УПРАВЛІННЯ В ТЕХНІЧНИХ СИСТЕМАХ

CONTROL IN TECHNICAL SYSTEMS

DOI: 10.20998/2079-0023.2025.01.02
УДК 004.056+004.8

А. І. ЛЕВТЕРОВ, кандидат технічних наук, професор, Харківський національний автомобільно-дорожній університет, професор кафедри комп'ютерних наук і інформаційних систем, м. Харків, Україна; e-mail: lai@khadi.kharkov.ua; ORCID: https://orcid.org/0000-0001-6586-1061
Г. А. ПЛЄХОВА, кандидатка технічних наук, доцентка, Харківський національний автомобільно-дорожній університет, завідувачка кафедри комп'ютерних наук і інформаційних систем, м. Харків, Україна; e-mail: plehovaanna11@gmail.com; ORCID: https://orcid.org/0000-0002-6912-6520
М. В. КОСТІКОВА, кандидатка технічних наук, доцентка, Харківський національний автомобільно-дорожній університет, доцентка кафедри комп'ютерних наук і інформаційних систем, м. Харків, Україна; e-mail: kmv_topaz@ukr.net; ORCID: https://orcid.org/0000-0001-5197-7389
А. О. ОКУНЬ, кандидат технічних наук, доцент, Національний технічний університет «Харківський політехнічний інститут», доцент кафедри комп'ютерного моделювання та інтегрованих технологій обробки тиском, м. Харків, Україна; e-mail: okunanton@gmail.com; ORCID: https://orcid.org/0000-0002-6467-4229

СИСТЕМА КОНТРОЛЮ ПОЛІТИКИ КІБЕРБЕЗПЕКИ З ЕЛЕМЕНТАМИ ШТУЧНОГО ІНТЕЛЕКТУ КОРПОРАТИВНОЇ МЕРЕЖІ ЗВ'ЯЗКУ

У сучасному цифровому просторі, де майже всі сфери життя тісно пов'язані з інтернетом, кібербезпека відіграє не просто важливу, а фундаментальну роль, стаючи невід'ємною складовою нашої реальності. Вона гарантує стабільне та безпечне функціонування різноманітних сервісів – від електронної пошти та онлайн-банкінгу до соціальних платформ і корпоративних мереж, які забезпечують життєдіяльність суспільства та економіки держав. Стрімкий розвиток штучного інтелекту у сфері кібербезпеки відкриває нові горизонти для покращення захисту даних, підвищення рівня безпеки інформаційних систем та створення ефективних механізмів протидії сучасним кіберзагрозам. Розроблена система належить до політики кібербезпеки з елементами штучного інтелекту корпоративної мережі зв'язку. Підвищення обґрунтованості формування і контролю політики кібербезпеки корпоративної мережі зв'язку за рахунок ідентифікації технік реалізації комп'ютерних атак з застосуванням штучного інтелекту та виявлення ситуації і взаємозв'язку вразливостей встановленого на елементах інфраструктури програмного забезпечення. Для досягнення поставленої мети необхідно розробити систему контроля політики кібербезпеки з елементами штучного інтелекту корпоративної мережі зв'язку. Ефективність розробленої системи розраховували шляхом порівняння коефіцієнтів Тейла для оцінки її валідності. Розроблена система обробляє та оцінює інформацію за допомогою штучного інтелекту, включаючи ідентифікацію компаратора, що дозволяє зрозуміти можливості та методи виконання кожної відомої комп'ютерної атаки. Він також використовує ситуаційний текстовий предикат для ідентифікації та аналізу ситуації кібератаки та прогнозування її траєкторії, визначення ймовірності кожної відомої атаки та порівняння її з ефективністю існуючих заходів захисту. Шляхом порівняння розрахованих коефіцієнтів Тейла системи з існуючим аналогом зроблено висновок, що обґрунтованість формування політики кібербезпеки з елементами штучного інтелекту в розробленій системі є вищою, ніж у аналога, що підтверджує досягнення запропонованого технічного результату. Використання штучного інтелекту в корпоративних мережах зв'язку дозволяє значно покращити процеси виявлення, аналізу та нейтралізації кіберзагроз, що сприяє більш оперативному та ефективному реагуванню на потенційні атаки. Завдяки цьому досягається високий рівень захисту від сучасних кіберзагроз, які постійно еволюціонують та стають дедалі складнішими. Інтеграція ШІ у систему кібербезпеки не лише зміцнює захисні механізми, а й підвищує загальну адаптивність до нових викликів, що виникають у динамічному цифровому середовищі. Таким чином, застосування штучного інтелекту у сфері кібербезпеки відкриває широкі перспективи для створення багаторівневої, надійної та гнучкої системи захисту, що є критично важливим фактором у забезпеченні цифрової безпеки як сьогодні, так і в майбутньому.

Ключові слова: кібербезпека, загрози, захист, корпоративні мережі, штучний інтелект, індекс Тейла.

Вступ. У сучасному цифровому просторі, де майже всі сфери життя тісно пов'язані з інтернетом, кібербезпека відіграє не просто важливу, а фундаментальну роль, стаючи невід'ємною складовою нашої реальності. Вона гарантує стабільне та безпечне функціонування різноманітних сервісів – від електронної пошти та онлайн-банкінгу до соціальних платформ і корпоративних мереж, які забезпечують життєдіяльність суспільства та економіки держав.

Зі зростанням обсягів передавання даних через мережі питання кібербезпеки стає дуже важливим. Комплексні заходи у цій сфері спрямовані на захист мережевих систем від несанкціонованого доступу, шкідливого програмного забезпечення (ПЗ), хакерських атак та інших загроз для стабільності і безпеки цифрових комунікацій. Надійне забезпечення конфіденційності, цілісності та доступності інформації під час її передавання є критично важливим як для окремих користувачів, так і для компаній. Кібербезпека охоп-

лює широкий спектр методів і технологій, спрямованих на захист інформаційних потоків [1].

Постановка задачі. Мета роботи – підвищення обґрунтованості формування і контролю політики кібербезпеки корпоративної мережі зв'язку за рахунок ідентифікації технік реалізації комп'ютерних атак (КА) з застосуванням штучного інтелекту (ШІ) та виявлення ситуації і взаємозв'язку вразливостей встановленого на елементах інфраструктури (ЕП) ПЗ.

Для досягнення поставленої мети необхідно розробити систему контроля політики кібербезпеки з елементами ШІ корпоративної мережі зв'язку.

Огляд літератури. У наш час передавання інформації в електронному вигляді є невід'ємною частиною діяльності як великих, так і малих підприємств, оскільки мережеві технології забезпечують швидкий і зручний обмін даними. Проте спосіб передавання супроводжується певними ризиками, оскільки інформація, що проходить через відкриті або недостатньо захищені мережі, може бути перехоплена, модифікована або використана в цілях, які можуть завдати шкоди організації. До того ж корпоративні інформаційні структури суттєво відрізняються від звичайних, оскільки мають складну архітектуру, що включає численні бази даних, розподілені та локальні системи, а також різнопланові бізнес-завдання. Така різноманітність відкриває ширші можливості для кіберзлочинців, які можуть використовувати вразливості технологічної інфраструктури для атак, що ставить перед організаціями нові виклики у сфері забезпечення кібербезпеки [1].

Фахівці виокремлюють п'ять ключових загроз для інформаційної безпеки корпоративних мереж, а саме:

- розкриття конфіденційної інформації;
- неправомірне втручання в роботу комп'ютерної системи (злам);
- виведення системи з ладу, зниження її працездатності;
- перевищення повноважень непривілейованим користувачем;
- знищення та спотворення інформації [1].

Стандарти безпеки активно впроваджуються в Україні, зокрема ISO/IEC 27001 [2], який є обов'язковим для всіх організацій незалежно від їхнього профілю, масштабу чи типу діяльності. Кібербезпека має критичне значення, оскільки злам корпоративної системи може спричинити не лише значні фінансові втрати, а й серйозні наслідки для користувачів [3].

Однією з найпоширеніших загроз для технічної інфраструктури та мереж є зловмисне ПЗ (Malware). Кіберзлочинці застосовують широкий спектр шкідливих програм, серед яких віруси, комп'ютерні хробаки, клавіатурні шпигуни та боти, з метою викрадення, пошкодження або знищення даних. Сучасне шкідливе ПЗ може не лише красти конфіденційну інформацію, а й блокувати доступ до файлів на пристрої жертви (програми-вимагачі), атакувати інформаційні системи, завдаючи шкоди всій мережевій інфраструктурі, або використовувати обчислювальні потужності пристроїв для розсилання спаму та підтримки процесів криптомайнінгу. Лише за першу половину 2023 року кількість атак, здійснених із використанням шкідливого ПЗ, сягнула 2,7 млрд. [4]. Крім того, глобальний рівень криптоджекінгу (неавторизованого видобутку криптовалюти через браузери жертв) побив усі попередні рекорди, досягнувши 332,3 мільйона випадків, що свідчить про колосальне зростання – 399 % у порівнянні з попередніми періодами [3].

Ведеться активна розробка та впровадження комплексних систем інформаційної безпеки [5]. Вони включають широкий набір організаційно-технічних заходів: від регламентації правил користування корпоративною мережею та розмежування рівнів доступу до інформаційних ресурсів і сервісів, а також встановлення та налаштування високоефективних апаратно-програмних комплексів [6–8].

З огляду на зростаючу складність кіберзагроз, використання ШІ в кібербезпеці набуває особливого значення. Сучасні методи та технології на основі ШІ є базовим елементом у вдосконаленні механізмів захисту, зокрема у сфері корпоративної кібербезпеки, що дозволяє ефективніше виявляти та нейтралізувати сучасні кіберзагрози [7].

Відомі системи комп'ютерної безпеки, які засновані, в тому числі, і на ШІ [8–10], які характеризуються тим, що система комп'ютерної безпеки оснащена пам'яттю і процесором, пов'язаним з пам'яттю. Крім того дана система комп'ютерної безпеки включає активний захист критичної інфраструктури за допомогою забезпечення багаторівневого захисту інформації в хмарній архітектурі (CIPR/CTIS), яка додатково включає довірену платформу. Ця платформа представляє собою мережу агентів, що повідомляють про діяльність хакерів, провайдера керованої мережі та послуг безпеки (MNSP). Вона забезпечує послуги та рішення щодо керованого безпечного шифрування, підключенням та сумісності, причому MNSP з'єднаний з довіреною платформою за допомогою віртуальної приватної мережі (VPN), яка надає канал зв'язку з довіреною платформою. Причому MNSP виконаний з можливістю аналізувати весь трафік у мережі підприємства. Цей трафік направляють до MNSP, який додатково включає логічний захист і миттєве реагування у реальному часі без створення баз даних (LIZARD). Вона дізнається про призначення та функцію зовнішнього коду та блокує його у разі наявності злого наміру або відсутності обґрунтованої мети, а також аналізує загрози самі по собі без звернення до минулих даних, штучні загрози безпеці (AST). Ці загрози являють собою гіпотетичний сценарій події в системі безпеки для перевірки ефективності правил безпеки. Творчий модуль, який входить до його складу, здійснює процес інтелектуального створення нових гібридних форм із існуючих форм, виявлення злого наміру. З цього модулю визначають взаємозв'язок інформації, виділяють зразки поведінки, що з системою безпеки, проводять регулярні фонові перевірки кількох підозрілих подій у системі безпеки, і, навіть, роблять спроби знайти взаємозв'язок між подіями, на перший погляд, не пов'язаними між собою. В модулі поведінки системи безпеки зберігаються та індексуються події в

системі безпеки, їх ознаки та відгук на них, причому відгуки є рішенням щодо блокування, так і з допуску. За допомогою модуля ітеративного зростання та розвитку інтелекту (I2GE), вивчають великі дані та розпізнають сигнатури шкідливого ПЗ, а також симулюють потенційні різновиди даного ПЗ шляхом поєднання AST з творчим модулем. А за допомогою пам'яті та сприйняття атаки, які засновані на критичному мисленні (CTMP), критично розглядають рішення щодо блокування або допуску інформації, а також забезпечують додатковий рівень безпеки шляхом вивчення перехресних даних, наданих I2GE, LIZARD та довіреною платформою, причому CTMP оцінює власний потенціал у формуванні об'єктивного рішення з цього питання і не нав'язує це рішення, якщо воно малонадійне [11].

Відома також система контролю політики безпеку елементів корпоративної мережі зв'язку [10], що містить:

- модуль збору даних, який дозволяє отримувати відомості від зовнішніх джерел даних про відомі вразливості ЕІ та внутрішніх джерел даних про активи інфраструктури мережі зв'язку;
- засоби зберігання інформації, що дозволяють формувати та зберігати групу структурованих даних;
- модуль управління даними, що дозволяє нормалізувати дані, що збираються модулем збору даних, забезпечуючи формування уніфікованого виду даних та формування атрибутивного складу залежно від типу ЕІ, а також формування профілю ЕІ, який містить атрибутивний склад ЕІ;
- модуль збагачення профілів ЕІ, виконаний з можливістю доповнення атрибутивного складу профілю ЕІ інформацією, яка включає інформацію про можливості мережевої взаємодії між активами інфраструктури, на підставі даних правил безпеки, правил трансляції та маршрутизації, визначених на мережевих елементах інфраструктури, інформацію про знайдені уразливості активів інфраструктури, дані про критичність функціонування логічних ЕІ та відомості про виявлені ризики, а також заходи щодо їх усунення;
- модуль аналітики, що дозволяє враховувати, аналізувати та здійснювати моніторинг зовнішнього периметра мережевої інфраструктури. Крім того модуль аналітики, дозволяє пошук за атрибутивним складом профілів активів, аналіз необроблених даних, що надходять із джерел даних управління ризиками за знайденими вразливістю, пошук та аналіз мережевих маршрутів між активами інфраструктури для визначення можливих шляхів розповсюдження загрози, а також розрахунок критичності вразливого активу інфраструктури за рахунок визначення впливу вразливостей на мережеву інфраструктуру та її функціонування. Модуль аналітики має режим усунення вразливостей, при якому виявляються активи інфраструктури для усунення знайдених на них вразливостей;
- модуль візуалізації, що забезпечує графічне подання оброблюваних даних, а також формування віджетів та/або звітів та/або інформаційних панелей;
- модуль адміністрування, який забезпечує управління політиками доступу, довідниками, налаштуваннями існуючих модулів системи;
- модуль інтеграції, що забезпечує передачу в уніфікованому форматі даних про КА у внутрішню інфраструктуру та забезпечує зв'язок із внутрішніми джерелами даних;
- модуль збору даних, що дозволяє отримувати відомості від внутрішніх джерел даних про склад та режими роботи засобів захисту від КА, а також зовнішніх джерел неструктурованих даних про раніше неописані техніки реалізації КА та зовнішніх джерел даних про відомі техніки реалізації КА;
- модуль обробки неструктурованих даних, що дозволяє за рахунок застосування алгоритмів аналізу тексту виділяти та формувати раніше неописані техніки реалізації КА із неструктурованих даних, розташованих на спеціалізованих інформаційних ресурсах;
- модуль збору відомостей про встановлене ПЗ, який здійснює інвентаризацію встановленого ПЗ на кожному засобі обробки, зберігання та передачі інформації, включаючи перелік ПЗ, версії ПЗ, версії отриманого оновлення ПЗ, загальних займаних кластерів у довгостроковій та оперативній пам'яті, загальних протоколів взаємодії та загальних файлів;
- модуль формування структури взаємодії ПЗ між собою, що дозволяє на основі визначення загальних зайнятих кластерів у довгостроковій та оперативній пам'яті, загальних протоколів взаємодії та загальних файлів визначити можливість взаємодії між собою;
- модуль аналізу поверхні захисту, що дозволяє зіставити відомі вразливості елементів інфраструктури мережі та засоби захисту від КА;
- модуль адміністрування, який додатково здійснює формування пропозицій щодо зміни політики безпеки, доповнення засобів захисту, оновлення застосовуваного ПЗ та/або зміни його налаштувань та конфігурації.

Недоліком цих систем є низька обґрунтованість формування і контролю політики безпеки корпоративної мережі зв'язку через недостатність обліку технік реалізації комп'ютерних мережних атак та взаємозв'язку вразливостей, встановленого на ЕІ, ПЗ.

Матеріали і методи. У якості аналогів системи контролю політики кібербезпеки корпоративної мережі зв'язку, були взяті системи представлені в [8–10] з доповненням елементами ШІ. На рис. 1 представлена структурна схема розробленої системи.

Розроблена система складається з модуля збору даних (1.4), з'єднаного через загальну інформаційну шину (1.5) з зовнішніми джерелами даних (1.2) про відомі вразливості ЕІ (наприклад, MaxPatrol, Tenable, Qualys, Rapid7 Nexpose, Nmap, Acunetix та ін.), які, у свою чергу, пов'язані з джерелом інформації (1.1), з внутрішніми джерелами даних (1.3) про активи інфраструктури мережі зв'язку (SCCM, uCMDB, HPSM, EMM (Enterprise Mobility Management – AirWatch), AD (Active Directory)), локальні сенсори та ін., із зовнішніми джерелами неструктурованих даних (2.1) та з зовнішніми джерелами даних про відомі техніки реалі-

зації КА (2.2), з модулем збору відомостей про встановлене ПЗ (2.4), а також із засобом зберігання інформації (1.6).

Засіб зберігання інформації (1.6) через модуль інтеграції (1.12) та загальну інформаційну шину (1.5) надає доступ до модуля управління даними (1.7), модуля збагачення профілів ЕІ (1.8), модуля аналітики (1.9), що дозволяє враховувати, аналізувати та здійснювати моніторинг зовнішнього периметра мережевої інфраструктури, пошуку за атрибутивним складом профілів активів, аналізу необроблених даних, що надходять із джерел даних управління ризиками за знайденими вразливістю, пошуку та аналізу мережевих маршрутів між активами інфраструктури для визначення можливих шляхів розповсюдження загрози, розрахунку критичності вразливого активу інфраструктури за рахунок визначення впливу вразливостей на мережеву інфраструктуру та її функціонування, а також режиму усунення вразливостей, при якому виявляються активи інфраструктури для усунення знайдених на них вразливостей, модулем обробки неструктурованих даних (2.3), модулем формування структури взаємодії ПЗ між собою (2.5), модулем аналізу поверхні захисту (2.6), модулем формування поверхні атаки (2.7).

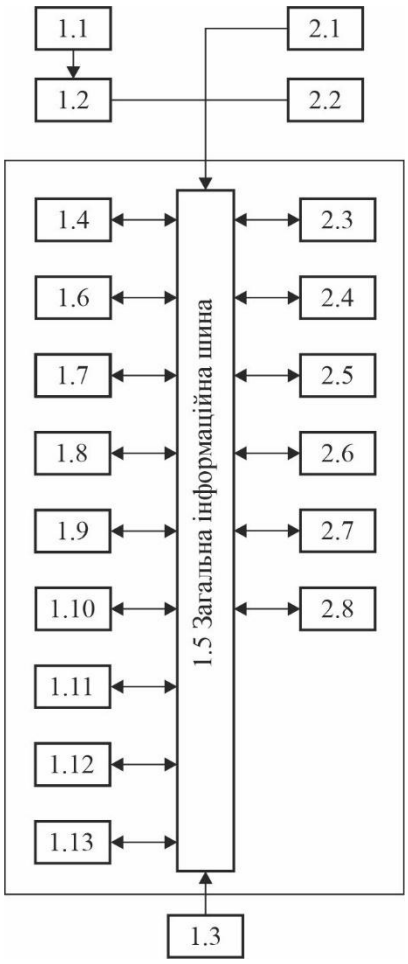

Рис. 1. Структурна схема системи контролю політики кібербезпеки із застосуванням ШІ корпоративної мережі зв'язку

Модуль компараторної ідентифікації (1.13) через загальну інформаційну шину (1.5) пов'язаний з модулем обробки неструктурованих даних (2.3), а модуль ситуаційно-текстового предикату (2.8) через загальну шину інформації (1.5) пов'язаний з модулем аналізу поверхні захисту (2.6).

Також засіб зберігання інформації (1.6) з'єднаного через загальну інформаційну шину (1.5) з модулем візуалізації (1.10) та модулем адміністрування (1.11) політики безпеки корпоративної мережі зв'язку.

Система контролю політики безпеки елементів корпоративної мережі зв'язку функціонує наступним чином. Із засобів передачі управляючих команд від модуля збору даних із джерел (1.4) дані надходять на внутрішні джерела даних про активи корпоративної мережі зв'язку (1.3) з метою інвентаризації ЕІ мережі. Вони включають відомості про застосовувані засоби обробки, зберігання та передачі інформації, їх технічні характеристики, фізичні та логічні сполуки ЕІ між собою, значення використовуваних інформаційних потоків та пропускної спроможності ліній зв'язку.

Модуль збору відомостей про встановлене ПЗ (2.5) розміщений з метою отримання відомостей про встановлене на кожному ЕІ ПЗ включаючи відомості про версії ПЗ, версії оновлень, загальних займаних кластерів у довгостроковій та оперативній пам'яті, загальних протоколів взаємодії та загальних файлів, а також склад і режими роботи засобів захисту від КА встановлених на кожному з ЕІ.

Зовнішні джерела даних про вразливості (1.2) з метою отримання атрибутів описують загальновідомі вразливості інформаційної безпеки (CVE). Зовнішні джерела даних про техніки реалізації КА (2.2) встановлені з метою отримання формалізованих відомостей про порядок дій порушника (наприклад, MITRE ATT&CK). Зовнішні джерела про неструктуровані дані про раніше неописані техніки реалізації КА (2.1), наприклад спеціалізованих інформаційних ресурсів (наприклад, ptsecurity.com, baksdao.com), розміщені з метою отримання текстового опису реалізації КА.

Після отримання текстового опису реалізації КА у модулі обробки неструктурованих даних (2.3) із застосуванням компараторної ідентифікації (1.13) виявляють внутрішні структури знайдених предикатів, що характеризують ті чи інші деталі механізму атаки, і далі з використанням спеціалізованого ПЗ розпізнавання та аналізу текстових документів обробляється, зіставляється та створюється формалізоване уявлення реалізації КА у вигляді послідовності вразливостей, що реалізуються. У часі кожна кібератака обмежена тривалістю її спостереження. Атака обмежуються також і її спрямованістю. Сприйняття атаки обмежується також рівнем ПЗ та кваліфікацією персоналу, обсягом його знань, спрямованістю його інтересів. У ролі текстів можуть виступати мовні повідомлення, оператори чи команди. Важливо виконати роботу з формального опису перетворення будь-яких повідомлень в тексти, що містяться в них, і далі, застосовуючи алгебру ситуаційно-текстових предикатів (2.8), математично висловити предикати.

Після отримання відомостей про склад встановленого ПЗ на кожному ЕІ та порядок його взаємодії між собою в модулі формування структури взаємодії ПЗ (2.6) формується граф, що репрезентує процес перетворення інформації на моделі взаємодії відкритих систем (МВВС). Вершинами графа є компоненти на кожному з рівнів МВВС, ребрами графа описують можливі процеси взаємодії між ПЗ. Сформований граф записується у відповідну комірку бази даних.

Після отримання відомостей про склад ЕІ, фізичні та логічні сполуки цих елементів, у модулі аналітики (1.9) формується граф, що відображає переміщення інформації між ЕІ. Сформований граф записується у відповідну комірку бази даних.

Після отримання відомостей про техніку реалізації КА від зовнішніх джерел даних про КА і модуля обробки неструктурованих даних) в модулі формування поверхні атаки (2.7), кожна з технік, що експлуатуються, зіставляються з вразливостями (див., наприклад, табл. 1).

Після заповнення баз даних про склад ЕІ, структуру мережі, відомі вразливості, застосовуваних засобів захисту від КА та технік реалізації КА, у модулі аналізу поверхні захисту (2.6), сформовані раніше графи доповнюються та уточняються таким чином, що вершини графа зіставляються з базою відомих вразливостей та перейменовуються згідно з класифікацією CVE (всі вершини графа, яким не присвоєна нумерація CVE виключаються з графа), вага вершини визначається характеристиками застосовуваних засобів захисту, що забезпечують захист на певному рівні МВВС заданого ПЗ від КА, а ребрами графа є переходи між вразливістю під час реалізації відомих технік КА.

Далі у модулі аналітики (1.9) з використанням сформованого у модулі аналізу поверхні захисту (2.6) графа розраховується ймовірність реалізації кожної з відомих КА.

Якщо розраховані значення реалізації КА перевищують допустимі значення, у модулі аналітики (1.9) формують пропозиції щодо застосування додаткових засобів захисту від КА, оновлення застосованого ПЗ та/або зміни налаштувань та режимів роботи ПЗ.

На підставі зібраних внутрішніми джерелами даних про активи (1.3) модуль збагачення профілів ЕІ (1.8) визначає критичність кожного з ЕІ для функціонування елементів системи та мережі в цілому.

На підставі зібраних зовнішніми джерелами неструктурованих даних (2.1), зовнішніх джерел даних про техніки реалізації КА (2.2) та модуля збору відомостей про встановлене ПЗ (2.4) у модулі збагачення профілів (1.8) формуються базові профілі для кожного ЕІ.

Модуль управління даних (1.7) забезпечує нормалізацію даних та формування профілю атрибутивного складу ЕІ в залежності від його типу.

Модуль інтеграції (1.10) забезпечує взаємодію всієї системи з джерелами даних.

Модуль візуалізації (1.11) забезпечує подання оброблюваних та збережених у базах даних у вигляді таблиць, графіків, віджетів та/або інформаційних панелей. Модуль візуалізації (1.11) забезпечує формування звітів.

Модуль адміністрування (1.12) забезпечує управління політиками доступу, довідниками, налаштуваннями існуючих модулів системи та, зокрема, забезпечує управління інформацією про користувачів, управління політиками доступу, видачу токенів для доступу до API, управління словниками (облік підмереж периметра та належність їх до територіального блоку та FW, словник ПЗ, який формується за результатами збору профілів активів і наступним накладенням на відповідні CVE-ідентифікатори вразливостей).

Під час експлуатації системи модуль збору даних з джерел (1.1) за допомогою передачі керуючих команд із заданою періодичністю на внутрішні джерела даних про активи мережі (1.3) проводить повторну інвентаризацію мережі з метою виявлення змін у структурі мережі, додавання ЕІ та/або установки ПЗ на ЕІ. У модулі збагачення профілю (1.8) здійснюється порівняння базових профілів ЕІ з профілями ЕІ, що зазнали змін, після чого приймається рішення про повторні розрахунки в модулі аналізу поверхні захисту (2.6), з подальшими діями в модулі аналітики (1.9).

У ході експлуатації системи модуль збору даних з джерел (1.1) за допомогою передачі керуючих команд із заданою періодичністю на зовнішні джерела даних про вразливості (1.2), зовнішні джерела неструктурованих даних (2.1) і зовнішні джерела даних про техніки реалізації КА (2.2) виявляють зміни в техніках реалізації КА та уточнюють у модулі формування поверхні атаки (2.4) вихідні дані. система з використанням елементів ШІ здійснює обробку та оцінку

Таблиця 1 – Зіставлення технік реалізації КА з вразливостями

T1138: Application Shimming	CVE-2019-0863 (Microsoft Windows Elevation of Privilege Vulnerability) CVE-2016-0092 (Microsoft Windows Elevation of Privilege Vulnerability) CVE-2016-0091 (Microsoft Windows Elevation of Privilege Vulnerability) CVE-2016-0090 (Microsoft Windows Elevation of Privilege Vulnerability) CVE-2016-0088 (Microsoft Windows Elevation of Privilege Vulnerability)
T1144: Rootkit	CVE-2019-1405 (Microsoft Windows Win32k Elevation of Privilege Vulnerability) CVE-2018-1038 (Microsoft Windows Elevation of Privilege Vulnerability) CVE-2018-1037 (Microsoft Windows Elevation of Privilege Vulnerability) CVE-2016-7255 (Microsoft Windows Elevation of Privilege Vulnerability) CVE-2016-7254 (Microsoft Windows Elevation of Privilege Vulnerability)
T1170: Mshta	CVE-2017-0199 (Microsoft Office/WordPad Remote Code Execution Vulnerability) CVE-2016-3298 (Microsoft Windows Scripting Engine Remote Code Execution Vulnerability) CVE-2016-3297 (Microsoft Windows Scripting Engine Remote Code Execution Vulnerability) CVE-2016-3296 (Microsoft Windows Scripting Engine Remote Code Execution Vulnerability)

інформації за допомогою модуля компараторної ідентифікації (1.13), який дозволяє визначити можливі техніки реалізації кожної з відомих КА. Додатково застосовується модель ситуаційно-текстового предикату (2.8), що дає змогу ідентифікувати поточну ситуацію з кібератакою, враховуючи її траєкторію реалізації. На основі цього система оцінює ймовірність реалізації кожної з атак та виконує порівняння з наявними можливостями ефективних засобів захисту. Уточнені дані обробляються в модулі аналізу поверхні захисту (2.6) і передаються в модуль збагачення профілю (1.8), де здійснюється порівняння базових профілів ЕІ з профілями ЕІ, що зазнали змін, після чого приймається рішення про повторні розрахунки в модулі аналізу поверхні захисту (2.7) з подальшими діями в модулі аналітики (1.9).

Експерименти. Розрахунок ефективності розробленої системи проводився як і в [10] , а саме – оцінка обґрунтованості проводиться шляхом порівняння коефіцієнтів Тейла [12]:

$$v = \frac{\sqrt{\sum_{i=1}^{T}\left(P_i - A_i\right)^2}}{\sqrt{\sum_{i=1}^{T}\left(A_i\right)^2}}, \qquad (1)$$

де T – загальна кількість ситуацій з КА; P_i та A_i – прогнозоване та фактичне (реальне) значення ймовірності реалізації КА на *i*-му кроці відповідно.

Якщо прогнозування є абсолютно точним (випадок ідеального прогнозу), то всі $P_i = A_i$, а $v = 0$. Коефіцієнт Тейла приймає значення одиниці ($v = 1$), коли точність прогнозування не вища, ніж у наївної моделі (наприклад, припущення нульового приросту), а отже, прогноз не має переваг, у порівнянні з екстраполяцією незмінності приростів, тобто середньоквадратична помилка залишається такою ж. Якщо ж прогнозування призводить до ще більшої похибки, ніж припущення про незмінність досліджуваного явища, то $v > 1$.

Зауважимо, що як і в [10, 12], в розробленій системі додатково обробляються та оцінюються відомості про реалізацію КА, які отримані від зовнішніх джерел даних про реалізацію КА та неструктурованих даних, і навіть даних про взаємозв'язок ПЗ встановленого кожному ЕІ. Якщо, наприклад, для однієї з атак прогнозована ймовірність дорівнює 3, а фактична – 6, то:

$$v^{\text{система}} = \frac{\sqrt{(3-6)^2}}{\sqrt{(6)^2}} = 0,5. \qquad (2)$$

Пропонована система оцінює ймовірність реалізації кожної з атак та виконує порівняння з наявними можливостями ефективних засобів захисту. Вона може обробляти більше інформації та типів атак, тобто для однієї з атак при $P_i = 6$, а $A_i = 8$:

$$v^{\text{система}} = \frac{\sqrt{(6-8)^2}}{\sqrt{8^2}} = 0,25. \qquad (3)$$

Далі проводимо порівняння розрахованих коефіцієнтів Тейла для представленої в [10, 12] та розробленої системи:

$$0,25 < 0,5. \qquad (4)$$

Результати. Зі зробленого порівняння розрахованих коефіцієнтів Тейла для системи, представленої в [10, 12] та розробленої системи, висновок, що обґрунтованість формування політики кібербезпеки з елементами ШІ заявленої системи нижче, ніж у [10, 12], що підтверджує досягнення запропонованого технічного результату.

Висновки. Впровадження штучного інтелекту в корпоративні мережі зв'язку дозволяє значно підвищити ефективність виявлення, аналізу та реагування на кіберзагрози, що сприяє посиленню захисту від сучасних кібератак. Завдяки інтеграції ШІ у сферу кібербезпеки зростає рівень безпеки мережевих систем, а також покращується здатність організацій оперативно адаптуватися до нових викликів цифрового середовища. Таким чином, використання ШІ у кібербезпеці відкриває широкі перспективи для створення більш надійних та ефективних механізмів протидії кіберзагрозам, що відіграє ключову роль у забезпеченні інформаційної безпеки в майбутньому.

Список використаної літератури

1. Організація каналу передачі даних для бізнесу. *GigaTrans Телеком оператор*. URL: https://gigatrans.ua/ua/services/organizaciya-kanala-peredachi-dannuh. (дата звернення: 20.01.2025).
2. *ДСТУ ISO/IEC 27001:2023 Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги (ISO/IEC 27001:2022, IDT)* / Нац. стандарт України. Київ: ДП «УкрНДНЦ», 2022. 26 с.
3. Безпека. *CityHost*. URL: https://cityhost.ua/uk/blog/bezopasnost/2/. (дата звернення: 20.01.2025).
4. 2024 SonicWall Cyber Threat Report. *Marlin Communications*. URL: https://marlincomms.co.uk/wp-content/uploads/2024/03/SonicWall-Marlin-Cybersecurity-Threat-Report-compressed.pdf. (дата звернення: 20.01.2025).
5. Грайворонський М. В., Новіков О. М. *Безпека інформаційно-комунікаційних систем*. Київ: Видавнича група BHV, 2009. 608 с.
6. Кучернюк П. В. Методи і технології захисту комп'ютерних мереж (фізичний та канальний рівні). *Мікросистеми, Електроніка та Акустика*. 2017. Т. 22, № 6(101). С. 64–70.
7. Smelyakov K., Chupryna A., Darahan D., Midina S. Effectiveness of modern text recognition solutions and tools for common data sources. *CEUR Workshop Proceedings*. 2021. Vol. 2870. P. 154–165.
8. Smelyakov K., Pribylnov D., Martovytskyi V., Chupryna A. Investigation of network infrastructure control parameters for effective intellectual analysis. *14th International Conference on Advanced Trends in Radioelecrtronics, Telecommunications and Computer Engineering (TCSET)*. Lviv-Slavske, Ukraine. 2018. P. 983–986.
9. Бондарчук О. І., Науменко Т. С., Товт Б. М. Розробка та впровадження інноваційних методів кібербезпеки у комп'ютерних системах. *Таврійський науковий вісник. Серія: Технічні науки*. 2024. № 4. С. 31–40.
10. Левтеров А. І., Плєхова Г. А., Шаронова Н. В., Неронов С. М. Пат. 157855 Україна. *Система контролю політики кібербезпеки з елементами штучного інтелекту корпоративної мережі зв'язку*. 2024.
11. Hasan S. K. Пат. 2017/0214701 A1 USA. *Computer security based on Artificial intelligence*. 2017.
12. Bellù L. G., Liberati P. Describing Income Inequality. Theil Index and Entropy Class Indexes. *Open knowledge*. URL: https://openknowledge.fao.org/server/ api/core/bitstreams/2d4181c9-30f3-4511-a1f8-f641ab0a13d8/ content. (дата звернення 20.01.2025).

References (transliterated)

1. Orhanizatsiia kanalu peredachi danykh dlia biznesu. [Organization of data transmission channel for business]. *GigaTrans Telecom operator*. Available at https://gigatrans.ua/ua/services/organizaciya-kanala-peredachi-dannuh. (accessed: 20.01.2025).
2. *DSTU ISO/IEC 27001:2023 Informatsiina bezpeka, kiberbezpeka ta zakhyst konfidentsiinosti. Systemy keruvannia informatsiinoiu bezpekoiu. Vymohy (ISO/IEC 27001:2022, IDT)* [Information Security, cybersecurity and privacy protection. Information security management systems. Requirements] / National Standart of Ukraine. Kyiv: DP «UkrNDNC» Publ., 2022. 26 p.
3. Bezpeka. [Safety]. *CityHost*. Available at https://cityhost.ua/uk/blog/bezopasnost/2/. (accessed: 20.01.2025).
4. 2024 SonicWall Cyber Threat Report. *Marlin Communications*. Available at https://marlincomms.co.uk/wp-content/uploads/2024/03/SonicWall-Marlin-Cybersecurity-Threat-Report-compressed.pdf. (accessed: 20.01.2025).
5. Hraivoronskyi M. V., Novikov O. M. *Bezpeka informatsiino-komunikatsiinykh system* [Security of information and communication systems]. Kyiv: BHV Publ., 2009. 608 p.
6. Kucherniuk P. V. Metody i tekhnolohii zakhystu komp'iuternykh merezh (fizychnyi ta kanalnyi rivni) [Methods and technologies for protecting computer networks (physical and channel levels)]. *Mikrosystemy, Elektronika ta Akustyka* [Microsystems, Electronics and Acoustics]. 2017. Vol. 22, Iss. 6(101). pp. 64–70.
7. Smelyakov K., Chupryna A., Darahan D., Midina S. Effectiveness of modern text recognition solutions and tools for common data sources. *CEUR Workshop Proceedings*, 2021, Vol. 2870, pp. 154–165.
8. Smelyakov K., Pribylnov D., Martovytskyi V., Chupryna A. Investigation of network infrastructure control parameters for effective intellectual analysis. *14th International Conference on Advanced Trends in Radioelecrtronics, Telecommunications and Computer Engineering (TCSET)*. Lviv-Slavske, Ukraine, 2018, pp. 983–986.
9. Bondarchuk O. I., Naumenko T. S., Tovt B. M. Rozrobka ta vprovadzhennia innovatsiinykh metodiv kiberbezpeky u komp'iuternykh systemakh. [Development and implementation of innovative cybersecurity methods in computer systems]. *Tavriiskyi naukovyi visnyk. Seriia: Tekhnichni nauky* [Tavria Scientific Bulletin. Series: Technical Sciences], 2024, Iss. 4, pp. 31–40.
10. Levterov A. I., Pliekhova H. A., Sharonova N. V., Neronov S. M. *Systema kontroliu polityky kiberbezpeky z elementamy shtuchnoho intelektu korporatyvnoi merezhi zv'iazku* [Cybersecurity policy control system with elements of artificial intelligence of a corporate communication network]. Patent UA, no.157855, 2024.
11. Hasan S. K. *Computer security based on Artificial intelligence*. Patent US, no. 2017/0214701 A1. 2017.
12. Bellù L. G., Liberati P. Describing Income Inequality. Theil Index and Entropy Class Indexes. *Open Knowledge*. Available at https://openknowledge.fao.org/ server/api/core/bitstreams/2d4181c9-30f3-4511-a1f8-f641ab0a13d8/content. (accessed 20.01.2025).

Надійшла (received) 14.02.2025

UDC 004.056+004.8

A. I. LEVTEROV, Candidate of Technical Sciences, Full Professor, Kharkiv National Automobile and Highway University, Professor at the Department of Informatics and Applied Mathematics, Kharkiv, Ukraine, e-mail: lai@khadi.kharkov.ua, ORCID: https://orcid.org/0000-0001-6586-1061

G. A. PLIEKHOVA, Candidate of Technical Sciences, Associate Professor, Kharkiv National Automobile and Highway University, Head of the Department of Informatics and Applied Mathematics, Kharkiv, Ukraine, e mail: plehovaanna11@gmail.com, ORCID: https://orcid.org/0000-0002-6912-6520

M. V. KOSTIKOVA, Candidate of Technical Sciences, Associate Professor, Kharkiv National Automobile and Highway University, Associate Professor at the Department of Informatics and Applied Mathematics, Kharkiv, Ukraine, e mail: kmv_topaz@ukr.net, ORCID: https://orcid.org/0000-0001-5197-7389

A. O. OKUN, Candidate of Technical Sciences, Associate Professor, National Technical University "Kharkiv Polytechnic Institute", Associate Professor at the Department of Computer Modeling and Integrated Forming Technologies, Kharkiv, Ukraine, e mail: okunanton@gmail.com, ORCID: https://orcid.org/0000-0002-6467-4229

CYBERSECURITY POLICY CONTROL SYSTEM WITH ELEMENTS OF ARTIFICIAL INTELLIGENCE OF THE CORPORATE COMMUNICATION NETWORK

In today's digital world, where almost all aspects of life are connected to the Internet, cybersecurity is not just important but an integral part of our reality. It ensures the smooth operation of services: from email to social and corporate networks across all sectors of critical infrastructure in countries worldwide. The development of artificial intelligence in the field of cybersecurity opens up significant potential for improving the effectiveness of information protection in all sectors of critical infrastructure. The developed system relates to the cybersecurity policy with artificial intelligence elements for corporate communication networks. The goal is to improve the accuracy of forming and controlling the cybersecurity policy of corporate communication networks by identifying techniques for executing computer attacks using artificial intelligence and analyzing the situation and vulnerabilities present in the software infrastructure. To achieve this goal, a cybersecurity policy control system with artificial intelligence elements for corporate communication networks was developed. The effectiveness of the developed system was calculated by comparing Theil coefficients to assess its validity. The developed system processes and evaluates information using artificial intelligence, including comparator identification, which allows for understanding the capabilities and techniques of executing each known computer attack. It also uses a situational text predicate to identify and analyze the situation of a cyberattack and predict its trajectory, determining the likelihood of each known attack and comparing it with the effectiveness of existing defense measures. By comparing the calculated Theil coefficients of the system with an existing analogue, it was concluded that the validity of forming a cybersecurity policy with artificial intelligence elements in the developed system is higher than that of the analogue, confirming the achievement of the proposed technical result. The use of AI in corporate communication networks enables faster and more efficient detection, analysis, and response to cyber threats, providing a high level of protection against modern cyberattacks. The integration of AI into cybersecurity also enhances security and improves the ability to respond to the challenges of today's digital environment. Thus, AI integration in the field of cybersecurity opens up new opportunities for ensuring effective and comprehensive protection against cyber threats in the modern digital world, becoming a key factor in ensuring future cybersecurity.

Keywords: cybersecurity, threats, protection, corporate networks, artificial intelligence, Theil index.

Повні імена авторів / Author's full names

Автор 1 / Author 1: Левтеров Андрій Іванович, Levterov Andrii Ivanovich
Автор 2 / Author 2: Плєхова Ганна Анатоліївна, Pliekhova Ganna Anatoliivna
Автор 3 / Author 3: Костікова Марина Володимирівна, Kostikova Maryna Volodymyrivna
Автор 4 / **Author 4:** Окунь Антон Олександрович, Okun Anton Oleksandrovych