COMPUTER SYSTEMS AND NETWORKS

Vol. 6, No. 1, 2024

DOI: https://doi.org/10.23939/csn2024.01.015

УДК 004.75; 004.8

РОЗРОБЛЕННЯ МЕТОДУ ДОСЛІДЖЕННЯ КІБЕРЗЛОЧИНІВ ЗА ТИПОМ ВІРУСІВ-ВИМАГАЧІВ З ВИКОРИСТАННЯМ МОДЕЛЕЙ ШТУЧНОГО ІНТЕЛЕКТУ В СИСТЕМІ МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

О. І. Гарасимчук, А. І. Партика, О. А. Нємкова, Я. Р. Совин, В. Б. Дудикевич

Національний університет "Львівська політехніка",
кафедра захисту інформації
E-mail: oleh.i.harasymchuk@lpnu.ua, andrii.i.partyka@lpnu.ua, olena.a.niemkova@lpnu.ua, yaroslav.r.sovyn@lpnu.ua, vdudykev@gmail.com

© Гарасимчук О. І., Партика А. І., Нємкова О. А., Совин Я. Р., Дудикевич В. Б., 2024

У цій статті автори зосередили увагу на аналізі можливостей застосування моделей штучного інтелекту для ефективного виявлення та аналізу кіберзлочинів. Розроблено та описано комплексний метод із використанням алгоритмів штучного інтелекту, таких як Випадковий ліс та Ізоляційний ліс, для виявлення програм-вимагачів, які є однією з основних загроз для систем управління інформаційною безпекою (ISMS) у сфері критичної інфраструктури. Результатом дослідження є визначення сумісності таких методів з вимогами ISO 27001:2022, акцентуючи на важливості інтеграції інноваційних технологій ШІ у наявні системи безпеки. Окрім того, в статті аналізуються потенційні переваги такої інтеграції, включно з відповідними вимогами міжнародних фреймворків інформаційної безпеки.

Ключові слова: Ізоляційний ліс, Випадковий ліс, Глибоке навчання, критична інфраструктура, система управління інформаційною безпекою, ISO 27001, кібербезпека, стандарт кібербезпеки, кіберзлочин, ISMS, віруси-вимагачі, siem, edr, моніторинг безпеки, антивірус, машинне навчання, комп'ютерні мережі, інформаційні системи.

Вступ

За останнє десятиліття кіберзлочинність значно зросла. Одним із основних 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 велике зацікавлення, і вони досліджувалися в багатьох дисциплінах із різними, часто досить новими підходами [1]. З огляду на дослідження, проведені провідними компаніями, що надають послуги інформаційної безпеки CISCO та IBM, система управління інформаційною безпекою критичної інфраструктури є пріоритетною ціллю кіберзлочинців.

Інтеграція штучного інтелекту (AI) в систему управління інформаційною безпекою критичної інфраструктури (CIISMS) є значним кроком вперед у боротьбі з кіберзлочинами. Оскільки кіберзагрози стають дедалі складнішими та відзначаються 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 цій статті розглядаються поточні дослідження, застосування та майбутні напрями штучного інтелекту для поліпшення виявлення та запобігання кіберзлочинам у межах 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 дає можливість 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, а саме: машинне навчання (ML), оброблення природної мови (NLP) і нейронні мережі, пропонують можливості для розпізнавання шаблонів, прогнозування потенційних загроз і автоматизації механізмів реагування. Їх впровадження в CIISMS зумовлене потребою попереджати, ідентифікувати та пом’якшувати кібератаки зі швидкістю та точністю, які значно 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 потрібна для забезпечення безперервної роботи критично важливих служб. Також системи дослідження кібератак на базі штучного інтелекту можуть аналізувати електронні листи та вебвміст у режимі реального часу, виявляючи та блокуючи спроби поширення шкідливого ПЗ, які часто передують серйознішим кібератакам на критичну інфраструктуру.

1. Огляд літературних джерел

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

Дослідження Джека Г’юза описує спільноти кіберзлочинців, які мають вирішальне значення для розроблення моделей штучного інтелекту, що передбачають і протидіють еволюції тактик програм-вимагачів [1]. Мануела Тваронавічене, Плета Томас 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 наявні 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 поліпшують здатність системи ефективно обробляти інциденти програм-вимагачів [3, 4]. Дослідження Харуна Оз, Ахмета Аріса, Альберта Леві та Сельчук Улуагач “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 пріоритетність загроз на основі штучного інтелекту, які підвищують ефективність моделей штучного інтелекту в сценаріях загроз у реальному часі [8, 9]. У своїй праці Апруцезе, Андреоліні, Коладжанні та Маркетті наголошують на потребі, 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 лише зміцнюють захист від програм-вимагачів, але й узгоджуються з глобальною практикою безпеки, забезпечуючи комплексну структуру для управління кібербезпекою в критичній інфраструктурі [12, 13].

2. Постановка завдання

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 наявні підходи до виявлення та запобігання кіберзлочинам часто неефективні щодо новітніх та вірусів-вимагачів, які швидко адаптуються. Використання алгоритмів штучного інтелекту (ШІ) може запропонувати нові можливості для поліпшення захисту інформаційних систем у цьому контексті. Однак дослідження, що вивчають застосування ШІ для боротьби з вірусами-вимагачами відповідно до ISO 27001:2022, залишаються обмеженими. Тому наше дослідження зосереджено на розробленні інноваційного методу використання алгоритмів ШІ для виявлення та нейтралізації вірусів-вимагачів, які загрожують інформаційній безпеці критично важливих інфраструктурних об’єктів, та визначення відповідності методу вимогам міжнародного стандарту ISO 27001:2022.

Мета статті. Метою цього дослідження є детальніший огляд можливостей алгоритмів ШІ для дослідження кіберзлочинів та розроблення методу виявлення вірусів-вимагачів у системах менеджменту інформаційної безпеки критичної інфраструктури, узгодженого зі стандартом ISO 27001:2022.

Завдання. Ця наукова стаття має такі завдання:

1) дослідити можливості алгоритмів штучного інтелекту, зокрема Ізоляційного лісу, Випадкового лісу та моделей Глибокого навчання;
2) дослідити характеристики програм-вимагачів;
3) провести порівняльний аналіз можливості виявлення програм-вимагачів алгоритмами Ізоляційного лісу, Випадкового лісу та моделями Глибокого навчання;
4) розробити метод дослідження кіберзлочинів за типом вірусів-вимагачів з використанням моделей штучного інтелекту в системі менеджменту інформаційної безпеки критичної інфраструктури;
5) визначити відповідність методу міжнародному стандарту ISO 27001:2022.

3. Огляд можливостей алгоритмів ШІ для дослідження кіберзлочинів

Зростання частоти та якості кібератак стимулює кіберсистеми з підтримкою ШІ. Зростання кількості інцидентів масштабних кібератак у всьому світі привернуло увагу організацій до потреби 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. Більшу частину кібератак здійснюють для отримання прибутку [4].

Детальний огляд літератури про використання ШІ сформовано у порівняльну табл. 1, дані для якої отримано з багатьох джерел, зокрема академічної літератури, галузевих звітів, практичних прикладів та думок 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

Модель / Особливість	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	Потребує 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, добре справляються із завданнями, що потребують 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 другого боку, неконтрольовані моделі, такі як Isolation Forest, здатні виявляти аномалії та нові шаблони без позначених даних, пропонуючи вирішальну перевагу у виявленні нових кіберзагроз, хоча і з тенденцією до більшої кількості помилкових спрацьовувань. Моделі глибокого навчання виділяються в аналізі складних типів даних, таких як зображення та послідовна інформація, потребуючи значної обчислювальної потужності та великих наборів даних, але забезпечуючи неперевершену глибину аналізу даних.

Разом ці моделі штучного інтелекту надають багатогранний набір інструментів для аналітиків безпеки, кожен зі своїми перевагами та обмеженнями, таким способом забезпечуючи комплексний підхід до виявлення, аналізу та пом’якшення кіберзагроз в інформаційних системах.

4. Характеристики програм-вимагачів

Останніми роками 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 є формою кіберзлочинності, яка заслуговує на особливу увагу через вплив на окремих осіб, підприємства та критичну інфраструктуру. Хоча вони становлять незначну частку кіберзлочинів, їх наслідки не прогнозовані, що заслуговує на цілеспрямований аналіз і стратегію реагування.

По-перше, атаки програм-вимагачів не прогнозовані. 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 із 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 становитимуть для світу 20 мільярдів доларів до 2031 року [6] проти 20 мільярдів доларів у 2020 році, що свідчить про швидке зростання економічного впливу цієї кіберзлочинності.

По-третє, атаки програм-вимагачів мають ширший суспільний вплив. Якщо атака спрямована на критично важливу інфраструктуру, наприклад служби охорони здоров'я, водоочисні споруди чи постачальників електроенергії, наслідки можуть виходити за межі 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 широкомасштабної 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 криптовалютах, які важко відстежити, ускладнюючи роботу правоохоронних органів.

Хоча інциденти з програмами-вимагачами можуть становити приблизно 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 наявність 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:

1) 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;

2) 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];

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

4) 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;

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

6) 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;

7) 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;

8) 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 вагоме значення для зменшення впливу атак програм-вимагачів. Організаціям і окремим особам треба навчитися розпізнавати ці ознаки та швидко реагувати, щоб стримати та усунути загрозу програм-вимагачів, зводячи до мінімуму втрату даних і час відновлення.

5. Порівняння можливостей виявлення програм-вимагачів алгоритмами ШІ

Щоб порівняти моделі штучного інтелекту для виявлення програм-вимагачів на основі визначених атрибутів, розглянемо кілька основних 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 подано порівняльну таблицю різних моделей ШІ, які зазвичай використовують для виявлення програм-вимагачів.

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 ІТ-іфраструктурі

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

6. Метод дослідження кіберзлочинів за типом вірусів-вимагачів із використанням моделі Isolation Forest та Random Forest у 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 потребує 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 способом багатошарову стратегію захисту.

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

Етап 1: Збір даних і попереднє оброблення. Треба 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 містить нормалізацію, оброблення значень, яких немає, 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 і 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 можна здійснювати за допомогою Xtrain, Ytrain, 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). Треба 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. Треба доповнити модель Random Forest Ізольованим лісом, щоб поліпшити 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 становити нові загрози програм-вимагачів. Для даних у реальному часі **x_realtime** обчислюємо:

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

b. IF_score(x_realtime) = IF(x_realtime) для визначення балів аномалій з Ізоляційного 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. Треба розгорнути навчені моделі для моніторингу мережевого трафіку та дій системи в реальному часі. Моделі мають 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 має автоматизувати початкові заходи стримування, щоб обмежити поширення атаки та повідомити персонал служби безпеки для подальшого розслідування. Для цього можна задати таку умову: якщо D(x_realtime) перевищує попередньо визначене порогове значення θ, потрібно ініціювати попередження та запустити протоколи відповіді.

Етап 6: Постійне навчання та оновлення. Треба регулярно оновлювати модель новими даними та аналізом загроз, щоб підтримувати її ефективність. Це містить 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 є потреба у проведенні майбутніх досліджень для аналізу ефективності запропонованого методу.

3. Результати дослідження

Результатами цього дослідження є встановлення відповідності 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:

1) **управління активами:** запропонований метод може ідентифікувати критично важливі дані та системи, які вагомі для діяльності організації, таким способом допомагаючи класифікувати та належно поводитися з активами відповідно до вимог ISO 27001:2022;

2) **контроль доступу:** виявляючи спроби несанкціонованого доступу або аномалії в поведінці користувачів, моделі Random Forest та Isolation Forest можуть сприяти посиленню контролю доступу, що є основною вимогою стандарту ISO 27001:2022;

3) **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;

4) **безпека зв'язку.** Аналізуючи мережевий трафік і журнали, метод ШІ допомагає визначити та зменшити ризики, пов'язані з переданням інформації, таким способом підтримуючи аспект безпеки ISO 27001:2022;

5) **придбання, розроблення та обслуговування системи:** розроблення та інтеграція моделей штучного інтелекту в ISMS демонструють відповідність вимогам ISO 27001:2022 щодо придбання,

розроблення та обслуговування системи, гарантуючи, що інформаційна безпека є невід'ємною частиною життєвого циклу системи, та можуть бути інтегровані у DevSecOps підхід [14];

6) **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.

З огляду на визначний вплив запропонованого методу на відповідність стандарту ISO 27001:2022 потрібно також вказати, що вказаний метод дослідження кіберзлочинів може бути використаний для поліпшення контролів інформаційної безпеки системи менеджменту інформаційної безпеки під час перехресного впровадження стандартів. У табл. 3 подано 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 ризиками	Безперервне керування вразливістю
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
Авдит і звітність	Внутрішній авдит	Процеси виявлення Захисні технології	Моніторинг і контроль облікових записів

Кожен стандарт має унікальні координаційні точки, але всі вони об'єднані спільною метою – покращення стану безпеки організацій, особливо в контексті критичної інфраструктури. 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 цій статті визначено можливості використання моделей штучного інтелекту (ШІ) для дослідження кіберзлочинів у межах системи менеджменту інформаційної безпеки критичної інфраструктури (CIISMS). Описано, як алгоритми штучного інтелекту та аналітика даних стають найголовнішими 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 дав можливість зрозуміти їх поведінку, механізми поширення та еволюцію, що стало критично важливим для розроблення 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 ця стаття пропонує метод виявлення кіберзлочинів за типом вірусів вимагачів на основі алгоритмів Random Forest та Isolation Forest. Для подальших досліджень треба оцінити ефективність і точність запропонованого методу.

Крім того, у статті підкреслено 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.

Підбиваючи підсумок, це 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, даючи розуміння його потенціалу та можливості застосування.

Список літератури

1. *Hughes Jack, Pastrana Sergio, Hutchings Alice, Afroz Sadia, Samtani Sagar, Li Weifeng, and Ericsson Santana Marin. (2024). The Art of Cybercrime Community Research. ACM Comput. Surv. 56, 6, Article 155 (June 2024), 26 pages. DOI:10.1145/3639362 (дата звернення: 01. 03. 2024).*

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. DOI: 10.3846/cibmee.2021.611 (дата звернення: 01. 03. 2024).*

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. DOI: 10.1007/s42979-021-00557-0 (дата звернення: 01. 03. 2024).*

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. DOI: 10.4108/eai.7-7-2021.170285 (дата звернення: 01. 03. 2024).*

5. *Oz Harun, Aris Ahmet, Levi Albert, and Selcuk Uluagac A. (2022). A Survey on Ransomware: Evolution, Taxonomy, and Defense Solutions. ACM Comput. Surv. 54, 11s, Article 238 (January 2022), 37 pages. DOI: 10.1145/3514229 (дата звернення: 01. 03. 2024).*

6. *Cybersecurity Ventures Report on Cybercrime [Електронний ресурс] // eSentire. – Режим доступу: https://www.esentire.com/cybersecurity-fundamentals-defined/glossary/cybersecurity-ventures-report-on-cybercrime (дата звернення: 01.03.2024).*

7. *FBI Releases 2022 Crime in the Nation Statistics [Електронний ресурс] // FBI – Режим доступу: https://www.fbi.gov/news/press-releases/fbi-releases-2022-crime-in-the-nation-statistics (дата звернення: 01. 03. 2024).*

8. *Vidyarthi Deepti, et al. Static malware analysis to identify ransomware properties. International Journal of Computer Science Issues (IJCSI), 2019, 16.3: 10–17. DOI: 10.5281/zenodo.3252963 (дата звернення: 01. 03. 2024).*

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, DOI: 10.1109/ACCESS.2020.3041837 (дата звернення: 01.03. 2024).*

10. *Apruzzese G., Andreolini M., Colajanni M. and Marchetti M. 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, DOI: 10.1109/TETCI.2019.2961157 (дата звернення: 01. 03. 2024).*

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. DOI: 10.1016/j.jisa.2019.102419 (дата звернення: 01. 03. 2024).*

12. *(2022). ISO/IEC 27001: Information security, cybersecurity and privacy protection — Information security management systems — Requirements. URL: https://www.iso.org/standard/82875.html. DOI:10.1016/j.jisa.2019.102419 (дата звернення: 01. 03. 2024).*

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. DOI:10.25008/bcsee.v1i1.2 (дата звернення: 01. 03. 2024).*

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

A. Partyka, O. Harasymchuk, E. Nyemkova, Y. Sovyn, V. Dudykevych

Lviv Polytechnic National University,
Information Security Department

© Harasymchuk O., Partyka A., Nyemkova E., Sovyn Y., Dudykevych V., 2024

In this article, the authors focused on analyzing the possibilities of using artificial intelligence models for effective detection and analysis of cybercrimes. A comprehensive method using artificial intelligence algorithms, such as Random Forest and Isolation Forest algorithms, is developed and described to detect ransomware, which is one of the main threats to information security management systems (ISMS) in the field of critical infrastructure. The result of the study is the determination of the compatibility of such methods with the requirements of ISO 27001:2022, emphasizing the importance of integrating innovative AI technologies into already existing security systems. In addition, the article analyzes the potential advantages of such integration, including compliance with the requirements of international information security frameworks.

Keywords: Isolation Forest, Random Forest, critical infrastructure, information security management system, ISO 27001, cyber security, cyber security standard, cybercrime, ISMS, ransomware, siem, edr, security monitoring, antivirus, machine learning, computer networks, information systems.