доступу	Інвентаризація та контроль апаратних засобів Інвентаризація та контроль програмних активів
Управління ризиками	Оцінка та лікування ризиків	Оцінка ризиків Стратегія управління	Безперервне керування вразливістю

Аспект відповідності	ISO 27001:2022	NIST CSF	CIS Critical Controls
		ризиками	
Управління доступом	Управління доступом	Управління ідентифікацією та контроль доступу	Контрольований доступ на основі потреби знати
Процеси виявлення	Управління інцидентами інформаційної безпеки	Виявлення аномалій Постійний моніторинг безпеки	Безперервна оцінка вразливості
Відповідь і відновлення	Управління інцидентами інформаційної безпеки. Управління безперервністю бізнесу	Планування реагування Планування відновлення	Управління реагуванням на інциденти Захист даних
Цілісність системи та інформації	Безпека операцій. Безпека зв'язку	Процеси та процедури захисту інформації	Захист електронної пошти та веб-браузера
Захист інформації	Криптографія	Безпека даних	Захист від шкідливих програм
Обізнаність і навчання	Безпека людських ресурсів	Обізнаність і навчання	Навчання навичкам безпеки
Технічне обслуговування	Придбання, розробка та обслуговування системи	Технічне обслуговування	Обслуговування, моніторинг та аналіз журналів аудиту
Аудит і звітність	Внутрішній аудит	Процеси виявлення Захисні технології	Моніторинг і контроль облікових записів

Дотримуючись конкретних критеріїв і засобів контролю, перелічених у кожному стандарті, організація може гарантувати, що її заходи кібербезпеки, керовані штучним інтелектом, є комплексними, оновленими та відповідають визнаним найкращим практикам і стандартам.

Висновки

У даній статті визначено можливості використання моделей ШІ для дослідження кіберзлочинів у рамках системи менеджменту інформаційної безпеки критичної інфраструктури (CIISMS). Описується як алгоритми штучного інтелекту та аналітика даних, стають все більш ключовими у виявленні, аналізі та протидії кіберзагрозам і злочинам у критичній інфраструктурі. Проаналізовано роль штучного інтелекту в CIISMS для виявлення незвичайних шаблонів кібератак, що вказують на кіберзагрози, автоматизацію стратегій реагування та покращення процесу прийняття рішень в операціях з кібербезпеки. Аналіз характеристик програм-вимагачів дозволив зрозуміти їх поведінку, механізми поширення та еволюцію, що стало критично важливим для розробки методу дослідження кіберзлочинів. Порівняльний аналіз показав, що хоча кожен із розглянутих алгоритмів штучного інтелекту має свої переваги, комбінування можливостей Ізоляційного та Випадкового Лісу може забезпечити виявлення вірусів-вимагачів. Тому, дана стаття пропонує метод виявлення кіберзлочинів за типом вірусів вимагачів на основі алгоритмів Random Forest та Isolation Forest. Для подальших досліджень необхідно оцінити ефективність і точність запропонованого методу. Крім того, у статті підкреслюється важливість інтеграції ШІ з традиційними методами кібербезпеки для створення надійного механізму захисту. Ця інтеграція узгоджується з вимогами стандарту ISO 27001:2022, гарантуючи, що критична інфраструктура залишається стійкою проти складних кіберзагроз. Підводячи підсумок, дане дослідження пропонує метод

використання комбінації випадкового лісу (Random Forest) та Ізоляційного Лісу (Isolation Forest) для виявлення програм-вимагачів у критичній інфраструктурі ISMS та визначає як штучний інтелект трансформує розслідування кіберзлочинів у рамках CIISMS, пропонуючи розуміння його потенціалу та можливості застосування.

Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

Конкуруючі інтереси

Автори заявляють, що у них немає конкуруючих інтересів.

Список використаних джерел

1. Jack Hughes, Sergio Pastrana, Alice Hutchings, Sadia Afroz, Sagar Samtani, Weifeng Li, and Ericsson Santana Marin. 2024. The Art of Cybercrime Community Research. ACM Comput. Surv. 56, 6, Article 155 (June 2024), 26 pages. https://doi.org/10.1145/3639362.
2. Tvaronavičienė, Manuela; Plėta, Tomas; Della Casa, Silvia. Cyber security management model for critical infrastructure protection. In: Proceedings of the Selected papers of the International Scientific Conference Contemporary Issues in Business, Management and Economics Engineering. 2021. https://doi.org/10.3846/cibmee.2021.611.
3. Sarker, Iqbal H.; Furhad, Md Hasan; Nowrozy, Raza. Ai-driven cybersecurity: an overview, security intelligence modeling and research directions. *SN Computer Science*, 2021, 2: 1-18. https://doi.org/10.1007/s42979-021-00557-0.
4. TAO, Feng; Akhtar, Muhammad Shoaib; Jiayuan, Zhang. The future of artificial intelligence in cybersecurity: A comprehensive survey. *EAI Endorsed Transactions on Creative Technologies*, 2021, 8.28: e3-e3. https://doi.org/10.4108/eai.7-7-2021.170285.
5. Harun Oz, Ahmet Aris, Albert Levi, and A. Selcuk Uluagac. 2022. A Survey on Ransomware: Evolution, Taxonomy, and Defense Solutions. ACM Comput. Surv. 54, 11s, Article 238 (January 2022), 37 pages. https://doi.org/10.1145/3514229.
6. Cybersecurity Ventures Report on Cybercrime [Електронний ресурс] // eSentire. – URL: https://www.esentire.com/cybersecurity-fundamentals-defined/glossary/cybersecurity-ventures-report-on-cybercrime.
7. FBI Releases 2022 Crime in the Nation Statistics [Електронний ресурс] // FBI – URL: https://www.fbi.gov/news/press-releases/fbi-releases-2022-crime-in-the-nation-statistics.
8. Vidyarthi, Deepti, et al. Static malware analysis to identify ransomware properties. International Journal of Computer Science Issues (IJCSI), 2019, 16.3: 10-17. https://doi.org/10.5281/zenodo.3252963.
9. Aminanto, M. E., Ban, T., Isawa, R., Takahashi T. and Inoue, D. "Threat Alert Prioritization Using Isolation Forest and Stacked Auto Encoder With Day-Forward-Chaining Analysis", in IEEE Access, vol. 8, pp. 217977-217986, 2020, https://doi.org/10.1109/ACCESS.2020.3041837.
10. G. Apruzzese, M. Andreolini, M. Colajanni and M. Marchetti, "Hardening Random Forest Cyber Detectors Against Adversarial Attacks", in IEEE Transactions on Emerging Topics in Computational Intelligence, vol. 4, no. 4, pp. 427-439, Aug. 2020, https://doi.org/10.1109/TETCI.2019.2961157.
11. Ferrag, Mohamed Amine, et al. Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. *Journal of Information Security and Applications*, 2020, 50: 102419. https://doi.org/10.1016/j.jisa.2019.102419.

12. (2022) ISO/IEC 27001: Information security, cybersecurity and privacy protection – Information security management systems – Requirements. Available from : https://www.iso.org/standard/82875.html. https://doi.org/10.1016/j.jisa.2019.102419.
13. Fathurohman, Adrian; Witjaksono, R. Wahjoe. Analysis and Design of Information Security Management System Based on ISO 27001: 2013 Using ANNEX Control (Case Study: District of Government of Bandung City). *Bulletin of Computer Science and Electrical Engineering*, 2020, 1.1: 1-11. https://doi.org/10.25008/bcsee.v1i1.2.

References

1. Jack Hughes, Sergio Pastrana, Alice Hutchings, Sadia Afroz, Sagar Samtani, Weifeng Li, and Ericsson Santana Marin. 2024. The Art of Cybercrime Community Research. ACM Comput. Surv. 56, 6, Article 155 (June 2024), 26 pages. https://doi.org/10.1145/3639362.
2. Tvaronavičienė, Manuela; Plėta, Tomas; Della Casa, Silvia. Cyber security management model for critical infrastructure protection. In: Proceedings of the Selected papers of the International Scientific Conference Contemporary Issues in Business, Management and Economics Engineering. 2021. https://doi.org/10.3846/cibmee.2021.611.
3. Sarker, Iqbal H.; Furhad, Md Hasan; Nowrozy, Raza. Ai-driven cybersecurity: an overview, security intelligence modeling and research directions. *SN Computer Science*, 2021, 2: 1-18. https://doi.org/10.1007/s42979-021-00557-0.
4. TAO, Feng; Akhtar, Muhammad Shoaib; Jiayuan, Zhang. The future of artificial intelligence in cybersecurity: A comprehensive survey. *EAI Endorsed Transactions on Creative Technologies*, 2021, 8.28: e3-e3. https://doi.org/10.4108/eai.7-7-2021.170285.
5. Harun Oz, Ahmet Aris, Albert Levi, and A. Selcuk Uluagac. 2022. A Survey on Ransomware: Evolution, Taxonomy, and Defense Solutions. ACM Comput. Surv. 54, 11s, Article 238 (January 2022), 37 pages. https://doi.org/10.1145/3514229.
6. Cybersecurity Ventures Report on Cybercrime [Електронний ресурс] // eSentire. – Available from : https://www.esentire.com/cybersecurity-fundamentals-defined/glossary/cybersecurity-ventures-report-on-cybercrime.
7. FBI Releases 2022 Crime in the Nation Statistics [Електронний ресурс] // FBI – Available from : https://www.fbi.gov/news/press-releases/fbi-releases-2022-crime-in-the-nation-statistics.
8. Vidyarthi, Deepti, et al. Static malware analysis to identify ransomware properties. International Journal of Computer Science Issues (IJCSI), 2019, 16.3: 10-17. https://doi.org/10.5281/zenodo.3252963.
9. Aminanto, M. E., Ban, T., Isawa, R., Takahashi T. and Inoue, D. "Threat Alert Prioritization Using Isolation Forest and Stacked Auto Encoder With Day-Forward-Chaining Analysis", in IEEE Access, vol. 8, pp. 217977-217986, 2020, https://doi.org/10.1109/ACCESS.2020.3041837.
10. G. Apruzzese, M. Andreolini, M. Colajanni and M. Marchetti, "Hardening Random Forest Cyber Detectors Against Adversarial Attacks", in IEEE Transactions on Emerging Topics in Computational Intelligence, vol. 4, no. 4, pp. 427-439, Aug. 2020, https://doi.org/10.1109/TETCI.2019.2961157.
11. Ferrag, Mohamed Amine, et al. Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. *Journal of Information Security and Applications*, 2020, 50: 102419. https://doi.org/10.1016/j.jisa.2019.102419.
12. (2022) ISO/IEC 27001: Information security, cybersecurity and privacy protection – Information security management systems – Requirements. Available from : https://www.iso.org/standard/82875.html. https://doi.org/10.1016/j.jisa.2019.102419.
13. Fathurohman, Adrian; Witjaksono, R. Wahjoe. Analysis and Design of Information Security Management System Based on ISO 27001: 2013 Using ANNEX Control (Case Study: District of Government of Bandung City). *Bulletin of Computer Science and Electrical Engineering*, 2020, 1.1: 1-11. https://doi.org/10.25008/bcsee.v1i1.2.