Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ПОЯСНЮВАЛЬНА ЗАПИСКА

кваліфікаційної роботи магістра

галузь знань *12 Інформаційні технології*
(шифр і назва галузі знань)

спеціальність *125 Кібербезпека*
(код і назва спеціальності)

освітній ступень *магістр*

освітньо-наукова програма *Кібербезпека*
(назва освітньої програми)

на тему: «Модель захисту об’єктів критичної інфраструктури від кібернетичних впливів»

Виконавець: студентка ІІ курсу, групи КБм-21

_____ **Анна МОСТОВЕНКО**
(підпис) (Ім’я, ПРІЗВИЩЕ)

	Ім’я, ПРІЗВИЩЕ	**Підпис**
Науковий керівник	Сергій ТОЛЮПА	
Нормоконтроль	Юрій ЩЕБЛАНІН	

Київ 2023

Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
В.о. завідувача кафедри
кібербезпеки
та захисту інформації
_____ Сергій ТОЛЮПА
«24» жовтня 2022 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

освітній ступень *магістр*

Здобувачки КБм-21 (група) Мостовенко Анни Віталіївни (прізвище ім'я по-батькові)

Тема дипломної роботи Модель захисту об'єктів критичної інфраструктури від кібернетичних впливів

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Рішення засідання кафедри кібербезпеки та захисту інформації факультету інформаційних технологій протокол № 3 від 20.10.2022

2. МЕТА ТА ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Об'єкт досліджень	Засоби і алгоритми захисту об'єктів критичної інфраструктури від кібернетичних впливів.
Предмет досліджень	Процес захисту об'єктів критичної інфраструктури від кібернетичних впливів.
Мета	Розробка алгоритму гібридної системи виявлення вторгнень для об'єктів критичної інфраструктури.

Вихідні дані для проведення роботи Методи захисту об’єктів критичної інфраструктури, алгоритми роботи систем виявлення вторгнень.

3. ОЧІКУВАНІ НАУКОВІ РЕЗУЛЬТАТИ

Наукова новизна Розробка нового гібридного алгоритму СВВ, а також зменшення відсотку хибно-позитивних спрацювань.

Практична цінність Покращення ефективності контролю раннього виявлення загроз для об’єктів критичної інфраструктури.

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Робота виконана у повному обсязі відповідно до теми.

5. ЕТАПИ ВИКОНАННЯ РОБОТИ

Найменування етапів робіт	Строки виконання робіт (початок-кінець)
Розробка плану для досягнення мети роботи	24.10.2022 – 22.01.2023
Аналіз літературних джерел	23.01.2023 – 15.02.2023
Розробка алгоритму гібридної системи виявлення вторгнень	16.02.2023 – 23.04.2023
Оформлення і друк пояснювальної записки	24.04.2023 – 19.05.2023

6. РЕАЛІЗАЦІЯ РЕЗУЛЬТАТІВ ТА ЕФЕКТИВНІСТЬ

Економічний ефект Зниження збитків через зменшення можливості атаки

Соціальний ефект Покращення технологій виявлення атак на об’єктах критичної інфраструктури.

7. ДОДАТКОВІ ВИМОГИ

Завдання видав _____ Сергій ТОЛЮПА
(підпис) (Ім’я, ПРІЗВИЩЕ)

Завдання прийняв до виконання _____ Анна МОСТОВЕНКО
(підпис) (Ім’я, ПРІЗВИЩЕ)

Дата видачі завдання: 24.10.2022 р.
Термін подання кваліфікаційної роботи до ЕК 19.05.2023 р.

УДК. 004.432.16

РЕФЕРАТ

Кваліфікаційна магістерська робота складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел, має 71 сторінку основного тексту, 3 формули та 10 рисунків. Список використаних джерел містить 34 найменування і займає 4 сторінки.

Об’єктом дослідження є засоби і алгоритми захисту об’єктів критичної інфраструктури від кібернетичних впливів.

Предметом дослідження є процес захисту об’єктів критичної інфраструктури від кібернетичних впливів.

Метою даної роботи є розробка алгоритму гібридної системи виявлення вторгнень для об’єктів критичної інфраструктури.

Наукова новизна: запропоновано алгоритм гібридної системи виявлення вторгнень для об’єктів критичної інфраструктури.

Результати роботи можуть використовуватися для побудови системи виявлення вторгнень на об’єкті критичної інфраструктури.

У роботі проаналізована існуюча література з класифікації об’єктів критичної інфраструктури у різних країнах світу, а також різноманітні класи та підвиди системи виявлення вторгнень та виявлено переваги та недоліки кожного підвиду.

Ключові слова: об’єкт критичної інфраструктури, система виявлення вторгнень, сигнатура, аномалія, алгоритм, Random Forest, Autoencoder .

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

AE	–	Autoencoder
BGP	–	Border Gateway Protocol
CPN	–	Coloured Petri nets
DoS	–	Denial of service
DDos	–	Distributed Denial of Service
IP	–	Internet Protocol
HTTP		Hyper Text Transfer Protocol
RF	–	Random Forest
SOC	–	Security Operations Center
SVM	–	Support vector machine
URI		Uniform Resource Identifier
ДР	–	Дерево рішень
КІ	–	Критична інфраструктура
ОКІ	–	Об’єкт критичної інфраструктури
СВВ	–	Система виявлення вторгнень
СКП	–	Середньоквадратична похибка

ЗМІСТ

ВСТУП

Актуальність даної роботи визначається тією обставиною, що масштабні атаки на об’єкти критично важливої інфраструктури мають місце ледве не кожного тижня з початку 2022 року з метою кібернетичної боротьби з Україною, аби взяти під контроль системи управління найбільш критичними підприємствами країни.

Росія федерація розпочала найбільш активні військові проти України 24 лютого 2022 року, але, нажаль, російські кібератаки проти України тривають із моменту незаконної анексії Росією автономної республіки Крим у 2014 році, посилившись безпосередньо перед повномасштабним вторгненням у 2022 році. За інформацією з відкритих джерел в цей період найбільше постраждали державно-адміністративний, енергетичний, медійний, фінансовий, бізнес та некомерційний сектори України. Починаючи з 24 лютого поодинокі та групові російські кібератаки значно ускладнили розподіл медикаментів першої необхідності , харчових продуктів та надзвичайної допомоги серед населення країни. Організації та уряди в усьому світі не залишилися байдужими до ризиків, що пов'язані з цією зловмисною активністю. За лідерством країн Європейського Союзу, США та НАТО реалізуються ініціативи, спрямовані на нейтралізацію кіберзагроз та захист життєво важливої інфраструктури України. У рамах цих ініціатив ЄС активізував роботу своїх команд швидкого реагування на кіберінциденти для посилення кібероборони нашої країни. Різні неурядові та приватні структури підтримують Україну та в якості допомоги проводять різні заходи для досягнення більшого рівня кіберстійкості. Незалежні хакерські групи (наприклад, Anonymous) від початку вторгнення здійснили значну кількість контратак, які вразили державно-управлінську, фінансову та медійну системи російської федерації. Європейський парламент на початку вторгнення виступив із закликом посилити допомогу Україні у сфері кібербезпеки та в повній мірі використовувати усі наявні важелі для введення ще більш жорстких кіберсанкцій ЄС проти осіб, організацій та установ, відповідальних за різні кібератаки на Україну або причетних до них. Одним з проявів підтримки України стало приєднання до Центру НАТО з питань співробітництва в галузі кіберзахисту (CCDCOE) 16 травня 2023 року.

Аналіз останніх досліджень та літератури. Вчені, які зробили вклад у вивчення моделей захисту об’єктів критичної інфраструктури від кібернетичних впливів: Carol V. Evans, Chris Anderson, Lidong Wang, Teresa Lunt, Якуб Пшетачник та інші.

Метою роботи є розробка алгоритму гібридної системи виявлення вторгнень для об’єктів критичної інфраструктури.

Для досягнення поставленої мети необхідно вирішити такі *завдання***:**

- проаналізувати існуючу вітчизняну та міжнародну нормативно-правову базу створену з метою захисту ОКІ;
- проаналізувати наявні методи виявлення вторгнень та обрати оптимальні для розроблюваного алгоритму;
- розробити алгоритм системи виявлення вторгнень для об'єктів критичної інфраструктури;
- розробити графічне представлення процесу навчання та процесу тестування розроблюваного алгоритму.

Об'єктом дослідження в даній роботі є засоби і алгоритми захисту об’єктів критичної інфраструктури від кібернетичних впливів.

Предметом дослідження в даній роботі є процес захисту об’єктів критичної інфраструктури від кібернетичних впливів.

Науковою новизною цієї кваліфікаційної роботи є опис нового алгоритму системи виявлення вторгнень, який буде комбінацією існуючих методів захисту з мінімізацією недоліків під час використання.

Методи дослідження у кваліфікаційній магістерській роботі:

- аналіз літератури;
- аналіз методів, що застосовуються в системі виявлення вторгнень;
- порівняння існуючих алгоритмів;
- вивчення та узагальнення вітчизняної і зарубіжної практики.

Апробація результатів роботи та публікації за темою кваліфікаційної роботи:

1. Толюпа С.В, Мостовенко А.В. Вразливості та запобігання загрозам в об’єктах критичної інфраструктури. Матеріали V Міжнародної науково-практичної

конференції "Проблеми кібербезпеки інформаційно-телекомунікаційних систем (PCSITS)" (Київ, 2022).

2. Толюпа С.В, Мостовенко А.В. БПЛА як загроза об'єктам критичної інфраструктури. Матеріали V Міжнародної науково-практичної конференції "Проблеми кібербезпеки інформаційно-телекомунікаційних систем (PCSITS)" (Київ, 2023).

3. Serhii Toliupa, Anna Mostovenko, Liza Hontkovska. Problematic aspects of solving issues of cyber influence on critical infrastructure objects. Scientific and Practical Cyber Security Journal (SPCSJ) № 3 (02) September 2023. (Грузія).

РОЗДІЛ 1
СТРАТЕГІЇ ЗАХИСТУ ОБ’ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

1.1 Український досвід

Україна, як і багато інших країн, приділяє велику увагу захисту об'єктів критичної інфраструктури. Особливо це стало актуальним у контексті гібридної війни з Росією, яка почалася у 2014 році.

Деякі з основних заходів, що вживаються для захисту об'єктів критичної інфраструктури в Україні, включають:

Правова база: Україна прийняла ряд законів та нормативно-правових актів, спрямованих на захист об'єктів критичної інфраструктури. Це включає закони про кібербезпеку, захист критичної інфраструктури, антитерористичну діяльність та інші.

Відповідно до закону України від 18 жовтня 2022 року «Про критичну інфраструктуру» встановлюються правові та організаційні засади створення та функціонування державної системи захисту критичної інфраструктури, об’єктів інфраструктури, систем, їх частин та цілого, мають вирішальне значення для економіки, національної безпеки та оборони, невиконання яких може підірвати життєво важливі національні інтереси.

До життєво важливих функцій та/або послуг, порушення яких призводить до негативних наслідків для національної безпеки України, належать, зокрема:

- урядування та надання найважливіших публічних (адміністративних) послуг;
- енергозабезпечення (у тому числі постачання теплової енергії);
- водопостачання та водовідведення;
- продовольче забезпечення;
- охорона здоров’я;
- фармацевтична промисловість;
- виготовлення вакцин, стале функціонування біолабораторій;

- інформаційні послуги;
- електронні комунікації;
- фінансові послуги;
- транспортне забезпечення;
- оборона, державна безпека;
- правопорядок, здійснення правосуддя, тримання під вартою;
- цивільний захист населення та територій, служби порятунку;
- космічна діяльність, космічні технології та послуги;
- хімічна промисловість;
- дослідницька діяльність.

Об’єкти критичної інфраструктури класифікуються за категоріями критичності для визначення рівня вимог щодо забезпечення захисту об’єктів критичної інфраструктури відповідно до їх важливості для забезпечення конкретних критичних функцій у секторі критичної інфраструктури. Серйозність об’єктів КІ має такі категорії:

- І категорія критичності — особливо важливі об’єкти, які мають загальнодержавне значення і значний вплив на інші об’єкти критичної інфраструктури, порушення функціонування яких призведе до виникнення кризової ситуації державного значення;
- ІІ категорія критичності — життєво важливі об’єкти, порушення функціонування яких призведе до виникнення кризової ситуації регіонального значення;
- ІІІ категорія критичності — важливі об’єкти, порушення функціонування яких призведе до виникнення кризової ситуації місцевого значення водопостачання та водовідведення;
- IV категорія критичності — необхідні об’єкти, порушення функціонування яких призведе до виникнення кризової ситуації локального значення.

Крім того, згідно із законом, для забезпечення формування та реалізації державної політики у сфері захисту критичної інфраструктури та управління

функціями захисту національної критичної інфраструктури буде створено уповноважений орган у сфері захисту критичної інфраструктури України. Система забезпечує координацію діяльності міністерств і операторів критичної інфраструктури щодо забезпечення стабільності та захисту об’єктів критичної інфраструктури. Діяльність уповноважених органів у сфері захисту критичної інфраструктури в Україні спрямовується, координується та контролюється Кабінетом Міністрів України [1].

В ЗУ «Про критичну інфраструктуру» також визначено особливості діяльності окремих органів, на які покладається формування та/або реалізація державної політики у сфері захисту критичної інфраструктури. Діяльність Національного банку України, уповноваженого органу у сфері захисту критичної інфраструктури України, центрального органу виконавчої влади, який забезпечує формування та реалізує державну політику у сфері цивільного захисту, Служби безпеки України, Національної гвардії України, Національної поліції України, Збройних Сил України, Державної спеціальної служби транспорту та Державної служби спеціального зв’язку та захисту інформації України з питань формування та/або реалізації державної політики у сфері захисту критичної інфраструктури здійснюється в рамках, визначених законом, та у порядку, встановленому законами України, що регламентують правові засади організації та діяльності зазначених [1].

Варто зазначити, що ЗУ «Про критичну інфраструктуру» був прийнятий під час широкомасштабного вторгнення російської федерації в Україну, а це означає, що не всі об’єкти, що підпадають під його дію, встигли впровадити вимоги ЗУ у свої операційні процеси. Тобто можна заявляти, що даний закон ще знаходиться на стадії імплементації об’єктами критичної інфраструктури. Даний процес може зайняти декілька років, аби була сформована чітко налагоджена система функціонування за вимогами даного закону.

Кібербезпека: Україна приділяє особливу увагу кібербезпеці об'єктів критичної інфраструктури. Для цього було створено Національний центр кібербезпеки, який відповідає за виявлення, аналіз та реагування на кібератаки. Центр співпрацює з операторами критичної інфраструктури, надає рекомендації з підвищення безпеки

інформаційних систем, а також проводить тренування та навчання фахівців з кібербезпеки. Крім того, проводяться тренування та аудити з кібербезпеки для забезпечення високого рівня захисту.

Фізичний захист: Особлива увага приділяється фізичному захисту об'єктів критичної інфраструктури. Активне використання БПЛА з двох сторін під час російсько-української війни демонструє світу, що БПЛА можуть бути не лише одиничними загрозами для об’єктів критичної інфраструктури, але й новим етапом розвитку військової та інженерної науки. Багато країн світу починають створювати свої системи протидії ворожим безпілотним апаратам. Наприклад, Агенція зв'язку і інформації НАТО розробила недорогий прототип рішення для швидкого виявлення, ідентифікації і локалізації малих дронів, які можуть становити загрозу. Цей прототип, відомий як система ARTEMIS використовує електромагнітні хвилі для ідентифікації безпілотників і передові методи виявлення і класифікації радіочастотних сигналів, які використовують дрони. Обладнання успішно пройшло випробування у відкритих польових умовах і показало дуже багатообіцяючі результати для використання у зменшенні загрози, яку становлять комерційні дрони [2].

Для фізичного захисту ОКІ використовуються різноманітні технології, такі як системи контролю доступу, відеоспостереження, охоронні системи, датчики руху тощо. Оскільки ніхто не відміняв базових правил фізичного захисту об’єктів, але у зв’язку з розвитком технологій додаються і нові вектори протидії загрозам. Усі ці заходи спрямовані на запобігання несанкціонованому доступу до об'єктів критичної інфраструктури і вчасне виявлення можливих загроз.

Антитерористичні заходи: Україна активно здійснює заходи для протидії терористичній діяльності та забезпечення безпеки об'єктів критичної інфраструктури. Це включає зміцнення контролю на кордонах, розвиток спеціальних підрозділів, спрямованих на захист об'єктів критичної інфраструктури, та співпрацю з міжнародними партнерами з питань боротьби з тероризмом.

Узгоджена діяльність: Для ефективного захисту об'єктів критичної інфраструктури в Україні встановлені механізми узгодженої діяльності між різними органами влади, правоохоронними структурами та іншими зацікавленими сторонами.

Наприклад, створено Комітет з питань захисту критичної інфраструктури при Раді національної безпеки і оборони України, який координує дії урядових органів та відповідальних структур для забезпечення безпеки об'єктів критичної інфраструктури. Це дозволяє швидко реагувати на загрози та координувати заходи забезпечення безпеки.

1.2 Міжнародний досвід

Хоча не існує стандартного або універсального визначення критичної інфраструктури, багато західних країн визначають цей термін як фізичні та кібернетичні системи та активи, які є настільки життєво важливими для країни, що їхня непрацездатність або руйнування матиме виснажливий вплив на фізичну або економічну безпеку країни, а також на здоров'я та безпеку населення.

Певна соціально-економічна діяльність є життєво важливою для повсякденного економічного функціонування та безпеки країн. Хоча немає єдиної думки щодо того, які сектори вважати критично важливими, більшість країн, що мають затверджену національну політику у сфері захисту або безпека та стійкість критичної інфраструктури, визначають деякі або всі сектори (рис.1.1), як критично важливі об'єкти інфраструктури.

Рисунок 1.1 – Сектори критичної інфраструктури

Щоб проілюструвати взаємозв'язки між секторами критичної інфраструктури (рис.1.2), використані сині та червоні рамки для визначення та розмежування різних секторів. Червоні квадратики - транспорт, водопостачання, енергетика та зв'язок - відомі як сектори життєзабезпечення. Враховуючи їхню унікальну природу, можна виділити чотири основні характеристики, які відрізняють сектори життєзабезпечення від інших секторів критичної від інших секторів критичної інфраструктури.

По-перше, сектори життєзабезпечення надають необхідні послуги і товари, які підтримують більшість домівок, підприємств, громад і рівнів влади. По-друге, вони надають послуги, які є звичними у повсякденному житті, але перебої в їх наданні можуть призвести до виникнення небезпечних для життя може призвести до виникнення небезпечних для життя ситуацій. По-третє, сектори життєзабезпечення включають складні фізичні та електронні та електронні мережі, які взаємопов'язані між собою в різних секторах та між собою.

Нарешті, порушення в одному секторі життєзабезпечення може вплинути на інші сектори або вивести їх з ладу, створюючи каскадні вивести з ладу інші сектори, створюючи каскадні або ескалаційні збої. Сині рамки вздовж зовнішнього кільця

ілюструють інші сектори критичної інфраструктури, які зазвичай залежать від секторів життєзабезпечення для безперервної роботи.

Рисунок 1.2 – Взаємозв'язки між секторами критичної інфраструктури за методикою Міністерства внутрішньої безпеки США

В країнах НАТО існує спеціальне Командування об'єднаних збройних сил (КОЗС), яке використовує декілька визначень для ідентифікації і розуміння типів інфраструктури, наявної в певній зоні відповідальності. КОЗС визначає критичну інфраструктуру як "національні інфраструктурні активи, об'єкти, системи, мережі і процеси, які підтримують військове, економічне, політичне і/або соціальне життя, від яких залежить країна і/або НАТО". КОЗС також описує три підкатегорії критичної інфраструктури на основі відповідного рівня впливу на національні служби і/або операції НАТО:

- критична національна інфраструктура: активи, об'єкти, системи, і мережі, визначені територіально приймаючою країною, які є є невід'ємною частиною безперервного надання і цілісності основних послуг, на які покладається нація. послуг, на які покладається нація, руйнування або компрометація яких може призвести до компрометація яких може призвести до серйозних військових, економічних, політичних економічних, політичних або соціальних наслідків для країни;

- життєво важлива інфраструктура місії: активи, об'єкти, системи та мережі в районі проведення спільних операцій, які НАТО/збройні сили країн, що надають війська, забезпечують життєдіяльність місії. на які покладаються збройні сили країн, що надають війська, для забезпечення польових сил і засобів, руйнування або виведення з ладу яких окремо створює вирішальну шкоду місії НАТО;
- ключова інфраструктура: активи, засоби, системи і мережі в районі проведення об'єднаних операцій, які приймаюча країна або країна, що надає війська, або НАТО/національні війська або країни, що надає війська, покладаються на польові сили і засоби, руйнування або виведення з ладу яких, окремо або разом, створює значні перешкоди для країни, що приймає країні або місії НАТО.

Важливим питанням, над яким має замислитись НАТО, є те, якою мірою її загальна готовність місії залежить від гарантованої доступності критично важливої інфраструктури, більша частина якої належить компаніям приватного сектора в різних країнах-членах країнах-членах. Сьогодні, і вже деякий час, відповідь на це питання полягає в тому, що НАТО значною мірою залежить від цієї гарантованої доступності критично важливої інфраструктури.

Під час великих операцій або навчань, наприклад, приблизно 90 відсотків військових перевезень покладаються на цивільні кораблі, залізниці і літаки [3].

1.3 Аналіз кібернетичних загроз на об’єкти критичної інфраструктури

Кібератаки на об'єкти державного регулювання відрізняються тим, що націлені на основні об'єкти інфраструктури, такі як мережі громадського транспорту, великі будівлі, електростанції, дамби, водопостачання тощо. Будь-яке пошкодження або переривання такої необхідної інфраструктури, викликане проникненням, завдає величезної шкоди суспільству. На даний момент точна кількість видів атак та їх методів, які були розроблені людством з часу появи поняття кібератаки й до сьогоднішнього дня, не відома. Сучасні дослідження не виявили фундаментальних досліджень на цю тему. Ф. Коен показав математичні основи вірусної технології і

довів, що, оскільки кількість злоякісних кодів, які є підмножиною кібератак, є нескінченною, то й самі атаки також є нескінченними [4].

Сучасні кібератаки класифікуються за такими ознаками:

1) *За метою впливу на об'єкт атаки*, яка може бути спрямована, наприклад, на порушення цілісності чи конфіденційності інформації, захисту від несанкціонованого доступу, а також забезпечення живучості системи та надійності її функціонування. Закордонний та вітчизняний досвід показує, що для вирішення цих задач використовують методи криптографії в поєднанні з перевіреним і ліцензованим програмним забезпеченням, а також надійні інтелектуальні носії особливо важливої інформації. Останнім часом особлива увага приділяється живучості, яка визначає готовність збройних сил, промисловості, економіки, сільського господарства та суспільства загалом до збройних конфліктів і ліквідації наслідків терористичних актів, стихійних лих і техногенних катастроф.

2) *За принципіальним впливом на об'єкт атаки*:

- використання прихованих каналів – це шляхи передачі інформації, що дозволяють процесам обмінюватися нею способом, який порушує політику безпеки.
- використання прав суб'єкта системи (користувача, процесу) до об'єкта (файлів даних, каналів зв'язку тощо).

3) *За характерним впливу на об'єкт атаки*:

- активний вплив – коли користувач виконує дії, що виходять за рамки його обов'язків і порушують наявну політику безпеки, наприклад, пересилання службових файлів через власну електронну пошту тощо.
- пасивний вплив – коли користувач прослуховує лінії зв'язку між двома вузлами мережі тощо.

4) *За способами впливів на об'єкт атаки*, зокрема на систему дозволів та доступ до даних, програм, служб, каналів зв'язку, шляхом використання привілеїв.

5) *За засобами впливів на об'єкт атаки*, що включають використання стандартного або спеціально розробленого програмного забезпечення.

6) *За самим об'єктом атаки*: атака може спрямовуватися на систему в цілому, на процеси і підпроцеси з участю користувачів системи, на програми і дані,

що знаходяться на зовнішніх (дискові приводи, мережеві пристрої, термінали) або внутрішніх (оперативна пам'ять, процесор) пристроях системи, а також у каналах передачі даних. Метою таких атак може бути прямий вплив на роботу процесу (його зупинення, зміна привілеїв і характеристик) або зворотний вплив (використання зловмисником привілеїв, характеристик тощо іншого процесу у своїх цілях).

7) *За станом об'єкта*: під час атаки інформація в об'єкті може зберігатися, передаватися або оброблятися. Наприклад, під час передачі інформації по лініях зв'язку між вузлами мережі або всередині вузла можливий доступ до фрагментів переданої інформації шляхом перехоплення пакетів на ретрансляторі мережі або прослуховування з використанням прихованих каналів.

8) *За використовуваною системою захисту*, кількістю атакуючих, джерелами атак, розміщенням атакуючого об'єкта відносно атакованого, наявністю зв'язку з атакованим об'єктом, рівнем еталонної моделі OSI об'єкта, на який здійснюється вплив, тощо. Помилки системи захисту інформації можуть бути зумовлені, наприклад, помилками адміністративного управління, помилками в алгоритмах програм, а також у зв'язках між ними, помилками в програмному коді, тощо.

Беручи до уваги те, що нині переважну кількість кібернетичних атак на практиці не застосовують, більш близькою до реального життя вважається класифікація, запропонована П. Нойманом, який пропонує зосередити увагу на двадцяти шести основних типах таких дій (рис. 1.3), які можуть бути спрямованими проти інформаційних систем на об’єктах критичної інфраструктури.

Тип атаки		Спосіб здійснення	Результат
Зовнішні		Візуальне спостереження	Спостереження за клавіатурою або монітором
		Омана	Омана операторів або користувачів
		Вилучення сміття	Вилучення інформації із сміттєвих корзин
Апаратні		Логічне відновлення	Вилучення інформації з викрадених носіїв
		Прослуховування	Перехоплення даних
		Втручання	
		Фізична атака	Руйнування або ушкодження обладнання, джерел живлення
		Фізичне видалення	Вилучення обладнання або сховищ даних
Маскувальні		Імітування	Використання хибних ідентифікаторів
		Узурпація ліній зв'язку або хостів	
		Атака з підміною параметрів	
		Заплутування мереж	Маскування фізичного місця розташування або маршруту
Злоякісні програмні коди		Троянські коні	Упровадження злоякісного коду
		Логічні бомби	Різновид троянських коней
		Черв'яки	Заволодіння розподіленими ресурсами
		Віруси	Прикріплення до програм та розповсюдження
		Обхід	Обхід механізмів безпеки
		Експлуатація уразливостей	
		Зламування паролів	
Зловживання	Активне	Інкрементальні атаки	Поступова ескалація привілей, повільне просування до мети
		Відмова в обслуговуванні	Здійснення масованих атак
	Пасивне	Огляд	Випадковий або вибірковий пошук
		Збір та виведення даних	Використання баз даних та аналіз трафіку
		Приховані канали	Використання прихованих каналів або інших способів витоку інформації

Рисунок 1.3 – Основні типи кібернетичних атак за класифікацією П. Ноймана

Найбільш поширеними способами їх здійснення є mailbombing, сніфер пакетів, DoS і DDoS атаки, парольні атаки, атаки на рівні додатків типу логічних бомб і троянських коней, вірусні атаки, атаки з використанням мережевих черв'яків та так звані ін'єкції [5].

Наприклад, mailbombing, як спосіб здійснення кібернетичної атаки, за класифікацією британського математика П. Ноймана та інших спеціалістів полягає в бомбардуванні персонального комп'ютера цілі атаки електронною поштою. Сьогодні mailbombing практично не використовується у зв'язку зі застарілістю метода.

Сніфер пакетів є програмою, яка використовує мережевий інтерфейс для перехоплення мережевого трафіку, призначеного для інших вузлів, та його поступового аналізу. Сніфер має кілька режимів роботи, зокрема:

- звичайного "прослуховування", коли він моніторить мережевий інтерфейс;
- підключення сніфера до розриву каналу;
- відгалуження трафіку і спрямування його копії на сніфер;
- аналізу побічних електромагнітних випромінювань і відновлення прослуховуваного трафіку;
- атаки на канальному або мережевому рівні, що призводить до перенаправлення трафіку жертви або всього сегменту на сніфер, з подальшим поверненням трафіку в належну адресу.

Сніфер дозволяє виявляти зловмисний, вірусний і закільцьований трафік, шкідливе і заборонене програмне забезпечення, такі як мережеві сканери, флудери, троянські програми і т.д. Він також може перехоплювати незашифрований (іноді зашифрований) трафік, що призначений для користувача, з метою отримання особистих даних та іншої інформації. Крім того, сніфер може допомогти локалізувати несправність мережі або помилку в конфігурації мережевих агентів .

DoS (Denial of Service) атаки - це атаки на комп'ютерну систему або мережу, які спрямовані на перевантаження ресурсів та зниження доступності системи для легітимних користувачів. Існує кілька різновидів DoS атак, які можуть бути використані зловмисниками з різними цілями. Ось кілька типових різновидів DoS атак:

Атаки з використанням великого обсягу трафіку (Flooding Attacks): атаки, в яких атакуюча сторона намагається перевантажити ресурси цільової системи шляхом надсилання великого обсягу некоректного або зайвого трафіку. Ці атаки спрямовані на перевантаження мережевих ресурсів, таких як пропускна спроможність, процесорний час, пам'ять або інші ресурси, що використовуються для обробки запитів.

Ось кілька типових Flooding Attacks:

- SYN Flood: Ця атака використовує недолік в протоколі TCP/IP. Коли клієнт надсилає запит на встановлення з'єднання (SYN пакет) до цільового сервера, він очікує підтвердження (SYN-ACK пакет) від сервера перед тим, як завершити

процес з'єднання. У випадку SYN Flood, атакуючий генерує велику кількість SYN запитів до сервера, але не закінчує процес з'єднання, не надсилаючи підтвердження (ACK пакет). Це призводить до того, що сервер витрачає ресурси на обробку недійсних з'єднань та очікування підтвердження, що призводить до перевантаження і зниження доступності сервера для легітимних користувачів;

- ICMP Flood (Ping Flood): В цій атаці зловмисник відправляє велику кількість ICMP Echo Request (Ping) пакетів до цільового сервера або мережі. Кожен пакет вимагає підтвердження (ICMP Echo Reply) від сервера. За великої кількості пакетів, що надсилаються, це може призвести до перевантаження пропускної спроможності мережі або обробки ICMP запитів на сервері, що спричиняє зниження доступності мережі для легітимних користувачів;
- UDP Flood: У цій атаці зловмисник надсилає велику кількість UDP (User Datagram Protocol) пакетів до цільового сервера або мережі. UDP пакети є пакетами, що не вимагають підтвердження доставки, що робить їх привабливими для зловмисників. Велика кількість недійсних UDP пакетів може спричинити перевантаження ресурсів сервера, таких як обробка запитів і відповідей, що призводить до зниження доступності.

Ці атаки націлені на перевантаження ресурсів цільової системи, що може призвести до зниження доступності для легітимних користувачів. Для захисту від Flooding Attacks, можна використовувати спеціалізовані мережеві пристрої, які виявляють і блокують такий надмірний трафік, а також конфігурувати сервери та мережеві пристрої для відповіді на такі атаки ефективним способом.

Атаки на ресурси (Resource Exhaustion Attacks): атаки, спрямовані на вичерпання ресурсів цільової системи шляхом перевантаження або виснаження певних ресурсів, необхідних для нормальної роботи системи. Ці атаки мають на меті використати обмежену природу ресурсів, таких як пропускна спроможність мережі, процесорний час, пам'ять або дисковий простір, для створення відмови в обслуговуванні.

Ось кілька типових Resource Exhaustion Attacks:

- Bandwidth Exhaustion: Ця атака спрямована на використання великого обсягу мережевого трафіку для перевантаження пропускної спроможності мережі. Атакуюча сторона намагається використати всю доступну пропускну спроможність шляхом надсилання великої кількості пакетів або великого обсягу даних до цільової системи. Це може призвести до витрати всієї пропускної спроможності і зниження доступності системи для легітимних користувачів;
- CPU Exhaustion: Ця атака має на меті виснажити процесорний час цільової системи. Зловмисник намагається завдати великого навантаження на процесор шляхом запуску інтенсивних обчислювальних завдань або надсилання великої кількості запитів, які вимагають значних обчислень для обробки. Це може спричинити зниження продуктивності системи і відмову в обслуговуванні;
- Memory exhaustion: Ця атака спрямована на вичерпання пам'яті цільової системи. Зловмисник надсилає велику кількість запитів або даних, які займають значну кількість пам'яті, або спричиняє утворення витоків пам’яті, що призводять до поступового вичерпання доступної пам'яті. Це може призвести до падіння системи або зниження її доступності;
- Disk space exhaustion: У цій атаки атакуюча сторона намагається заповнити дисковий простір цільової системи, створюючи великий обсяг даних або файлів. Це може призвести до вичерпання дискового простору, що може призвести до відмови в обслуговуванні або неможливості зберігання додаткових даних.

Ці атаки намагаються використати обмежені ресурси системи для створення відмови в обслуговуванні або зниження доступності. Для захисту від Resource Exhaustion Attacks, важливо використовувати механізми моніторингу та управління ресурсами, які можуть виявляти надмірне використання ресурсів і застосовувати відповідні заходи для обмеження впливу атак. Також важливо належним чином конфігурувати систему та мережеві пристрої для запобігання надмірному використанню ресурсів та обробки некоректних або шкідливих запитів.

Атаки на вразливості програмного забезпечення: атаки, які використовують вразливості або слабкі місця в програмному забезпеченні для отримання несанкціонованого доступу до системи або виконання шкідливого коду. Вразливості

програмного забезпечення можуть виникати через помилки у розробці, недостатню перевірку введених даних, недостатню обробку помилок або використання застарілих компонентів.

Ось кілька типових атак на вразливості програмного забезпечення:

- використання вразливостей буферу: Ця атака використовує недолік у програмі, який дозволяє зловмиснику записувати додаткові дані поза виділену область пам'яті буферу. Зловмисник може змінити значення змінних, викликати некоректну роботу програми або виконати віддалений код;
- використання SQL-ін'єкцій: Ця атака використовує вразливість, коли вхідні дані, передані в SQL-запит, не перевіряються або очищуються від небезпечних символів. Зловмисник може використовувати цю вразливість, щоб виконати шкідливі SQL-запити, отримати доступ до бази даних або змінити, видалити чи викрасти дані;
- Cross-site scripting (XSS): Ця атака використовує вразливість, коли вхідні дані, які вводяться користувачем, не достатньо фільтруються перед виведенням на веб-сторінку. Зловмисник може вбудувати шкідливий скрипт у сторінку, який буде виконуватися в браузері користувача, що може призвести до крадіжки сесійних файлів, перехоплення даних або виконання інших шкідливих дій;
- використання вразливостей веб-додатків: Ця атака використовує вразливості веб-додатків, такі як недостатня перевірка доступу, використання слабких алгоритмів шифрування або недостатня перевірка коректності введених даних. Зловмисник може отримати доступ до неприпустимих даних, змінити конфігурацію додатку або зламати систему [6].

Для захисту від атак на вразливості програмного забезпечення, важливо приділяти увагу безпеці під час розробки програмного забезпечення. Це включає правильну перевірку та обробку введених даних, використання безпечних алгоритмів шифрування, регулярне оновлення компонентів та бібліотек, а також проведення тестування на вразливості. Також можна використовувати захисні механізми, такі як брандмауери, системи виявлення вторгнень (IDS) та веб-файрволи, для виявлення та блокування атак на вразливості програмного забезпечення.

Атаки на протоколи мережі: ці атаки спрямовані на вразливості або слабкі місця в протоколах комунікації, використовуваних у комп'ютерних мережах. Протоколи мережі встановлюють правила і процедури обміну даними між комп'ютерами, і вразливості в цих протоколах можуть бути використані зловмисниками для здійснення різних видів атак.

Ось кілька типових атак на протоколи мережі:

- ARP (Address Resolution Protocol) Spoofing: Ця атака використовує вразливість в ARP протоколі, який використовується для відображення IP-адрес на MAC-адреси в локальних мережах. Зловмисник надсилає фальшиві ARP-повідомлення, щоб перехопити мережевий трафік, перенаправити його до свого комп'ютера або змінити дані, які передаються;
- DNS (Domain Name System) Spoofing: Ця атака використовує вразливість в DNS протоколі, який використовується для перетворення доменних імен на IP-адреси. Зловмисник може вплинути на записи DNS або надіслати фальшиві DNS-відповіді, що призводить до перенаправлення користувачів на хибні веб-сторінки або перехоплення їхньої комунікації;
- TCP/IP Hijacking: Ця атака використовує вразливості в TCP/IP протоколах, які використовуються для передачі даних в мережі. Зловмисник може перехоплювати пакети даних, змінювати їх вміст або надсилати фальшиві пакети, що може призвести до підробки ідентичності або втручання в комунікацію між двома сторонами;
- ICMP (Internet Control Message Protocol) Flooding: Ця атака використовує перевантаження мережі широкомовними ICMP-повідомленнями. Зловмисник надсилає велику кількість ICMP-пакетів до цільового комп'ютера, що призводить до перевантаження його ресурсів, включаючи мережеву пропускну здатність, процесор та пам'ять;
- SYN Flooding: Ця атака використовує вразливість в протоколі TCP при встановленні з'єднання. Зловмисник надсилає велику кількість підроблених SYN-пакетів до цільового сервера, не завершуючи процесу рукостискання (handshake). Це

призводить до вичерпання ресурсів сервера та недоступності для легітимних користувачів [7].

Для захисту від атак на протоколи мережі важливо використовувати механізми захисту на рівні мережі та системи, такі як брандмауери, IDS/IPS системи, шифрування комунікації та автентифікація. Також важливо регулярно оновлювати програмне забезпечення та протоколи, щоб виправити виявлені вразливості та використовувати захищені версії протоколів, які включають у себе вдосконалення безпеки.

Атака на пропускну спроможність (Bandwidth Attacks): атака, що має на меті перевантаження мережевої пропускної здатності, щоб знизити або блокувати доступ легітимним користувачам до ресурсів мережі. Це досягається широким використанням ресурсів мережі, таких як пропускна здатність, ширина смуги або оброблювальна потужність, що перевищує їхні можливості.

Ось кілька типових атак на пропускну спроможність:

- UDP (User Datagram Protocol) Flood: Ця атака використовує перевантаження мережі UDP-пакетами. Зловмисник надсилає велику кількість UDP-пакетів до цільового сервера або мережевого пристрою, що призводить до переповнення мережевого каналу і витрати пропускної здатності;
- TCP (Transmission Control Protocol) SYN Flood: Ця атака використовує вразливість в протоколі TCP при встановленні з'єднання. Зловмисник надсилає велику кількість підроблених SYN-пакетів до цільового сервера, не завершуючи процесу рукостискання (handshake). Це викликає зайве навантаження на сервер та витрату пропускної здатності;
- ICMP Echo Request Flood (Ping Flood): Ця атака використовує перевантаження мережі ICMP Echo Request пакетами (протокол Ping). Зловмисник надсилає велику кількість запитів Ping до цільового пристрою, вимагаючи відповідей, що призводить до переповнення пропускної здатності і недоступності для легітимного мережевого трафіку;
- HTTP (Hypertext Transfer Protocol) Flood: Ця атака використовує велику кількість запитів HTTP до веб-сервера або веб-додатка. Зловмисник надсилає велику

кількість запитів, намагаючись перевантажити сервер і знизити пропускну здатність, що призводить до витрати ресурсів і недоступності для легітимних користувачів [8].

Для захисту від атак на пропускну спроможність можна використовувати різні методи та технології:

- брандмауери та фільтри: Налаштуйте брандмауери та фільтри, щоб обмежити кількість пакетів, які можуть пройти через мережеві пристрої. Це допоможе виявити та блокувати атаки, що спрямовані на перевантаження пропускної здатності;
- використання технологій Quality of Service (QoS): Встановлення правил QoS дозволяє пріоритезувати трафік у мережі, гарантуючи важливим даним високу пропускну здатність. Це дозволяє забезпечити ефективне використання пропускної здатності і запобігти перевантаженню;
- інтелектуальні системи виявлення вторгнень (IDS) та системи запобігання вторгнення (IPS): Використання IDS/IPS дозволяє виявляти та блокувати атаки, які спрямовані на перевантаження пропускної здатності. Вони можуть розпізнавати аномальний мережевий трафік та вживати заходів для його обмеження;
- моніторинг трафіку: Ретельний моніторинг мережевого трафіку може допомогти виявити атаки на пропускну спроможність та забезпечити вчасну реакцію. Це дозволяє виявляти незвичайний або надмірний трафік та вживати заходів для його обмеження;
- розподілені системи мережевого оброблення: Використання розподілених систем мережевого оброблення може допомогти розподілити навантаження та запобігти перевантаженню окремих ресурсів. Це дозволяє підвищити загальну пропускну здатність і забезпечити більшу стійкість до атак;
- регулярне оновлення: Важливо підтримувати оновлення мережевих пристроїв та програмного забезпечення, включаючи патчі безпеки та оновлення протоколів. Це допоможе заповнити вразливості, які можуть бути використані зловмисниками для атак на пропускну спроможність [9].

Використання комбінації цих заходів допоможе забезпечити ефективну захисту пропускної спроможності мережі і запобігти перевантаженню, забезпечуючи доступ до ресурсів легітимним користувачам.

Вище було описано лише кілька прикладів типових DoS атак та заходів захисту. Зловмисники постійно шукають нові способи атаки на системи та мережі, тому важливо бути завжди свідомими про потенційні загрози та захищатися від них за допомогою відповідних заходів безпеки.

Враховуючи, що нинішнє століття ознаменувалося стрімким зростанням темпу розвитку інформаційних технологій та їх широким застосуванням у всіх сферах людської діяльності. З одного боку, це дало змогу суттєво збільшити продуктивність праці, а, з іншого, поклало початок такому інформаційному виду злочинності.

Виходячи з усього переліченого, можна стверджувати, що позбутися деструктивного впливу кібернетичних атак сьогодні практично неможливо. Тим не менш, є можливість використати певні загальні шляхи для послаблення їх негативних наслідків.[4].

1.4 Атаки на ОКІ за час широкомасштабного вторгнення російської федерації в Україну

Росія оголосила війну Україні 24 лютого 2022 року, але після незаконної анексії Росією Криму в 2014 році російські кібератаки на Україну тривали та посилювалися перед повномасштабним вторгненням у 2022 році (Рисунок 1.4). У цей період найбільше постраждали державний, енергетичний, медійний, фінансовий, комерційний та некомерційний сектори України. Поодинокі російські кібератаки перешкоджають розподілу медикаментів, продуктів харчування та екстреної допомоги з 24 лютого. Ці атаки мали різні наслідки – від блокування доступу до основних сервісів до викрадення даних і поширення дезінформації, в тому числі за допомогою методів «deepfake». Інша зловмисна кіберактивність включає фішингові електронні листи, розподілені атаки на відмову в обслуговуванні, зловмисне

програмне забезпечення для знищення даних, бекдори, програмне забезпечення для спостереження та крадіжку інформації [10].

Рисунок 1.4 – Хронологія кібернетичних атак на Україну

За словами заступника міністра енергетики з питань цифрового розвитку, цифрових трансформацій та цифровізації Фаріда Сафарова, за весь 2021 рік було

зафіксовано 900 000 кібератак у енергетичному секторі. Сафаров наголосив, що інтенсивні кібератаки на український енергетичний сектор ворог почав ще до 24 лютого 2022 року, але успіху не досяг. Загальна кількість кібератак за перші 9 місяців війни складає понад 1,2 млн випадків. Кількість DDos-атак на сайти ключових енергетичних компаній і Міністерства енергетики сягнула понад 50. Для порівняння з початку фіксації такого типу атак з 2019 року їх було тільки 5 [11].

Атака 15 лютого 2022 року

В якості перевірки стійкості системи кібернетичної безпеки основних об'єктів критичної інфраструктури перед широкомасштабним вторгненням, під керівництвом відповідальних департаментів Головного управління Генерального штабу Збройних Сил РФ, було проведено одну з найбільших у світі атак націлених на об'єкти однієї країни. У ніч з 15 на 16 лютого Україною прокотилася хвиля масштабних кібератак. Найбільше постраждали банки, потім сайти українських правоохоронних органів (ЗСУ, Міноборони тощо). У ніч на 16 лютого були атаковані урядові портали та інші державні установи. Спочатку користувачі мережі скаржилися на проблеми з доступом до "Приватбанку". Це сталося 15 лютого близько 17:00. У банку заявили, що збій стався через проблеми з сервером. Банкомати працюють нормально. Цікаво, що раніше цього дня багатьом українцям прийшли смс-повідомлення нібито від «приватних банків» із попередженням про те, що «банкомати не працюватимуть». Пізніше клієнти Ощадбанку почали скаржитися: мовляв, додаток і онлайн-сервіси недоступні, вони не можуть зняти або внести гроші на свої картки. Водночас співзасновник monobank зазначив, що майже всі банки постраждали від атаки — деякі відчули менше, деякі більше. Потім стало гірше. Перестав працювати сайт Збройних сил України, іноді виникали проблеми з ресурсами МВС, а також сайту Міністерства оборони. Хакери також атакували Дія. За словами міністра цифрової трансформації Михайла Федорова: «600 тис. пакетів шкідливого трафіку в секунду надходить з Росії та Китаю. Після того, як цю хвилю було відкинуто, атаки повернулися — вже з Чехії та Узбекистану». Серйозні збої, хоча деякі користувачі помітили проблеми з програмою. Усі ці збої були спричинені масовими DDoS-атаками, пояснили в Центрі стратегічних комунікацій та інформаційної безпеки. Після невеликої перерви наступ

продовжився вночі з 15 на 16 лютого. Зокрема, виникли труднощі з доступом до сайту Кабінету Міністрів України. станом на 1 ночі 16 лютого не було доступу до сайтів Міносвіти та науки, Держслужби з надзвичайних ситуацій, Міністерства молоді та спорту, Міністерства інформаційної політики, Збройних сил України. З перебоями працювали сайти Мін'юсту, Мінфіну, Мінінфраструктури, Мінцифри, Служби безпеки, МВС, МЗС, Офісу генпрокурора та Національної поліції. Користувачі мережі повідомляли й про проблеми на сайті президента [12].

За інформацією урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA, було виділено основні способи реалізації зловмисного задуму:

- розсилання фейкових SMS-повідомлень громадянам про, начебто, порушення штатного режиму функціонування банкоматів окремих державних фінансових установ;
- розсилання електронних поштових повідомлень серед низки фінансових установ про мінування приміщень та будівель останніх. Було встановлено, що зазначена діяльність може здійснюватися мешканцем Донецької області;
- проведення розподілених атак на відмову в обслуговуванні (DDoS) у відношенні веб-ресурсів українських банків та державних установ. В рамках дослідження, в тому числі, з урахуванням інформації від партнерів, визначено, що до здійснення атак, серед іншого, залучено бот-мережі Mirai (https://twitter.com/360Netlab/status/1493797519725367302) та Meris (шкідливий інформаційний потік спрямовується через тисячі зламаних маршрутизаторів Mikrotik та ряду інших IoT пристроїв з фільтрацією джерел за допомогою ACL, що дозволяє приховати згадані пристрої від пошукових систем на кшталт Shodan). Зазначене, з високим рівнем впевненості, дозволяє припустити, що для проведення атак використано наявні потужності зловмисників, що надаються як послуга (DDoS as a Service).;
- унеможливлення доступу до веб-ресурсів в зоні gov.ua шляхом здійснення DDoS-атаки на обслуговуючі DNS-сервери (https://hostmaster.ua/news/?pr20220216). Виведення з ладу декількох серверів доменних імен призвело до тимчасового порушення доступу до значної кількості веб-

ресурсів державних органів у зв'язку з неможливістю визначення А-запису (IP-адреси) для відповідних доменних імен;

- підозріла маніпуляція з налаштуваннями автономних систем на рівні протоколу BGP. Так, за даними Cisco Crosswork (http://bgpstream.com/event/287011) протягом більше ніж двох годин, починаючи з 15:30 15.02.2022, префікс 217.117.7.0/24, який фактично належить Inq-Digital-Nigeria-AS (AS16284), було анонсовано від імені автономної системи Приватбанку (AS15742) через автономну систему нігерійського оператора телекомунікацій AS37148 [13].

Можна вважати, що атака не принесла бажаних результатів зловмиснику, оскільки не було повідомлено про масовий витік даних чи вагомий збиток, що міг бути нанесений цілям атаки. Спеціалісти зазначають, що найімовірніше атака була здійснена з метою розвідки для визначення рівня кібербезпеки атакованих цілей.

Атака 28 березня 2022 року

За словами голови дирекції інформаційних технологій АТ «Укртелеком» Кирила Гончарука: «Укртелеком як частина критичної інформаційної інфраструктури України постійно перебуває у центрі уваги хакерів. Ми спостерігаємо зростання кількості кібератак на нашу інфраструктуру від самого початку вторгнення в Україну. Атака, яка відбулась 28 березня, була потужною та складною».

Кібератака на "Укртелеком" проводилася в два етапи. Перший – фаза дослідження (discovery). Атака була здійснена з території України, яка нещодавно була тимчасово окупована Росією. Хакери використовували скомпрометовані облікові записи співробітників компанії для отримання розвідувальної інформації. Під час першого етапу вони також намагалися скомпрометувати облікові записи інших співробітників. Під час кібератаки хакери намагаються проаналізувати, як влаштована IT-інфраструктура постачальника. Команда SOC Укртелекому оперативно виявила та нейтралізувала цю кібератаку.

Другим етапом стала кібератака 28 березня, під час якої хакери намагалися вивести з ладу обладнання та сервіси компанії та взяти під контроль мережу та обладнання «Укртелекому». Спробуйте змінити паролі для корпоративних облікових записів співробітників, пристроїв і брандмауерів. Друга спроба атаки на

інфраструктуру була зафіксована протягом 15 хвилин після її початку, і IT-спеціалісти «Укртелекому» негайно вжили заходів для протидії кібератаці. Для захисту критичної інформаційної інфраструктури, а також безперервного надання послуг військовим та критичній інфраструктурі країни Укртелеком тимчасово обмежив доступ до послуг приватним користувачам та бізнесу. Трафік у мережі упав до 13% від нормального режиму функціонування мережі. Доступ до інтернету для клієнтів почали відновлювати ввечері 28 березня. Наступного дня сервіси Укртелекому стали майже повністю доступними для всіх споживачів.

Укртелеком попередив про кібератаку Держспецзв'язку та координувався з фахівцями служби під час її усунення. До ліквідації наслідків кібератаки були залучені як вітчизняні, так і міжнародні партнери провайдера, зокрема Cisco, Microsoft та ISSP.

Відповідно до поточних результатів розслідування, внаслідок кібератаки дані користувачів не постраждали і не були скомпрометовані [14].

Висновки за розділом 1

Проаналізовано українські та міжнародні стратегії захисту об’єктів критичної інфраструктури і найбільші кібернетичні атаки на ОКІ за час повномасштабного вторгнення російської федерації.

Розглянуто вимоги Закону України «Про критичну інфраструктуру» від 18.10.2022, в якому визначено життєво важливі функції та/або послуги і категорії критичності ОКІ. Нажаль, закон було прийнято занадто пізно (під час широкомасштабного вторгнення) і багато об’єктів, що підпадають під дію закону мають впроваджувати визначені вимоги у нештатному робочому процесі.

Приведено критерії, за якими виділяють об’єкти критичної інфраструктури різноманітні країни світу. Найбільш популярними та деталізованими є методики Сполучених Штатів Америки та країн військового блоку НАТО. Визначено сектори та взаємозв’язки між об’єктами, а також три підкатегорії критичної інфраструктури на основі відповідного рівня впливу на національні служби.

Проаналізовано найпоширеніші типи атак на об’єкти критичної інфраструктури. Визначено їх ключові особливості реалізації. Проаналізовано класифікацію типів атак, що дозволяє організаціям володіти точною інформацією про тип системи захисту інформації, яку слід використати відповідно до встановлених в організації стандартів безпеки і типу інформаційної системи. . З кожним роком з’являються все нові і нові шляхи несанкціонованого доступу до конфіденційної інформації, зловмисники підвищують свою кваліфікацію та все більше спроб порушення працездатності інформаційних системна об’єктах критичної інфраструктури. Вони становлять суттєву загрозу не тільки самим ОКІ, а й суспільству та державі. Тому активна розбудова систем захисту інформації від найбільш можливих видів кібернетичних атак є пріоритетним напрямком уповноважених органів.

Проаналізована статистика кібернетичних атак на українські об’єкти критичної інфраструктури за час початку повномасштабної агресії російської федерації. Детально розглянуто 2 атаки. Атака 15 лютого 2022 року була підготовчою задля визначення рівня кібернетичної стійкості ОКІ України. Дана DDoS-атака на кілька годин заблокувала доступ до веб-сайтів українських державних установ, банків, радіостанцій. Атака 28 березня 2022 була націлена на АТ «Укртелеком» - одну з найбільших телекомунікаційних компаній країни. Зловмисники намагалися проникнути в роботу та захопити керування системою управління компанії. За інформацією з відкритих джерел, кібернетичні атаки не досягли своєї мети повністю.

З усього вище наведеного можна зробити висновок, що об’єкти критичної інфраструктури в усьому світі являються пріоритетними цілями не тільки для зловмисних кібернетичних угрупувань, але й для державних структур, що таким чином намагаються вести протиборчі дії з державами–опонентами. Тому захист ОКІ є одним з важливих напрямків національної оборони держави.

РОЗДІЛ 2
СУЧАСНІ МЕТОДИ ВИЯВЛЕННЯ СТОРОННІХ КІБЕРНЕТИЧНИХ ВПЛИВІВ У КОМП'ЮТЕРНІЙ МЕРЕЖІ

Одним з найпрогресивніших рішень задля виявлення сторонніх кібернетичних впливів є впровадження рішення, здатного виявити сторонній вплив на мережу. Система виявлення вторгнень (атак) (англ. Intrusion Detection System, IDS) — програмний або апаратний засіб, призначений для виявлення фактів несанкціонованого доступу в комп'ютерну систему або мережу або несанкціонованого управління ними в основному через Інтернет [15]. СВВ можуть класифікуватися за багатьма ознаками: за методами виявлення, за об'єктом моніторингу, за способом прийняття рішень, за технологією прийняття рішення, за способом реакції на атаку, за часом реакції на атаку. Але для детального вивчення варто обрати одну з ознак. Отож, за методами виявлення системи поділяються на:

- сигнатурний пошук;
- виявлення аномалій ;
- гібридний метод.

2.1 Огляд систем виявлення вторгнень

2.1.1 Історія розвитку систем виявлення вторгнень

Історія розвитку систем виявлення вторгнень починається з розповсюдження комп'ютерних мереж у 1980-х роках. З тих пір системи СВВИ постійно еволюціонували та адаптувалися до зростаючих загроз та нових технологій. Оригінальна концепція СВВ народилася завдяки Джеймсу Андерсону та його статті 1980 року «Моніторинг і моніторинг загроз комп'ютерній безпеці». У 1984 році Фред Коен заявив, що неможливо виявити всі вторгнення, і що в міру використання комп'ютерних технологій ресурси, необхідні для виявлення вторгнень, збільшуються.

Дороті Деннінг за сприяння Пітера Ньюмана в 1986 році опублікувала модель СВВ [16], яка лягла в основу більшості сучасних систем. Їхня модель використовувала статистичні методи для виявлення вторгнень і отримала назву IDES (Intrusion Detection Expert System). Система працювала на робочій станції Sun і перевіряла як мережевий трафік, так і дані користувача програми [17]. IDES використовував два підходи до виявлення вторгнень.

Експертні системи використовувалися для визначення відомих типів вторгнень і використовувася компоненти виявлення на основі статистичних методів і профілів користувачів і систем у захищеній мережі. Тереза Лунт запропонувала використовувати штучну нейронну мережу як третій компонент для підвищення ефективності виявлення [18]. У 1993 році за IDES послідувала NIDES (Експертна система виявлення вторгнень наступного покоління). MIDAS (Multics Intrusion Detection and Alerting System), експертна система, яка використовувала P-BEST і LISP, була розроблена в 1988 році на основі роботи Деннінга і Неймана [19]. У цьому ж році була розроблена система Haystack на основі статистичних методів [20]. W&S (Wisdom & Sense) — це детектор аномалій, заснований на статистичних методах, розроблений у 1989 році в Національній лабораторії Лос-Аламоса [21]. W&S створив правила на основі статистичного аналізу та використовував ці правила для виявлення аномалій. У 1990 році виявлення аномалій було реалізовано в Time-based Induction Machine (TIM) з використанням індуктивного навчання на основі узгоджених шаблонів користувача мовою Common LISP [22]. Ця програма була розроблена для VAX 3500. Приблизно в той же час був розроблений NSM (Network Security Monitor) для виявлення аномалій на робочих станціях Sun 3/50 шляхом порівняння матриць доступу [23]. У тому ж 1990 році було розроблено ISOA (Assistant Information Security Officer) [24], який включає багато стратегій виявлення, включаючи статистику, перевірку профілю та експертні системи. Розроблений у AT&T Bell Labs, ComputerWatch використовує статистичні методи та правила для аналізу даних і виявлення зловмисників [25].

2.1.2 Сучасні системи виявлення вторгнень

Найбільш популярними на ринку є три системи виявлення вторгнень – Snort, Suricata та OSSEC, що зарекомендували себе як сучасні комплекси на різноманітних підприємствах.

Snort (розробка компанії Sourcefire, США) на світовому рівні є найпоширенішою безкоштовною мережевою системою виявлення та запобігання вторгнень.

Основні особливості системи Snort:

- аналіз мережевого трафіку: Snort виявляє потенційно шкідливі або несправедливі дії, аналізуючи мережевий трафік. Він зчитує трафік з мережевих інтерфейсів або зчитує пакети з раніше записаного дампу;
- виявлення вторгнень: Snort застосовує набір правил для виявлення патернів, характерних для відомих атак або аномальної поведінки. Ці правила описують типи атак, сигнатури зловмисного програмного забезпечення або ненормальні пакети, що вказують на можливі вторгнення;
- гнучкість налаштування: Snort дає можливість користувачам налаштувати систему залежно від їх потреб і середовища. Вони можуть використовувати існуючі правила, редагувати їх або створювати власні правила для виявлення специфічних загроз або вразливостей;
- логування та сповіщення: Snort може записувати подробиці про виявлені атаки або події, пов'язані з кібербезпекою, у журнали. Крім того, він може надсилати сповіщення адміністраторам через електронну пошту, SMS або інші механізми сповіщення;
- інтеграція з іншими системами: Snort може використовуватись як самостійний інструмент або інтегруватись з іншими системами, такими як системи керування подіями та інцидентами (SIEM) або системи автоматизації безпеки.

Архітектура системи розроблена з урахуванням ефективності та швидкості в роботі. Тому, вона абсолютно проста і складається з:

- декодера пакетів;

- ядра виявлення;
- підсистеми оповіщення та реагування.

Декодер виконує набір процедур для послідовної розборки пакетів згідно з рівнями мережевого стека. Він перетворює прийнятий кадр на пакет, сегмент і блок даних, враховуючи атрибути сигнатур, специфічні для кожного рівня мережі. Протоколи канального рівня, такі як Ethernet, SLIP, PPP і ATM, підтримуються.

Ядро системи інтегрує існуючі правила в ланцюжки, які утворюють двовимірні послідовності для кожного пакета. Підсистема оповіщення та реагування відповідає за збереження результатів аналізу трафіку в журналах Snort або передачу їх системним службам реєстрації подій ОС.

Система використовує просту мову опису атак, що дозволяє адміністраторам розширювати базу сигнатур самостійно. Кожне правило містить умову застосування і дії. В останніх версіях системи з'явилася конструкція для класифікації мережевого трафіку за ступенем потенційної небезпеки, визначеної експертом, який формує атрибути кібератаки. Snort також виконує функції протоколювання, аналізу та пошуку за вмістом і широко використовується для блокування або виявлення різних типів атак, таких як атаки на переповнення буфера, сканування портів, атаки на веб-додатки, SMB-зондування, визначення ОС тощо.

Snort працює на основі сигнатурного методу, який дозволяє швидко виявляти задекларовані кібератаки, але не здатний до повного виявлення нових атак. Він є програмним продуктом з відкритим вихідним кодом, що дозволяє легко змінювати його структуру. Snort може реєструвати пакети та аналізувати трафік в реальному часі в IP-мережах. Відкрита архітектура та початковий текст системи сприяють її швидкому розвитку та інтеграції з різними програмними продуктами, включаючи бази даних журналів виявлення, аналізатори журналів реєстрації тощо.

Модуль аналізу трафіку використовує правила (сигнатури) для виявлення атак. Модулі сторонніх розробників (препроцесори) можуть інтегруватися до ядра виявлення й здійснювати аналіз на певному рівні розбору пакетів. Такі модулі дозволяють розширити функціональність ядра виявлення та реалізувати різні методи

виявлення. Крім того, Snort було розширено, щоб включити модуль статистичного аналізу, призначений для виявлення аномалій у мережевому трафіку.

Ця система реалізує централізоване управління станціями. Snort є системою з відкритим кодом, тому продукт можна легко розширити та адаптувати до ваших потреб. Ця система дозволяє ефективно використовувати існуючі правила та створювати власні нові правила для виявлення атак виключно на основі аналізу мережевого трафіку. Підсистема Alert and Response містить основні способи реагування на кібератаки (відключення або блокування об'єктів атаки). Механізм захисту Snort реалізований протоколом SNMPv2, який використовує шифрування пароля під час передачі даних. Програмне забезпечення Snort працює на Unix, Linux і Windows [26].

Suricata (розробка компанії Open Information Security Foundation, Бостон, США) має відкритий код, є безкоштовним, швидким, надійним та перспективним засобом виявлення мережевих загроз. Він призначений для запобігання та виявлення вторгнень у режимі реального часу, моніторингу мережевої безпеки, автоматичного аналізу та обробки PCAP–файлів.

Основні особливості системи Suricata:

- мережевий аналіз: Suricata використовує різноманітні методи аналізу мережевого трафіку для виявлення потенційно шкідливих або несправедливих дій. Вона підтримує розподілене аналізованої трафіку, аналіз трафіку в реальному часі, розпізнавання протоколів та інші техніки для ефективного виявлення загроз;
- виявлення загроз: Suricata використовує набір правил і навчальних алгоритмів для виявлення сингатур атак, аномальної поведінки та вразливостей. Ці правила описують різноманітні типи загроз, включаючи відомі сигнатури атак, а також використовуються алгоритми машинного навчання для виявлення незвичайної активності;
- мультиплатформеність: Suricata є мультиплатформеною системою, що підтримує різні операційні системи, включаючи Linux, Windows і FreeBSD. Це дозволяє використовувати Suricata в різних середовищах та інтегрувати його з різноманітними мережевими інфраструктурами;

- швидкодія: Suricata володіє високою швидкодією обробки мережевого трафіку завдяки використанню розподіленої архітектури та оптимізованих алгоритмів. Вона здатна працювати на високопродуктивних мережах з великим обсягом трафіку;
- інтеграція з іншими системами: Suricata може легко інтегруватись з іншими системами, такими як системи керування подіями та інцидентами (SIEM) або системи автоматизації безпеки. Це дозволяє забезпечити комплексний підхід до безпеки мережі.

Засоби перевірки HTTP-трафіку в Suricata базуються на бібліотеці HTP. Вони забезпечують контроль файлів, що передаються через HTTP, розбір стисненого контенту та ідентифікацію за URI, cookie, заголовками та іншими атрибутами. Можна виділити контент у потоці за допомогою масок і регулярних виразів, а також ідентифікувати файли за їх назвою, типом або контрольною MD5-сумою [27].

Програмний засіб Suricata має централізоване управління та швидко виявляє уразливості та атаки завдяки розподіленій роботі між ядрами процесора та потоками. Він здійснює спостереження за системою на системному та мережевому рівнях.

У випадку кібератаки Suricata оперативно реагує, якщо порушено принаймні одне з налаштованих правил, шляхом маркування отриманих пакетів даних за допомогою одного з трьох маркерів:

- NF_ACCESS (доступ наданий);
- NF_DROP (доступ заборонений);
- NF_REPEAT (пакети маркуються та повторно направляються на правила брандмауера, який і вирішує подальше призначення відповідного пакету).

Це дозволяє швидко і ефективно реагувати на потенційні загрози та забезпечує безпеку мережі.

OSSEC (Open Source SECurity, розробка Daniel B., корпорація Atomicorp є виробником ОС Linux, яка включає OSSEC як одну з основних технологій, США) це масштабована, багатоплатформерна, вузлова СВВ на основі хоста з відкритим вхідним кодом.

Основні особливості системи OSSEC:

- розподілена архітектура: OSSEC працює у розподіленій архітектурі, що дозволяє розгортати агенти на кількох хостах і централізовано управляти цими агентами. Це особливо корисно для великих мереж або розподіленої інфраструктури;
- виявлення вторгнень: OSSEC виявляє атаки та вторгнення, аналізуючи журнали подій, реєстраційні файли, мережевий трафік та інші джерела інформації. Вона використовує набір правил та розпізнавання сигнатур для виявлення ненормальної активності, специфічних сигнатур атак або підозрілих дій;
- централізоване керування: OSSEC надає централізоване керування всіма агентами та серверами, що дозволяє адміністраторам налаштовувати правила виявлення, перевіряти статус системи та отримувати сповіщення про події через один інтерфейс;
- попередження та реагування: OSSEC може надсилати сповіщення адміністраторам через електронну пошту, SMS або інші механізми сповіщення, щоб швидко реагувати на виявлені загрози. Вона також підтримує автоматичні дії, такі як блокування IP-адрес або виконання скриптів для миттєвої реакції на вторгнення;
- цілісність файлів: OSSEC надає можливість моніторити цілісність системних файлів та інших важливих файлів. Вона порівнює хеш-суми файлів з попередньо визначеними значеннями, щоб виявити зміни, що можуть свідчити про підміну файлів або компрометацію системи;
- розвиток і спільнота: OSSEC має активну спільноту розробників, що забезпечує постійне оновлення системи, виправлення помилок та розробку нових функціональностей. Крім того, OSSEC підтримує розширення за допомогою модулів, які дозволяють розширити можливості системи.

При виникненні вторгнень, OSSEC використовує відповідні журнали, які можуть бути надіслані на електронну пошту, щоб повідомити про атаки та вжити необхідні заходи. Крім того, OSSEC може експортувати попередження в будь-яку систему SIEM за допомогою системного журналу, що дозволяє користувачам отримувати аналітичні матеріали в режимі реального часу та проглядати і аналізувати події в системі безпеки.

Також OSSEC має низку аналізаторів для виявлення загроз з різних джерел даних, контролю цілісності файлової системи, виявлення сигнатур відомих троянських закладок (rootkits) та інших функцій. Вона може бути адаптована до власних потреб безпеки завдяки широким можливостям налаштування, включаючи правила сповіщення та написання скриптів для реагування на порушення безпеки. OSSEC також може бути модифікована шляхом зміни початкового коду для розширення її функціональних можливостей.

Система використовує сигнатурні методи для виявлення кібератак і може бути встановлена як в одиночній конфігурації на одному вузлі, так і у розподіленій конфігурації на декількох вузлах. При цьому управління агентами здійснюється централізовано з сервера. OSSEC працює з журналами реєстрації додатків і операційних систем та дозволяє використовувати будь-які команди для реагування на атаку, застосовуючи відповідні події, команди та параметри їх виклику. При передачі інформації про поточний стан системи здійснюється шифрування за протоколом SSL [28 – 31]. Вона працює на ОС Linux, OpenBSD, FreeBSD, MacOS, Solaris, Windows та іншими.

2.2 Системи виявлення вторгнень на основі сигнатур

Аналіз сигнатур був першим методом виявлення вторгнень. Він заснований на простій концепції зіставлення послідовності з шаблоном. Вхідні пакети скануються байт за байтом і порівнюються з сигнатурами, які є характерними рядками програм, що характеризують шкідливий трафік. Такі сигнатури можуть містити ключові фрази та команди, пов’язані з атакою. Попередньо визначені специфікації атаки мають бути надані СВВ для виявлення сигнатури, що вимагає ручного аналізу даних, пов’язаних з атаками, і формулювання специфікації атаки фахівцем з безпеки. Специфікації атаки можуть бути створені автоматично за допомогою різних автоматизованих методів. Однак більшість систем виявлення вторгнень не мають такої можливості, і зосереджені на даних, отриманих з одного джерела. Є чотири категорії сигнатур:

- сигнатури рядків: механізми сигнатури рядків підтримують зіставлення шаблонів регулярних виразів і функцію повідомлення про інцидент;
- сигнатури підключення: вони генерують повідомлення про інцидент на основі відповідності та дійсності мережевих підключень і протоколів;
- сигнатури DoS: вони містять описи поведінки, які вважаються характеристиками DoS-атаки;
- сигнатури експлойтів: вони зазвичай ідентифікують шаблон трафіку, унікальний для конкретного експлойту; отже, кожен варіант експлойту може потребувати окремої сигнатури. Зловмисники можуть обійти систему виявлення, дещо змінивши корисне навантаження атаки. Часто доводиться створювати сигнатуру експлойту для кожного варіанта інструменту атаки.

Сучасні антивірусні рішення вразливі до атак нульового дня, оскільки вони базуються на сигнатурах, а виявлення аномалій не має надійного механізму для побудови точного профілю, щоб відрізнити атаки від звичайних подій. Хоча надзвичайно важко розробити ефективне рішення для захисту від усіх невідомих атак, адже відомо, що більшість із них мають одну спільну рису — прихований виконуваний вміст. Антивірусні продукти використовують підхід виявлення на основі сигнатур, який ідентифікує загрози за допомогою відомих функцій. Цей метод забезпечує високу точність для вже відомих атак, але неефективний для атак нульового дня. Атаки нульового дня включають загрози нового типу та варіації існуючих атак, які не мають ознак специфічних особливостей при їх першому запуску. Єдиним рішенням для захисту від атак нульового дня є виявлення аномалій незалежно від конкретних сигнатур [32].

2.3 Системи виявлення вторгнень на основі виявлення аномалій

Система виявлення вторгнень на основі виявлення аномалій приваблює багатьох академічних дослідників завдяки своєму потенціалу для боротьби з новими атаками. Виявлення новизни — це ідентифікація нових або невідомих даних, про які система машинного навчання не знає під час навчання. Система виявлення вторгнень

на основі виявлення аномалій має дві основні переваги перед СВВ на основі сигнатур. Перша перевага — здатність виявляти невідомі атаки, а також атаки «нульового дня». Це пов’язано зі здатністю систем виявлення аномалій моделювати нормальну роботу системи/мережі та виявляти відхилення від них. Друга перевага полягає в тому, що вищезазначені профілі звичайної активності налаштовані для кожної системи, програми та/або мережі, і тому зловмиснику дуже важко точно знати, які дії він може виконувати, не будучи виявленим.

Повна таксономія систем виявлення вторгнень на основі виявлення аномалій показана на рисунку 2.1.

Рисунок 2.1 – Таксономія систем виявлення вторгнень на основі виявлення аномалій

Статистичне виявлення аномалій

Статистичне моделювання є одним із найперших методів, які використовуються для виявлення вторгнень в комп’ютерні системи. Статистичні методи виявлення аномалій використовують статистичні властивості та статистичні тести, щоб визначити, чи «спостережувана поведінка» значно відхиляється від «очікуваної поведінки». Статистичні методи виявлення аномалій використовують статистичні властивості (наприклад, середнє значення та дисперсію) нормальних дій

для побудови статистичного нормального профілю та використовують статистичні тести для визначення того, чи суттєво відхиляються спостережувані дії від нормального профілю. СВВ продовжує оцінювати аномальну діяльність. Щойно ця оцінка перевищить певний поріг, згенерується сигнал тривоги. Система виявлення вторгнень на основі статистичних аномалій — це двоетапний процес: спочатку встановлюються профілі поведінки для нормальної діяльності та поточної діяльності. Потім ці профілі зіставляються на основі різних методів для виявлення будь-яких відхилень від нормальної поведінки. СВВ на основі статистичних аномалій також можна класифікувати за такими категоріями:

- операційна модель або порогова метрика. Ця модель базується на робочому припущенні, що аномалію можна виявити, порівнюючи спостереження із заздалегідь визначеною межею. На основі кардинальності спостережень, які відбуваються протягом певного періоду часу, надсилається повідомлення про нестандартну поведінку. Операційна модель найбільш застосовна до метрик, де досвід показує, що певні значення часто пов'язані з вторгненнями. Наприклад, лічильник подій для кількості невдалих спроб введення пароля протягом короткого періоду, коли більше, ніж 10, свідчить про невдалий вхід;
- модель Маркова. Модель використовується з метрикою лічильника подій для визначення нормальності певної події на основі подій, які їй передували. Модель характеризує кожне спостереження як певний стан і використовує матрицю переходів між станами, щоб визначити, чи є ймовірність події високою (нормальною) на основі попередніх подій. Ця модель є особливо корисною, коли послідовність дій є особливо важливою. Ця модель в основному використовується в двох основних підходах: ланцюги Маркова та приховані моделі Маркова. Ланцюг Маркова відстежує вторгнення, перевіряючи систему через фіксовані проміжки часу, і веде запис її стану. Якщо відбувається зміна стану, він обчислює ймовірність цього стану на заданому часовому інтервалі. Якщо ця ймовірність низька на цьому часовому інтервалі, то ця подія вважається аномальною;
- статистичні моменти або модель середнього та стандартного відхилення. Ця модель базується на традиційному статистичному визначенні нормальності

спостереження на основі його положення відносно заданого довірчого інтервалу. У цій моделі подія, що виходить за межі заданого інтервалу, буде оголошена аномальною;

- багатоваріантна модель. Цю модель можна застосувати до виявлення вторгнень для моніторингу та виявлення аномалій процесу в інформаційній системі. Ця модель схожа на модель середнього та стандартного відхилення, за винятком того, що вона базується на кореляціях між двома або більше ознаками. Буде корисною в ситуації, коли дві або більше ознак пов'язані між собою. Модель дозволяє ідентифікувати потенційні аномалії, коли складність ситуації вимагає порівняння декількох параметрів;
- модель часових рядів. Модель намагається виявити аномалії, переглядаючи порядок і часовий інтервал активності в мережі. Якщо ймовірність виникнення спостереження низька, то подія позначається як аномальна. Ця модель надає можливість розвиватися з часом на основі активності користувачів. Аномалії в даних часових рядів - це точки даних, які суттєво відхиляються від нормальної структури послідовності даних.

Переваги СВВ на основі статистичних аномалій:

- не вимагає попереднього знання недоліків безпеки та/або самих атак. У результаті ці системи можуть виявити «нульові дні» або надзвичайно нову атаку;
- статистичні підходи можуть забезпечити точне сповіщення про зловмисну діяльність, яка зазвичай відбувається протягом тривалих періодів часу та є хорошими індикаторами загрозливих атак типу «відмова в обслуговуванні»;
- потенційно прості в обслуговуванні, оскільки немає необхідності оновлювати сигнатури, і система не залежить від конкретних атак або умов;
- генерують сповіщення на основі наявності незвичної діяльності;
- здатні виявляти «низькі та повільні» атаки;
- шукають окремі елементи, які можуть бути частиною вторгнення, не чекаючи;
- завершення цілої послідовності певної діяльності.

Недоліки СВВ на основі статистичних аномалій:

- статистичні методи потребують точних статистичних розподілів, але не всю поведінку можна моделювати за допомогою суто статистичних методів;
- більшість статистичних методів виявлення аномалій вимагають припущення про квазістаціонарний процес, що неможливо припустити для більшості даних, оброблених системами виявлення аномалій;
- процес навчання займає дні або тижні, щоб стати точним і ефективним;
- встановлення надто високого порогу не попередить про необхідний трафік, а встановлення надто низького спричинить надлишок помилкових спрацьовувань;
- генерація неприйнятної кількості помилкових сповіщень, оскільки відсутня здатність адаптуватися до законних змін у поведінці користувача.

Інтелектуальний аналіз даних

Оскільки СВВ може виявляти лише відомі атаки, але не може виявляти інсайдерські атаки, кращим рішенням для СВВ може бути інтелектуальний аналіз даних, за своєю суттю це «пошук шаблонів» і визначається як «процес вилучення корисних і раніше непомічених моделей або шаблонів з великих сховищ даних». Процес інтелектуального аналізу даних, як правило, зменшує кількість даних, які необхідно зберігати для історичних порівнянь мережевої активності, створюючи дані, які є більш значущими для виявлення аномалій. Підхід, що базується на інтелектуальному аналізі даних, можна класифікувати на наступні методи:

- кластеризація даних за різними категоріями. Кластеризація - це неконтрольована техніка для пошуку закономірностей у нерозмічених даних з багатьма вимірами (кількістю атрибутів). Здебільшого кластеризація за методом k-середніх використовується для пошуку природних груп схожих даних. Записи, які знаходяться далеко від будь-якого з цих кластерів, вказують на незвичайну активність, яка може бути частиною нової атаки;
- виявлення правил асоціацій. Видобуток асоціативних правил, хоча і є дуже популярною технікою, зазвичай працює дуже повільно, і її замінюють інші потужні методи, такі як кластеризація та класифікація. Видобуток асоціативних правил знаходить кореляцію між атрибутами;

- класифікація. Виявлення вторгнень можна розглядати як проблему класифікації: ми хочемо класифікувати кожен екземпляр як нормальний або як певний вид вторгнення (атаки). Класифікація є одним з основних методів, що використовуються в інтелектуальному аналізі даних. Його основна мета полягає в тому, щоб навчитися на навчальних прикладах, позначених класами, передбачати класи нових або раніше не бачених даних: приклади в навчальному наборі мають мітки. Нові дані класифікуються на основі навчального набору. По суті, будується дерево класифікації (також зване деревом рішень), щоб передбачити категорію, до якої належить конкретний екземпляр.

Переваги підходу на основі інтелектуального аналізу даних:

- видалення звичайної активності з даних про сповіщення, щоб дозволити аналітикам зосередитися на реальних атаках;
- виявлення генераторів хибних сповіщень та "поганих" сигнатур датчиків;
- пошук аномальну активність, яка вказує на справжню атаку;
- виявлення тривалих, постійних сигнатур (різні IP-адреси, однакова активність).

Виявлення на основі знань

Метод виявлення на основі знань може використовуватися як для СВВ на основі сигнатур, так і для СВВ на основі аномалій. Відбувається накопичення знань про конкретні атаки та вразливості системи. Використовуються ці знання для використання атак і вразливостей для генерування тривоги. Будь-яка інша подія, яка не розпізнається як атака, приймається. Тому точність систем виявлення вторгнень, заснованих на знаннях, вважається хорошою. Однак їх повнота вимагає регулярного оновлення знань про атаки.

Техніку виявлення вторгнень, засновану на знаннях, можна класифікувати наступним чином:

- аналіз переходів стану. Метод, запропонований Поррасом і Кеммерером, був реалізований спочатку в UNIX, а потім і в інших середовищах. Концептуально ця методика ідентична міркуванням на основі моделей, вона описує атаки за допомогою набору цілей і переходів, і представляє їх у вигляді діаграм переходів станів. Діаграма

переходів станів - це графічне представлення дій, які виконує зловмисник, щоб приховати компрометацію системи. В аналізі переходів станів вторгнення розглядається як послідовність дій, виконаних зловмисником, яка призводить з деякого початкового стану комп'ютерної системи до цільового скомпрометованого стану. Діаграми аналізу переходів станів визначають вимоги та компрометацію проникнення. Вони також перераховують ключові дії, які повинні відбутися для успішного завершення вторгнення;

- експертні системи. Експертна система містить набір правил, які описують атаки. Потім події аудиту перетворюються в експертній системі на факти, що несуть їх семантичне значення, і механізм виведення робить висновки, використовуючи ці правила і факти. Цей метод підвищує рівень абстракції даних аудиту, додаючи їм семантику. Він також кодує знання про минулі вторгнення, відомі вразливості системи та політику безпеки. У міру збору інформації експертна система визначає, чи були дотримані якісь правила;
- сигнатурний аналіз. Сигнатурний аналіз використовує той самий підхід до отримання знань, що й експертні системи, але отримані знання використовуються по-іншому. Семантичний опис атак перетворюється на інформацію, яку можна легко знайти в аудиторському сліді. Наприклад, сценарії атак можуть бути переведені в послідовності аудиторських подій, які вони генерують, або в шаблони даних, які можна шукати в аудиторському сліді, що генерується системою. Цей метод знижує семантичний рівень опису атак. Цей метод дозволяє дуже ефективну реалізацію і тому застосовується в різних комерційних продуктах для виявлення вторгнень, наприклад, Haystack;
- мережі Петрі. Система виявлення вторгнень на основі знань, розроблена в Університеті Пердью, використовує кольорові мережі Петрі (CPN). Перевагами CPN є їх загальність, концептуальна простота і графічна репрезентативність. Системним адміністраторам надається допомога в написанні власних сигнатур атак та їх інтеграції. Завдяки загальності CPN, досить складні сигнатури можуть бути легко написані. Однак зіставлення складного підпису з аудиторським слідом може стати дуже дорогим з точки зору обчислень.

Переваги методів виявлення, заснованих на знаннях:

- висока точність;
- низький рівень помилкових спрацьовувань;
- надійність, гнучкість та масштабованість;
- збір знань відбувається детально, що полегшує співробітнику служби безпеки вжиття превентивних або коригувальних заходів.

Недоліки методу виявлення на основі знань:

- повнота цього методу вимагає регулярного оновлення знань про атаки;
- це складне і трудомістке завдання, оскільки підтримка бази знань вимагає ретельного і детального аналізу кожної вразливості;
- ці підходи стикаються з проблемою узагальнення.

Виявлення на основі машинного навчання

Машинне навчання можна визначити як здатність програми та/або системи навчатися та покращувати свою ефективність при виконанні певного завдання або групи завдань з плином часу. Методи машинного навчання зосереджені на створенні системи, яка покращує свою роботу на основі попередніх результатів, тобто методи машинного навчання мають здатність змінювати свою стратегію виконання на основі нової отриманої інформації. Ця особливість може зробити їх бажаними для використання у всіх ситуаціях, але основним недоліком є їхня недостатність ресурсів. У багатьох випадках техніка машинного навчання збігається зі статистичними методами та методами інтелектуального аналізу даних.

Цей метод можна розділити на:

- Байєсівський підхід. Байєсівський підхід - це графічна модель, яка кодує імовірнісні зв'язки між змінними, що представляють інтерес. Це популярне представлення для кодування невизначених експертних знань в експертних системах. Зовсім недавно дослідники розробили методи навчання байєсівських мереж на основі даних. Розроблені методи є новими і все ще розвиваються, але вони виявилися надзвичайно ефективними для деяких проблем аналізу даних;
- нейронні мережі. У нейромережевому підході системи навчаються передбачати наступну команду на основі послідовності попередніх команд

конкретного користувача. Нейронні мережі забезпечують вирішення проблеми моделювання поведінки користувачів при виявленні аномалій, оскільки вони не вимагають будь-якої явної моделі користувача;

- нечітка логіка. Методи нечіткої логіки використовуються у сфері комп'ютерної та мережевої безпеки з кінця 1990-х років. Частина системи, що використовує нечітку логіку, в основному відповідає за обробку великої кількості вхідних параметрів і боротьбу з неточністю вхідних даних. У поєднанні з інтелектуальним аналізом даних вона зменшує розмір вхідних наборів даних і вибирає ознаки, які підкреслюють аномалії; нечітка логіка може бути ефективним засобом визначення мережевих атак;
- генетичні алгоритми. Генетичні алгоритми спочатку були запроваджені в галузі обчислювальної біології. Вона використовує комп'ютер для реалізації природного відбору та еволюції. Ця концепція походить від "адаптивного виживання в природних організмах". Алгоритм починається з випадкової генерації великої популяції програм-кандидатів. Використовується певна міра придатності для оцінки продуктивності кожної особини в популяції. Потім виконується велика кількість ітерацій, під час яких низькопродуктивні програми замінюються генетичною рекомбінацією високопродуктивних програм. Тобто програма з низьким показником пристосованості видаляється і не доживає до наступної комп'ютерної ітерації;
- методи опорних векторів. Метод опорних векторів (SVM) був запропонований Вапніком у 1998 році. SVM спочатку відображає вхідний вектор у вимірний простір ознак, а потім отримує оптимальну розділювальну гіперплощину у вимірному просторі ознак. Більше того, межа рішення, тобто розділова гіперплощина, визначається опорними векторами, а не всією навчальною вибіркою, і, таким чином, є надзвичайно стійкою до викидів. Зокрема, SVM-класифікатор призначений для бінарної класифікації [33].

2.4 Гібридні системи виявлення вторгнень

Гібридні системи виявлення вторгнень містять в собі поєднання двох методів виявлення. Це може бути комбінація методів на основі сигнатурного пошуку та виявлення аномалій чи комбінація двох та більше методів сигнатурного пошуку або двох та більше методів пошуку на основі аномалій. Будь-яке вторгнення характеризується певними ознаками, які, з одного боку, можна представити у вигляді сигнатури, а з іншого - описати як якесь відхилення від штатної поведінки інформаційної системи. Найбільш ефективно поєднання обох методів, при цьому для отримання необхідних вихідних даних застосовні будь-які (хостові або мережеві) датчики.

Ефективне виявлення атак на етапах атакуючого впливу і розвитку атаки можливо тільки за допомогою поведінкових методів. Оскільки дії порушників залежать від цілей проведеної атаки і фіксованою безліччю сигнатур атак однозначно не визначаються. З огляду на той факт, що на двох останніх стадіях життєвого циклу інформаційної атаки найхарактерніші об'єкти - це хости, в даному випадку найбільш доцільно застосування хостових датчиків.

На основі досліджених даних, можна зробити висновок, що реалізовані в даний час в СВВ методи засновані на загальних уявленнях розпізнавання образів. Відповідно до них для виявлення аномалії формується образ нормального функціонування інформаційної системи. Цей образ виступає як сукупність значень параметрів оцінки. Його зміна вважається проявом аномального функціонування системи. Після виявлення аномалії і оцінки її ступеня формується судження про природу змін: чи є вони наслідком вторгнення або допустимим відхиленням. Для виявлення зловживань також використовується образ (сигнатура), однак тут він відображає заздалегідь відомі дії атакуючого.

За результатами вище проведеного аналізу і із розрахунком перспективи подальшого впровадження перспективних технологій захисту інформації використання сигнатурного методу та методу виявлення аномалій забезпечують додатковий рівень захисту інформаційної системи, доповнюючи "традиційні" засоби

захисту - міжмережеві екрани, криптографічні маршрутизатори, сервери аутентифікації та ін. Але найперспективнішим методом можна вважати комбінований метод, що використовує спільно алгоритми, визначені в сигнатурних методах і методах виявлення аномалій. Варто зазначити, що може бути комбінація двох та більше методів сигнатурного пошуку або двох та більше методів пошуку на основі аномалій. Так як, тільки комплексний підхід може значно знизити ризик вторгнення в ІС і виключити втрату цінних даних [34].

Висновки за розділом 2

Проаналізовано історія розвитку, різновиди та характерні особливості систем виявлення вторгнень. А також проаналізовано функції та переваги різноманітних підвидів СВВ на основі сигнатур та виявлення аномалій.

Розглянуто історію створення сучасних СВВ. Виявлено ключових дослідників та проаналізовано їх фундаментальні статті в процесі становлення. Розглянуто системи, які були прообразами сучасних СВВ. Проведено аналіз трьох найпопулярніших систем виявлення вторгнень на даний час – Snort, Suricata та OSSEC. Наведено основні режими функціонування, принцип архітектури та основні характеристики розглянутих систем.

Проаналізовано системи виявлення вторгнень на основі сигнатур. Виявлено, що існує основні 4 типи сигнатур: рядків, підключення, DoS та експлойтів. Незважаючи на стрімкий розвиток та ускладнення рівнів атак, дані методи досі використовуються та демонструють високу ефективність у виявлені відомих системі атак, тобто сигнатура яких занесена в базу знань СВВ.

Наступним пунктом був аналіз систем на основі аномальної поведінки. Дані інструменти розділені на основні чотири класи такі, як системи з статистичним виявленням аномалій, інтелектуальним аналізом даних, виявленням на основі знань та виявленням на основі машинного навчання. Кожен клас систем також поділяється на різні підтипи у залежність від використовуваного математичного алгоритму у свої

логіці. Виявлено переваги використання кожного з класів, що є зручним при виборі системи для вирішення різного типу задач.

Наприкінці було проаналізовано гібридні системи , що можуть поєднувати у собі різноманітні методи виявлення. Наразі такі системи є найбільш цікавими для підприємств, оскільки є декілька різних методів перевірки вхідної інформації, що знижує рівень помилкових сповіщень.

Загалом, система виявлення вторгнень є лише частиною комплексного підходу для захисту інформації на об’єктах критичної інфраструктури. Необхідно розробити стратегію функціонування системи захисту інформації для об’єкта, де усі наявні інструментарії будуть формувати потужну багатоетапну систему раннього попередження, виявлення та захисту від кібернетичних загроз.

РОЗДІЛ 3
АЛГОРИТМ ГІБРИДНОЇ СИСТЕМИ ВИЯВЛЕННЯ ВТОРГНЕНЬ НА ОСНОВІ КОМБІНАЦІЇ МЕТОДІВ RANDOM FOREST ТА AUTOENCODER

3.1 Метод Random Forest

Метод Random Forest (RF) є одним з найпопулярніших алгоритмів машинного навчання, який використовується для задач класифікації, регресії та інших типів прогнозування. Він базується на ідеї ансамблю дерев рішень (ДР), де кожне дерево вирішує проблему прогнозування, а потім комбінується для отримання остаточного результату.

Основна ідея Random Forest полягає у випадковому створенні багатьох рішучих дерев, які вирішують проблему прогнозування. Кожне дерево створюється за допомогою процесу, який називається бутстрепінг (від англ. bootstrap aggregation), де з навчального набору даних випадково обираються заміщенням вибірки (вибірка з повторенням). Крім того, при побудові кожного розгалуження в дереві вибирається лише підмножина випадково вибраних ознак.

Після створення багатьох дерев, коли потрібно зробити прогноз для нового прикладу, кожне дерево випускає свій власний прогноз, а результат комбінується за допомогою голосування для отримання остаточного прогнозу RF.

Одним із ключових переваг Random Forest є його здатність до обробки великих наборів даних з великою кількістю ознак. Він також має властивість уникати проблеми перенавчання, оскільки рандомізація в процесі будування дерев та комбінування прогнозів дерев допомагає знизити дисперсію моделі.

Щоб отримати кращу ефективність прогнозування, ансамблеві методи використовують кілька базових класифікаторів для прийняття рішень. Цей підхід, як правило, демонструє підвищену ефективність класифікації порівняно з одним базовим класифікатором. Метод RF є ієрархічними деревовидними структурами, що

складаються з правил рішень виду "if–then" для класифікації даних. Схематичне представлення ДР показано на Рисунку 3.1.

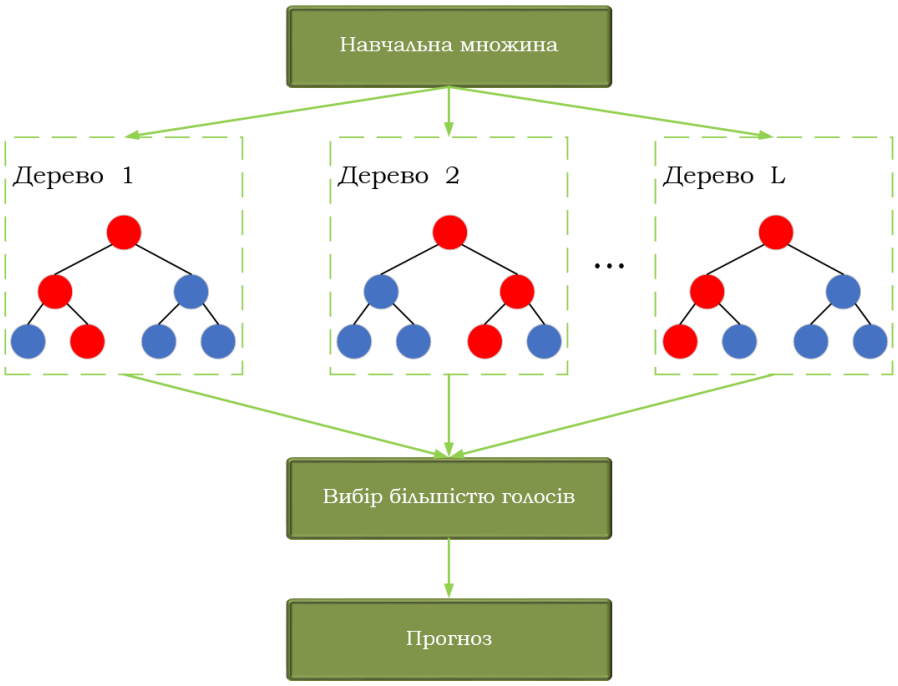

Рисунок 3.1 – Схематичне представлення множинного дерева рішень

Bagging підхід є однією з найпоширеніших ансамблевих стратегій для побудови декількох класифікаторів. Використовуючи бутстреп із заміною для вибірки даних, велика кількість класифікаторів навчається незалежно.

Як показано на Рисунку 3.1, на навчальній множині є L різних класифікаторів ДР. Для отримання остаточних результатів прогнозування використовується більшість голосів для об'єднання прогнозів від кожного ДР. Далі представлено детальну процедуру навчання для методу RF. Розглянемо розмічений набір даних з вибірками $\{x_1,x_2,\cdots,x_N\}$ та мітками $\{y_1,y_2,\cdots,y_N\}$, де N – кількість вибірок, а кожна вибірка містить j ознак, для навчання RF, тобто основною задачею є навчити L різних ДР. Загальний крок можна підсумувати наступним чином:

- вибірка з навчальної множини з N вибірками за допомогою бутстрапу із заміною;
- побудова класифікатора ДР за відібраними зразками.

Щоб побудувати одне ДР, спочатку обирається k ознак з j ознак. Значення k задається як sqrt(j) . Після цього обирається найкращий елемент розбиття з обраних k

елементів і вершина розбивається на дві дочірні вершини. Критерієм поділу для вершини, що розділяється, є критерій Джині. Необхідно повторити цикл цих процедур і створити якомога більше дерево.

Для прогнозування вхідної вибірки метод RF використовує «голоси» дерев рішень у побудованому лісі, зважені за їхніми ймовірнісними оцінками. Нехай p позначає ймовірність бути передбаченим як атака. Тоді, ймовірність того, що це буде нормальна ситуація, дорівнює q і q=1–p. Прогнозовані ймовірності класів вхідної вибірки обчислюються як середні прогнозовані ймовірності класів дерев у лісі. Ймовірність класу одного дерева – це частка зразків одного класу у кінцевому вузлі.

Зазвичай, зразки можна віднести до одного класу з найбільшою ймовірністю. Однак при такому підході деякі зразки, що належать до невідомих атак, можуть бути помилково класифіковані як нормальні. Варто визначити поріг S, щоб допомогти процесу розпізнавання зразків. Якщо ймовірність p належності до атаки більша за поріг S, вибірки можуть бути класифіковані як атаки. Таким чином, маючи вибірку x_i та відповідну ймовірність p_i, можливо визначити функцію прийняття рішення $f(x_i)$. Результати позначено ±1, де +1 – аномальні зразки. Розрахунок показано нижче:

$$f(x_i) = \begin{cases} -1, \text{якщо } p_i \leq S \\ +1, \text{ якщо } p_i > S \end{cases} \quad (3.1)$$

3.2 Метод Autoencoder

Метод Autoencoder (AE) є одним з нейромережевих алгоритмів, який використовується для безперервного навчання з представленням даних та зменшення розмірності. Він базується на концепції нейронних мереж, де модель намагається відтворити вхідні дані на виході, що дозволяє отримати компактне кодування даних. Глибоке навчання виявилося досить ефективним у різних галузях досліджень. Воно вивчає представлення даних за допомогою декількох шарів нейронної мережі. Цей метод обрано для другої частини розроблюваної моделі. Оскільки вона може відновлювати вхідні дані, помилка реконструкції може слугувати оцінкою для

виявлення аномалій. Структура виявлення аномалій за допомогою метода AE зображено на Рисунку 3.2.

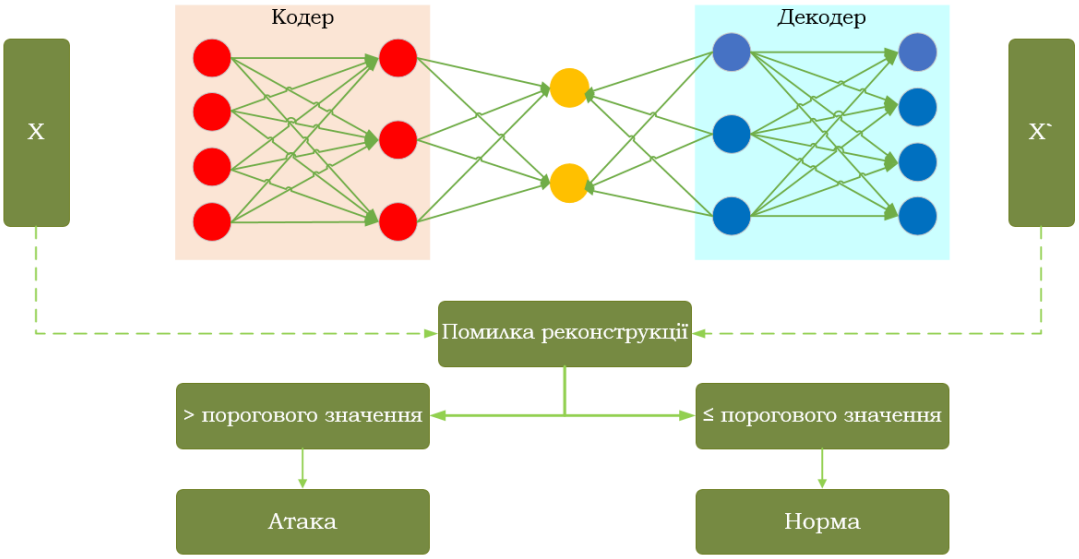

Рисунок 3.2 – Структура виявлення аномалій за допомогою метода Autoencoder

Метод AE зазвичай має симетричну структуру. Як показано на рисунку 3.2, його можна розділити на дві частини: кодер і декодер. Кодер приймає вхідні дані і перетворює їх на скомпресоване представлення, яке називається кодуванням. Декодер приймає це кодування і намагається відтворити вхідні дані з нього. І кодер, і декодер складаються з декількох прихованих шарів. Мета AE полягає в тому, щоб кодування максимально точно представляло вхідні дані, тобто реконструкція на виході має бути якомога ближчою до вхідних даних. Зазвичай, приховані представлення мають меншу розмірність, ніж оригінальний вхідний сигнал. Декодер намагається відновити оригінальний вхідний сигнал зі стисненої форми. Для розробки алгоритму буде використано середньоквадратичну похибку (СКП) для кількісної оцінки втрат при відновленні. Для вхідних даних x_i та реконструйованих вихідних даних $\hat{x}_i$, СКП e_i обчислюється наступним чином:

$$e_i = \| x_i - \hat{x}_i \|^2 \quad (3.2)$$

Навчальний процес спрямований на мінімізацію втрат від реконструкції. Після навчання, за допомогою добре підготовленого АЕ можливо ідентифікувати аномальні зразки за допомогою СКП. Подібно до процесу обробки ймовірності методу RF із заздалегідь визначеним порогом S, ми використовуємо функцію $f(x_i)$ для прийняття рішення, де +1 позначає аномальний зразок:

$$f(x_i) = \begin{cases} -1, \text{якщо } e_i \leq S \\ +1, \text{ якщо } e_i > S \end{cases} \quad (3.3)$$

3.3 Цілісна модель гібридної системи виявлення вторгнень на основі комбінації методів Random Forest та Autoencoder

Для створення цілісної моделі системи виявлення вторгнень розглянемо сценарій, коли зібрано зразки, що належать до певних типів атак, але можуть існувати і невідомі атаки, оскільки варіації або нові типи атак продовжують з'являтися.

Коли існують невідомі атаки, традиційний RF класифікатор атак неправильно класифікує їх як звичайні, тому варто застосувати імовірнісний підхід для прийняття рішення. Крім того, щоб зменшити кількість хибних сповіщень, буде застосовано метод АЕ для повторної перевірки атак.

Таким чином, інтегрується два методи, використовуючи імовірнісний метод RF та метод АЕ. Підхід складається з двох частин: навчання та тестування. Детальне представлення цих двох частин на Рисунку 3.3. На етапі навчання кожна модель тренується на окремій підмножині набору даних. Беручи до уваги наявний маркований набір даних, є можливість навчити бінарний класифікатор за допомогою класифікатора RF. Потім будується додатковий АЕ, який використовує лише нормальні вибірки з навчальної множини. Оскільки RF навчається на маркованому наборі даних, ми використовуємо його вихідну ймовірність для прийняття рішень щодо виявлення зразків атак.

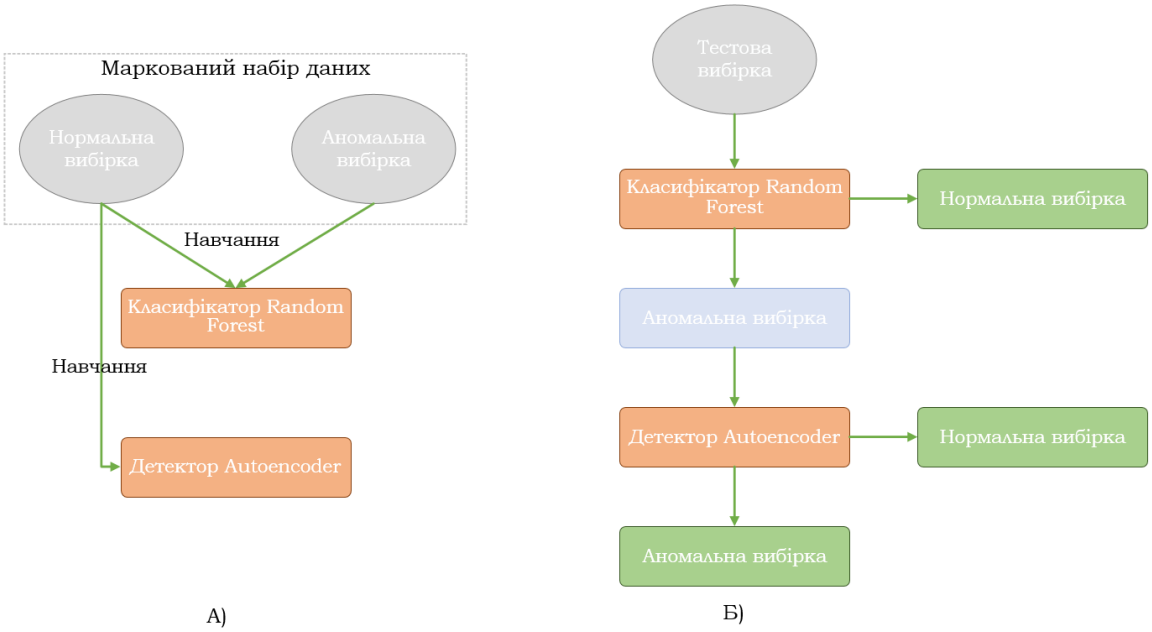

Рисунок 3.3 – Огляд розроблюваного методу. (А) Процес навчання; (Б) Процес тестування

Оскільки АЕ навчається лише на нормальних даних, нормальні вибірки матимуть нижчий СКП, ніж аномальні. З цієї точки зору, можливо визначити нижчий поріг, і вибірки, нижчі за цей поріг, мають вищу ймовірність приналежності, до нормального класу. За такого припущення відбувається інтеграція цих двох процесів прийняття рішень. Після отримання навченої моделі, на етапі тестування, застосовується двоетапна стратегія виявлення. Процедура виявлення описана в Алгоритмі 1 наведеному на рисунку 3.4.

Дані: початкове введення даних x_i. Навчена Random Forest модель L_1 і Autoencoder модель L_2. Порогові значення S_1 і S_2.

Результат: результат виявлення аномалії y_i для x_i.

```
/* Крок 1: розрахувати ймовірність pi за RF моделлю L1 */
 1 pi ← L1 (xi)
/* Крок 2: розрахувати середньоквадратичну похибку ei за AE
моделлю L2 */
 2 x̂i ← L2 (xi)
 3 ei ← || xi - x̂i, ||^2
/* Крок 3: класифікація вибірки за моделлю RF  */
 4 if pi > S1 then
 5 |  yi ← 1
 6 else
 7 |  yi ← -1
 8 end
/* Крок 4: перевірка прогнозованої аномальної вибірки  */
 9 if yi == 1 then
10 |   if ei ≤ S2 then
11 |   |  yi ← -1
12 |   end
13 end
```

Рисунок 3.4 – Алгоритм 1.Тестовий процес розроблюваного методу

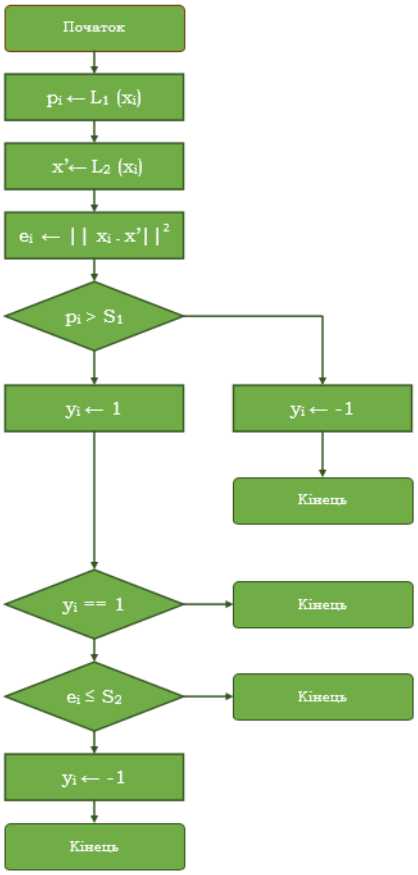

Рисунок 3.5 – Блок-схема Алгоритму 1.

Для прийняття рішення розглядаються два параметри. Перший - це S_1 який використовується для ймовірності RF, а другий - S_2, який використовується для СКП. На початку вибірка x_i класифікується за допомогою RF класифікатора. Коли ймовірність зразка більша за S_1, він класифікується як атака. Після цього ми використовуємо AE, щоб знову дослідити зразок атаки, передбачений RF. У цій частині, коли помилка відновлення менша за S_2 зразок змінює класифікацію як нормальний.

Висновки за розділом 3

Проаналізовано роботу методів Random Forest та Autoencoder. Сформовано основні формули для розроблюваного алгоритму. Для створення цілісного алгоритму системи інтегровано два методи, що розглядалися вище. Розроблюваний алгоритм

складається з двох частин: навчання та тестування. На етапі навчання кожна модель тренується на окремій підмножині набору даних. Спочатку проводиться навчання бінарного класифікатора за допомогою класифікатора RF. Потім будується додатковий AE, який використовує лише нормальні вибірки з навчальної множини. За такого припущення відбувається інтеграція цих двох процесів прийняття рішень. Після отримання навченої моделі, на етапі тестування, застосовується двоетапна стратегія виявлення. Для прийняття рішення розглядаються два параметри: S_1 - для ймовірності RF; S_2, - для СКП. На початку вибірка x_i класифікується за допомогою RF класифікатора. Коли ймовірність зразка більша за S_1, він класифікується як атака. Після цього ми використовуємо AE, щоб знову дослідити зразок атаки, передбачений RF. У цій частині, коли помилка відновлення менша за S_2 зразок змінює класифікацію як нормальний.

Розроблений алгоритм гібридної системи виявлення вторгнень є оптимальним для впровадження на об’єктах критичної інфраструктури, оскільки в його робочу логіку закладено двоетапну перевірку, що підвищить рівень виявлення вторгнень, навіть не відомих атак, і зменшить кількість помилкових сповіщень.

ВИСНОВКИ

Проаналізовано різноманітні підходи до захисту об’єктів критичної інфраструктури у світі та в Україні. В нашій країні процес захисту об’єктів критичної інфраструктури знаходиться на початковій стадії з огляду національної політики. Усі напрацювання, що були до того створювалися регуляторами окремих об’єктів в необов’язковому порядку. Але, після аналізу різноманітних атак на ОКІ за час широкомасштабного вторгнення російської федерації, варто визнати, що системи захисту, що були побудовані на різних об’єктах виявили достатньо високий ступінь надійності. Адже, за офіційними повідомленнями, жодна зі здійснених кібернетичних атак не завдала невідворотного збитку. Наразі, відбувається активна стадія впровадження ЗУ «Про критичну інфраструктуру» та ОКІ змінюють свої наявні процеси захисту інформації на більш сучасні та поглиблені.

Кібернетичні атаки з моменту їх розвитку несуть неймовірно високий ступінь ризику для інформаційних систем об’єктів критичної інфраструктури. Адже, успішне проведення такої атаки, хоч і є набагато складнішим, ніж на більш простий інформаційний об’єкт, але несуть набагато більшу вигоду для груп, що здійснюють таку атаку. На стороні зловмисника працює високопрофесійна група, тому для адекватного захисту група професіоналів необхідна і стороні, що обороняється. Існує декілька основних типів стратегій захисту, що запропоновані ведучими світовими корпораціями в області кіберзахисту, але найкращим варіантом є комбінація запропонованих технік для побудови стратегії захисту, що необхідна певному підприємству. Але, на жаль, за недостатністю професіоналів високого рівня та мінімальним фінансуванням секторів інформаційної безпеки на об’єктах досить часто стратегії захисту достатньо обмежені. Останнім часом, державний сектор об’єктів критичної інфраструктури активно співпрацює з бізнес структурами для обміну досвідом, розбудови сучасних стратегій захисту, оптимізації процесів, допомоги у виборі систем захисту. Якщо ця тенденція продовжиться, об’єкти критичної інфраструктури зможуть інтегрувати важливий досвід бізнесу в свої процеси задля підвищення рівня обороноздатності.

З наявності на ринку величезної кількості різноманітних систем, що стосуються інформаційної безпеки, багато спеціалістів забувають, що раннє виявлення і попередження планованого вторгнення в мережу підприємства є більш прогресивною стратегією, аніж реакція на вже здійснену атаку. Система виявлення вторгнень є одним з таких інструментів, що при правильному налаштуванні та експлуатації допоможе виявити стороннє проникнення в систему та несанкціоновані дії зловмисників. Існують різноманітні СВВ в робочу логіку яких закладено різноманітні алгоритми роботи. За методами виявлення системи поділяються на ті, що в своїй основі використовують сигнатурний пошук, виявлення аномалій та гібридний метод.

Гібридні системи виявлення вторгнень у сучасному світі набувають все більше та більше популярності, адже можливість комбінувати різні методи виявлення значно підвищити якість виявлення різноманітних загроз, зменшити кількість помилкових сповіщень, посилити надійність системи та розширити список охоплюваних загроз. Так як зловмисники мають широкий арсенал інструментів для нападу, сторона, що захищається має демонструвати адекватні методи захисту. Тому комбінація математичних методів тільки посилить рівень кібернетичного захисту об’єкту.

Розроблений алгоритм гібридної системи виявлення вторгнень засновано на двох сучасних методах виявлення аномалій. Однією з переваг такої системи є те, що показники ефективності з плином часу будуть зростати, адже система увесь час експлуатації навчається. Алгоритм є оптимальним рішенням для впровадження на об’єктах критичної інфраструктури, оскільки реалізація можлива без залучення великих сторонніх корпорацій, підтримка функціонування може виконуватися невеликою групою спеціалістів, а надійні та передові математичні алгоритми, підвищать рівень виявлення вторгнень, навіть не відомих атак, і зменшить кількість помилкових сповіщень.

Процес протидії та захисту атакам на об’єктах критичної інфраструктури є надзвичайно широкомасштабним та важливим не тільки для забезпечення сталої роботи підприємства, а й для безперебійного надання послуг громадянам країни. З початком пандемії коронавірусу ОКІ по всьому світу пришвидшили перехід критично важливих бізнес процесів в онлайн формат. В умовах реальних загроз об’єктами

критичної інфраструктури держави створення системи підготовки кваліфікованих кадрів щодо підвищення рівня захисту та стійкості критичної інфраструктури повинно і має здійснюватися випереджувальними темпами, адже людський фактор є ключовим чинником успішності реформування сектору безпеки держави. Тому для кожного ОКІ розробити стратегію захисту, долучити професіоналів, які здатні втілити її в життя, впроваджувати в роботу нові засоби захисту, навчати співробітників правильному поводженню в інформаційному просторі та постійно вдосконалюватися – це і є запорука ефективного захисту та стабільного робочого процесу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Закон України «Про критичну інфраструктуру». [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/1882-20

2. Толюпа С.В, Мостовенко А.В. БПЛА як загроза об'єктам критичної інфраструктури. Матеріали V Міжнародної науково-практичної конференції "Проблеми кібербезпеки інформаційно-телекомунікаційних систем (PCSITS)" (Київ, 2023)

3. Carol V. Evans, Chris Anderson, Malcom Baker, Ronald Bearse, Salih Biçakci, Steve Bieber, Sungbaek Cho, Adrian Dwyer, Geoffrey French, David Harell, Alessandro Lazari, Raymond Mey, Theresa Sabonis-Helf, and Duane Verner. Enabling NATO’s Collective Defense: Critical Infrastructure Security and Resiliency (NATO COE-DAT Handbook 1). – Carlisle, PA: US Army War College Press, 2022. [Електронний ресурс]. – Режим доступу: https://press.armywarcollege.edu/monographs/955

4. Толюпа С.В, Мостовенко А.В. Вразливості та запобігання загрозам в об’єктах критичної інфраструктури. Матеріали V Міжнародної науково-практичної конференції "Проблеми кібербезпеки інформаційно-телекомунікаційних систем (PCSITS)" (Київ, 2022).

4. Лукова–Чуйко Н.В. Методи інтелектуального розподілу даних в системах виявлення мережевих вторгнень та функціональна стійкість інформаційних систем до кібератак. / Н.В. Лукова–Чуйко, С.В. Толюпа, В.С. Наконечний, М.М. Браіловський: монографія – К.: Формат, 2021. – 370 с. .

5. Бурячок, В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д–ра техн. наук, професора В. Б. Толубка.— К.: ДУТ, 2015.— 288 с.

6. Tewari N., Bhardwaj A. Flow Statistics Based Detection of Low Rate and High Rate DDoS Attacks // International Journal of Scientific & Engineering Research. – 2013. – Vol. 4, no. 5. – P. 348 – 353.

7. Fall K. R., Stevens W. R. TCP/IP illustrated, volume 1: The protocols. – addison–Wesley, 2011.

8. Хакерські атаки на Україну [Електронний ресурс] – Режим доступу: https://is.gd/6lkWHY

9. Якуб Пшетачник, Сімона Тарпова. Війна Росії проти України: хронологія кібератак. [Електронний ресурс]. – Режим доступу: https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI%282022%29733549_XL.pdf

10. Про загальну кількість кібератак за 2022 рік [Електронний ресурс] — Режим доступу до ресурсу: https://espreso.tv/z-pochatku-povnomasshtabnogo-vtorgnennya-rosiyani-zdiysnili-ponad-12-mln-kiberatak-na-energetichnu-infrastrukturu-ukraini

11. Олесь Друкач. Усе про кібератаку на Україну 15 лютого: постраждали банки, уряд та сайти силових відомств. [Електронний ресурс] — Режим доступу до ресурсу: https://24tv.ua/use-pro-kiberataku-ukrayinu-15-lyutogo-postrazhdali-golovni-novini_n1868773

12. Інформація щодо кібератак 15 лютого 2022 року. [Електронний ресурс]. – Режим доступу: https://cert.gov.ua/article/37139

13. Кібератака на Укртелеком 28 березня: деталі. [Електронний ресурс]. – Режим доступу: https://cip.gov.ua/ua/news/kiberataka-na-ukrtelekom-28-bereznya-detali

14. Система виявлення вторгнень. [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/Система_виявлення_вторгнень

15. Denning, Dorothy. An Intrusion Detection Model. Proceedings of the Seventh IEEE Symposium on Security and Privacy, May 1986, pages 119—131.

16. Lunt, Teresa. IDES: An Intelligent System for Detecting Intruders. Proceedings of the Symposium on Computer Security; Threats, and Countermeasures; Rome, Italy, November 22-23, 1990, pages 110—121.

17. Lunt, Teresa. Detecting Intruders in Computer Systems. 1993 Conference on Auditing and Computer Technology, SRI International

18. Sebring, Michael M., and Whitehurst, R. Alan. Expert Systems in Intrusion Detection: A Case Study. The 11th National Computer Security Conference, October, 1988.

19. Smaha, Stephen E. Haystack: An Intrusion Detection System. The Fourth Aerospace Computer Security Applications Conference, Orlando, FL, December, 1988.

20. Vaccaro, H.S., and Liepins, G.E. Detection of Anomalous Computer Session Activity. The 1989 IEEE Symposium on Security and Privacy, May, 1989.

21. Teng, Henry S., Chen, Kaihu, and Lu, Stephen C-Y, Adaptive Real-time Anomaly Detection Using Inductively Generated Sequential Patterns, 1990 IEEE Symposium on Security and Privacy.

22. Heberlein, L. Todd, Dias, Gihan V., Levitt, Karl N., Mukherjee, Biswanath, Wood, Jeff, and Wolber, David. A Network Security Monitor. 1990 Symposium on Research in Security and Privacy, Oakland, CA, pages 296—304.

23. Winkeler, J.R. A UNIX Prototype for Intrusion and Anomaly Detection in Secure Networks. The Thirteenth National Computer Security Conference, Washington, DC., pages 115—124, 1990.

24. Dowell, Cheri, and Ramstedt, Paul. The ComputerWatch Data Reduction Tool. Proceedings of the 13th National Computer Security Conference, Washington, D.C., 1990.

25. Snort 2.1. Обнаружение вторжений: книга / Джей Бил [и др.]. М. : Биномпресс, 2006. Изд. 2. 656 с.

26. Snort / Snort team // Snort Blog: the Official Blog of the World Leading OpenSource IDS/IPS Snort : San Jose : Cisco Systems Inc, 2017. [Електронний ресурс]. – Режим доступу: https://blog. snort.org/2017/10/snort–29110–has–been–released.html.

27. SNORT / Snort team. San Jose : Cisco Systems Inc, 2018. [Електронний ресурс]. – Режим доступу: https://www.snort.org/.

28. OSSEC–HIDS Capabilities, Architecture and plans / Ozturk. Ahmet // Presentation at the 5th Linux and Free Software Festival. Ankara, 2006.

29. Zeek / Vern Paxson// Zeek.org :. Geneva : Zeek (Bro), 2018. [Електронний ресурс]. – Режим доступу: https://www.bro.org/download/ index.html (viewed on September 6, 2018).

30. A. Conry-Murray. Protect Web applications from abuse and misuse [Електронний ресурс]. — Режим доступу:

https://www.researchgate.net/publication/297840775_Protect_Web_applications_from_abuse_and_misuse

31. The SAMHAIN file integrity / host–based intrusion detection system / Rainer Wichmann // Samhain. Boston : Samhain Services, 2011.

32. Lidong Wang. Big Data in Intrusion Detection Systems and Intrusion Prevention Systems. [Електронний ресурс]. – Режим доступу: http://pubs.sciepub.com/jcn/4/1/5/index.html.

33. Manasi Gyanchandani, J.L.Rana, R.N.Yadav. Taxonomy of Anomaly Based Intrusion Detection System: A Review / M. Gyanchandani, J.L.Rana, R.N.Yadav. // International Journal of Scientific and Research Publications. – Volume 2. – Issue 12. – December 2012.

34. Аналіз та класифікація методів виявлення вторгнень в інформаційну систему / В. В. Бєрковський, О. С. Безсонов // Системи управління, навігації та зв'язку. - 2017. - Вип. 3. - С. 57-62. - [Електронний ресурс] – Режим доступу: http://nbuv.gov.ua/UJRN/suntz_2017_3_17