DOI: **10.33099/2311-7249/2024-49-1-77-85**

УДК: 004.056.57

Савіцький Леонід Миколайович [1]
Безносенко Сергій Юрійович [2]
Горбач Роман Ярославович [3]

[1] ***Командування Військ зв'язку та кібербезпеки Збройних сил України, Київ, Україна***
[2] ***Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, Київ, Україна***
[3] ***Командування сухопутних військ Збройних сил України, Київ, Україна***

КОНЦЕПТУАЛЬНІ ПОГЛЯДИ НА ПОБУДОВУ СИСТЕМИ ЗАХИСТУ ВІД КІБЕРАТАК ІЗ ЗАСТОСУВАННЯМ МЕТОДІВ ШТУЧНОГО ІНТЕЛЕКТУ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ

Зважаючи на значущу роль інформаційно-комунікаційних систем на сучасному театрі бойових дій і враховуючи отриманий досвід ведення бойових операцій на сході України та після повномасштабного вторгнення російської федерації 24 лютого 2022 року, кібербезпека набуває надзвичайно важливого значення. Метою статті є огляд існуючих алгоритмів захисту та висловлення концептуальних поглядів на побудову систем захисту від кібератак із використанням методів штучного інтелекту. У статті застосовано теоретичні методи, а саме аналіз публікацій і досліджень за тематикою протидії кібератакам та захист систем передачі інформації. Також були використані загальнонаукові методи досліджень, серед яких використано аналітичні методи в оцінюванні ефективності системи, що розглядається у статті. Під час побудови графіків вжито елементи статистики та графо-аналітичні методи. Застосований методичний підхід дав змогу проаналізувати матеріали за темою дослідження, піддати аналізу отримані дані та удосконалити існуючі концептуальні погляди. У статті викладено сутність таких підходів до вирішення проблеми забезпечення безпеки інформаційно-комунікаційних систем як фрагментарний і комплексний. Також ретельно проаналізовано основні методи виявлення кібератак, а саме сигнатурний аналіз (метод виявлення зловживань) та метод виявлення аномалій. За результатами ретельного дослідження цих методів можна зазначити, що для досягнення високого рівня захищеності інформаційних ресурсів в інформаційно-комунікаційних системах обов'язково слід застосовувати методи, що базуються на виявленні аномалій. Ці методи проявляють неперевершену здатність виявляти найновіші кібератаки 0-day. Крім того, у статті проведено всебічний огляд основних засобів для виявлення та протидії кібератакам. Серед них такі технології: «Система виявлення вторгнень/Система запобігання вторгненням» (Intrusion Detection System/Intrusion Prevention System), «Мережевий екран» (Firewall), антивірусні програми та технології зі штучним інтелектом «Управління подіями та інформацією про безпеку» (Security information and event management). Пропонується для підвищення ефективності систем захисту в галузі кібербезпеки застосовувати елементи штучного інтелекту. Крім того, проведено огляд вже відомих даних і рішень у сфері кібербезпеки та виклад концептуальних поглядів авторів на застосування штучного інтелекту у цій сфері. На основі цих даних запропоновані нові та більш досконалі рішення. Основна мета інтегрування штучного інтелекту до системи захисту від кібератак полягає у його спроможності виявляти невідомі раніше кібератаки на основі сигнатур уже відомих атак. У роботі авторами також запропоновано визначення терміну «шаблон атаки». Спираючись на розглянуті в статті методи та запропоновані рішення можна покращити кіберзахист воєнно-оборонної сфери. Робота сприяє вдосконаленню процесів захисту від кібератак, що є критично важливим як для військових, так і для цивільних структур. Отже, ця стаття не лише спрямована на розвиток теоретичних основ захисту від кібернетичних загроз, але й має безпосередню практичну значущість у підвищенні рівня безпеки та ефективності захисних механізмів в інформаційно-комунікаційних системах. Впровадження такого підходу не лише дасть змогу істотно підвищити рівень кібернетичної захищеності в інформаційно-комунікаційних системах, але й може стати платформою для автоматичного створення експлойтів і сигнатур кібератак на підставі виявлених аномалій.

Ключові слова: *кіберзагроза, кібератака, кіберзахист, аномалія, зловживання, мережевий екран, штучний інтелект.*

Вступ

Постановка проблеми. Кібератака (далі – КА) становить значну загрозу як для оборонного, так і для громадського сектору України [1]. З 2014 року на підприємства (установи, організації) економічної та інфраструктурної сфери України здійснюється чимала кількість КА різного рівня складності. Серед них атаки на об'єкти енергетичної інфраструктури, а також на Міністерство фінансів, Держказначейство та Пенсійний фонд тощо. Протягом 2023 року, Урядова команда реагування на комп'ютерні надзвичайні події CERT-UA зафіксувала близько 7 тисяч інцидентів [2]. За статистичними даними, *фішинг* залишається одним із найпоширеніших методів незаконного проникнення, паралельно з використанням інших вразливостей систем. Фішинг може використовуватись як окрема атака або бути частиною більш широкої атаки. На жаль, в Україні існує проблема, пов'язана з тим, що не всі адміністратори систем вчасно оновлюють програмне забезпечення (далі – ПЗ) і навіть не всі використовують ліцензійне ПЗ. Поширеною практикою є завантаження на торент-трекери неліцензійного ПЗ, яке було зламане і містить шкідливі компоненти.

Аналіз КА свідчить, що потрібно підвищувати рівень кібербезпеки в Україні. Враховуючи наведені вище факти кількісного та якісного збільшення кіберзагроз для України, автори викладають концептуальні погляди на побудову системи захисту від КА в інформаційно-комунікаційних системах (далі – ІКС).

Аналіз останніх досліджень і публікацій. У публікації [3] вказані основні методи виявлення КА, зокрема, сигнатурний аналіз і метод виявлення аномалій. Пояснюється, які підходи можуть бути використані для виявлення вторгнень в систему і як вчасно реагувати на КА. Також описано різні засоби захисту, які можуть бути використані для забезпечення кібербезпеки. Зокрема, детально розглядаються технології систем виявлення і запобігання вторгнень (Intrusion Detection System/ Intrusion Prevention System (далі – IDS/IPS)), антивірусні програми та мережеві екрани (Firewall). Приведено аналіз вразливостей інформаційних систем, а також описано побудову безпечної інфраструктури, яка допомагає запобігати КА і захищати дані. В цій публікації не розглянуто алгоритми реагування та відновлення після КА.

У [4] проведено аналіз негативних наслідків КА на інформаційні ресурси об'єктів критичної інфраструктури держави. Дослідження зосереджене на вивченні впливу КА на системи, що відіграють критичну роль у функціонуванні держави, зокрема, енергетичні системи, транспортні мережі, комунікаційні інфраструктури тощо. Робота розглядає можливі вразливості, що існують у системах об'єктів критичної інфраструктури, і оцінює ризики, пов'язані з можливими КА. У цій роботі не розглянуто можливості відновлення та резервування інфраструктури після КА.

У статті [5] розглядаються основні аспекти та методи захисту інформації в ІКС. Описані поняття та принципи інформаційної безпеки, зазначені загрози і ризики, пов'язані із захистом інформації. Робота висвітлює дослідження послідовності дій, які можуть відбуватися під час КА на об'єкти критичної інфраструктури, з метою зрозуміти їхні наслідки та виявити можливі патерни атак. Приведено методи захисту інформації, які зберігаються і обробляються у хмарних обчислювальних середовищах. Проте в ній не розглянуто оцінювання збитків, які можуть бути завдані внаслідок кібератак.

У науковій праці [6] описано методи захисту таких мережевих компонентів як мережеві маршрутизатори, комутатори, брандмауери від КА. Розглядаються також проблеми і методи виявлення та реагування на кіберінциденти, зокрема, – використання системи управління інцидентами SIEM. Надаються поради щодо розробки ефективних планів реагування на інциденти і відновлення роботи після атаки. Особлива увага надається застосуванню захисту у хмарних обчислювальних середовищах. Однак, автори не провели докладного дослідження технічних деталей механізмів роботи та використання різних видів зловмисницького ПЗ.

Публікація [9] присвячена аспектам виявлення вторгнень на основі аномалій за наявності викидів та запропоновано модель системи виявлення вторгнень, яка використовує нейронну мережу на основі самоорганізованої карти, яка покращує виявлення вторгнень

У публікації [10] автори досліджують підходи до виявлення та аналізу кібератак і пропонують модель системи виявлення вторгнень з використанням нейронної мережі з неконтрольованим глибинним навчанням застосовуючи мережу глибоких переконань (Deep Belief Network) для виявлення вторгнень.

Проаналізувавши вищерозглянуті наукові праці можна стверджувати, що у них розглянуто проблеми виявлення та протидії кіберзагрозам, сигнатурний аналіз і метод виявлення аномалій, які за комбінованих КА на ІКС можуть виявлятися недостатньо ефективними. Також розглянуто використання моделей нейронних мереж з неконтрольованим глибинним навчанням для аналізу КА та виявлення вторгнень. Проте у наукових публікаціях приділяється недостатньо уваги питанням дослідження алгоритмів реагування та відновлення після КА, висвітлюють можливості відновлення та резервування інфраструктури після КА, здійснюють оцінювання збитків, що можуть бути завдані внаслідок кібератак. Також не виявлено докладного дослідження технічних деталей механізмів роботи та використання різних видів зловмисницького ПЗ. Вважаємо, що важливим є також завдання

з нейтралізації кіберзагроз в ІКС. Ураховуючи це, обрана тема статті є актуальною.

Мета статті полягає у викладенні концептуальних поглядів на побудову системи захисту від кібератак із застосуванням методів штучного інтелекту в інформаційно-комунікаційних системах для покращення безпеки центрів управління таких систем.

Виклад основного матеріалу дослідження

Існує два підходи до вирішення проблеми забезпечення безпеки ІКС, а саме фрагментарний і комплексний [3–8]. *Фрагментарний підхід* спрямований на протидію чітко визначеним загрозам в заданих умовах. Прикладами реалізації такого підходу є застосування засобів управління доступом, автономних засобів шифрування, спеціалізованих антивірусних програм тощо. Суттєвою перевагою цього підходу є його вибірковість, спрямованість на конкретні загрози. Однак недоліком є відсутність єдиного захищеного середовища обробки інформації. Фрагментарні заходи захисту можуть забезпечувати безпеку лише для конкретних об'єктів ІКС і, навіть, незначні зміни загрози можуть зробити їх ефективність недостатньою.

Комплексний підхід орієнтований на створення захищеного середовища обробки інформації в ІКС, що об'єднує в собі різноманітні заходи протидії загрозам. Він містить багато різнорідних заходів і розглядає безпеку ІКС як комплексну проблему. Організація захищеного середовища обробки інформації дає змогу забезпечити певний рівень безпеки ІКС, що є безперечною перевагою комплексного підходу. Проте до його недоліків можна віднести обмеження свободи дій користувачів ІКС, чутливість до помилок встановлення і налаштування засобів захисту, а також складність управління.

Одним із ключових аспектів комплексного підходу є розробка ефективної політики безпеки, що регламентує роботу засобів захисту ІКС і охоплює всі особливості процесу обробки інформації. Надійна система безпеки мережі не може бути створена без такої політики, яка визначає поведінку системи в різних ситуаціях і враховує потенційні загрози.

Багаторівневий підхід до побудови системи захисту ІКС (Defense in Depth) (рис. 1.) [2] полягає у створенні послідовних захисних шарів з різноманітними контрольними засобами для забезпечення максимального рівня безпеки. За таких умов, побудова системи захисту ІКС починається із зовнішнього шару і просувається глибше до внутрішніх компонентів системи, аж до її основи – даних.

На зовнішньому рівні застосовуються політики та процедури безпеки, що стосуються всієї організації або мережі. Це можуть бути правила доступу, паролі, політики використання інтернету, тощо. Далі йде рівень фізичної безпеки, який містить у собі фізичний контроль (наприклад, охоронці, замки на дверях) для захисту фізичного доступу до обладнання та приміщень.

Рисунок 1 – Багаторівневий підхід до побудови системи захисту інформаційно-комунікаційних систем (Defense in Depth) [2]

Наступним рівнем є захист мережі від зовнішніх загроз, тут можуть використовуватись різні технології, такі як «Зона демілітаризованого доступу» (Demilitarized Zon (далі – DMZ)), «Віртуальна приватна мережа» (Virtual Private Network (далі – VPN)), аудит, тестування на проникнення та аналіз вразливостей. Подальше забезпечення безпеки мережі охоплює контроль доступу, аутентифікацію та інші механізми для захисту внутрішніх ресурсів. Останнім рівнем є захист окремих хостингів і даних, де застосовуються антивірусні програми, шифрування, мережеві екрани Firewall та інші інструменти, які захищають окремі системи та інформацію.

Цей багаторівневий підхід до забезпечення безпеки ІКС дає змогу знизити ризик успішних атак, оскільки зламування одного шару не забезпечує автоматичного доступу до інших рівнів. Використання різноманітних технологій та заходів захисту робить систему більш стійкою і надійною.

У таблиці 1 наведена системна класифікація загроз безпеці інформації в ІКС. Таблиця була розроблена на основі аналізу джерел [3–6] для узагальнення та структурування інформації.

Загалом, методи виявлення КА можна розділити на дві групи – виявлення мережевих аномалій на основі аналізу показників мережевого трафіку (далі – МТ) та виявлення зловживань у ньому.

До визначення КА в мережі передує виявлення кіберінцидентів, що базується на аналізі мережевих аномалій або зловживань у МТ. Аналіз аномалій допомагає виявити значні зміни в трафіку мережевих пристроїв порівняно з нормальним профілем трафіку для цих пристроїв. Зазвичай, нормальний шаблон трафіку формується на основі статистичних даних і навчальних вибірок, зібраних протягом певного часового періоду. Аналіз телеметрії, який оцінює основні параметри трафіку, дозволяє виявляти аномалії без необхідності проводити детальне вивчення вмісту кожного пакету даних, що проходить у мережі.

Прикладами аномалій, виявлених на основі аналізу телеметрії трафіку, можуть бути раптове збільшення інтенсивності трафіку від певної

робочої станції або зміна структури трафіку порівняно зі звичайними щоденними показниками для даної мережі або пристрою. Блок-схема виявлення мережевих аномалій на основі показників МТ візуалізована на рис. 2.

Таблиця 1

Системна класифікація загроз безпеці інформації [3–6]

Параметри класифікації	Значення параметрів	Зміст значення параметрів
Види	Фізична цілісність Логічна структура Зміст Конфіденційність Право власності	Знищення (викривлення). Викривлення структури. Несанкціонована модифікація. Несанкціоноване отримання. Привласнення чужого права.
Природа походження	Випадкова Навмисна	Відмови, збої в роботі системи, помилки, стихійні лиха, побічні впливи. Злочинні дії людей.
Передумова появи	Об’єктивні Суб’єктивні	Кількісна недостатність елементів системи, якісна недостатність елементів системи. Розвідувальні органи іноземних держав, промисловий шпіонаж, кримінальні елементи, кіберзлочинні групи, недобросовісні співробітники.
Джерело загроз	Люди Технічні пристрої Моделі, алгоритми, програми Технологічні схеми обробки Зовнішнє середовище	Сторонні особи, користувачі, персонал. Реєстрації, передачі, зберігання, видачі. Загального призначення, прикладні, допоміжні. Ручні, інтерактивні, внутрішньо машинні, мережеві. Стан середовища (погодні умови та природні катаклізми, побічні шуми, побічні сигнали.

Рисунок 2 – Блок-схема виявлення мережевих аномалій на основі показників мережевого трафіку [2]

На рис. 3 авторами зображено графік залежності МТ від часу на виявлення аномалій в мережі. Зазначені рисунки розроблено авторами з використанням [2].

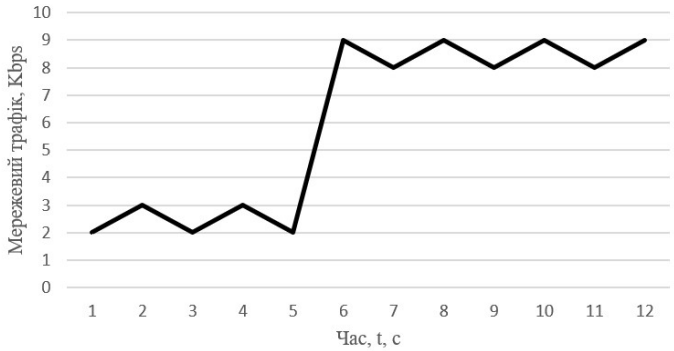

Рисунок 3 – Графік мережевого трафіку за виявлення аномалій у мережі [2]

Помилки виявлення аномалій можуть бути двох типів: помилкова тривога (1-го роду) та пропуск події (2-го роду). Помилкова тривога виникає, коли система помилково визначає нормальні події або звичайний трафік як аномальні, що може призвести до непотрібних або недоцільних реакцій. Пропуск події виникає, коли система не виявляє дійсно аномальних подій або зловживань, що створює ризик для безпеки, оскільки злочинці можуть діяти непоміченими.

Перевага методу виявлення зловживань в МТ (рис. 4.) полягає в тому, що він дозволяє ідентифікувати несанкціоновані дії, якщо відомо який профіль трафіку, можна спостерігати під час атаки [2]. *Шаблон атаки* – це опис конкретної атаки за допомогою правил зіставлення та виведення, що дозволяють однозначно визначити, чи належить об'єкт цій атаці. Дане визначення запропоновано авторами.

На рис. 5. показано графік залежності МТ від часу за виявлення зловживань у мережі. Розроблено авторами за інформацією з [2].

Рисунок 4 – Блок-схема методу виявлення зловживань в мережевому трафіку [2]

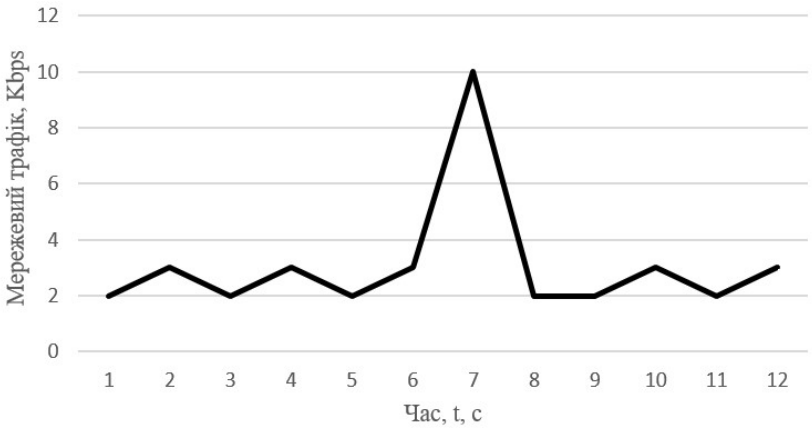

Рисунок 5 – Графік мережевого трафіку за виявлення зловживань в мережі

Однак існують суттєві проблеми, пов'язані з ефективністю проєктування механізму визначення правил і можливою складністю системи через їх численність. Також, цей підхід може не бути ефективним для виявлення невідомих атак або атак з новими модифікаціями. Для підвищення ефективності потрібні загальні правила, що охоплюють патерни усіх відомих атак. Також їх необхідно постійно оновлювати у процесі виявлення їхніх нових патернів. Адже в іншому випадку, система може пропускати нові атаки, що не вписуються у встановлені шаблони.

На підставі аналізу розглянутих методів можна зробити висновок, що для підвищення рівня захищеності інформаційних ресурсів ІКС доцільно застосовувати методи на основі виявлення аномалій, оскільки ці методи ефективно можуть викривати КА, включно з тими, що відбуваються безпосередньо після їх виявлення (так звані атаки 0-day).

Основними засобами захисту від КА є антивірусне програмне забезпечення (далі – АПЗ) для захисту від шкідливих програм, система запобігання/виявлення вторгнень IPS/IDS для моніторингу та виявлення небажаних активностей, а також мережеві екрани (Firewal) для контролю доступу до мережевих ресурсів та захисту від несанкціонованого доступу. У таблиці 2 зведено основні характеристики систем захисту від КА на основі проаналізованих даних.

Таблиця 2

Основні характеристики систем захисту від кібератак

Функції	Засоби захисту			
	Firewall	IPS/IDS	Антивірусні програми	SIEM
Дані, що аналізуються	МТ	МТ	МТ, Дані в операційній системі	Дані журналу
Механізм виявлення підозрілої активності	«Список контролю доступу» (Access control list (далі – ACL)), аналіз зловживань	Аналіз зловживань	Аналіз зловживань аналіз поведінки	Аналіз за прикладами попередніх інцидентів
Оновлення бази для розпізнавання нових загроз	Надається розробником	Надається розробником. Задається користувачем	Надається розробником	Задається користувачем на основі даних розробника
Синтаксичний аналіз Parsing	Не є необхідним	Частково необхідний	Не є необхідним	Необхідний
Блокування загрози	Є	Немає	Є	Немає

Для виявлення та запобігання вторгнень застосовуються системи IDS/IPS, IDS виявляє незвичайні активності та повідомляє про можливі вторгнення, а IPS блокує або призупиняє такі атаки на основі заздалегідь встановлених правил.

Системи «Управління подіями та інформацією про безпеку» (Security information and event management (далі – SIEM)) – системи реєстрації та аналізу журналів. Такі системи у реальному часі забезпечують аналіз подій безпеки, а також активності пристроїв і користувачів, що дає змогу реагувати на них до того, як буде завдано шкоди. Програми SIEM збирають інформацію з серверів, контролерів доменів, firewall і багатьох інших мережевих пристроїв і надають її у вигляді звітів. Ці дані не обов'язково пов’язані з безпекою. З їхньою допомогою, наприклад, можна зрозуміти, як функціонує мережева інфраструктура і розробити план з її оптимізації. Але головне, звісно, це виявлення потенційних вразливих місць у системі, а також локалізація та ліквідація наявних загроз. Такі дані надаються завдяки збору та об’єднанню даних журналів мережевих пристроїв. Після збору інформації (ця процедура відбувається автоматично із заданими інтервалами) здійснюється ідентифікація та класифікація подій. Потім (знову ж таки, відповідно до заданих налаштувань) надсилаються сповіщення, що ті чи інші дії обладнання, програми або користувачі можуть бути потенційно небезпечними.

Враховуючи означене, пропонується, на рівні законодавчих органів, розробити концепцію системи захисту від КА, в якій буде визначено використання штучного інтелекту (далі – ШІ). Однією з переваг його застосування у такій системі є його спроможність виявляти невідомі КА на основі сигнатур уже відомих атак. Навчений ШІ може забезпечити захист від комбінованих атак, що наразі є складною задачею для існуючих систем. ШІ є перспективною технологією в галузі кібербезпеки. Штучний інтелект повинен працювати в синергії з існуючими методами, доповнюючи їх та компенсуючи їх недоліки, тим самим підіймаючи ефективність усієї системи. Також необхідна система автоматизації, що буде забезпечувати координацію дій всіх засобів та методів виявлення та протидії КА. Ця система забезпечуватиме за обмін командами управління та критичними даними між всіма інструментами під час аудиту подій в ІКС.

До прикладу, у випадку виявлення IDS/IPS мережевої КА на основі наявної аномалії у системі, система автоматизації може надати брандмауеру команду на блокування IP-адреси, з якої відбувається підозріла активність, користуючись даними, отриманими від IDS/IPS. У випадку, коли зафіксована підозріла активність без чіткої ідентифікації атаки, система автоматизації може надати команду управління антивірусному програмному забезпеченню для вжиття необхідних заходів. Цей підхід дозволяє забезпечити злагоджений та ефективний захист, який охоплює широкий спектр загроз, завдяки спільній роботі та обміну інформацією між різними засобами захисту.

В умовах обмеженої інформації, якою володіє керуюча система на основі ШІ, стає необхідною розроблення моделі протидії загрозам, яка дозволяє вибрати раціональний керуючий вплив. Це досягається завдяки створенню гнучкої моделі, яка дозволяє адаптуватись до змінних умов і збільшує ефективність взаємодії з іншими засобами захисту. З метою негайного припинення КА адміністратор безпеки повідомляється першим за всіх. Він отримує сповіщення засобами

електронної пошти, виведенням повідомлень на консоль тощо. Одразу припиняються мережеві сесії та користувальницькі реєстраційні записи, а також заповнюється протокол дій атакуючої сторони.

У межах розробки концепції системи захисту від КА, висловимо авторський погляд на те, яка архітектура (централізована, децентралізована чи гібридна) є найбільш доцільною для побудови цієї системи. Її архітектура визначає структуру і взаємодію між компонентами системи.

Централізована архітектура розташовується на одному сервері. Така архітектура є простою і легкою в реалізації, але вона може бути недостатньо масштабованою для захисту великих і складних ІКС.

Децентралізована архітектура складається з компонентів системи розташованих на різних серверах. Така архітектура є більш масштабованою, але вона також більш складна в реалізації і управлінні.

Гібридна архітектура складається з компонентів системи розташовані на різних серверах, але вони взаємодіють один з одним через централізовану систему управління. Така архітектура є більш масштабованою, ніж централізована архітектура і більш простою в реалізації, ніж децентралізована архітектура. Вона забезпечує баланс між масштабованістю, простотою реалізації і зручністю управління.

Найбільш доцільною у даному випаду архітектурою для побудови системи захисту від КА буде *гібридна*, оскільки вона вдало поєднує переваги *централізованої* та *децентралізованої* архітектури.

Оцінити ефективність системи захисту від КА можна використовуючи формулу:

$$E = \frac{(M - N)}{(M + V + N)} * 100\% * (1 - B), \quad (1)$$

де E – ефективність системи;

M – кількість кібератак, виявлених і заблокованих системою;

N – кількість кібератак, попереджених системою;

V – кількість кібератак, які пройшли систему кіберзахисту;

B – відсоток помилкових спрацювань, що генерує система.

Вираз має сенс лише за умов: M>N і B∈[0;1).

Атаки попереджені системою – це кібератаки, що були виявлені системою кіберзахисту, але не були заблоковані. Система кіберзахисту може попередити користувачів про ці атаки, щоб вони могли вжити заходів для їх нейтралізації. До таких атак відносять фішингові атаки, зловмисне програмне забезпечення та несанкціоноване проникнення в мережу. Система кіберзахисту може попередити користувачів про фішингові атаки, якщо вона виявить підозрілі електронні листи або веб-сайти, або про зловмисне програмне забезпечення, якщо вона виявить підозрілі процеси.

Навчання ШІ повинно проводитися на основі широкого набору даних, включно з даними про відомі атаки, потенційні загрози та реальний світ. Дані є основою для будь-якої системи кіберзахисту на основі ШІ. Для цього система повинна отримувати дані з таких різних джерел як системи виявлення та запобігання вторгнень, антивірусне програмне забезпечення, системи управління журналами та інші. Дані мають бути репрезентативними для кібератак, які система повинна виявляти і попереджати. Значною мірою результат навчання залежить від кількості та якості даних, які залучені до навчання ШІ.

Спираючись на вимоги, що висуваються до системи, а саме висока точність виявлення загроз, пропонуємо обрати мультимодальну систему ШІ. Цей метод поєднує статистичні та детерміновані моделі. Завдяки цьому ми компенсуємо недоліки обох методів, що дасть змогу відповідати сформульованим до системи вимогам.

Децентралізовані компоненти системи, такі як система машинного навчання і система штучного інтелекту, можуть бути реалізовані на основі платформ машинного навчання, наприклад, Google Cloud AI Platform або Azure Machine Learning. Система автоматизації має бути розроблена так, щоб забезпечити швидке і ефективне реагування на КА. Для цього система має бути інтегрована з системами виявлення і запобігання вторгнень, антивірусним програмним забезпеченням та іншими системами захисту

Висновки й перспективи подальших досліджень

Отже, на основі вищевикладеного можна зробити висновки щодо переваг і недоліків методу виявлення зловживань та методу виявлення мережевих аномалій. *Метод виявлення зловживань*, на основі шаблонів атак, дає змогу ідентифікувати заздалегідь відомі атаки, проте його ефективність може бути обмеженою за виявлення невідомих атак або атак з новими модифікаціями. Натомість, *метод виявлення мережевих аномалій,* на основі показників мережевого трафіку, має свої переваги у вигляді спроможності виявляти нові атаки. Його ефективність залежить від правильної побудови профілю трафіку та уникнення помилкових рішень, що можуть призвести до помилкових спрацювань або пропуску потенційно небезпечних подій.

Після аналізу методів захисту від кібератак зазначимо, що хоча ці методи є ефективними для виявлення та протидії кібератакам, проте, на сьогодні відсутній єдиний універсальний метод захисту від всіх видів атак на інформаційно-комунікаційну систему. Водночас, методи, що базуються на виявленні аномалій, виявилися доцільнішими для підвищення рівня захищеності інформаційних ресурсів інформаційно-комунікаційної системи.

Запропонована система захисту від кібератак, що широко використовує в своїй роботі штучний інтелект, може усунути основний недолік вищерозглянутих методів, а саме – виявлення невідомих атак або атак з новими модифікаціями. Означена система дасть змогу підвищити рівень захисту інформаційно-комунікаційної системи за рахунок гібридизації функціоналу основних програмно- апаратних засобів захисту. Цей підхід може бути ефективним і перспективним для поліпшення кібернетичної безпеки інформаційно-комунікаційної системи.

Провівши порівняння різних варіантів архітектури для побудови запропонованої системи обрано найкращою гібридну архітектуру. Для штучного інтелекту було обрано мультимодальну систему, яка спроможна забезпечити високі вимоги до точності виявлення.

Точність виявлення загроз, значною мірою, залежить від якості навчання штучного інтелекту. А якість навчання, в свою чергу, залежить від кількості та якості даних, на яких навчається штучний інтелект. Тому необхідно надати особливу увагу цьому аспекту.

Подальшим напрямом наукових досліджень є детальне вдосконалення системи та розробка конкретних варіантів реалізації запропонованих рішень. Це охоплює розширення спектру можливих загроз, а також розгляд різних варіантів інцидентів та підходів до протидії їм. Додаткова робота над системою захисту від кібератак дасть змогу враховувати більш різноманітні сценарії й побудувати більш гнучку та адаптивну систему захисту від кіберзагроз.

Список бібліографічних посилань

1. Україна з 14 січня 2022 року залишається на першому місці у світі за кількістю кібератак проти неї – заступник голови Держспецзв'язку. Інтерфакс-Україна. 23.05.2023. URL: https://interfax.com.ua/news/interview/911979.html (дата звернення: 05.01.2024).

2. Державна служба спеціального зв'язку та захисту інформації України. Урядова команда CERT-UA в 2023 році опрацювала 2543 кіберінциденти. URL: https://cip.gov.ua/ua/news/uryadova-komanda-cert-ua-v-2023-roci-opracyuvala-2543-kiberincidenti (дата звернення: 12.03.2024). **3. Жилін А. В., Шаповал О. М., Успенський О. А.** Технології захисту інформації в інформаційно-телекомунікаційних системах : навч. посіб. Київ : КПІ ім. Ігоря Сікорського, 2020. 213 с. **4. Дрейс Ю., Мовчан М.** Аналіз негативних наслідків кібератак на інформаційні ресурси об'єктів критичної інфраструктури держави. *Актуальні питання забезпечення кібербезпеки та захисту інформації:* Міжнародна науково-практична конференція. Європейський університет. 2017. № 3. С. 71–74. **5. Остапов С. Е., Євсеєв С. П., Король О. Г.** Технології захисту інформації : навч. посіб. Харків : ХНЕУ, 2013. 476 с. **6. Vacca J. R**. Network and system security. *Journal of Computer Science and Information Security.* 2014. № 2. P. 96. **7. Грайворонський М. В., Новіков О. М.** Безпека інформаційно-комунікаційних систем : навч.-метод. матеріали. Київ : Вид. група BHV, 2009. 698 с. **8. Голубенко О. Л., Хорошко В. О., Петров О. С., Головань С. М., Яремчук Ю. Є.** Політика інформаційної безпеки: підручник. Луганськ : Вид-во СНУ ім. В. Даля, 2009. 300 с. **9. Alom M. Z., Bontupalli V., Taha T. M.** Intrusion detection using deep belief networks, in: 2015 *National Aerospace and Electronics Conference* (NAECON). 2015. P. 339–344. DOI: 10.1109/NAECON.2015. 7443094. **10. Karami A.,** Ananomaly-based intrusion detection system in presence of benign outliers with visualization capabilities. *Expert Systems with Applications.* 2018. № 108. С. 36–60.

CONCEPTUAL VIEWS ON BUILDING, OF THE SYSTEM OF PROTECTION AGAINST CYBER ATTACKS WITH THE USE OF ARTIFICIAL INTELLIGENCE IN INFORMATION AND COMMUNICATION SYSTEMS

Savitskyi Leonid [1]
Beznosenko Serhii [2]
Gorbach Roman [3]

[1] ***Command of the Communications and Cyber Security Troops of the Armed Forces of Ukraine, Kyiv, Ukraine***
[2] ***Kruty Heroes Military Institute of Telecommunications and Informatization, Kyiv, Ukraine***
[3] ***Land Forces Command of the Armed Forces of Ukraine, Kyiv, Ukraine***

Formulation of the problem in general. *This article addresses the critical need to fortify cybersecurity measures within information and communication systems, particularly in light of the escalating role of these systems in contemporary operational landscapes. To achieve this, the article utilized a comprehensive research approach involving literature review, analysis of recent cyber warfare experiences, and in-depth examination of cybersecurity methodologies.*

Research methods. *In writing this article, theoretical methods were used, namely, the analysis of publications and research on the topics of countering cyberattacks and protecting information transmission systems. General scientific research methods were also applied, including analytical methods in assessing the effectiveness of the system. Elements of statistics and graph-analytical methods were used in the construction of graphs. The applied methodological approach makes it possible to analyze the material on the research topic, to analyze the data obtained and to improve the existing methods of protection.*

Analysis of recent researches and publications. *Recent research and experiences, including those from the conflict in eastern Ukraine and the full-scale invasion by the russian federation, underscore the urgent necessity of robust cybersecurity measures. The article extensively reviewed two primary approaches to securing information resources: fragmentary and comprehensive. Through an in-depth analysis, the superiority of anomaly detection methods over signature analysis in identifying the latest cyber threats, including 0-day attacks, was established.*

Presenting the main material*. The article outlines the essential tools for detecting and countering cyber attacks, encompassing Intrusion Detection/Prevention Systems, Firewalls, antivirus programs, and Security Information and Event Management technologies. It emphasizes the promising role of artificial intelligence in bolstering cybersecurity systems. A proposed protective scheme combining these tools was thoroughly analyzed, leading to a recommendation for the development of a cyber attack protection system integrated with artificial intelligence.*

Elements of scientific novelty. *The article provides an overview of the already known data and solutions in the field of cybersecurity and presents the authors' conceptual views on the use of artificial intelligence in this area. Based on this data, the authors propose to develop new and more advanced solutions. The main goal of integrating artificial intelligence into a cyberattack defense system is its ability to detect previously unknown cyberattacks based on the signatures of already known attacks. In this paper, the authors propose a definition of the term «attack pattern».*

Theoretical and practical significance of the article. *The research findings hold significant importance for the military and defense sectors, offering actionable insights to fortify cybersecurity measures. The author proposes to use elements of artificial intelligence to improve the effectiveness of defense systems in the field of cybersecurity.*

Conclusion and the perspectives of future researches*. In conclusion, the integration of artificial intelligence presents a promising avenue to fortify cybersecurity in information and communication systems. Future research should focus on the practical implementation and refinement of artificial intelligence-driven cyber attack detection systems, further strengthening defense against evolving threats.*

Keywords: *cyber threat, cyber attack, cyber defense, anomaly, firewall, abusive practices, artificial intelligence.*

References

1. Interfax-Ukraine, (2023). Since January 14, 2022, Ukraine remains in the first place in the world in terms of the number of cyber attacks against it - the deputy head of the State Intelligence Service. *Interfax-Ukraine* [online]. May 23, 2023. [Accessed January 5, 2024]. Access mode: https://interfax.com.ua/news/interview/911979.html 2. State Service for Special Communications and Information Protection of Ukraine, (2024). Governmental CERT-UA team handled 2543 cyber incidents in 2023 [online]. https://cip.gov.ua. [Accessed March 12, 2024]. Access mode: https://cip.gov.ua/ua/news/uryadova-komanda-cert-ua-v-2023-roci-opracyuvala-2543-kiberincidenti.

3. Zhilin, A., Shapoval, O. and Uspenskyi, O., (2020). *Information protection technologies in information and telecommunication systems*. Kyiv: KPI named after Igor Sikorsky. **4. Dreis, Y. and Movchan, M.,** (2017). Analysis of the negative consequences of cyberattacks on the information resources of critical state infrastructure facilities. *international scientific and practical conference topical issues of cyber security and information protection, European University*. (3), 71–74.. **5. Ostapov, S. E., Yevseev, S. P. and Korol, O. G.,** (2013*). Information protection technologies*. Kharkiv: Khneu. **6A. Vacca J. R.**, (2014). Network and system security. *Journal of Computer Science and Information Security*. 2, 96. **7. Graivoronskyi, M. V. and Novikov, O. M.,** (2009). *Security of information and communication systems. Kyiv:* BHV Publishing Group. **8. Golubenko, O. L., Khoroshko, V. O., Petrov, O. S., Golovan, S. M., Yaremchuk, Yu. Ye.,** (2009). *Information security policy Information protection. Technical protection of information.*. Luhansk: V. Dalya State University.

9. Alom, M. Z., Bontupalli, V., Taha, T. M., (2015). Intrusion detection using deep belief networks. In: 2015 National Aerospace andElectronics Conference (NAECON), 339–344. doi:10.1109/NAECON.2015.7443094.

10. Karami, A., (2018) Ananomaly-based intrusion detection system in presence of benign outliers with visualization capabilities, Expert Systems with Applications. 108, 36–60.