DOI: 10.25140/2411-5363-2024-3(37)-143-152
УДК 004.891

Максим Валерійович Міщенко

аспірант кафедри інформаційних технологій та програмної інженерії
Національний університет «Чернігівська політехніка» (Чернігів, Україна)
Email: max.mishchenko771@gmail.com. **ORCID**: https://orcid.org/0000-0001-9769-9759

ФУНКЦІОНАЛЬНА МОДЕЛЬ СИСТЕМИ ВИЯВЛЕННЯ ТА ПРОГНОЗУВАННЯ КІБЕРЗАГРОЗ ДЛЯ КОРПОРАТИВНИХ КОМП'ЮТЕРНИХ МЕРЕЖ З ВИКОРИСТАННЯМ ЕКСПЕРТНИХ ОЦІНОК

У роботі представлено функціональне моделювання системи виявлення та прогнозування кіберзагроз для корпоративних комп'ютерних мереж із використанням модуля експертних оцінок. У створеній моделі пропонується використовувати компоненти для виявлення та прогнозування кіберзагроз як джерело наповнення бази знань експертної системи, що в поєднанні з експертними оцінками та моделлю на основі теорії ігор, дозволить генерувати звіти та рекомендації щодо кібербезпеки. У роботі описано активності системи, ресурси та механізми виконання згідно зі специфікаціями IDEF0. Зроблено декомпозицію активності «виявлення та прогнозування кіберзагроз із використанням експертних систем» та «виявлення кіберзагроз та мережевих аномалій».

Ключові слова: *кібербезпека; експертні системи; функціональне моделювання; IDEF0; Теорія ігор.*
Рис.: 3. Бібл.: 17.

Актуальність теми дослідження. Забезпечення кібербезпеки в сучасному світі є актуальним як для окремих користувачів, так і для організацій та корпоративних мереж. Одним з підходів до управління та моніторингу кібербезпеки корпоративних мереж є створення експертних систем, що можуть бути адаптовані відповідно до конкретних конфігурацій корпоративних мереж та потенційних загроз з використанням експертних оцінок. Експертна система – це програмний засіб, що використовує знання експертів у певній предметній області для емуляції процесу міркування людини-експерта [1]. Використанням експертних систем представлено в багатьох дослідженнях у сфері кібербезпеки [2-7].

У своїх дослідженнях різні автори вивчають аспекти застосування експертних систем, як окремої сутності, проте мало робіт присвячено дослідженню розробки комплексного підходу, у якому експертна система містить інші методи та моделі виявлення та прогнозування кіберзагроз для наповнення бази знань. Такий підхід потенційно дозволить експертам більш точно оцінити ризики кібербезпеки та визначити стратегії їх вирішення на основі інформації про виявлені та прогнозовані кіберзагрози.

Постановка проблеми. Використання експертних систем, як окремої сутності для вирішення проблем кібербезпеки є досить детально дослідженим питанням, у той час як створення композиції методів, які б містили в собі компоненти виявлення та прогнозування кіберзагроз для наповнення бази знань експертних систем є мало дослідженою проблемою. Моделювання такого комплексного підходу може розширити можливості експертної системи та підвищити точність оцінки ризиків кібербезпеки та можливих протидій кіберзагрозам.

Мета дослідження. Метою дослідження є створення функціональної моделі та архітектури інформаційної системи, функціонал якої спрямований на виявлення та прогнозування кіберзагроз для корпоративних комп'ютерних мереж із використанням експертних систем. Для моделювання буде використана функціональна модель IDEF0.

Аналіз останніх досліджень та публікацій. Для адаптації під середовище виконання модулів виявлення та прогнозування кіберзагроз часто використовують нейронні мережі, статистичні моделі та інші методи штучного інтелекту. Наприклад, у своєму дослідженні A. M. S. N. Amarasinghe та W. A. C. H. Wijesinghe запропонували використовувати згорткову нейронну мережу (Convolutional Neural Network) для виявлення загроз та статистичну модель SARIMA для прогнозування загроз [8]. У роботі Shaukat Kamran та ін. дослідили можливість застосування моделей машинного навчання до задач виявлення спам e-mail,

класифікації шкідливого забезпечення та виявлення вторгнень 3-х типів: виявлення вторгнень на основі сигнатур, виявлення вторгнень на основі аномалій та гібридний підхід до виявлення вторгнень. Автори дійшли висновку, що до кожного з типів кіберзагроз мають бути застосовані різні окремі моделі машинного навчання. Зокрема, з виявленням спам email найкраще справилися моделі дерева рішень та Deep belief network (DBN) – глибока мережа переконань; з виявленням вторгнень найкраще справилась DBN; з виявленням шкідливого забезпечення найкраще справилась модель дерева рішень.

Використання експертних систем для вирішення проблем кібербезпеки є доволі поширеним і дослідженим. Наприклад, у своїй роботі Wirkuttis, N. та ін. [2] розглянули застосування експертних систем для формування реакції та відповіді на кіберзагрозу. Були проаналізовані 2 типи експертних систем: Case-Based Reasoning та Rule-Based Reasoning. У результаті дослідники дійшли висновку, що CBR системи здатні вивчати нові правила та модифікувати наявні, що, на відміну від RBR систем, дає їм змогу адаптуватись під динамічно змінювані середовища, якими є комп'ютерні мережі. Іншим прикладом є дослідження авторів Lakhno, V. та ін. [6], які запропонували модель адаптивної експертної системи, що базується на обчисленні інформаційного критерію на основі ентропії та критерію Kullback–Leibler для кластеризації атрибутів розпізнавання в комп'ютерних системах, генеруючи вхідну матрицю нечітких правил. Змодельована система показала точність виявлень від 76,5 до 99,1 %.

Як комплексний підхід до виявлення та прогнозування загроз для комп'ютерних мереж дослідники застосовують моделювання систем виявлення вторгнень – IDS. Наприклад, автори An L та ін. розробили архітектуру системи вторгнень, базуючись на алгоритмі ансамблю дерев рішень та фреймворку розподіленої обробки великих даних Spark [10]. Мотивацією дослідження стала проблема обробки великої кількості мережевих даних за мінімально можливий проміжок часу для вчасної реакції на кіберзагрози. Автори досягли результатів середнього часу виявлення загроз у 13,3 мс, та F1-score від 0,797 до 0,985. В іншому дослідженні, Ayuba John та ін. поставили задачу вирішення проблеми малої точності та великої кількості false-positive спрацювань деяких систем IDS, що пов'язано з великою розмірністю атрибутів мережевого трафіку. Як вирішення цієї проблеми автори запропонували використовувати техніку методу головних компонент PCA для зменшення розмірності атрибутів мережевого трафіку та ансамблеву модель AdaBoost для підвищення точності виявлення вторгнень. У результаті, автори отримали точність 92, 89 та 67,9 % на різних датасетах мережевого трафіку [11]. Проблему підвищення точності систем виявлення вторгнень також розглянули у своїй роботі Abed R.A. та ін. Використавши модель ridge класифікатору на тестовому наборі даних мережевого трафіку, автори досягли точності у 99,85 %. [12]. У роботі Sivasubramanian A. та ін. змоделювали систему виявлення вторгнень з використанням моделі нейронних мереж типу «автокодувальник», що після обробки мережевого трафіку, налаштування та тренування моделі видала результати у 79,18 % точності [13].

Також дослідники використовують методологію функціонального моделювання IDEF0 для моделювання комплексних систем у сфері кібербезпеки. Наприклад, Marko S. та ін. [14] створили модель IDEF0 системи виявлення та реакції на кіберзагрози, пов'язані з шахрайством з використанням методів штучного інтелекту, що дозволила виділити та деталізувати окремі процеси для вибудови стратегій захисту від AI шахрайства.

Виклад основного матеріалу. Модель IDEF0 – є абревіатурою, що означає ICAM DEFinition of Function Modelling. Концепти IDEF0 полягають у тому, що валідна активність повинна мати 5 ознак [15]:

1. Кожна активність має входи, які можуть бути вимогами, виходами інших процесів тощо.

2. Кожна активність використовує ресурси, які забезпечують виконання активності. До ресурсів можуть належати людські, матеріальні, нематеріальні ресурси тощо.

3. Активність має виконуватись згідно зі стандартом і керуватися механізмом контролю.

4. Активність здійснюється згідно з процесом для впливу на щось або маніпулювання чимось.

5. Активність має генерувати вихід або результат.

Першим етапом моделювання комплексної системи з виявлення та прогнозування кіберзагроз для корпоративної комп'ютерної мережі стало створення загальної функціональної моделі, що зображена на рис. 1.

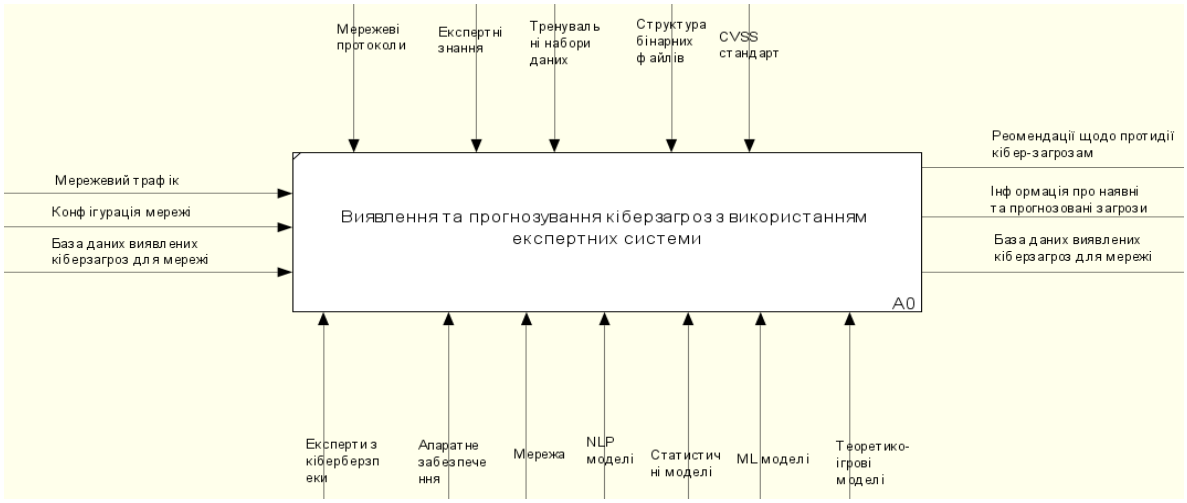

Рис. 1. Функціональна модель процесу виявлення та прогнозування кіберзагроз з використанням експертних систем

Вхідною інформацією для процесу виводу експертної системи було визначено мережевий трафік, конфігурація мережі та база даних виявлених кіберзагроз для мережі. Механізмами контролю є: експертні знання спеціалістів з кібербезпеки, що подаються на вхід рушія висновків експертної системи; мережеві протоколи - використовуються для визначення атак та аномалій трафіку; тренувальні набори даних – використовуються для тренування моделей машинного навчання та статистичних моделей для класифікації шкідливих бінарних файлів та прогнозування аномалій мережевого трафіку; структура бінарних файлів слугує вхідною інформацією для проведення класифікації та виявлення зловмисного ПЗ; CVSS стандарт слугує для оцінки рівня тяжкості виявлених загроз та побудови їх подання на вхід рушія висновків експертної системи. До механізмів керування відносяться експерти з кібербезпеки, апаратне забезпечення, мережа, NLP моделі, статистичні моделі, ML моделі та теоретико-ігрові моделі. На виході отримуємо інформацію про виявлені та прогнозовані кіберзагрози та рекомендації з протидії кіберзагрозам.

Мережевий трафік є найбільшим джерелом кіберзагроз для комп'ютерної мережі. Він може містити в собі шкідливі бінарні файли, аномальний трафік, загрози транспортного та прикладних рівнів. Необроблений мережевий трафік подається на вхід до модулів виявлення та прогнозування загроз. Модулі виконують декомпозицію мережевих пакетів, аналізуючи пакети на різних рівнях OSI. Виявлення загроз відбувається шляхом класифікації елементів трафіку, таких як бінарні файли, та статистичного аналізу трафіку, зокрема виявлення аномалій його кількісних компонент, таких як розмір мережевих пакетів.

Конфігурація мережі є одним з компонентів, що використовується для генерації рекомендацій з протидії загроз. Володіючи інформацією про наявні безпекові конфігурації для мережі та для кожного її вузла, можна робити висновки про необхідність коригування або додавання нових правил та вжиття інших заходів із протидії загрозам.

База даних виявлених кіберзагроз для мережі містить історичні дані про виявлені модулями виявлення кіберзагрози та слугує вхідними даними для побудови мереж Баєса з метою прогнозування ймовірностей майбутніх кіберзагроз.

Базовим механізмом контролю методу виявлення та прогнозування загроз є мережеві протоколи. Кібератаки використовують окремі конкретні протоколи, тому знання протоколів є основою для виявлення атак. Оскільки метод, що розроблюється, здатний працювати з обмеженою множиною кібератак, то відповідні обмеження накладаються й на протоколи, з якими буде працювати метод.

Тренувальні набори даних є механізмом контролю, що використовується моделями машинного навчання та статистичними моделями для попереднього тренування та валідації отриманих результатів. Такі набори даних представлені датасетами шкідливих та безпечних бінарних файлів та датасетами нормального та аномального мережевого трафіку.

Окремим механізмом контролю є структура бінарних файлів. Розроблювана система здатна виявляти шкідливі Linux ELF [17] та Windows PE файли за допомогою моделей машинного навчання. Як вхідні дані для виявлення подаються різні програмні секції файлів, що векторизуються за допомогою NLP технік та моделей та подаються на вхід до класифікатора.

Також як механізм керування використовується CVSS стандарт, що дозволяє експертам з кібербезпеки кількісно оцінити ступінь загрози, що несе та чи інша кібератака.

Експерти з кібербезпеки в розроблюваній системі являють собою людей, що мають знання в предметній області кіберзахисту та оцінюють ризики тих чи інших кібератак із застосуванням кількісної метрики CVSS [15]. Також експерти задають набір протидій атакам, застосовуючи які, рівень CVSS може бути зменшено або нейтралізовано.

Апаратне забезпечення є ресурсом та являє собою компонент корпоративної мережі, на якому розміщується експертна система. Може бути представлений у вигляді роутера або proxy-сервера. До апаратного забезпечення також належить вебсервер, який представляє інтерфейс експертної системи та серверне обладнання для тренування ML моделей.

Мережа є сукупністю елементів та механізмів, що забезпечують передачу та отримання трафіку. Вхідна інформація для системи виявлення та прогнозування загроз формується виходячи зі стану мережі та мережевого трафіку. Також для формування рекомендацій експертної системи важлива інформація про кожен вузол та загальну топологію мережі, що дає основу для конкретизації рекомендацій щодо протидії кібератакам.

NLP моделі використовуються для векторизації та класифікації байткодів та окремих секцій бінарних файлів, що дозволяє отримати висновок про шкідливість того чи іншого файлу та інформацію про тип вірусу в файлі, якщо він присутній.

Статистичні моделі дозволяють виявляти аномалії мережевого трафіку та робити прогнози щодо його кількісних показників. Інформація про виявлені та передбачені аномалії передається на вхід експертної системи, де експерти оцінюють їх за шкалою CVSS та встановлюють можливі протидії.

ML моделі використовуються для класифікації шкідливих бінарних Windows PE та Linux ELF файлів та для класифікації шкідливого мережевого трафіку. Результати виявлення загроз передаються вхід до експертної системи, де проходять експертну оцінку та слугують для формування рекомендацій з кіберзахисту.

Теоретико-ігрові моделі використовуються як рушій експертної системи. Базуючись на виявлених та прогнозованих кіберзагроз та експертних знаннях про ці загрози, формується матрична антагоністична стратегічна гра, гравцями якої виступають кіберзлочинець та експерт з кібербезпеки. Вирішуючи гру та знаходячи оптимальні стратегії, експертна система формулює звіт з доцільності застосування тої чи іншої стратегії експертом з кібербезпеки та рекомендації щодо пріоритетності застосування стратегій з кіберзахисту.

Інформація щодо виявлених та прогнозованих кіберзагроз повертається системою у вигляді звіту з деталізацією про час виявлення, горизонт прогнозування та інформацією про вузли мережі, для яких виявлено або прогнозовано кіберзагрози. Ця інформація базується на результатах роботи модулів із виявлення та прогнозування загроз. Дана інформація може бути використана системним адміністратором або працівниками департаменту з кіберзахисту як підґрунтя для створення власних стратегій протидії кіберзагрозам.

Рекомендації щодо протидії кіберзагрозам повертаються системою у вигляді звіту з відсортованими за пріоритетом застосування стратегій з кіберзахисту. Звіт формується на основі висновків про оптимальні стратегії кіберзахисту, отриманих рушієм висновків експертної системи. Експертна система використовує знання експертів та результати модулів виявлення і прогнозування кіберзагроз як базу знань, а теоретико-ігрові моделі як математичний апарат рушія висновків. Проаналізувавши цю інформацію, системний адміністратор або працівники департаменту з кіберзахисту можуть вжити запропоновані стратегії на свій розсуд.

Після кожної ітерації роботи експертної системи – а саме після кожного надходження оновленої інформації щодо виявлених або прогнозованих загроз, що оновлюється в реальному часі – база даних виявлених та загроз поповнюється інформацією про нові виявлені загрози.

Для більш детального огляду функціональної моделі було виконано її декомпозицію, що зображена на рис. 2. У результаті декомпозиції процесу виявлення та прогнозування загроз з використанням експертних систем, було виділено 7 робіт:

1. Розбір мережевого трафіку;
2. Виявлення мережевих аномалій та кіберзагроз;
3. Передбачення кіберзагроз та аномалій;
4. Заповнення бази знань експертами;
5. Формування стратегічної матричної гри;
6. Вирішення матричної гри;
7. Формування звітів з кіберзахисту.

Першою роботою процесу виявлення та прогнозування кіберзагроз та мережевих аномалій є розбір мережевого трафіку. Мережевий трафік сканується в реальному часі та аналізується відповідно до мережевого протоколу, який використовується для здійснення конкретних кібератак. Для виявлення мережевих аномалій використовуються часові ряди, сформовані з кількісних показників мережевого трафіку, таких як кількість отриманих та відправлених байтів, кількість вхідних та вихідних пакетів, ping time та ін. Для класифікації мережевого трафіку на шкідливий та безпечний виділяється інформація про ір-адреси, корисне навантаження, тип протоколу, довжину пакета. Для виявлення шкідливого ПЗ із пакетів виділяється файлове навантаження у вигляді сирих байтів. Парсер мережевого трафіку розміщується на роутері, що слугує вхідною точкою для всього мережевого трафіку. У результаті виконання даної роботи отримуємо корисні дані мережевого трафіку, що використовуються для виконання наступної роботи – передбачення кіберзагроз та мережевих аномалій.

Отримавши необхідні елементи мережевого трафіку, система виконує виявлення мережевих кіберзагроз та аномалій. Процес виявлення мережевих кіберзагроз відбувається в реальному часі та без втручання людини. Однак даний процес вимагає попереднього тренування моделей машинного навчання та статистичних моделей на тестових наборах даних. Тестові набори даних зберігаються та періодично оновлюються на окремому фізичному пристрої, що являє собою ftp сервер. Натреновані моделі для класифікації трафіку та виявлення аномалій розгортаються на мережевому обладнанні – роутері, разом з парсером мережевого трафіку, що дозволяє мінімізувати часові затримки обміну даними.

Моделі можуть дотреновуватись на нових даних, що дозволяє підвищити точність виявлення кіберзагроз та аномалій. Виявлені кіберзагрози та аномалії передаються на вхід до роботи «Передбачення кіберзагроз та аномалій».

Для передбачення кіберзагроз та аномалій використовуються мережі Баєса, що за допомогою обчислення умовної ймовірності дозволяють визначити ймовірність виникнення певних відомих загроз у майбутньому, володіючи інформацією про існуючі кіберзагрози.

Отримавши набір виявлених та передбачених кіберзагроз та мережевих аномалій, відбувається заповнення бази знань експертної системи генерації звітів з виявлених та прогнозованих кіберзагроз та рекомендацій щодо протидії наявним кіберзагрозам. Для оцінки рівня серйозності кіберзагроз використовується метрика CVSS. Механізмом виконання даного процесу є експерти з кібербезпеки – саме вони визначають значення CVSS для кожної загрози та можливі протидії їй. Зібравши необхідну експертну інформацію, система створює або оновлює платіжну матрицю гри, що використовується для визначення оптимальних стратегій кіберзлочинця та спеціаліста з кіберзахисту. Елементами платіжної матриці гри є значення CVSS для відповідної стратегії кібернападу та кіберзахисту.

Вирішення матричної гри дозволяє отримати чисті або змішані оптимальні стратегії для кіберзлочинця та спеціаліста з кіберзахисту. Механізмом виконання даного процесу є теоретико-ігрові моделі, а саме метод фіктивного розігрування Брауна-Робінсона.

Отримавши вирішення матричної гри в чистих або змішаних стратегіях, експертна система може сформулювати рекомендації з кіберзахисту. Також система виводить звіти по виявлених та прогнозованих загрозах на цей момент часу. При кожному виявлені нових загроз система обчислює матричну гру та оновлює рекомендації та звіти.

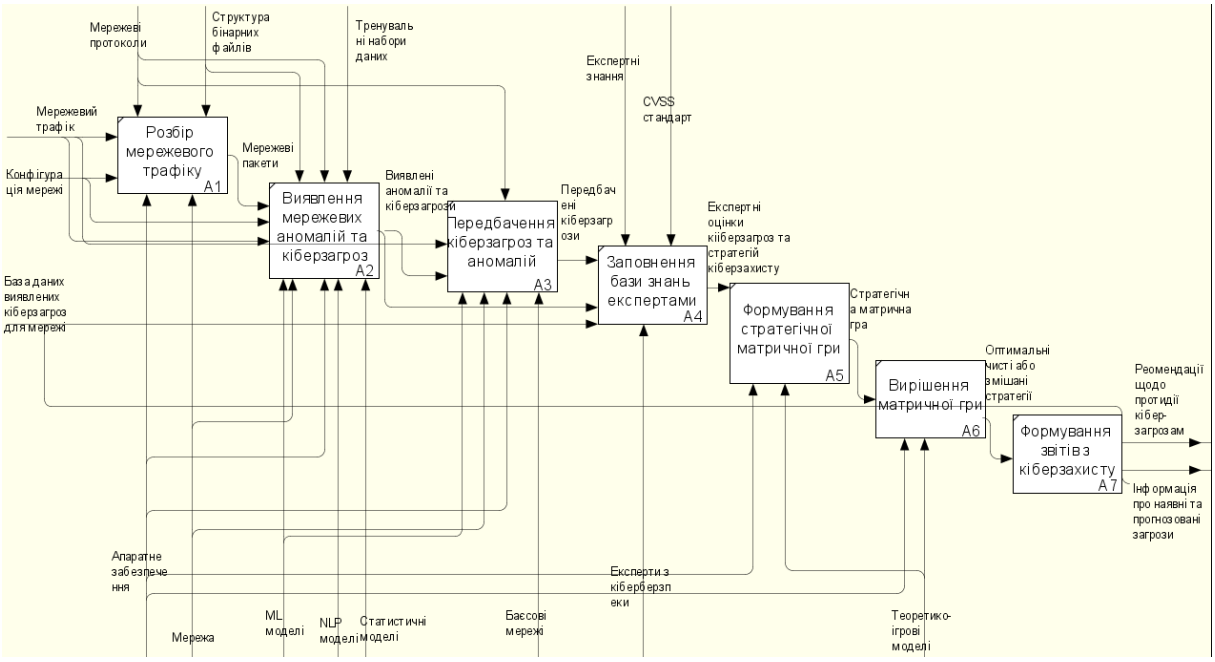

Рис. 2. Декомпозиція функціональної моделі «Виявлення та прогнозування кіберзагроз із використанням експертних систем»

Оскільки процес виявлення мережевих аномалій та кіберзагроз складається з декількох окремих робіт, доцільно виконати декомпозицію цього процесу. Декомпозиція процесу «Виявлення кіберзагроз і мережевих аномалій» представлена на рис. 3.

Для класифікації шкідливого мережевого трафіку використовуємо ML моделі, а саме модель градієнтного бустингу XGBoost, що натренована на датасеті мережевого трафіку з наявністю кібератак та безпечного трафіку. Механізмами керування даного процесу є датасет мережевого трафіку. Механізмами виконання є апаратне забезпечення у вигляді серверного обладнання для тренування та розгортування моделі, а також моделі-класифікатори XGBoost.

Для виявлення аномалій мережевого трафіку використовується EWMA-статистика та обчислення коефіцієнта Ляпунова. Вхідними даними для цього процесу є мережевий трафік, механізмом контролю є мережеві протоколи. На виході отримуємо виявлений аномальний мережевий трафік, інформація про який надходить до процесу прогнозування кіберзагроз.

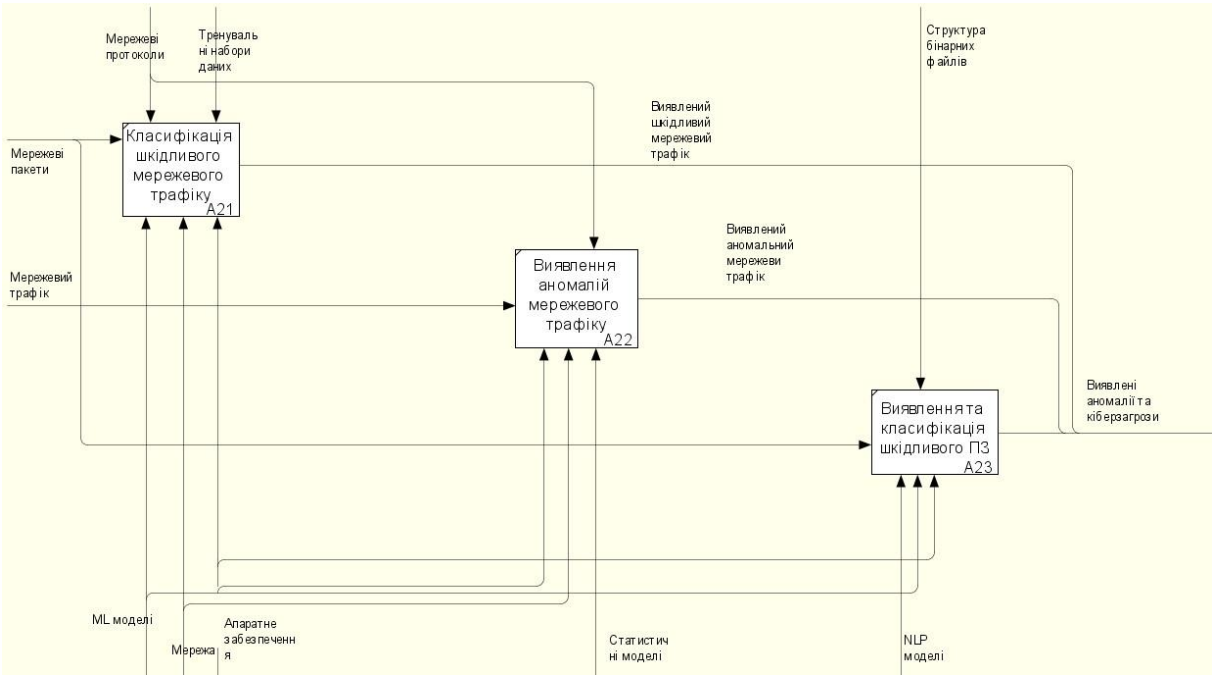

Рис. 3. Декомпозиція процесу «Виявлення кіберзагроз та мережевих аномалій»

Виявлення та класифікація шкідливого ПЗ відбувається на основі мережевих пакетів, з яких вилучається файлове навантаження – послідовність байтів, що являють собою файл. Як механізм керування для роботи використовується структура бінарних файлів, а як механізм виконання слугують NLP моделі для обробки та векторизації байткоду та окремих секцій файлу, апаратне забезпечення та ML моделі, що виконують класифікацію векторизованих файлів, виявляючи та класифікуючи шкідливі файли.

Висновки відповідно до статті. У результаті дослідження існуючих робіт із застосування експертних систем та методів штучного інтелекту до вирішення проблеми кібербезпеки, було виявлено, що більшість досліджень акцентують увагу на використанні даних методів окремо, не приділяючи уваги можливості композиції методів штучного інтелекту та експертних систем. Для вирішення цієї проблеми, було створено функціональну модель IDEF0, що репрезентує комплексний метод виявлення та прогнозування кіберзагроз із використанням експертних систем. Створена модель комплексної системи складається з модулів виявлення та прогнозування кіберзагроз для корпоративних комп'ютерних мереж, результати роботи яких є вхідними даними для експертної системи, що генерує звіти та рекомендації з кібербезпеки.

Список використаних джерел

1. Hu, S.D. Expert Systems for Software Engineers and Managers / S. D. Hu. – Chapman and Hall, New York, New York, 1987. – 303 p.

2. Wirkuttis, N. Artificial Intelligence in Cybersecurity / N. Wirkuttis, H. Klein // Cyber, Intelligence, and Security. – 2017. – № 1. – Pp. 103-119.

3. Hodhod, Rania. CyberMaster: An Expert System to Guide the Development of Cybersecurity Curricula / Rania Hodhod, Shamim Khan, Shuangbao Wang // International Journal of Online and Biomedical Engineering (iJOE). – 2019. – № 15. – Pp. 70-81. DOI: https://doi.org/10.3991/ijoe.v15i03.9890.

4. Goztepe, Kerim. Designing Fuzzy Rule Based Expert System for Cyber Security / Kerim Goztepe // International Journal of Information Security Science. – 2012. –№ 1. – Pp. 13-19.

5. Hodhod, Rania. Cybersecurity Curriculum Development Using AI and Decision Support Expert System / Rania Hodhod, Shuangbao Wang, Shamim Khan // International Journal of Computer Theory and Engineering. – 2018. – Vol. 10, №. 4. – Pp. 111-115. DOI: https://doi.org/10.7763/IJCTE.2018.V10.1209.

6. Development of adaptive expert system of information security using a procedure of clustering the attributes of anomalies and cyber attacks / V. Lakhno, Y. Tkach, T. Petrenko, S. Zaitsev, V. Bazylevych // Eastern-European Journal of Enterprise Technologies. – 2016. – Vol. 6, №. 9 (84). – Pp. 32-44. https://doi.org/10.15587/1729-4061.2016.85600

7. Donepudi, Praveen Kumar. Crossing point of Artificial Intelligence in cybersecurity / Donepudi, Praveen Kumar //American journal of trade and policy. – 2015. – Vol. 2.3 – Pp. 121-128.

8. AI Based Cyber Threats and Vulnerability Detection, Prevention and Prediction System / A. M. S. N. Amarasinghe, W. A. C. H. Wijesinghe, D. L. A. Nirmana, A. Jayakody and A. M. S. Priyankara // International Conference on Advancements in Computing (ICAC). – 2019. – Pp. 363-368. DOI: https://doi.org/10.1109/ICAC49085.2019.9103372.

9. Cyber Threat Detection Using Machine Learning Techniques: A Performance Evaluation Perspective / Kamran Shaukat, Suhuai Luo; Shan Chen; Dongxi Liu, All Authors // International Conference on Cyber Warfare and Security (ICCWS). – 2020. DOI: https://doi.org/10.1109/ICCWS48432.2020.9292388.

10. Design of distributed network intrusion prevention system based on Spark and P2DR models / L. An, J. Qiu, H. Zhang, C. Liu // Cluster Computing. – 2024. – Vol. 27. – Pp. 10757-10776. DOI: https://doi.org/10.1007/s10586-024-04487-3.

11.Ayuba John Enhanced intrusion detection model based on principal component analysis and variable ensemble machine learning algorithm / Ayuba John, Ismail Fauzi Bin Isnin, Syed Hamid Hussain Madni, Farkhana Binti Muchtar // Intelligent Systems with Applications. – 2024. – Vol. 24. – Pp. 2667-3053. DOI: https://doi.org/10.1016/j.iswa.2024.200442.

12. Abed, R. A. A modified CNN-IDS model for enhancing the efficacy of intrusion detection system / R. A. Abed, E. K. Hamza, A. J. Humaidi // Measurement: Sensors. – 2024. – № 35. – 101299, DOI: https://doi.org/10.1016/j.measen.2024.101299.

13. Sivasubramanian, A. Feature Extraction and Anomaly Detection Using Different Autoencoders for Modeling Intrusion Detection Systems / A. Sivasubramanian, M. Devisetty, P. Bhavukam // Arabian Journal for Science and Engineering. – 2024. – № 49(9). – Pp. 13061–13073. DOI: https://doi.org/10.1007/s13369-024-08951-5.

14.Ensuring Cybersecurity in the Modern World: Challenges from Artificial Intelligence-Based Fraud Posing a Threat to the Environment / S. Marko, Y. Tsaruk, H. Skhidnytska, M. Kryshtanovych, U. Nikonenko // Journal of Ecohumanism. – 2024. – № 3 (4). – Pp. 1436-1442. DOI: https://doi.org/10.62754/joe.v3i4.3673.

15.Філдінг, П. Д. Як керувати проєктами / Пол Дж. Філінг. – 2020. – 240 с.

16.Common Vulnerability Scoring System Version 4.0 [Electronic resource] // First.ORG. – 2023. – Access mode: https://www.first.org/cvss/v4-0/.

17.Mishchenko, M. Semantic analysis and classification of malware for UNIX-like operating systems with the use of machine learning methods / M. Mishchenko, M. Dorosh // Applied Aspects of Information Technology = Прикладні аспекти інформ. технологій. – 2022. – Vol. 5, № 4. – Pp. 371-386. DOI: https://doi.org/10.15276/aait.05.2022.25.

References

1. Hu, S. D. (2013). Expert Systems for Software Engineers and Managers. Switherland: Springer US. DOI: 10.1007/978-1-4613-1065-5

2. Wirkuttis, N. and Klein, H. (2017). Artificial Intelligence in Cybersecurity. *Cyber, Intelligence, and Security, 1,* 103-119.

3. Hodhod, R. & Khan, S. & Wang, S. (2019). CyberMaster: An Expert System to Guide the Development of Cybersecurity Curricula. *International Journal of Online and Biomedical Engineering (iJOE).* DOI: https://doi.org/10.3991/ijoe.v15i03.9890.

4. Goztepe, K. (2012). Designing Fuzzy Rule Based Expert System for Cyber Security. *International Journal of Information Security Science, 1,* 13-19.

5. Hodhod, R. & Wang, S. & Khan, S. (2018). Cybersecurity Curriculum Development Using AI and Decision Support Expert System. *International Journal of Computer Theory and Engineering, 10,* 111-115. DOI: https://doi.org/10.7763/IJCTE.2018.V10.1209.

6. Lakhno, V., Tkach, Y., Petrenko, T., Zaitsev, S., & Bazylevych, V. (2016). Development of adaptive expert system of information security using a procedure of clustering the attributes of anomalies and cyber attacks. *Eastern-European Journal of Enterprise Technologies, 6 (9(84),* 32–44. DOI: https://doi.org/10.15587/1729-4061.2016.85600.

7. Donepudi, P. K. (2015). Crossing point of Artificial Intelligence in cybersecurity. *American journal of trade and policy, 2.3,* 121-128.

8. Amarasinghe, A. M. S. N., Wijesinghe, W. A. C. H., Nirmana, D. L. A., Jayakody, A. and Priyankara, A. M. S. (2019). AI Based Cyber Threats and Vulnerability Detection, Prevention and Prediction System. International Conference on Advancements in Computing (ICAC), Malabe, Sri Lanka. P. 363-368. DOI: https://doi.org/10.1109/ICAC49085.2019.9103372.

9. Shaukat, K., Luo, S. & Chen, S. & Liu, D. (2020). Cyber Threat Detection Using Machine Learning Techniques: A Performance Evaluation Perspective. DOI: https://doi.org/10.1109/ICCWS48432.2020.9292388.

10.An, L., Qiu, J., Zhang, H., Liu, C. (2024). Design of distributed network intrusion prevention system based on Spark and P2DR models. *Cluster Computing, 27,* 10757–10776. DOI: https://doi.org/10.1007/s10586-024-04487-3.

11.John, A., Isnin, I. F. B., Madni, S. H. H., Muchtar, F. B. (2024). Enhanced intrusion detection model based on principal component analysis and variable ensemble machine learning algorithm. *Intelligent Systems with Applications, 24.* DOI: https://doi.org/10.1016/j.iswa.2024.200442.

12. Abed, R. A., Hamza, E. K., Humaidi, A. J. (2024). A modified CNN-IDS model for enhancing the efficacy of intrusion detection system. *Measurement: Sensors, 35.* art. no. 101299. DOI: https://doi.org/10.1016/j.measen.2024.101299.

13. Sivasubramanian, A., Devisetty, M., Bhavukam, P. (2024). Feature Extraction and Anomaly Detection Using Different Autoencoders for Modeling Intrusion Detection Systems. *Arabian Journal for Science and Engineering, 49(9),* 13061-13073. DOI: https://doi.org/10.1007/s13369-024-08951-5.

14. Marko, S., Tsaruk, Y., Skhidnytska, H., Kryshtanovych, M., Nikonenko, U. (2024). Ensuring Cybersecurity in the Modern World: Challenges from Artificial Intelligence-Based Fraud Posing a Threat to the Environment. *Journal of Ecohumanism, 3(4),* 1436-1442. DOI: https://doi.org/10.62754/joe.v3i4.3673.

15.Fielding, P. J. (2020). How to manage projects. Kogan Page.

16.Common Vulnerability Scoring System Version 4.0. (2023). First.ORG. URL: https://www.first.org/cvss/v4-0/.

17.Mishchenko, M., Dorosh, M. (2022). Semantic analysis and classifi-cation of malware for UNIX-like operating systems with the use of machine learning methods. *Applied aspects of information technologies, 5*(4)*,* 371-386. DOI: https://doi.org/10.15276/aait.05.2022.25.

Отримано 07.10.24

UDC 004.891

Maksym Mishchenko

postgraduate of the Department of Information Technologies and Software Engineering
National University «Chernihiv Polytechnic» (Chernihiv, Ukraine)
Email: max.mishchenko771@gmail.com. **ORCID**: https://orcid.org/0000-0001-9769-9759

FUNCTIONAL MODEL OF THE CYBER THREATS DETECTION AND PREDICTION SYSTEM FOR CORPORATE COMPUTER NETWORKS USING EXPERT ASSESMENTS

The use of expert systems as a separate entity for solving cyber security problems is a sufficiently detailed researched issue. In contrast, the creation of a composition of methods that would contain components of cyber threat detection and forecasting to fill the knowledge base of expert systems is a problem that is less researched. Modeling such a comprehensive approach can expand the capabilities of the expert system and increase the accuracy of assessing cyber security risks and possible countermeasures against cyber threats. In this work, we present functional modeling using IDEF0 diagrams of the cyber threat detection and forecasting system for corporate computer networks using expert assessments. In the created model, it is proposed to use components for detecting and predicting cyber threats as a source of filling the expert system's knowledge base, which, combined with expert assessments and the Game theory model, will generate reports and recommendations on cyber security. We suggest to use CVSS score of a cyber threats with or without countermeasures as a quantitative measure for the expert assessments. For generating cyber defense recommendations, we create a zero-sum matrix game which is solved with an iterative algorithm. CVSS assessments are used as the payoffs in the matrix game. Detection of network traffic anomalies using Chaos Theory and Ewma statistics, classification of malicious network traffic, and classification of malicious binary files are proposed as methods of threat detection. To predict the probabilities of network threats, the application of the Bayesian network is proposed. The work describes system activities, resources, and execution mechanisms according to IDEF0 specifications. Decomposition of the activity "detection and prediction of cyber threats using expert systems" and "detection of cyber threats and network anomalies" was made. As a result, we presented a model for detecting and predicting cyber threats using expert assessments, which allows us to expand the capabilities of the expert system for the assessment of cyber security risks and possible countermeasures against cyber threats.

Keywords: *cybersecurity; expert systems; functional modelling; IDEF0; Game theory.*

Fig.: 3. References: 17.

Міщенко М. В. Функціональна модель системи виявлення та прогнозування кіберзагроз для корпоративних комп'ютерних мереж з використанням експертних оцінок. *Технічні науки та технології.* 2024. № 3(37). С. 143-152.