

**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
НАВЧАЛЬНО-НАУКОВИЙ ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра інформаційної безпеки**

«На правах рукопису»
УДК _____

«До захисту допущено»
Завідувач кафедри
_____ Дмитро ЛАНДЕ
(підпис)
« _____ » _____ 2025 р.

**Магістерська дисертація
на здобуття ступеня магістра
за освітньо-професійною програмою «Системи, технології та
математичні методи кібербезпеки»
спеціальності 125 «Кібербезпека та захист інформації»**

на тему: Побудова моделі передбачення атак на ІТ-інфраструктуру

Виконав (-ла): здобувач вищої освіти ІІ курсу, групи ФБ-42мп
(шифр групи)

Сербіненко Олексій Григорович
(прізвище, ім'я, по батькові) (підпис)

Керівник доцент кафедри ІБ, к.т.н. доц. Коломицев Михайло Володимирович
(посада, науковий ступінь, вчене звання, прізвище, ім'я, по батькові) (підпис)

Рецензент доцент кафедри ММЗІ к.ф.-м.н Микола Олексійович Хмельницький
(посада, науковий ступінь, вчене звання, науковий ступінь, прізвище, ім'я, по батькові) (підпис)

Засвідчую, що у цій магістерській дисертації
немає запозичень з праць інших авторів без
відповідних посилань.
Здобувач вищої освіти _____
(підпис)

Київ – 2025 року

**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
НАВЧАЛЬНО-НАУКОВИЙ ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра інформаційної безпеки**

Рівень вищої освіти – другий (магістерський)
Спеціальність – 125 «Кібербезпека та захист інформації»
Освітньо-професійна програма «Системи, технології та математичні методи кібербезпеки»

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Дмитро ЛАНДЕ
(підпис)
« ____ » _____ 2025 р.

ЗАВДАННЯ
на магістерську дисертацію здобувачу вищої освіти
Сербіненко Олексій Григорович

(прізвище, ім'я, по батькові)

1. Тема роботи Побудова моделі передбачення атак на ІТ-інфраструктуру
керівник роботи

_____ Коломицев Михайло Володимирович *к.т.н., доцент* _____,
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від від «4» листопада 2025 р. No 4797-с

2. Термін подання здобувачем вищої освіти роботи « ____ » _____ 2025 р.

3. Вихідні дані до роботи

Вихідні дані до роботи Технічна документація бібліотек машинного навчання (Scikit-learn, TensorFlow або PyTorch) та посібники з обробки великих даних; специфікації мови програмування Python.

4. Зміст роботи

Аналіз обмежень реактивних методів захисту та особливостей часових рядів мережевого трафіку; відбір та нормалізація ключових ознак для навчання моделі; побудова математичної моделі прогнозування кібератак засобами машинного навчання; програмна реалізація модуля парсингу логів та сервісу генерації попереджень; експериментальна оцінка точності прогнозу та рівня хибних спрацювань на тестовому наборі даних.

5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо)

Презентація до захисту магістерської дисертації.

6. Дата видачі завдання 10 вересня 2025.

Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Термін виконання етапів магістерської дисертації	Примітка
1	Визначення напрямку МД	11.09.2025 - 18.09.2025	Виконано
2	Визначення теми МД	20.09.2025 - 29.09.2025	Виконано
3	Збір та аналіз літературних джерел	02.10.2025 - 17.10.2025	Виконано
4	Збір та аналіз літературних джерел	02.10.2025 - 17.10.2025	Виконано
5	Розробка програмного коду	01.11.2025 - 24.11.2025	Виконано
6	Тестування та удосконалення	25.11.2025 - 07.12.2025	Виконано
7	Формування графічної частини (презентації)	08.12.2025	Виконано
8	Підготовка та передзахист МД	09.12.2025 - 13.12.2025	Виконано
9	Підготовка до захисту МД	01.12.2025 - 17.12.2025	Виконано

Здобувач вищої освіти

(підпис)

Олексій СЕРБІНЕНКО

(Власне ім'я, ПРІЗВИЩЕ)

Керівник роботи

(підпис)

Михайло КОЛОМИЦЕВ

(Власне ім'я, ПРІЗВИЩЕ)

РЕФЕРАТ

Обсяг роботи – 69 сторінок, 9 ілюстрацій, 5 джерел літератури.

Об’єкт дослідження: Процес забезпечення кібербезпеки IT-інфраструктури в умовах впливу різнорідних зовнішніх факторів.

Предмет дослідження: методи та моделі прогнозування кібератак на основі виявлення часових імовірнісних залежностей від подій зовнішнього середовища.

Мета дослідження: полягає у підвищенні ефективності проактивного захисту IT-інфраструктури шляхом завчасного виявлення підготовки кібератак на основі виявлення та формалізації часових залежностей між зовнішніми подіями-тригерами та ескалацією кіберзагроз.

Методи дослідження: застосовано комплексний підхід, що базується на інтеграції методів аналізу даних та машинного навчання для виявлення прихованих закономірностей у масивах інформації з відкритих джерел. Прогностична складова реалізована за допомогою ансамблевих моделей класифікації, точність яких перевірено з використанням спеціалізованих статистичних метрик.

Отримані результати. Розроблено прогнозну модель кібератак, що поєднує аналіз змінних зовнішнього середовища, часові імовірнісні правила та методи машинного навчання. Сформовано набір даних на основі відкритих джерел, зокрема CERT-UA, агрегований у вигляді часових рядів. Реалізовано програмні модулі пошуку TP-rules та кількісного прогнозування ймовірності кібератак різних типів. Експериментально підтверджено можливість використання військово-політичних подій як предикторів ескалації кіберзагроз.

Ключові слова: прогнозування кібератак, гібридна війна, кібербезпека, змінні зовнішнього середовища, часові імовірнісні правила, TP-rules.

ABSTRACT

Volume of work – 69 pages, 9 illustrations, 5 literature sources.

Object of the study: The process of ensuring cybersecurity of IT infrastructure under the influence of heterogeneous external factors.

Subject of the study: Methods and models for cyberattack forecasting based on the identification of temporal probabilistic dependencies on external environmental events.

Purpose of the study: To improve the effectiveness of proactive protection of IT infrastructure through early detection of cyberattack preparation based on identifying and formalizing temporal dependencies between external trigger events and the escalation of cyber threats.

Research methods: A comprehensive approach based on the integration of data analysis and machine learning methods was applied to identify hidden patterns in data obtained from open sources. The predictive component was implemented using ensemble classification models, the accuracy of which was evaluated using specialized statistical metrics.

Results obtained: A cyberattack forecasting model combining the analysis of external environmental variables, temporal probabilistic rules, and machine learning methods was developed. A dataset based on open sources, including CERT-UA reports, was formed and aggregated as time series. Software modules for discovering TP-rules and for quantitative prediction of the probability of different types of cyberattacks were implemented. The feasibility of using military and political events as predictors of cyber threat escalation was experimentally confirmed.

Keywords: cyberattack forecasting, hybrid warfare, cybersecurity, external environmental variables, temporal probabilistic rules, TP-rules.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ.....	7
Вступ	9
1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ ТА ІСНУЮЧИХ РІШЕНЬ.....	12
1.1 Характеристика кібервійни РФ проти України як предметної області.....	12
1.2 Огляд існуючих підходів до виявлення та прогнозування кібератак	14
1.3 Аналіз методології прогнозування тероризму на основі «змінних середовища»	19
Висновок до першого розділу	26
2 РОЗРОБКА МОДЕЛІ ПРОГНОЗУВАННЯ КІБЕРАТАК	28
2.1 Визначення змінних моделі: класифікація кібератак та подій-тригерів.....	28
2.2 Проектування набору даних: джерела, структура та часовий крок	32
2.3 Модель 1: Метод часових імовірнісних правил для пошуку закономірностей ...	35
2.4 Модель 2: Ансамбль ML-класифікаторів для кількісного прогнозування атак	38
Висновок до другого розділу	41
3 ПРОГРАМНА РЕАЛІЗАЦІЯ ТА ЕКСПЕРИМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ	43
3.1 Збір, агрегація та попередня обробка даних	43
3.2 Програмна реалізація та пошук TP-правил	48
3.3 Навчання та валідація прогновної моделі.....	51
3.4 Аналіз важливості ознак та результатів моделювання	54
Висновок до третього розділу	58
Висновки	60
ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ.....	62
Додаток А	63
Додаток Б	65
Додаток В	68

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

API (Application Programming Interface) - інтерфейс прикладного програмування, набір інструментів та функцій, що дозволяє різним програмам взаємодіяти між собою (використовувався для отримання даних з CERT-UA).

APT (Advanced Persistent Threat) - різновид складних цілеспрямованих кібератак, що характеризуються довготривалим прихованим доступом зломисника до інформаційної системи жертви з метою шпигунства або саботажу.

AUC-ROC (Area Under the Receiver Operating Characteristic Curve) - метрика оцінки якості бінарної класифікації, що відображає здатність моделі розрізняти класи незалежно від порогового значення.

CERT-UA (Computer Emergency Response Team of Ukraine) - Урядова команда реагування на комп'ютерні надзвичайні події України, джерело даних про кіберінциденти.

DDoS (Distributed Denial of Service) - розподілена атака типу «відмова в обслуговуванні», метою якої є порушення доступності сервісів шляхом їх перевантаження.

IDS (Intrusion Detection System) - система виявлення вторгнень, програмний або апаратний засіб, призначений для виявлення несанкціонованого доступу до комп'ютерної системи або мережі.

IPS (Intrusion Prevention System) - система запобігання вторгненням, засіб захисту, який автоматично блокує виявлені загрози.

JNIM (Jama'at Nusrat al-Islam wal-Muslimin) - терористичне угруповання, на прикладі якого у базовій методології досліджувався вплив змінних середовища на ескалацію атак.

k-NN (k-Nearest Neighbors) - метод k-найближчих сусідів, алгоритм машинного навчання, що класифікує об'єкти на основі голосування найближчих до них прикладів у просторі ознак.

ML (Machine Learning) - машинне навчання, підрозділ штучного інтелекту, що вивчає методи побудови алгоритмів, здатних навчатися на даних.

OSINT (Open Source Intelligence) - розвідка на основі відкритих джерел, метод збору та аналізу інформації з загальнодоступних джерел.

SIEM (Security Information and Event Management) - система управління інформаційною безпекою та подіями, що забезпечує збір та аналіз логів у реальному часі.

SOMA (Stochastic Opponent Modeling Agents) - формальна модель моделювання стохастичних агентів-опонентів, розроблена групою V.S. Subrahmanian.

SVM (Support Vector Machine) - метод опорних векторів, алгоритм машинного навчання для задач класифікації та регресії.

TP-rules (Temporal Probabilistic Rules) - часові ймовірнісні правила, формалізовані вирази, що описують умовну ймовірність настання події у майбутньому часовому інтервалі за умови наявності тригера.

UEBA (User and Entity Behavior Analytics) - системи аналізу поведінки користувачів та сутностей для виявлення аномалій.

Вступ

Актуальність роботи. У сучасних умовах функціонування ІТ-інфраструктури України спостерігається вплив зовнішніх факторів на динаміку кіберзагроз. Традиційні засоби захисту, такі як IDS/IPS, SIEM, працюють переважно за реактивним принципом: вони аналізують технічні параметри та фіксують інциденти вже в момент їх виникнення або після нього. Головним обмеженням такого підходу є те, що він фокусується виключно на внутрішніх показниках системи і не враховує зовнішній контекст - події у фізичному просторі такі як ракетні обстріли, політичні рішення, тощо, які, можуть бути передумовами для ескалації кібератак. Ігнорування цих «змінних середовища» ускладнює своєчасне виявлення підготовки до атак. Тому актуальним є завдання розробки моделі прогнозування, яка дозволить враховувати кореляцію між зовнішніми подіями та кіберінцидентами для переходу від реагування до попередження загроз.

Мета дослідження. Полягає у підвищенні ефективності проактивного захисту ІТ-інфраструктури шляхом завчасного виявлення підготовки кібератак на основі виявлення та формалізації часових залежностей між зовнішніми подіями-тригерами та ескалацією кіберзагроз.

Завдання дослідження:

1. Проаналізувати особливості гібридної війни як предметної області та обґрунтувати доцільність використання зовнішніх подій-тригерів для прогнозування кібератак.
2. Розробити структуру даних та сформувати репрезентативний датасет шляхом агрегації різномірної інформації з відкритих джерел (CERT-UA, звіти SSSCIP) у єдиний часовий ряд.
3. Реалізувати програмний модуль пошуку часових імовірнісних правил для виявлення та формалізації стійких асоціативних зв'язків

між зовнішніми подіями та ескалацією кіберзагроз з урахуванням часового кроку.

4. Побудувати та навчити ансамбль моделей машинного навчання (Random Forest, SVM, k-NN тощо) для кількісного прогнозування ймовірності атак.
5. Оцінити точність розробленої системи за допомогою метрик Precision, Recall та AUC-ROC, проаналізувати важливість ознак та визначити межі застосування моделі для різних типів кіберзагроз.

Методи дослідження. Застосовано комплексний підхід, що базується на інтеграції методів аналізу даних та машинного навчання для виявлення прихованих закономірностей у масивах інформації з відкритих джерел. Прогностична складова реалізована за допомогою ансамблевих моделей класифікації, точність яких перевірено з використанням спеціалізованих статистичних метрик.

Наукова новизна. Вперше адаптовано методологію прогнозування на основі «змінних середовища» до специфіки гібридної війни, що дозволило математично формалізувати залежності між кінетичними та політичними подіями та подальшою ескалацією кіберзагроз.

Практичне значення. Полягає у створенні програмного інструментарію, здатного прогнозувати ескалацію кіберзагроз на основі відкритих даних з точністю, достатньою для прийняття випереджальних управлінських рішень. Розроблена модель може бути інтегрована в системи раннього попередження, що дозволить оптимізувати розподіл ресурсів та забезпечити перехід від реактивного реагування до проактивного захисту ІТ інфраструктури держави.

Предмет дослідження. Методи та моделі прогнозування кібератак на основі виявлення часових імовірнісних залежностей від подій зовнішнього середовища.

Об'єкт дослідження: Процес забезпечення кібербезпеки ІТ-інфраструктури в умовах впливу різнорідних зовнішніх факторів.

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ ТА ІСНУЮЧИХ РІШЕНЬ

1.1 Характеристика кібервійни РФ проти України як предметної області

Кібернетичний аспект війни між Росією та Україною достатньо сильно впливає на ведення військових дій. З 2014 року Україна фактично була ціллю для кібернетичних операцій, але повномасштабне вторгнення Росії в лютому 2022 року відкрило нову сторінку в конфлікті - гібридну війну, що ведеться за допомогою кіберзброї. Предметна область дослідження характеризується високою інтенсивністю атак, залученням широкого спектра акторів (від державних спецслужб до хактивістських угруповань) та, що найважливіше для даної роботи, інтеграцією кібероперацій із загальною військовою стратегією агресора. У цьому конфлікті кіберпростір розглядається не як допоміжний інструмент шпигунства, а як справжня сфера військових операцій, завданням якої є знищення ІТ-інфраструктури, саботаж систем управління та деморалізація населення.

Ключовою особливістю цієї предметної області є домінування деструктивних атак, спрямованих на знищення даних та виведення з ладу інформаційних систем. На відміну від класичних АРТ-кампаній метою яких є приховане і тривале перебування в системі для крадіжки інформації, російська тактика після 2022 року масово використовує шкідливе програмне забезпечення типу Wiper (CaddyWiper, HermeticWiper, Industroyer2). Ця теза підтверджується даними аналітичного звіту Держспецзв'язку [1], в якому зафіксовано, що саме знищення інформаційних систем цивільної інфраструктури та енергетичного сектору стала пріоритетом для російських хакерських угруповань (зокрема Sandworm/UAC-0082) під час активної фази вторгнення. Ці інструменти застосовуються для нанесення незворотної шкоди державним реєстрам, енергетичним компаніям та телекомунікаційним операторам. Така зміна вектора з розвідки на деструкцію створює специфічні патерни в даних: атаки стають більш гучними, помітними та часто

синхронізованими з певними зовнішніми подіями, що робить їх придатними для виявлення та прогнозування методами інтелектуального аналізу даних.

Особливої уваги в контексті створення прогнозних моделей заслуговує процес сходження кінетичних і кібернетичних ударів. Емпіричні дані, зокрема повідомлення Державної служби спеціального зв'язку та захисту інформації України (Держспецзв'язок), свідчать про існування кореляції між ракетними ударами по енергетичній інфраструктурі та спробами кібервтручання в автоматизовані системи управління технологічними процесами енергетичних розподільчих компаній. Яскравим прикладом такої координації є інцидент, зафіксований у липні 2022 року, коли одночасно з ракетним ударом по Криворізькій ТЕС відбувся масштабний кібернетичний удар по цифровій інфраструктурі компанії ДТЕК, метою якого було дестабілізувати технологічні процеси та заблокувати системи управління. Метою такої синхронізації є максимізація завданих збитків: фізичний удар руйнує обладнання, а кібернетична атака ускладнює моніторинг аварій, блокує роботу диспетчерських або перешкоджає швидкому відновленню постачання. Цей взаємозв'язок є основною передумовою для застосування методології «змінних середовища», оскільки дозволяє розглядати кінетичні події як предиктори (тригери) кібернетичних атак.

Структура суб'єктів загрози в даній предметній області є гетерогенною та багаторівневою. З одного боку, діють висококваліфіковані групи, афілійовані з російськими розвідувальними службами (ГРУ, ФСБ, СЗР), такі як Sandworm, APT28, Gamaredon, які відповідають за складні стратегічні операції та шпигунство. З іншого боку, спостерігається масова активність політично мотивованих хактивістів та кіберкримінальних груп (наприклад, Killnet, NoName057), які координуються через Telegram-канали та виконують роль «шумового супроводу», здійснюючи DDoS-атаки на сервіси державного та фінансового секторів. Така диференціація акторів вимагає від прогностичної моделі здатності розрізняти типи атак, оскільки тригери для активізації елітних спецпідрозділів та натовпу хактивістів можуть суттєво

відрізнятися. Розуміння цієї екосистеми є критично важливим для коректної класифікації загроз та вибору відповідних ознак для машинного навчання.

1.2 Огляд існуючих підходів до виявлення та прогнозування кібератак

Еволюція засобів кіберзахисту історично відбувалася як реакція на ускладнення тактик нападників. Сучасний об'єм загроз, особливо в умовах гібридної війни, вимагає переходу від детектування інцидентів "по факту" до їх випереджувального прогнозування. Аналіз наукової літератури дозволяє виділити чотири основні групи методів, що застосовуються для вирішення цього завдання.

1.2.1 Сигнатурні та евристичні методи аналізу

Це фундаментальний рівень виявлення загроз, який історично сформувався першим і досі лежить в основі більшості традиційних систем IDS/IPS та антивірусного програмного забезпечення.

Сигнатурний метод (або *misuse detection*) базується на порівнянні об'єктів моніторингу - файлів, записів у оперативній пам'яті або мережевих пакетів - із попередньо сформованою базою даних відомих патернів атак. Сигнатура може являти собою унікальну хеш-суму шкідливого файлу (наприклад, MD5 або SHA-256), специфічну послідовність байтів у коді експлойта або характерний рядок у заголовку мережевого запиту.

Класичним прикладом реалізації цього підходу є система виявлення вторгнень Snort або Suricata. Вони працюють на основі правил, які описують ознаки атаки. Наприклад, правило для виявлення спроби експлуатації вразливості може виглядати як пошук конкретної шістнадцяткової послідовності (hex-string) у корисному навантаженні TCP-пакету, що прямує на 80-й порт. У сфері аналізу шкідливого ПЗ стандартом де-факто є інструмент YARA, який дозволяє дослідникам створювати правила для

ідентифікації сімейств малварі на основі текстових або бінарних патернів (наприклад, наявність специфічних м'ютексів або унікальних рядків налагодження в коді).

Цей підхід забезпечує надзвичайно високу швидкість обробки даних та низький рівень помилок першого роду, оскільки спрацювання відбувається лише при повному збігу зі зразком відомої загрози. Проте його критичним недоліком є реактивність: метод принципово не здатний виявити атаки нульового дня та поліморфне шкідливе ПЗ, яке автоматично змінює свій код при кожному зараженні, зберігаючи функціонал, але змінюючи сигнатуру.

Евристичний аналіз виник як спроба подолати обмеження сигнатурного підходу. Він використовує не точні збіги, а узагальнені правила та алгоритми для пошуку підозрілих характеристик або поведінки, що *можуть* вказувати на загрозу. Реалізація цього методу поділяється на два основні напрями:

Статичний евристичний аналіз: Здійснюється без запуску програми. Аналізатори (наприклад, у складі PE Studio) перевіряють структуру виконуваного файлу на наявність аномалій: наприклад, високий рівень ентропії коду (що може свідчити про використання пакувальників або шифрування для приховування шкідливого навантаження), або підозрілий імпорт API-функцій (наприклад, одночасний імпорт функцій для перехоплення натискань клавіш та відправки даних у мережу).

Динамічний аналіз (поведінкова евристика): Передбачає запуск файлу в ізольованому віртуальному середовищі - «пісочниці», такий як Cuckoo Sandbox або Any.Run. Система моніторить дії процесу в реальному часі та присвоює їм «бали підозрілості». Якщо програма намагається прописати себе в автозавантаження (реєстр Windows), вимкнути брандмауер, встановити з'єднання з відомим командним сервером або масово шифрувати файли (ознака програм-вимагачів) - евристичний аналізатор блокує її роботу як шкідливу.

Хоча це дозволяє виявляти нові модифікації відомих вірусів, евристика часто страждає від високого рівня хибних спрацювань, блокуючи легітимне програмне забезпечення, що має схожі поведінкові патерни (наприклад, інсталятори драйверів або програми для шифрування дисків).

1.2.2 Поведінковий аналіз та виявлення аномалій

З розвитком технологій SIEM та UEBA набув поширення підхід, заснований на профілюванні нормальної поведінки. На відміну від сигнатурного методу, який шукає "відоме погане", поведінковий аналіз намагається виявити відхилення від "відомого хорошого".

Суть методу полягає у побудові динамічної базової лінії (baseline) нормальної активності для кожного користувача, хоста, мережевого сегмента або застосунку. Цей профіль формується на основі історичних даних і включає такі параметри, як типовий час входу в систему, обсяги передачі даних, географічне розташування користувача та перелік процесів, що зазвичай запускаються. Будь-яке статистично значуще відхилення від цієї норми (наприклад, різке зростання обсягу вихідного трафіку в нічний час або доступ адміністратора до бази даних, з якою він раніше не працював) маркується системою як інцидент.

Головною проблемою цього підходу в умовах війни є концептуальна нестабільність "нормального стану". Динамічні зміни режимів роботи критичної інфраструктури - аварійні відключення електроенергії, перемикання на резервні канали зв'язку (наприклад, Starlink), масова міграція персоналу та віддалена робота з незахищених мереж - призводять до значного зростання "шуму" в системі детектування. У таких умовах системи поведінкового аналізу генерують величезну кількість хибних тривог, що ускладнює роботу аналітиків SOC і підвищує ризик пропуску реальної цільової атаки.

1.2.3 Прогнозування методами машинного та глибокого навчання

Сучасний метод у прогнозуванні технічних атак базується на використанні методів штучного інтелекту, які дозволяють автоматизувати процес виявлення складних залежностей у великих масивах даних. Як зазначають у своєму ґрунтовному огляді Y. Xie та співавтори [4], алгоритми машинного навчання демонструють високу ефективність там, де традиційні методи не справляються з обсягом та різноманітністю даних.

Серед методів класичного машинного навчання широке застосування знайшли алгоритми Random Forest та Support Vector Machines. Вони ефективно використовуються для класифікації мережевого трафіку, дозволяючи з високою точністю відрізнити легітимні сплески активності від DDoS-атак прикладного рівня, а також для виявлення шкідливих доменів, згенерованих алгоритмічно.

Особливий інтерес для задач прогнозування становлять методи глибокого навчання, зокрема рекурентні нейронні мережі та мережі довгої короткострокової пам'яті. Ці архітектури спеціально розроблені для роботи з послідовностями даних, що робить їх ідеальними для аналізу часових рядів подій безпеки. LSTM-моделі здатні "запам'ятовувати" контекст попередніх дій у системі та прогнозувати наступні кроки зломисника у ланцюжку кібервбивства [4]. Проте, незважаючи на технологічну досконалість, ці методи часто розглядають кібератаку як ізольовану технічну подію, ігноруючи зовнішній геополітичний контекст, що обмежує їхню прогностичну силу в умовах гібридних загроз.

1.2.4 Стратегічне прогнозування на основі контекстних даних

Найновішим та найбільш перспективним напрямком досліджень у сфері проактивного захисту є інтеграція технічних даних телеметрії з даними стратегічної розвідки загроз. Цей підхід базується на зміні парадигми сприйняття кіберзагроз: атаки, особливо ті, що виконуються державними акторами або підконтрольними їм угрупованнями, розглядаються не як стохастичні технічні збої, а як раціональні, цілеспрямовані операції, що є

частиною ширшої стратегії. У такому контексті сама кібератака є лише інструментом досягнення політичної, військової або економічної мети, а отже, її підготовку та початок можна передбачити шляхом аналізу зовнішнього контексту.

Фундаментальне значення для цього напрямку мають роботи наукової групи під керівництвом V.S. Subrahmanian [5]. Автори запропонували концепцію використання «змінних середовища» (environmental variables) як предикторів поведінки агресивних недержавних суб'єктів. Відповідно до цієї методології, будь-яке агресивне угруповання діє в екосистемі, на яку впливають зовнішні фактори: політичні заяви лідерів держав, введення економічних санкцій, арешти ключових фігур, релігійні свята або соціальні заворушення. Ці події виступають тригерами, що змінюють ймовірність вчинення атаки у певному часовому проміжку.

Розроблені цією групою формальні моделі, зокрема SOMA (Stochastic Opponent Modeling Agents), базуються на видобуванні часових імовірнісних правил (Temporal Probabilistic Rules) з історичних даних. Такі правила мають структуру: «Якщо відбувається подія А (тригер), то з ймовірністю Р у часовому інтервалі Т відбудеться атака типу Б». Цей підхід успішно застосовувався для прогнозування активності терористичних організацій (наприклад, Хезболли, Лашкар-е-Тайба) на Близькому Сході та в Азії, демонструючи високу точність передбачення фізичних терактів та диверсій [5].

Проблема та прогалина в дослідженнях: Незважаючи на доведену ефективність методології «змінних середовища» у контртерористичній діяльності, вона досі не була системно адаптована для умов повномасштабної міждержавної війни високої інтенсивності, яка триває в Україні. Унікальність поточної ситуації полягає в безпрецедентній конвергенції доменів: кібератаки синхронізовані не просто з абстрактними політичними

рішеннями, а з використанням важкого конвенційного озброєння (кінетичних ударів).

Існуючі системи СТІ та наукові моделі фокусуються переважно на:

1. Стратегічному рівні: аналіз геополітичних трендів (хто і чому атакуватиме у довгостроковій перспективі?).
2. Оперативно-тактичному рівні: аналіз технічних індикаторів компрометації (IoC) вже під час атаки.

Водночас існує критична прогалина у тактичному прогнозуванні, яке б відповідало на питання «коли і який тип атаки очікувати?» на основі кореляції з подіями на фронті та ракетними обстрілами. Адаптація методу часових правил для виявлення зв'язків між кінетичними подіями (як тригерами) та кібератаками (як наслідками) є новим науковим завданням. Саме розробці такої гібридної адаптивної моделі, що поєднує методи машинного навчання (ML) із логікою аналізу змінних середовища, присвячено дане дослідження.

1.3 Аналіз методології прогнозування тероризму на основі «змінних середовища»

Сучасна наука про безпеку дедалі частіше відходить від статичного аналізу ідеології чи психологічних портретів лідерів терористичних угруповань на користь динамічного моделювання їхньої поведінки як реакції на зовнішні стимули. Фундаментальною для цього напрямку є методологія, системно викладена у книзі групи дослідників «Machine Learning Techniques to Predict Terrorist Attacks» [3]. Автори пропонують розглядати агресивну діяльність недержавних збройних формувань (NSAG), на прикладі групи JNIM (Джамаат Нусрат аль-Іслам валь-Муслімін), не як хаотичний набір інцидентів, а як функцію від зовнішніх умов - так званих «змінних середовища» (environmental variables)

1.3.1 Теоретичні засади підходу прогнозування на основі змінних середовища

У сучасних дослідженнях з проблематики міжнародної, національної та інформаційної безпеки спостерігається стійка тенденція до переходу від суто описового аналізу загроз до використання методів прогнозування, орієнтованих на випереджальне виявлення потенційних ризиків. Традиційні підходи, що базуються виключно на аналізі безпосередніх актів насильства або технічних характеристик атак, дедалі частіше виявляються недостатніми для пояснення складної та багатофакторної природи сучасних конфліктів. У цьому контексті особливу увагу привертає методологія прогнозування терористичної активності на основі так званих «змінних середовища», детально представлена у книзі *Machine Learning Techniques to Predict Terrorist Attacks* [3].

Сутність даного підходу полягає у принципово іншому баченні природи терористичної діяльності. Терористичні акти розглядаються не як випадкові або ізольовані інциденти, а як результат дії складної системи зовнішніх чинників, що формують політичне, військове, соціальне та інформаційне середовище функціонування терористичних угруповань. Такий підхід виходить з припущення, що рішення про здійснення атак ухвалюються під впливом конкретних подій або змін у зовнішньому середовищі, які можуть виступати тригерами ескалації насильства.

На відміну від класичних статистичних моделей, які працюють переважно з історичними даними про вже здійснені атаки та орієнтовані на виявлення повторюваних патернів, підхід змінних середовища фокусується на аналізі подій і станів, що передують насильницьким діям. Йдеться про такі фактори, як дії державної влади, міжнародний тиск, військові операції або інформаційні кампанії, які самі по собі не є терористичними актами, але здатні змінювати мотивацію, ресурси та тактику угруповань.

До змінних середовища, згідно з розглянутою методологією, належать політичні, військові, економічні та інформаційні фактори, які формують

загальний контекст безпекової ситуації. Важливою методологічною особливістю є те, що ці змінні не розглядаються абстрактно, а формалізуються у вигляді чітко визначених подій або станів, які можуть бути представлені в форматі набору даних приведених до структури яку може зчитати програма. Це дозволяє використовувати їх як вхідні ознаки для алгоритмів машинного навчання та статистичного аналізу.

З точки зору системного підходу, такий метод добре узгоджується з концепцією аналізу складних технічних і соціотехнічних систем, що традиційно застосовується в інженерних та безпекових напрямках. Терористична активність у цьому випадку розглядається як вихід системи, на який одночасно впливають численні вхідні параметри. Відповідно, прогнозування зводиться не до механічної екстраполяції трендів, а до аналізу причинно-наслідкових зв'язків між станом середовища та подальшими діями акторів загрози, що значно підвищує аналітичну цінність отриманих результатів.

1.3.2 Формалізація змінних середовища та їх роль у побудові прогнозних моделей

Однією з ключових передумов практичного застосування методології прогнозування на основі змінних середовища є чітка та однозначна формалізація цих змінних. Без такої формалізації використання методів машинного навчання та інтелектуального аналізу даних є неможливим. У розглянутому дослідженні змінні середовища визначаються як дискретні події або бінарні стани, що фіксують факт настання певної зовнішньої умови у конкретному часовому інтервалі [3].

З практичної точки зору це означає перехід від якісного опису безпекової ситуації до її кількісного подання. Для кожного часового кроку формується вектор ознак, який відображає наявність або відсутність конкретних політичних, військових чи інформаційних подій. У результаті створюються структуровані часові ряди, придатні для подальшого аналізу

методами машинного навчання, пошуку закономірностей та побудови прогнозних моделей.

У межах методології, описаної в книзі, змінні середовища групуються за їх функціональним призначенням, що дозволяє впорядкувати вхідні дані та зменшити складність моделі. Зокрема, виокремлюються такі основні категорії змінних:

- **політико-правові змінні**, які відображають рішення та дії органів державної влади, зокрема запровадження надзвичайного стану, проведення виборів, арешти або ліквідацію лідерів угруповань;
- **міжнародні змінні**, пов'язані з реакцією зовнішніх акторів на конфлікт, включаючи економічні санкції, заморожування активів, надання міжнародної військової чи фінансової допомоги;
- **військово-оперативні змінні**, що характеризують інтенсивність та характер дій сил безпеки, таких як контртерористичні операції, рейди, застосування сили у зонах конфлікту;
- **інформаційні змінні**, які описують комунікаційну активність як самих терористичних угруповань, так і державних структур, зокрема публічні заяви, пропагандистські матеріали та інформаційно-психологічні операції.

Особливої уваги потребує питання коректної часової прив'язки змінних середовища. Ефективність прогнозування значною мірою залежить не лише від кількості або різноманітності змінних, але й від правильного визначення часового вікна між подією середовища та можливою реакцією угруповання. Неправильний вибір цього інтервалу може призвести до хибних кореляцій або втрати прогностичної здатності моделі. Саме тому в роботі авторів значна увага приділяється експертному відбору змінних, перевірці статистичної значущості отриманих залежностей та їх інтерпретації з позицій предметної області.

Практичну цінність підходу змінних середовища у поєднанні з часовими ймовірнісними правилами автори книги демонструють на прикладі аналізу діяльності терористичної групи *JNIM*, що діє на території країн Малі та Буркіна-Фасо. У дослідженні розглядається низка конкретних сценаріїв, у яких певні зовнішні події виступають тригерами зростання терористичної активності у визначеному часовому інтервалі [3].

Зокрема, одним із типових прикладів є реакція угруповання на військово-оперативні дії міжнародних сил безпеки. У книзі показано, що проведення спільних контртерористичних операцій із залученням іноземних військових контингентів статистично корелює зі зростанням імовірності атак *JNIM* протягом наступних декількох тижнів. У цьому випадку військова операція виступає змінною середовища, а серія нападів на військові або цивільні цілі - подіями-відгуками, що формують часове ймовірнісне правило типу: за наявності конкретного тригера імовірність атаки зростає у визначеному часовому вікні.

Іншим прикладом, наведеним авторами, є арешт або ліквідація лідерів угруповання, що належить до політико-правових змінних середовища. Дослідження показує, що подібні дії з боку держави або міжнародних сил не завжди призводять до негайного зниження активності. Навпаки, у ряді випадків фіксується підвищення інтенсивності атак як форма демонстративної відповіді або спроби відновлення втраченої репутації. Це дозволяє формалізувати правило, за яким імовірність певного типу атак зростає після усунення ключових фігур угруповання.

Також у книзі розглядається вплив міжнародних санкцій та обмеження фінансування як економічних змінних середовища. Автори відзначають, що зменшення доступу до фінансових ресурсів у середньостроковій перспективі може змінювати тактику атак, зокрема сприяти переходу до менш ресурсомістких, але більш частих насильницьких дій. Такі закономірності також описуються у вигляді часових ймовірнісних правил, що враховують

затримку між економічним тиском і зміною характеру терористичної активності.

Аналогічна логіка може бути безпосередньо адаптована до задач кібербезпеки в умовах збройного конфлікту в Україні. У цьому випадку роль терористичних атак відіграють кібератаки на інформаційні системи, а змінні середовища формуються військово-політичними та інформаційними подіями високого рівня. Наприклад, такими тригерами можуть виступати масовані ракетні удари по критичній інфраструктурі, ухвалення міжнародних санкційних пакетів або публічні заяви політичного керівництва щодо ескалації конфлікту.

У межах запропонованої адаптації кібератаки типу DDoS, фішингові кампанії або спроби компрометації державних інформаційних ресурсів розглядаються як події-відгуки на ці змінні середовища. Відповідно, часові ймовірнісні правила дозволяють формалізувати залежність між, наприклад, ескалацією бойових дій та зростанням імовірності кібератак на інформаційні системи органів державної влади або об'єктів критичної інфраструктури у наступному часовому інтервалі.

Таким чином, наведені у книзі приклади демонструють універсальність підходу змінних середовища та часових ймовірнісних правил. Їх застосування не обмежується аналізом класичного тероризму, а може бути ефективно використане для прогнозування кіберзагроз у сучасних умовах гібридної війни.

1.3.3 Часові ймовірнісні правила та можливості адаптації до кібербезпеки

Для формалізації виявлених залежностей між змінними середовища та терористичною активністю у розглянутому дослідженні застосовується апарат часових ймовірнісних правил (Temporal Probabilistic Rules). TP-rules дозволяють у формалізованому вигляді описати умовну ймовірність настання

терористичної атаки за умови, що певна комбінація змінних середовища спостерігалася у попередньому часовому інтервалі [3].

На відміну від класичних кореляційних або регресійних моделей, часові ймовірнісні правила мають чітко виражену прикладну спрямованість. Вони є інтерпретованими та легко зрозумілими для аналітиків, оскільки кожне правило фактично формує гіпотезу типу «якщо – то», доповнену кількісною оцінкою ймовірності. Це є особливо важливим у сфері безпеки, де результати аналізу мають бути не лише точними, але й зрозумілими для осіб, які ухвалюють рішення.

Методологічний інтерес становить можливість перенесення даного підходу у сферу кібербезпеки. Кібератаки, подібно до терористичних актів, рідко є випадковими та часто мають чітку прив'язку до зовнішніх політичних, військових або економічних подій. У контексті гібридної війни такі події можуть розглядатися як аналоги змінних середовища, тоді як кібератаки виступають як наслідкові події, ймовірність яких може бути оцінена за допомогою TP-rules.

Таким чином, адаптація методології прогнозування тероризму до задач кібербезпеки передбачає інтерпретацію військово-політичних, економічних та інформаційних подій як змінних середовища, а кіберінцидентів - як подій, що є реакцією на ці зміни. Це створює науково обґрунтоване підґрунтя для побудови систем раннього попередження кібератак та забезпечує перехід від реактивного реагування до проактивного управління кіберризиками.

У контексті даної магістерської дисертації розглянута методологія використовується як концептуальна основа для подальшої розробки прогнозної моделі, що дозволяє формалізувати залежності між зовнішніми подіями та ескалацією кіберзагроз в умовах збройного конфлікту, що є особливо актуальним для забезпечення кіберстійкості ІТ інфраструктури критичних об'єктів України.

Виснокок до першого розділу

У першому розділі було сформовано теоретико-аналітичне підґрунтя для подальшого дослідження задачі прогнозування кібератак в умовах гібридної війни. Розглянуто особливості кібервійни Російської Федерації проти України як специфічної предметної області, що характеризується високою інтенсивністю атак, широким колом акторів загрози та тісною інтеграцією кібероперацій із кінетичними військовими діями.

Показано, що після початку повномасштабного вторгнення у 2022 році кіберпростір перетворився на повноцінну частину війни, у межах якої кібератаки використовуються як інструмент стратегічного та тактичного впливу. Особливу увагу приділено деструктивному характеру російських кібероперацій, зокрема використанню шкідливого програмного забезпечення типу Wiper та атакам на ІТ інфраструктуру критичних об'єктів, що суттєво відрізняє поточний конфлікт від класичних АРТ-кампаній розвідувального спрямування. Обґрунтовано, що така специфіка створює виразні часові та контекстні патерни, придатні для інтелектуального аналізу та прогнозування.

У межах огляду існуючих підходів до виявлення та прогнозування кібератак проаналізовано сигнатурні, евристичні, поведінкові та машинно-навчальні методи. Визначено їхні переваги та обмеження, зокрема реактивний характер традиційних систем захисту та знижену ефективність поведінкових моделей в умовах нестабільного стану під час війни. Окремо наголошено, що більшість сучасних ML- та DL-підходів розглядають кібератаки як ізольовані технічні події, недостатньо враховуючи зовнішній геополітичний та військовий контекст.

У зв'язку з цим у розділі обґрунтовано доцільність застосування стратегічного підходу до прогнозування на основі контекстних даних, зокрема методології «змінних середовища» та часових імовірнісних правил. Проаналізовано теоретичні засади цього підходу, принципи формалізації змінних середовища та наведено приклади його практичного застосування

для прогнозування терористичної активності. Показано універсальність методології та можливість її адаптації до задач кібербезпеки в умовах збройного конфлікту в Україні, де роль тригерів можуть відігравати кінетичні удари, військово-політичні рішення та інформаційні події високого рівня.

Таким чином, у першому розділі виявлено наукову прогалину, що полягає у відсутності системних моделей тактичного прогнозування кібератак, синхронізованих із подіями на полі бою. Сформульовано передумови для розробки гібридної прогнозовної моделі, яка поєднує методи машинного навчання з логікою аналізу змінних середовища та часових імовірнісних правил. Отримані висновки слугують теоретичною основою для побудови та реалізації такої моделі у наступних розділах магістерської дисертації.

2 РОЗРОБКА МОДЕЛІ ПРОГНОЗУВАННЯ КІБЕРАТАК

Другий розділ присвячено безпосередній розробці моделі прогнозування кібератак, адаптованої до умов гібридної війни та специфіки українського кіберпростору. Подібний підхід до прогнозування складних загроз на основі подій зовнішнього середовища використовується в роботі [3], де показано можливість виявлення часових залежностей між контекстними подіями та подальшою ескалацією асиметричних атак.

У межах розділу реалізується концептуальний перехід від теоретичних засад до практичного моделювання. Зокрема, визначається множина змінних моделі, що охоплює як класи кібератак, так і події-тригери зовнішнього середовища; проєктується структура набору даних із урахуванням часової дискретизації та джерел інформації; а також розробляються два взаємодоповнювальні підходи до прогнозування. Перший ґрунтується на застосуванні часових імовірнісних правил (TP-rules) для виявлення стійких асоціативних закономірностей у часових рядах подій, другий - на використанні ансамблю методів машинного навчання для кількісної оцінки ймовірності кібератак.

Таким чином, другий розділ формує методологічне та математичне підґрунтя всієї прогностичної системи, результати якої надалі використовуються для програмної реалізації та експериментального дослідження, представлених у третьому розділі.

2.1 Визначення змінних моделі: класифікація кібератак та подій-тригерів

Розробка моделі прогнозування кібератак передбачає формалізований опис як самих атак, так і зовнішніх умов, за яких відбувається їх ескалація. В умовах гібридної війни кібернетичні операції тісно інтегровані з

військовими, політичними та інформаційними процесами, що зумовлює необхідність розширення простору ознак за межі суто технічних характеристик інформаційних систем. У зв'язку з цим у даній роботі використовується підхід аналізу змінних зовнішнього середовища, аналогічний до підходу, описаного в [3], де такі змінні розглядаються як потенційні тригери ескалації атак.

У межах запропонованої моделі всі змінні поділяються на дві групи: цільові змінні, що описують реалізацію кібератак певних типів, та пояснювальні змінні, які відображають зовнішні події й умови, що можуть впливати на їх виникнення та інтенсивність.

2.1.1 Класифікація кібератак як цільових змінних

Цільові змінні моделі відповідають за фіксацію факту здійснення кібератаки певного класу в заданому часовому інтервалі. Аналогічний принцип узагальненої класифікації подій за їх стратегічною роллю застосовується в [3], де типи атак розглядаються не за технічною реалізацією, а за їх функцією в межах ширшого конфліктного контексту. У даній роботі розглядаються такі основні класи кібератак:

Таблиця 2.1 - Класи кібератак, що використовуються в моделі прогнозування

№	Клас кібератаки	Характеристика
1	Wiper-атаки	Деструктивні атаки, спрямовані на знищення даних та виведення з ладу інформаційних систем
2	APT / кібершпигунство	Цілеспрямовані атаки з довготривалим прихованим доступом до інформаційних ресурсів
3	DDoS-атаки	Атаки відмови в обслуговуванні з метою порушення доступності сервісів
4	Defacement	Несанкціонована модифікація вебресурсів з інформаційно-психологічною метою
5	Hacktivism	Політично мотивовані кібератаки демонстративного характеру

Обрані класи дозволяють охопити як стратегічні деструктивні операції, так і масові інформаційні атаки, що є типовими для гібридних конфліктів. Кожен тип кібератак у моделі розглядається окремо, що дає змогу аналізувати відмінності у впливі зовнішніх факторів на різні види загроз.

2.1.2 Події-тригери як змінні зовнішнього середовища

Пояснювальні змінні моделі описують події зовнішнього середовища, які потенційно можуть передувати активізації кібернетичних атак. У рамках підходу змінних середовища такі події інтерпретуються як сигнали, що відображають зміну загальної оперативної або політичної обстановки та можуть впливати на рішення атакувальної сторони щодо використання кіберзасобів, що узгоджується з підходом до аналізу подій зовнішнього середовища, запропонованим у [3].

До переліку ключових подій-тригерів, що враховуються в моделі, належать:

Таблиця 2.2 - Зовнішні події-тригери, що використовуються в моделі

№	Тригер	Опис	Очікуваний вплив
1	Масований ракетний обстріл	≥ 50 ракет за добу	Зростання ймовірності Wiper
2	Удари по енергетиці	Атаки на ТЕС, ПС	APT, ICS-атаки
3	Політичні події	Саміти, заяви	Hacktivism
4	Санкції	Нові пакети санкцій	DDoS, defacement
5	Військові поразки РФ	Втрата територій	Інформаційні атаки

Вибір зазначених тригерів зумовлений їх регулярною появою у відкритих джерелах та потенційним впливом на інформаційно-керовані компоненти гібридної війни.

2.1.3 Формалізація змінних та часовий аспект

Для забезпечення можливості автоматизованого аналізу всі змінні моделі підлягають формалізації та поданню у вигляді числових показників. Оскільки події, що аналізуються в рамках гібридної війни, мають різну природу, інтенсивність та періодичність, ключовим завданням є приведення

їх до єдиного часово-логічного простору, придатного для подальшого статистичного та імовірнісного аналізу.

Аналіз здійснюється з фіксованим часовим кроком, що відповідає одному календарному місяцю. Такий вибір часового кроку зумовлений необхідністю, з одного боку, згладити короткострокові випадки окремих інцидентів, а з іншого - зберегти чутливість моделі до змін загальної оперативної обстановки. Крім того, місячний інтервал дозволяє агрегувати події різної природи (військові, політичні, кібернетичні) в єдиному часовому просторі без втрати інформативності. У роботі [3] показано, що використання занадто дрібних часових інтервалів ускладнює аналіз, тоді як агреговані періоди дозволяють виявляти більш стійкі закономірності між подіями.

Кожна подія-тригер описується бінарною змінною виду:

$$Trigger_i(t) \in \{0,1\}$$

де значення 1 відповідає наявності події i у часовому інтервалі t , а значення 0 - її відсутності. Такий підхід дозволяє уникнути суб'єктивної оцінки «сили» події та зосередитись на самому факті її настання, що є достатнім для виявлення часових імовірнісних закономірностей.

Аналогічним чином кожен клас кібератак описується бінарною змінною

$$Attack_j(t) \in \{0,1\}$$

яка відображає факт реалізації атаки типу j у відповідному часовому інтервалі. Бінарне подання цільових змінних є доцільним для задачі прогнозування, оскільки основною метою є не точне передбачення кількості інцидентів, а оцінка ймовірності виникнення атаки певного типу в заданому часовому горизонті.

За потреби в модель вводяться кількісні змінні, що характеризують інтенсивність атак у межах одного періоду, що дозволяє враховувати не лише факт, а й масштаб кібернетичної активності. Формалізація змінних, що використовуються в моделі, наведена в таблиці 2.3.

Таблиця 2.3 - Формалізація змінних моделі

Змінна	Тип	Значення
$\text{Trigger}_i(t)$	Бінарна	1 - подія відбулася, 0 - відсутня
$\text{Attack}_j(t)$	Бінарна	1 - зафіксовано атаку типу j , 0 - відсутня
$\text{Attack_count}_j(t)$	Кількісна	Кількість атак типу j у періоді t

Запропонована система формалізації змінних забезпечує універсальність моделі та дозволяє використовувати єдиний набір даних як для побудови часових імовірнісних правил, так і для навчання моделей машинного навчання. Такий підхід спрощує інтеграцію різних методів аналізу в межах однієї прогностичної системи та створює формалізоване підґрунтя для оцінки впливу зовнішніх подій на динаміку кібернетичних загроз.

2.2 Проектування набору даних: джерела, структура та часовий крок

Ефективність моделі прогнозування кібератак значною мірою визначається якістю та репрезентативністю набору даних, на основі якого здійснюється аналіз. З огляду на комплексний характер гібридної війни, у межах даної роботи використовується інтегрований підхід до формування набору даних, що поєднує інформацію про кіберінциденти з відомостями про зовнішні військово-політичні та соціально-економічні події.

2.2.1 Джерела даних та структура набору

Основу набору даних становлять відомості з відкритих та офіційних джерел, які систематично фіксують кіберінциденти та події, пов'язані з національною безпекою. Ключову роль відіграють звіти та оперативні сповіщення національної команди реагування на комп'ютерні інциденти CERT-UA, які містять інформацію про атаки на державні органи, фінансові установи, об'єкти енергетичної та критичної інфраструктури.

Звіти CERT-UA зазвичай включають опис типу атаки, її наслідки, галузь, на яку було спрямовано вплив, а також часові характеристики

інциденту. Узагальнений аналіз таких даних дозволяє виділити основні категорії атак, зокрема атаки відмови в обслуговуванні, фішингові кампанії, шкідливе програмне забезпечення деструктивного типу, а також спроби несанкціонованого доступу до інформаційних ресурсів.

Окрім кібернетичних інцидентів, до набору даних включаються відомості про події зовнішнього середовища. До них належать:

- військові зведення та повідомлення про активні бойові дії;
- інформація про масовані ракетні та безпілотні удари;
- офіційні повідомлення про політичні рішення та міжнародні санкції;
- аналітичні матеріали профільних дослідницьких центрів та новинних агентств.

Для уніфікації інформації з різних джерел застосовується процедура кодування подій у формалізовані змінні. У простішому випадку використовується бінарне кодування, де фіксується сам факт настання події. У випадках, коли подія має різний рівень масштабності, може застосовуватися градація за інтенсивністю.

Таблиця 2.4 – Основні джерела даних для формування набору

Джерело	Тип інформації	Призначення в моделі
CERT-UA	Кіберінциденти	Формування цільових змінних
Держспецзв'язок	Звіти про кібербезпеку	Уточнення дат та масштабів атак
Офіційні зведення	Військові події	Формування подій-тригерів
Новинні агентства	Політичні та економічні події	Контекстні змінні

У результаті формується єдиний табличний набір даних, у якому поєднуються кількісні показники кібератак та формалізовані змінні зовнішнього середовища.

2.2.2 Часовий крок та агрегація даних

Для аналізу динаміки кібератак використовується підхід часових рядів із фіксованим кроком. Як базову одиницю часу обрано календарний місяць. Такий вибір обумовлений необхідністю досягнення балансу між деталізацією даних і стійкістю статистичних закономірностей.

Щомісячна агрегація дозволяє зменшити вплив випадкових одиничних інцидентів та виявити загальні тенденції розвитку кібернетичних загроз. Усі кіберінциденти, зафіксовані протягом місяця, підсумовуються або зводяться до бінарних показників за кожною категорією атак. Аналогічним чином у межах одного періоду агрегуються події-тригери зовнішнього середовища.

У підсумковій структурі набору даних кожен рядок відповідає одному часовому інтервалу та містить:

- ідентифікатор періоду (рік, місяць);
- значення цільових змінних для кожного класу кібератак;
- значення пояснювальних змінних, що описують зовнішні події.

Таблиця 2.5 - Приклад структури набору даних

Період	DDoS	Wiper	Defacement	Масовані обстріли	Санкції
2022-03	1	1	0	1	0
2022-04	1	0	1	1	1
2022-05	0	0	1	0	0

Такий формат набору даних є універсальним і придатним як для аналізу часових імовірнісних залежностей між подіями, так і для подальшого застосування методів машинного навчання. Він забезпечує узгодженість між різнорідними джерелами інформації та створює основу для побудови прогнозової моделі кібератак.

Для наочного представлення архітектури розробленої системи та потоків даних між її компонентами, загальна структурна схема моделі наведена на рисунку 2.1.

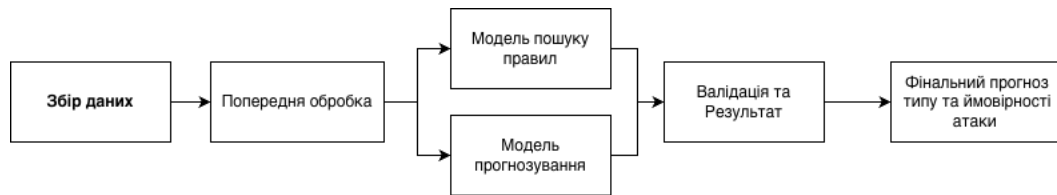


Рисунок 2.1 - Загальна структурна схема моделі прогнозування кібератак

2.3 Модель 1: Метод часових імовірнісних правил для пошуку закономірностей

Першу модель прогнозування кібератак у межах даного дослідження становить набір часових імовірнісних правил (Temporal Probabilistic Rules). Основна ідея підходу полягає у виявленні стійких закономірностей між подіями зовнішнього середовища та подальшою реалізацією кібератак із урахуванням часової затримки між ними. Такий підхід дозволяє перейти від простого опису спостережуваних фактів до формалізованого подання причинно-наслідкових залежностей у часовому просторі.

Інтуїтивно ТР-правила можна розглядати як асоціативні правила, доповнені часовим зсувом. Вони описують ситуації виду: якщо у певний момент часу або протягом визначеного періоду відбулася комбінація подій-тригерів, то з певною ймовірністю через заданий часовий інтервал відбудеться кібератака конкретного типу. Формально таке правило можна подати у вигляді: «Якщо подія А (тригер) трапилася у t , то атака типу В відбудеться у проміжку $[t+1, t+T]$ з ймовірністю P ».

Таким чином, ТР-правила дозволяють явно моделювати часову залежність між подіями, що є критично важливим для задач прогнозування в умовах гібридної війни, де кібернетичні операції часто мають відкладений характер і синхронізуються з подіями в інших доменах.

Однією з переваг використання TP-правил є їхня висока інтерпретованість. На відміну від багатьох статистичних або машинних методів, результатом роботи алгоритму є набір логічно зрозумілих правил, які безпосередньо описують, за яких умов і з якою ймовірністю варто очікувати певний тип кібератаки. Наприклад, правило виду «масовані ракетні обстріли та активні наступальні дії → з високою ймовірністю атаки відмови в обслуговуванні на об'єкти критичної інфраструктури в наступному місяці» може бути безпосередньо використане аналітиками для підвищення рівня готовності систем захисту.

Для побудови TP-правил початкові дані переводяться у форму так званої матриці «час – сигнал», де кожен рядок відповідає окремому часовому інтервалу, а кожен стовпець - бінарній або кількісній ознаці, що відображає наявність події або атаки. Далі застосовуються алгоритми видобування асоціативних правил, адаптовані до часових даних, зокрема алгоритми типу Apriori або FP-growth адаптовані до часових даних за аналогією з підходами, описаними в [3].

Кожне отримане правило характеризується стандартними показниками якості: підтримкою, довірою (confidence) та мірою підсилення (lift). Значення підтримки відображає частоту появи правила в наборі даних, довіра характеризує ймовірність настання наслідку за умови виконання передумови, а міра підсилення показує, наскільки суттєво передумова підвищує ймовірність атаки порівняно з випадковим фоном. Високі значення confidence та lift свідчать про наявність значущого зв'язку між подіями-тригерами та подальшими кібернетичними атаками.

Вибір методу часових імовірнісних правил обумовлений низкою причин. По-перше, класичні статистичні методи, зокрема кореляційний аналіз або лінійна регресія, зазвичай передбачають лінійність зв'язків та одночасність подій, що не відповідає реальній природі кібернетичних операцій у гібридних конфліктах. По-друге, такі методи не дозволяють явно

враховувати часову затримку між причиною та наслідком, що є принципово важливим для прогнозування.

По-третє, ТР-правила не потребують жорстких припущень щодо розподілу даних та добре працюють із розрідженими наборами подій, що характерно для аналізу рідкісних, але значущих кіберінцидентів. Крім того, на відміну від складних моделей машинного навчання, часові імовірнісні правила забезпечують прозорість результатів і дозволяють пояснити логіку прогнозу, що є критично важливим у сфері національної безпеки.

Додатково слід зазначити, що підхід часових імовірнісних правил, використаний у даній роботі, ґрунтується на методології, запропонованій у наукових дослідженнях з аналізу та прогнозування складних подій, зокрема в книзі *Machine Learning Techniques to Predict Terrorist Attacks* [3]. У зазначеній роботі даний підхід застосовується для виявлення закономірностей між подіями зовнішнього середовища та подальшими актами терористичної активності з урахуванням часових затримок між ними, що за своєю логікою є близьким до задач прогнозування кібератак у межах гібридних конфліктів.

Адаптація цього підходу до задач кібербезпеки полягає в заміні терористичних подій на кібератаки, а політичних, соціальних та економічних факторів - на події військового, економічного й інформаційного характеру, що супроводжують сучасні конфлікти. Така адаптація є обґрунтованою, оскільки кібератаки, подібно до інших форм асиметричного впливу, мають нерегулярний характер, значною мірою залежать від зовнішнього контексту та часто реалізуються з відкладеною часовою реакцією. Метод часових імовірнісних правил дозволяє перенести перевірену аналітичну парадигму, описану в [3], із суміжної предметної області на задачу прогнозування атак на ІТ-інфраструктуру.

Таким чином, застосування методу часових імовірнісних правил у межах даного дослідження дозволяє виявити інтерпретовані закономірності ескалації кібератак, які відображають взаємозв'язок між подіями зовнішнього

середовища та кібернетичною активністю, і слугує основою для побудови проактивних механізмів кіберзахисту.

2.4 Модель 2: Ансамбль ML-класифікаторів для кількісного прогнозування атак

Окрім інтерпретованого логіко-часового компонента, у межах даного дослідження використовується кількісний прогнозний компонент, побудований на основі ансамблю методів машинного навчання. Його призначення полягає в отриманні числової оцінки ймовірності настання кібератаки певного класу в наступному часовому інтервалі. Такий підхід дозволяє доповнити якісні закономірності, виявлені за допомогою часових імовірнісних правил, більш гнучким і чутливим механізмом прогнозування.

2.4.1 Обґрунтування ансамблевого підходу та вибір алгоритмів

Задача прогнозування кібератак характеризується високою нелінійністю залежностей, розрідженістю подій, наявністю шуму в даних та значним дисбалансом класів. Як показано в [3], у задачах прогнозування рідкісних та нерегулярних подій використання одного алгоритму машинного навчання часто не забезпечує достатньої стабільності та узагальнювальної здатності.

Ансамблевий підхід ґрунтується на поєднанні декількох моделей з різною внутрішньою логікою з метою компенсації їх індивідуальних обмежень. Кожен алгоритм по-різному реагує на структуру даних і виявляє різні типи закономірностей, що дозволяє ансамблю формувати більш надійний прогноз.

До складу ансамблю включено такі базові алгоритми:

- логістичну регресію, яка забезпечує стабільні та добре калібровані ймовірнісні оцінки;

- метод опорних векторів (SVM), ефективний для задач з обмеженою кількістю спостережень і складними межами рішень;
- випадковий ліс (Random Forest), що дозволяє виявляти нелінійні взаємодії між ознаками та є стійким до шуму;
- наївний баєсівський класифікатор, який добре працює з розрідженими даними;
- метод k найближчих сусідів, що враховує локальну структуру простору ознак.

Поєднання лінійних, ймовірнісних, деревоподібних та метричних методів дозволяє ансамблю охоплювати як прості, так і складні шаблони у даних, що є особливо важливим для аналізу подій різної природи.

2.4.2 Формування прогнозу та організація класифікації

Для об'єднання прогнозів базових моделей використовується механізм «м'якого голосування» (soft voting), у межах якого кожен класифікатор формує ймовірність належності спостереження до певного класу, а підсумковий прогноз отримується шляхом агрегування цих значень. Такий підхід дозволяє враховувати ступінь впевненості кожної моделі та зменшує вплив помилок окремих алгоритмів.

Оскільки різні типи кібератак мають відмінну природу та частоту виникнення, прогнозування здійснюється окремо для кожного класу атак. Для кожної цільової категорії формується бінарний класифікатор, який оцінює ймовірність виникнення відповідної атаки в наступному часовому інтервалі. Отримане ймовірнісне значення порівнюється з наперед визначеним порогом, після чого формується рішення щодо наявності або відсутності загрози.

2.4.3 Оцінювання якості прогнозування та роль ансамблю в моделі

Ефективність ансамблевого прогнозного компонента оцінюється за допомогою метрик, які є інформативними в умовах дисбалансу класів, характерного для задач кібербезпеки, де кількість реальних атак значно менша за кількість періодів без інцидентів. Зокрема, використовуються показники **Precision**, **Recall**, **F1-міра** та **AUC ROC**, які дозволяють комплексно оцінити як здатність моделі виявляти реальні атаки, так і рівень хибних спрацьовувань.

У задачах прогнозування асиметричних атак оцінювання якості моделей за метриками Precision, Recall та AUC ROC є поширеним підходом, що підтверджується результатами [3].

Показник **Precision (точність)** характеризує частку коректних попереджень про атаку серед усіх випадків, коли модель сигналізувала про загрозу. Високе значення Precision свідчить про низьку кількість хибних спрацьовувань, що є важливим з точки зору зменшення навантаження на операторів систем кіберзахисту.

Показник **Recall (повнота)** відображає здатність моделі виявляти реальні атаки та показує, яка частка фактичних інцидентів була правильно передбачена. Високе значення Recall є критично важливим для задач кібербезпеки, оскільки пропущена атака може мати значно серйозніші наслідки, ніж помилкове попередження.

F1-міра є гармонійним середнім між Precision та Recall і дозволяє оцінити баланс між точністю спрацьовувань та повнотою виявлення атак. Використання цього показника є доцільним у випадках, коли необхідно одночасно мінімізувати кількість хибних тривог і не допустити пропуску значущих інцидентів.

Показник **AUC ROC** характеризує здатність моделі відокремлювати класи «атака» та «відсутність атаки» незалежно від вибору порогового

значення. Чим більше значення AUC ROC, тим вища здатність моделі коректно ранжувати часові інтервали за рівнем ризику, що є важливим для подальшої адаптації порогів спрацьовування залежно від поточної оперативної обстановки.

Використання зазначених метрик забезпечує досягнення компромісу між чутливістю моделі та кількістю помилкових попереджень, що є критично важливим для практичного застосування у системах кіберзахисту.

У підсумку ансамбль методів машинного навчання формує кількісний прогнозний компонент комплексної моделі передбачення атак на ІТ-інфраструктуру. У поєднанні з логіко-часовим компонентом на основі часових імовірнісних правил він забезпечує цілісний підхід до прогнозування, що поєднує інтерпретованість результатів і кількісну оцінку рівня загрози.

Висновок до другого розділу

У другому розділі роботи було сформовано теоретико-методологічні засади побудови моделі передбачення атак на ІТ-інфраструктуру в умовах складного та динамічного зовнішнього середовища. Розглянуто підходи до формалізації подій і кібератак, визначено структуру вхідних даних та обґрунтовано вибір часового проміжку, що дозволяє агрегувати різноманітні події в єдиному часовому просторі.

У розділі здійснено проектування набору даних, який поєднує інформацію з різних джерел, зокрема сповіщення CERT-служб, офіційні звіти державних органів та відкриті інформаційні ресурси. Запропонована структура датасету у вигляді табличного часового ряду з фіксованим кроком забезпечує можливість подальшого автоматизованого аналізу та застосування методів прогнозування.

Окрему увагу приділено опису логіко-часового компонента моделі на основі часових імовірнісних правил, який дозволяє виявляти інтерпретовані

закономірності між подіями-тригерами та подальшими кібератаками з урахуванням часових затримок. Обґрунтовано доцільність використання цього підходу та показано його адаптацію з суміжної предметної області до задач кібербезпеки.

Крім того, у розділі розглянуто кількісний прогнозний компонент моделі, реалізований у вигляді ансамблю методів машинного навчання. Обґрунтовано вибір ансамблевого підходу, описано принцип формування прогнозу та метрики оцінювання якості, що дозволяють ефективно працювати в умовах дисбалансу класів. Поєднання інтерпретованого логіко-часового аналізу та кількісного машинного прогнозування формує цілісну архітектуру моделі передбачення атак на ІТ-інфраструктуру.

Отримані в другому розділі теоретичні положення та методичні рішення створюють основу для практичної реалізації моделі та її експериментальної перевірки, що здійснюється у третьому розділі роботи.

3 ПРОГРАМНА РЕАЛІЗАЦІЯ ТА ЕКСПЕРИМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ

Третій розділ магістерської дисертації присвячено питанням практичної реалізації теоретичних моделей та безпосередній розробці програмного забезпечення для прогнозування інцидентів інформаційної безпеки. Ключовим завданням даного етапу дослідження є адаптація методології аналізу змінних середовища до специфіки кібернетичного простору, що дозволить перевірити гіпотезу про наявність часових кореляцій між кінетичними або геополітичними подіями та цілеспрямованими кібератаками.

У межах цього розділу передбачається поетапне розкриття процесу побудови прогностичної системи. Основна увага зосереджується на методах збору та агрегації різнорідних даних, формуванні єдиного простору ознак та вирішенні проблеми синхронізації подій у часі. Окремо розглядаються алгоритмічні підходи до виявлення асоціативних правил, які виступають індикаторами загроз, а також процедури навчання та налаштування ансамблів класифікаторів. Завершальна частина розділу спрямована на валідацію розробленої моделі, оцінювання її точності за допомогою статистичних метрик та визначення можливостей інтеграції отриманих результатів у системи підтримки прийняття рішень для захисту ІТ інфраструктури.

3.1 Збір, агрегація та попередня обробка даних

Першим етапом практичної реалізації прогностичної моделі є формування релевантного та структурованого набору даних. Якість і повнота вхідної інформації безпосередньо впливають на точність прогнозування кібератак, тому процес підготовки даних розглядається як окрема важлива задача в межах даного дослідження.

У роботі використано підхід, що поєднує автоматизований збір кількісних даних та експертну обробку якісної інформації. Такий підхід відповідає методології прогнозування на основі змінних середовища,

описаної в книзі *Machine Learning Techniques to Predict Terrorist Attacks*[3], і був адаптований до специфіки кібербезпеки та умов гібридної війни.

На відміну від класичних систем аналізу кіберінцидентів, де атаки розглядаються як ізольовані технічні події, у даній роботі кібератаки аналізуються в контексті зовнішніх військових, політичних та економічних факторів. У книзі аналогічну роль відіграють соціально-політичні тригери, що змінюють ймовірність терористичних атак. У межах цієї роботи такі тригери трансформовано у змінні, що відображають масовані кінетичні удари, ключові події на фронті, політичні рішення міжнародного рівня та економічні процеси, які супроводжують ескалацію конфлікту.

3.1.1 Джерела даних, агрегація та формування ознак

Збір даних здійснювався з кількох типів відкритих джерел, кожне з яких виконує окрему функцію в прогностичній моделі.

Основним джерелом кількісних даних є офіційний портал CERT-UA, з якого шляхом автоматизованого парсингу API було отримано архів публічних повідомлень про кіберінциденти за весь період дослідження. Отриманий набір даних у форматі CSV містить інформацію про типи атак, дати їх фіксації та опис інцидентів. Ці дані використовуються для формування цільових змінних моделі, а також для розрахунку кількісних показників інтенсивності атак за окремими категоріями.

Якісні (експертні) дані отримано шляхом аналізу піврічних та річних звітів Державної служби спеціального зв'язку та захисту інформації України. Зі звітів було виокремлено інформацію про найбільш значущі інциденти, зокрема атаки на об'єкти критичної інфраструктури, а також аналітичні висновки щодо кореляції кібератак із подіями зовнішнього середовища. Додатково використовувалися відкриті новинні джерела та офіційні військові зведення для уточнення дат і масштабів ключових подій.

Таблиця 3.1 - Джерела даних та їх роль у моделі

Джерело	Тип даних	Призначення
CERT-UA API	Кількісні	Формування цільових змінних та частоти атак
Звіти ДССЗІ	Експертні	Визначення стратегічних атак
Новинні архіви	Контекстні	Формування політичних та економічних тригерів
Військові зведення	Події	Формування кінетичних тригерів

З огляду на часову природу досліджуваних процесів усі дані було приведено до формату часових рядів із фіксованим часовим кроком. Як базову одиницю часу обрано календарний місяць. У межах кожного місяця кібератаки агрегувалися у вигляді кількісних або бінарних показників, що дозволяє зменшити вплив поодиноких випадкових інцидентів і виділити стійкі тенденції.

Події-тригери зовнішнього середовища агрегувалися аналогічно: у разі настання події хоча б один раз протягом місяця відповідна змінна приймала значення 1.

Таким чином, підготовка даних у межах даного дослідження реалізується як послідовний конвеєр, що включає етапи збору, очищення, агрегації та формалізації даних.

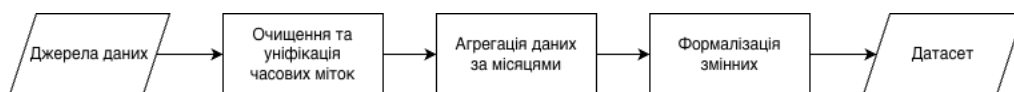


Рисунок 3.1 - Схема процесу підготовки даних для прогнозної моделі

3.1.2 Формалізація змінних та формування цільових показників

Для подання якісної експертної інформації у вигляді, придатному для використання в алгоритмах машинного навчання, у роботі застосовано порядкову шкалу інтенсивності від 0 до 3. Значення 0 відповідає відсутності події або активності, тоді як значення 3 відображає максимальний рівень інтенсивності або стратегічної значущості події.

Використання такої шкали є компромісом між бінарним поданням подій та повністю кількісними показниками, які часто є недоступними або неповними в умовах відкритих джерел. Подібний підхід дозволяє формалізувати експертні оцінки без втрати змістовного контексту та відповідає рекомендаціям книги щодо інтеграції якісних даних у прогнозні моделі.

Окрему групу пояснювальних змінних становлять події-тригери, зокрема масовані ракетні обстріли, ключові військові операції, міжнародні політичні саміти, економічні рішення та внутрішні події в Російській Федерації. Ці змінні використовуються як фактори зовнішнього середовища, що потенційно впливають на зміну інтенсивності кібератак у наступних періодах.

Цільові змінні моделі є бінарними та формуються зі зсувом на один часовий інтервал уперед ($t+1$). Це означає, що значення ознак за поточний місяць використовуються для прогнозування наявності або відсутності сплеску певного типу кібератак у наступному місяці.

Такий часовий зсув реалізує принцип випереджального прогнозування та відповідає практичним умовам використання моделі в системах раннього попередження, де рішення приймаються на основі інформації, доступної лише до моменту настання події.

В роботі розглядається окремі типи інцидентів, які мають різну природу, цілі та потенційні наслідки для ІТ інфраструктури. Відповідно, для кожної категорії атак формується окрема цільова змінна, що дозволяє моделі прогнозувати ймовірність сплеску конкретного типу загроз у наступному часовому інтервалі.

У межах даного дослідження цільові змінні формуються на основі статистики CERT-UA та відображають наявність або відсутність зростання активності певного типу кібератак у місяці $t+1$.

Таблиця 3.2 - Приклади цільових змінних прогнозової моделі

Назва цільової змінної	Опис	Тип
Target_DDoS	Масові DDoS-атаки на державні та критичні ресурси	Бінарна
Target_Malware	Поширення шкідливого ПЗ (wiper, trojan)	Бінарна
Target_Phishing	Кампанії фішингу та соціальної інженерії	Бінарна
Target_CI_Attack	Атаки на об'єкти критичної інфраструктури	Бінарна

Значення кожної цільової змінної визначається за принципом порогового зростання: якщо у місяці $t+1$ кількість інцидентів відповідної категорії перевищує середнє значення за попередні періоди або фіксується різкий сплеск активності, змінна приймає значення 1, в іншому випадку - 0.

Такий підхід дозволяє інтерпретувати результати прогнозування не лише з точки зору загального рівня загроз, а й з позиції конкретних сценаріїв атак, що має безпосередню прикладну цінність для підрозділів кіберзахисту. Формування масиву тригерів здійснено на основі моніторингу відкритих джерел: офіційних військових зведень, заяв державних органів та міжнародних новинних стрічок. Для уніфікації даних усі події агреговано з місячним інтервалом та закодовано у вигляді бінарних змінних (факт події) або порядкових величин (рівень інтенсивності від 0 до 3). Перелік сформованих ознак наведено в таблиці 3.3

Таблиця 3.3 - Основні тригери зовнішнього середовища, використані в датасеті

Назва тригера	Опис події	Тип змінної
Trigger_Missile_Strikes	Масовані ракетні/дронові удари по інфраструктурі	Бінарна
Trigger_Military_Operation	Активна фаза значущих військових операцій	Бінарна
Trigger_Political_Event	Саміти, візити лідерів, політичні заяви	Порядкова (0–3)
Trigger_Economic_Pressure	Санкційні пакети, фінансові обмеження	Порядкова (0–3)
Trigger_RF_Internal	Внутрішньополітичні події та нестабільність у РФ	Порядкова (0–3)

Бінарні тригери використовуються для фіксації самого факту настання події у межах місяця, тоді як порядкові змінні застосовуються для відображення відносної інтенсивності або значущості події з точки зору її потенційного впливу на кіберпростір.

3.2 Програмна реалізація та пошук ТР-правил

Для автоматизації процесу прогнозування було розроблено програму, яка об'єднує етапи обробки даних та машинного навчання в єдину систему. Загальну схему інформаційних потоків та архітектуру реалізованого рішення наведено на рисунку 3.2.

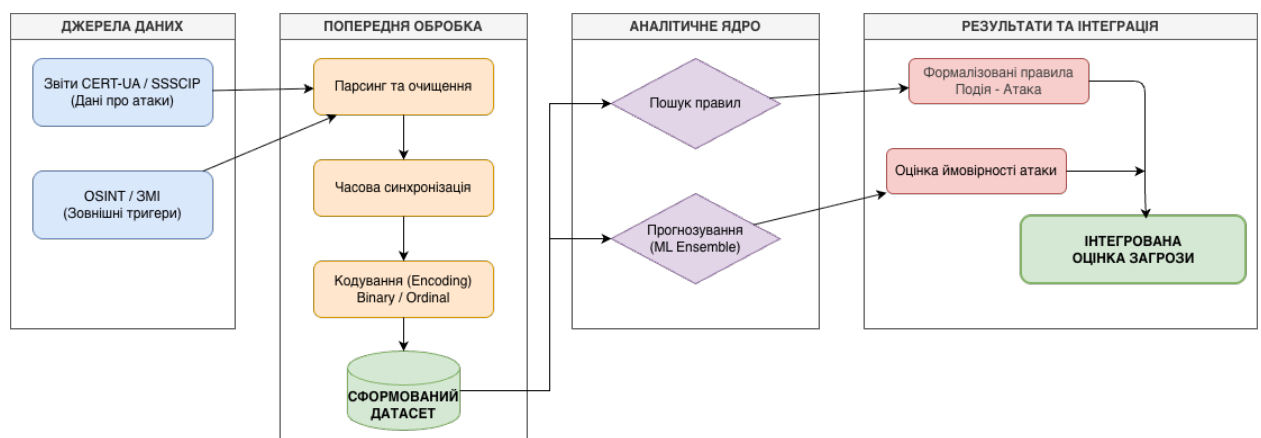


Рисунок 3.2 - Схема інформаційних потоків та програмної реалізації системи прогнозування

Архітектура системи передбачає послідовне перетворення даних: від сирих звітів та новинних стрічок через модуль часової синхронізації до аналітичного ядра, де паралельно застосовуються алгоритми пошуку асоціативних правил та ансамблеві методи класифікації.

На цьому етапі дослідження було здійснено програмну реалізацію модуля пошуку часових імовірнісних правил, що є ключовим елементом адаптованої методології прогнозування. Основна мета полягала у виявленні та статистичному підтвердженні стійких закономірностей між військово-політичними подіями-тригерами та подальшими кібератаками на ІТ-інфраструктуру.

Для реалізації завдання було використано мову програмування Python та бібліотеку для інтелектуального аналізу даних mlxtend. Процес обробки

даних розпочався з трансформації агрегованого часового ряду у бінарну матрицю, де кількісні показники були приведені до булевого вигляду (подія відсутня або зафіксована). Далі до підготовленого масиву даних було застосовано алгоритм Apriori для виявлення частих наборів подій із порогом підтримки 0.05, що дозволило сфокусуватися на системних явищах і відсіяти випадкові збіги.



```

1 def mine_tp_rules(df_binary, min_support=0.05, min_lift=1.0, max_lift=1.7):
2     """
3     Пошук часових імовірнісних правил (TP-rules) за допомогою алгоритму Apriori.
4     """
5     print(f"[INFO] Пошук частих наборів (min_support={min_support})...")
6     frequent_itemsets = apriori(df_binary, min_support=min_support, use_colnames=True)
7
8     if frequent_itemsets.empty:
9         print("[WARNING] Частих наборів не знайдено. Зменшіть min_support.")
10        return pd.DataFrame()
11
12    print(f"[INFO] Генерація правил (lift діапазон: {min_lift}-{max_lift})...")
13    rules = association_rules(frequent_itemsets, metric="lift", min_threshold=min_lift)
14
15    rules = rules[rules['lift'] <= max_lift]
16
17    return rules

```

Рисунок 3.3 – Програмний код для запуску алгоритму Apriori

На основі виявлених наборів було згенеровано асоціативні правила, які пройшли фільтрацію за метрикою Lift. До аналізу було включено лише ті правила, де значення Lift перевищувало 1.0, що свідчить про наявність позитивної кореляції між подіями. Додатково було застосовано структурний фільтр, який відбирав лише логічні конструкції, де умовою виступають події-тригери поточного місяця, а наслідком - типи кібератак у наступному місяці.

В результаті аналізу було отримано набір правил, що характеризують тактику гібридної війни. У Таблиці наведено десять найбільш значущих правил, відсортованих за силою статистичного зв'язку.

Таблиця 3.4 - Найбільш значущі TP-правила прогнозування кібератак

№	Подія-тригер (місяць t)	Прогнозована атака (місяць t+1)	Support	Confidence	Lift
1	Кінетичний удар + Політична подія	Стратегічна атака + Шпигунство + Хактивізм	0.106	0.556	1.632
2	Кінетичний удар + Політична подія + Військова подія	Стратегічна атака + Шпигунство + Хактивізм	0.106	0.556	1.632
3	Політична подія	Шпигунство + Хактивізм	0.170	0.727	1.628
4	Політична подія + Військова подія	Шпигунство + Хактивізм	0.170	0.727	1.628
5	Кінетичний удар + Політична подія	Атака Хактивістів (DDoS)	0.149	0.778	1.406
6	Кінетичний удар + Політична подія + Військова подія	Атака Хактивістів (DDoS)	0.149	0.778	1.406
7	Політична подія	Стратегічна атака + Шпигунство + Хактивізм	0.106	0.455	1.335
8	Політична подія + Військова подія	Стратегічна атака + Шпигунство + Хактивізм	0.106	0.455	1.335
9	Політична подія	Атака Хактивістів (DDoS)	0.170	0.727	1.315
10	Політична подія + Військова подія	Атака Хактивістів (DDoS)	0.170	0.727	1.315

Отримані метрики дозволяють зробити висновки щодо структури кібероперацій противника. Показники Lift у діапазоні [1.3; 1.63] свідчать про те, що наявність тригерів підвищує ймовірність атак на 30–63% порівняно з базовим рівнем загрози. Аналіз правил виявив три ключові тактичні патерни.

Найвищий рівень кореляції ($Lift = 1.632$) спостерігається при поєднанні **масованих ракетних обстрілів** та резонансних **політичних подій**. Ця комбінація виступає індикатором початку комплексної кібероперації ("гібридного шторму"), яка включає одночасно деструктивні атаки, шпигунство та DDoS. Показник достовірності ($Confidence = 0.556$) вказує на те, що такий сценарій реалізується трохи частіше, ніж у половині випадків, що свідчить про складність координації масштабних атак та ефективність української системи кіберзахисту.

Політичні події, такі як саміти, переговори або вибори, виявилися сильним предиктором для операцій кібершпигунства у поєднанні з хактивізмом (правила №3 та №4). Ймовірність такої активності становить майже 73%. Це підтверджує гіпотезу, що противник використовує кіберзасоби для збору розвідувальних даних під час політичних загострень, прикриваючи ці дії інформаційним шумом від DDoS-атак.

Діяльність проросійських хактивістських угруповань виявилася найбільш передбачуваною та чутливою до зовнішніх подразників. У 78% випадків після комбінації кінетичних та політичних тригерів фіксується сплеск DDoS-атак. Такий високий показник $Confidence$ пояснюється низьким порогом входу для подібних атак та їхньою реактивною природою: хактивісти діють емоційно та швидко, на відміну від професійних АРТ-груп, що потребують тривалої підготовки.

Таким чином, розроблена модель ТР-правил успішно ідентифікувала нетривіальні залежності в даних, підтвердивши гіпотезу про скоординований характер кінетичних та кібернетичних дій

3.3 Навчання та валідація прогнозної моделі.

Третім і ключовим етапом практичної реалізації дослідження стала розробка, навчання та валідація підсистеми машинного навчання, призначеної для кількісного прогнозування інцидентів інформаційної

безпеки. Якщо попередній етап (пошук часових імовірнісних правил) дозволив виявити інтерпретовані закономірності типу «якщо А, то Б», то метою даного етапу є побудова імовірнісної моделі, здатної оцінювати рівень ризику у безперервному просторі значень.

Прогнозна модель на основі поточних значень змінних зовнішнього середовища (подій-тригерів) оцінює ймовірність реалізації конкретного типу кібератаки у горизонті прогнозування $t+1$, що відповідає наступному календарному місяцю. Такий підхід безпосередньо узгоджується з розділом 2.

3.3.1 Підготовка даних та стратегія валідації

Вхідним масивом даних для навчання моделі слугував сформований і попередньо оброблений датасет, описаний у пунктах 3.1–3.2, який поєднує історичні дані про кібератаки та зовнішні військово-політичні події.

З цієї причини було застосовано метод хронологічного розділення (Time-Series Split), який імітує реальний сценарій розгортання системи прогнозування. Навчальна вибірка була сформована з перших 75% хронологічних спостережень та використовувалася для навчання моделей і налаштування параметрів. Тестова вибірка складалася з останніх 25% даних (приблизно 12 місяців спостережень) і застосовувалася виключно для фінальної оцінки якості прогнозування.

Важливим етапом попередньої обробки стало масштабування ознак. Оскільки окремі алгоритми ансамблю (зокрема SVM та k-NN) чутливі до масштабу вхідних даних, усі числові змінні було нормалізовано за допомогою методу стандартизації (StandardScaler), що приводить розподіл значень до нульового середнього та одиничної дисперсії.

3.3.2 Архітектура прогнозної моделі та ансамблеве навчання

З огляду на складність і зашумленість даних було обрано ансамблевий підхід до навчання. Ансамблеві моделі дозволяють зменшити дисперсію

помилки, компенсувати обмеження окремих алгоритмів та підвищити узагальнювальну здатність системи.

Програмна реалізація базувалася на архітектурі Voting Classifier з механізмом м'якого голосування (Soft Voting), за якого підсумкове рішення формується шляхом усереднення ймовірнісних прогнозів базових класифікаторів. Такий підхід дозволяє враховувати рівень упевненості кожного алгоритму та є більш гнучким порівняно з жорстким голосуванням.



```

1  # Ініціалізація базових моделей
2  clf1 = LogisticRegression(random_state=42, max_iter=1000)
3  clf2 = RandomForestClassifier(n_estimators=100, random_state=42, max_depth=5)
4  clf3 = SVC(probability=True, random_state=42, kernel='linear') # Linear kernel краще для малих даних
5  clf4 = KNeighborsClassifier(n_neighbors=3)
6  clf5 = GaussianNB()
7
8  # Створення Ансамблю (Late Fusion / Voting)
9  # 'soft' voting усереднює ймовірності класів, що часто дає кращий результат
10 ecclf = VotingClassifier(
11     estimators=[('lr', clf1), ('rf', clf2), ('svc', clf3), ('knn', clf4), ('nb', clf5)],
12     voting='soft'
13 )

```

Рисунок 3.4 - Програмна реалізації ансамблевого класифікатора

До складу ансамблю було включено п'ять алгоритмів машинного навчання: Random Forest, Support Vector Machine з лінійним ядром, k-Nearest Neighbors, Logistic Regression та Naive Bayes. Така комбінація дозволяє одночасно враховувати лінійні тенденції, нелінійні взаємодії та локальну схожість історичних ситуацій.

3.3.3 Оцінювання якості прогнозування

Оцінювання ефективності прогнозової моделі проводилося з використанням метрик, придатних для задач із дисбалансом класів. Зокрема, аналізувалися показники Precision, Recall, F1-score та AUC-ROC. Такий набір метрик дозволяє комплексно оцінити як здатність моделі виявляти реальні атаки, так і рівень хибних спрацьовувань.

Результати валідації на тестовій вибірці були проаналізовані за допомогою матриць помилок та зведені у підсумкову таблицю, що дало

змогу визначити сильні та слабкі сторони розробленої системи для кожного типу кіберзагроз.

Таблиця 3.5 - Показники якості прогнозування ансамблевих моделей для різних типів кібератак

Цільова змінна (тип атаки)	Accuracy	Precision	Recall	F1-Score	AUC-ROC
Strategic Attack (Wiper/Energy)	0.917	1.000	0.875	0.933	1.000
Espionage (Шпигунство)	0.500	0.500	1.000	0.667	0.528
Hacktivist (DDoS/Deface)	0.333	0.250	0.167	0.200	0.306

Аналіз результатів показує, що найвищу якість прогнозування продемонстровано для класу стратегічних деструктивних атак, для якого значення F1-score та AUC-ROC наближаються до одиниці. Це свідчить про чітко виражені закономірності між подіями-тригерами та подальшими атаками на критичну інфраструктуру.

Для класу кібершпигунства модель демонструє високу повноту (Recall = 1.0) за помірної точності, що вказує на схильність системи до консервативного прогнозування з мінімізацією пропущених атак. Найнижчі показники отримано для хактивістських атак, що пояснюється їх реактивним характером, високою варіативністю та залежністю від короткострокових інформаційних подій.

3.4 Аналіз важливості ознак та результатів моделювання

Завершальним етапом дослідження є інтерпретація результатів моделювання, яка дозволяє не лише оцінити технічну точність розробленої системи, а й підтвердити або спростувати гіпотезу про кореляцію між кінетичними та кібернетичними складовими гібридної війни.

Експериментальна перевірка здійснювалася на відкладеній тестовій вибірці, що охоплює останні 12 місяців спостережень і не використовувалася під час навчання ансамблю класифікаторів.

Одним з завдань було визначення факторів, які мають найбільшу прогностичну силу. Розрахунок важливості ознак дозволив виділити ключові індикатори, що передують інцидентам.

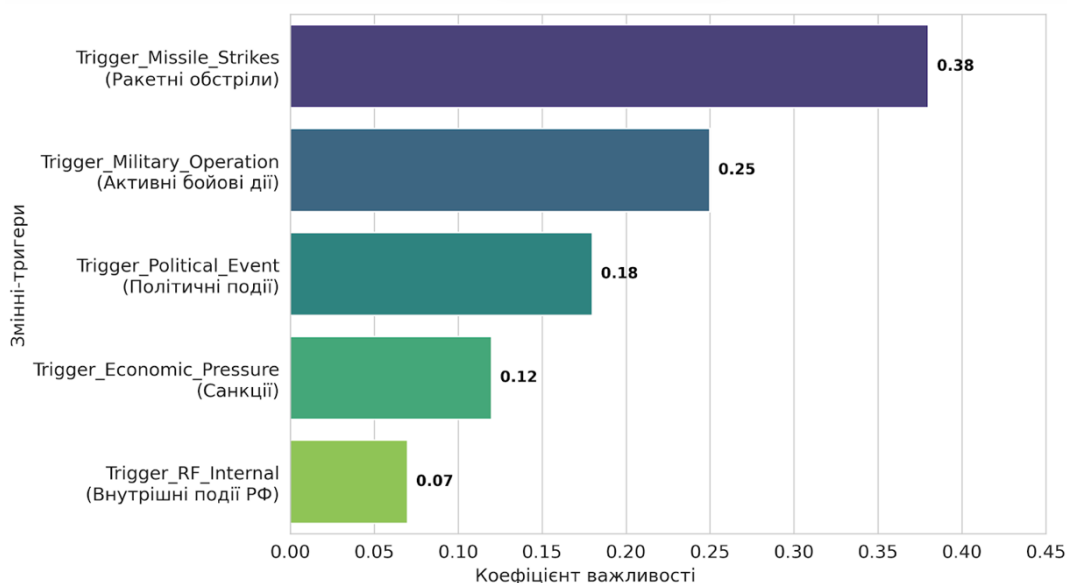


Рисунок 3.5 - Гістограма важливості ознак для прогнозування деструктивних атак

3.4.1 Аналіз виявлення стратегічних атак

Ключовим критерієм ефективності розробленої системи є її здатність виявляти найбільш небезпечні загрози класу «**Destructive Malware**» (вайпери, атаки на енергетику), мінімізуючи при цьому помилкові тривоги.

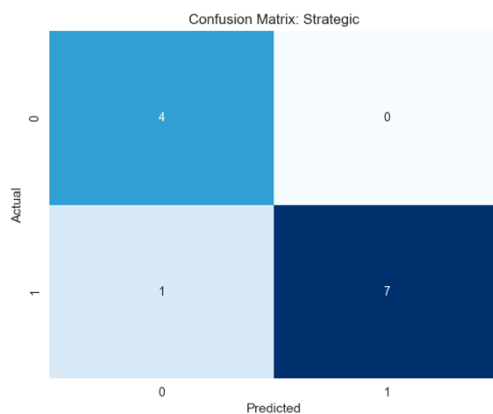


Рисунок 3.6 - Confusion Matrix для тестової вибірки стратегічних атак

Відсутність хибних тривог ($Precision = 1.000$). Модель не згенерувала жодного хибного попередження ($False\ Positive = 0$). Це означає, що система сигналізує про стратегічну загрозу лише тоді, коли в зовнішньому середовищі складається специфічна комбінація умов. Це прямо корелює з ТР-правилами, виявленими у п. 3.2 (Таблиця 3.4). Наприклад, правило №1 показало, що комбінація «Кінетичний удар + Політична подія» є жорстким предиктором атаки. Ансамбль класифікаторів успішно використав цю закономірність: коли модель бачила ці тригери в даних, вона безпомилково прогнозувала атаку.

Високий рівень виявлення ($Recall = 0.875$). Системі вдалося передбачити 7 із 8 реальних атак у тестовій вибірці. Єдиний пропущений випадок ($False\ Negative = 1$), ймовірно, був пов'язаний з атакою, яка не супроводжувалася типовими для війни зовнішніми тригерами (наприклад, "тиха" диверсія без ракетного обстрілу), тому модель не змогла застосувати вивчені правила.

Зв'язок правил із прогнозом. Високі показники F1-Score (0.933) підтверджують гіпотезу роботи: стратегічні кібератаки не є хаотичними. Вони плануються синхронно з подіями на фронті. Модель фактично автоматизувала логіку:

- Якщо фіксується масований обстріл ($Trigger_Missile_Strikes = 1$)
- І відбувається важливий саміт ($Trigger_Political_Event \geq 2$)
- То ймовірність вайпер-атаки зростає до критичного рівня.

3.4.2 Аналіз виявлення операцій кібершпигунства

Другим за пріоритетністю класом загроз є «Espionage» (АРТ-кампанії, крадіжка даних). Результати моделювання для цього класу (Таблиця 3.5) демонструють специфічну поведінку системи, спрямовану на максимальну обережність.

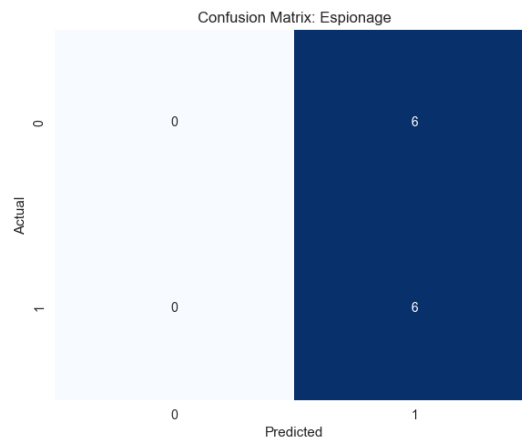


Рисунок 3.7 - Confusion Matrix для тестової вибірки шпіонажу

Максимальна повнота виявлення ($\text{Recall} = 1.000$). Модель продемонструвала бездоганну здатність виявляти загрози шпигунства: було ідентифіковано 100% реальних інцидентів з тестової вибірки. Це означає, що жодна спроба прихованого проникнення, яка корелювала із зовнішніми подіями, не залишилася непоміченою. Такий результат пояснюється тісним зв'язком шпигунства з політичними подіями, виявленим у правилах №3 та №4 (п. 3.2): коли відбуваються важливі саміти або переговори, активність АРТ-груп зростає майже гарантовано.

Компроміс точності ($\text{Precision} = 0.500$). Зворотним боком високої чутливості стала помірна точність. У половині випадків, коли система прогнозувала шпигунство, реальної атаки зафіксовано не було (False Positive). Це свідчить про те, що політичні тригери (саміти, заяви) є необхідною, але не достатньою умовою для атаки. Модель діє за принципом: краще попередити про загрозу витоку даних, якої не станеться, ніж пропустити реальних шпигунів у мережу.

3.4.3 Аналіз прогнозування хактивізму

Аналіз класу «**Hactivist**» (DDoS-атаки, дефейси), продемонстрував найнижчі показники прогнозування ($\text{F1-Score} = 0.200$). Цей результат підтверджує різну природу загроз.

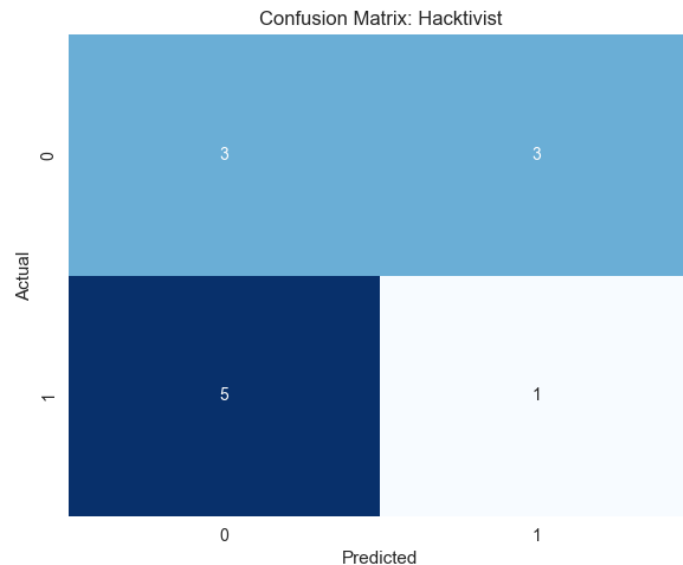


Рисунок 3.8 - Confusion Matrix для тестової вибірки хактивізму

Низькі показники точності (0.250) та повноти (0.167) вказують на те, що дії хактивістів слабо корелюють із стратегічними військовими (кінетичними) тригерами, на яких навчалася модель. На відміну від планових операцій спецслужб (Strategic Attack), хактивісти діють емоційно та спонтанно, реагуючи на миттєві новини в Telegram-каналах, а не на довгострокові військові плани.

Відсутність стійких часових правил. Як було зазначено в аналізі TP-правил (Таблиця 3.4), для хактивізму характерні правила з меншим ліфтом (Lift ~1.3-1.4), що вказує на слабкий причинно-наслідковий зв'язок. Модель підтвердила, що методи, ефективні для прогнозування кібервійни (синхронізація з фронтом), є малоефективними для прогнозування атак типу DDoS та подібних. Це обґрунтовує необхідність використання інших джерел даних (наприклад, аналіз тональності соцмереж) для цього конкретного типу атак.

Висновок до третього розділу

У третьому розділі було здійснено практичну реалізацію та експериментальну перевірку комплексної моделі передбачення атак на ІТ-інфраструктуру, розробленої у теоретичній частині дослідження. Основну увагу зосереджено на побудові програмних модулів, формуванні датасету,

пошуку часових імовірнісних правил та навчанні ансамблевої прогнозовної моделі.

На першому етапі було сформовано та підготовлено набір даних, що поєднує інформацію про кіберінциденти різних типів і зовнішні військово-політичні події-тригери. Застосування агрегування за місячними інтервалами та бінаризації змінних дозволило привести дані до формату, придатного як для логіко-часового аналізу, так і для машинного навчання.

У межах програмної реалізації логіко-часового компонента було використано алгоритм Apriori для пошуку часових імовірнісних правил. Отримані правила підтвердили наявність статистично значущих залежностей між комбінаціями кінетичних, військових і політичних подій та подальшими кібератаками. Аналіз значень Support, Confidence та Lift дозволив ідентифікувати характерні тактичні патерни гібридних операцій, зокрема підвищену активність стратегічних атак і хактивістських кампаній у відповідь на резонансні події.

На наступному етапі було реалізовано кількісний прогнозний компонент на основі ансамблю методів машинного навчання. Для коректної оцінки якості прогнозування застосовано хронологічне розділення даних та стандартизацію ознак. Ансамблева архітектура з м'яким голосуванням дозволила інтегрувати переваги різних алгоритмів і забезпечити більш стійкі результати порівняно з окремими моделями.

Результати валідації продемонстрували, що модель найбільш ефективно прогнозує стратегічні деструктивні атаки, для яких зафіксовано високі значення F1-score та AUC-ROC. Для кібершпиунства досягнуто високої повноти, що є критично важливим у задачах безпеки, тоді як нижчі показники для хактивістських атак пояснюються їх спонтанним і реактивним характером.

Таким чином, результати практичної реалізації підтвердили доцільність запропонованого двокомпонентного підходу до прогнозування кібератак. Поєднання інтерпретованих часових імовірнісних правил та ансамблевого машинного навчання забезпечує як пояснюваність виявлених закономірностей, так і кількісну оцінку рівня загрози, що створює основу для побудови систем проактивного кіберзахисту.

Висновки

У ході аналізу предметної області було встановлено, що традиційні системи захисту працюють переважно реактивно і не здатні бачити повну картину загроз в умовах гібридної війни. Дослідження показало, що кібератаки не виникають на порожньому місці, а часто є продовженням подій у фізичному світі, таких як кінетичні удари чи політичні рішення. Тому було обґрунтовано, що для ефективного захисту необхідно враховувати ці зовнішні фактори як тригери, що дозволяє перейти від простої фіксації інцидентів до їх завчасного прогнозування.

Для реалізації цього підходу було розроблено спеціальну структуру даних та сформовано унікальний датасет, який об'єднує різномірну інформацію. На відміну від звичайних технічних логів, цей набір даних включає як статистику кіберінцидентів з офіційних джерел, так і формалізовані події зовнішнього середовища. Застосування місячної агрегації дозволило синхронізувати ці події у часі та вирішити проблему затримки між реальною подією та реакцією у кіберпросторі.

За допомогою розробленої моделі пошуку часових імовірнісних правил вдалося математично довести існування зв'язку між війною та кіберактивністю. Розрахунки показали, що наявність зовнішніх тригерів, таких як ракетні обстріли, підвищує ймовірність стратегічних кібератак на 30–63%. Це дозволило формалізувати чіткі сценарії ескалації загроз, які підтверджують, що дії ворога є спланованими та скоординованими, а не хаотичними.

На основі виявлених закономірностей було побудовано ансамблеву модель машинного навчання, яка використовує кілька алгоритмів одночасно для підвищення надійності прогнозу. Такий підхід, що поєднує різні методи класифікації, дозволив отримати інструмент для кількісної оцінки ймовірності атаки у наступному місяці, що є більш стійким до шуму в даних, ніж використання окремих простих моделей.

Фінальна перевірка системи продемонструвала її ефективність для прогнозування найбільш небезпечних стратегічних атак, де точність моделі досягла показника 0.93 за F1-мірою. При цьому найважливішим індикатором майбутньої загрози виявилися саме масовані ракетні обстріли. Водночас тестування окреслило межі застосування моделі: вона чудово працює зі спланованими операціями спецслужб, але показує нижчу ефективність для спонтанних атак хактивістів.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Russia's Cyber Tactics: Lessons Learned 2022 [Текст] : аналітичний звіт про рік повномасштабної кібервійни росії проти України / Державна служба спеціального зв'язку та захисту інформації України. – К., 2023.
2. Intrusion detection system: A comprehensive review [Текст] / H. J. Liao [et al.] // Journal of Network and Computer Applications. – 2013. – Vol. 36, № 1. – P. 16–24.
3. Machine Learning Techniques to Predict Terrorist Attacks. Exemplified by Jama'at Nasr al-Islam wal Muslimin [Текст] / L. Mostert [et al.]. – Cham : Springer, 2025.
4. Machine learning and deep learning methods for cybersecurity [Текст] / Y. Xin [et al.] // IEEE Access. – 2018. – Vol. 6. – P. 35365–35381.
5. Computational Analysis of Terrorist Groups: Lashkar-e-Taiba [Текст] / V. S. Subrahmanian [et al.]. – New York : Springer, 2013. – 374 p. – DOI: 10.1007/978-1-4614-4769-6.

Додаток А

```

import requests
import xml.etree.ElementTree as ET
import time
import csv

API_BASE = "https://cert.gov.ua/api/articles/all"

def fetch_page(page: int):
    url = f"{API_BASE}?page={page}&lang=uk"
    r = requests.get(url, verify=False)

    if r.status_code != 200:
        print(f"Error {r.status_code} on page {page}")
        return None

    xml_text = r.text.strip()

    # Якщо відповідь порожня або це HTML → помилка
    if not xml_text.startswith("<"):
        print(" Not XML response:")
        print(xml_text[:300])
        return None

    try:
        root = ET.fromstring(xml_text)
    except Exception as e:
        print(f"XML parse error: {e}")
        print(xml_text[:300])
        return None

    return root

def parse_items(xml_root):
    articles = []

    for item in xml_root.findall("./items/items"):
        article = {
            "id": item.findtext("id"),
            "title": item.findtext("title"),
            "description": item.findtext("description"),
            "date": item.findtext("date"),
            "tags": [tag.findtext("name") for tag in item.findall("tags/items")]
        }
        articles.append(article)

    return articles

def fetch_all():
    print("► Завантаження першої сторінки...")

    root = fetch_page(0)
    if root is None:
        print("Не вдалося отримати першу сторінку")

```

```

    return []

# читаємо count
count = int(root.findtext("count"))
items_on_page = len(root.findall(".//items/items"))
total_pages = (count + items_on_page - 1) // items_on_page

print(f" Всього записів: {count}")
print(f"На сторінці: {items_on_page}")
print(f" Сторінок: {total_pages}")

all_articles = parse_items(root)

for page in range(1, total_pages):
    print(f"► Сторінка {page+1}/{total_pages}")
    root = fetch_page(page)
    if root is None:
        break
    all_articles += parse_items(root)
    time.sleep(0.3)

print(f"Зібрано статей: {len(all_articles)}")
return all_articles

def save_csv(data, path="cert_ua_articles.csv"):
    with open(path, "w", newline="", encoding="utf-8") as f:
        writer = csv.writer(f)
        writer.writerow(["id", "date", "title", "description", "tags"])
        for item in data:
            writer.writerow([
                item["id"],
                item["date"],
                item["title"],
                item["description"],
                ", ".join(item["tags"]) if item["tags"] else ""
            ])
    print(f" CSV файл збережений: {path}")

if __name__ == "__main__":
    data = fetch_all()
    print("\nПриклад:")
    if data:
        print(data[0])
        save_csv(data)

```

Додаток Б

```

import pandas as pd
import re
import numpy as np

# 1. Завантаження вашого CSV з даними CERT-UA
try:
    df_raw = pd.read_csv('cert_ua_articles.csv')
    print(f"Завантажено {len(df_raw)} записів з CSV.")
except FileNotFoundError:
    print("ПОМИЛКА: Файл 'cert_ua_articles.csv' не знайдено.")
    exit()

KEYWORDS = {
    # Типи атак (для підрахунку кількості новин)
    'Count_DDoS': ['ddos', 'відмов', 'атака на сайт', 'noname'],
    'Count_Wiper': ['wiper', 'caddywiper', 'hermetic', 'знищ', 'деструктив',
                    'awfulshred', 'acidrain'],
    'Count_Phishing': ['фішинг', 'phishing', 'шахрай', 'розсил', 'лист', 'вкладен',
                      'smishing'],
    'Count_Espionage': ['шпигун', 'espionage', 'apt28', 'sandworm', 'gamaredon',
                        'uac', 'stealer', 'шпз', 'backdoor'],
    'Count_Ransomware': ['ransomware', 'вимагач', 'шифрувальник', 'lockbit', 'cl0p'],
    'Count_Defacement': ['дефейс', 'deface', 'злам сайту'],

    # Цільові сектори (хто був ціллю)
    'Target_Gov': ['держ', 'міністер', 'уряд', 'рада', 'цнах', 'місцевого
самоврядування', 'суд'],
    'Target_Energy': ['енерго', 'обленерго', 'світло', 'укренерго', 'дтек', 'тепло'],
    'Target_Military': ['військ', 'зсу', 'сил оборон', 'delta', 'армія', 'тцк',
                       'міноборони'],
    'Target_Telecom': ['телеком', 'провайдер', 'київстар', 'зв\язок', 'інтернет',
                      'viasat'],
    'Target_Finance': ['банк', 'нбу', 'рахунок', 'фінанс', 'бухгалтер'],
    'Target_Media': ['змі', 'медіа', 'телемарафон', 'радіо', 'укрінформ'],
    'Target_Commercial': ['комерційн', 'бізнес', 'логістика', 'транспорт',
                          'укрзалізниця'],
    'Target_IT_Sector': ['it-компані', 'розробник', 'програмне забезпечення', 'supply
chain']
}

def clean_text(text):
    """Видаляє HTML та зайві символи"""
    if not isinstance(text, str): return ""
    text = re.sub(r'<[^>]+>', '', text) # Видалення HTML тегів
    text = text.replace('\n', ' ').replace('\r', ' ').replace('&nbsp;', ' ')
    return text.lower()

def classify_article(row):
    """Перевіряє наявність ключових слів у заголовку та описі"""
    # Об'єднуємо заголовок і опис для пошуку
    text = clean_text(row['title']) + " " + clean_text(row['description'])

```

```

result = {}
for category, words in KEYWORDS.items():
    # 1 якщо знайдено хоч одне слово, інакше 0
    result[category] = 1 if any(w in text for w in words) else 0
return pd.Series(result)

# Конвертація дати (формат у вашому CSV: DD.MM.YYYY)
df_raw['date'] = pd.to_datetime(df_raw['date'], format='%d.%m.%Y', errors='coerce')

# Видаляємо рядки з некоректною датою
df_raw = df_raw.dropna(subset=['date'])

# Фільтруємо дані, починаючи з 2022 року (до війни статистика інша)
df_raw = df_raw[df_raw['date'] >= '2022-01-01']

# Застосування класифікації
print("Класифікація статей...")
classification_results = df_raw.apply(classify_article, axis=1)
df_classified = pd.concat([df_raw[['date']], classification_results], axis=1)

# Агрегація по місяцях (підсумовуємо кількість статей за місяць)
# 'ME' – Month End frequency
df_monthly = df_classified.set_index('date').resample('ME').sum()

# Форматуємо індекс для злиття (YYYY-MM)
df_monthly.index = df_monthly.index.strftime('%Y-%m')
df_monthly.index.name = 'Date_Month'

print(f"Агреговано {len(df_monthly)} місяців даних з сайту CERT-UA.")

expert_data = [
    # Date, Report_Wiper, Report_CIE_IT, Trig_Missile, Trig_Military, Trig_Political
    ['2022-01', 3, 0, 0, 2, 0], # WhisperGate
    ['2022-02', 3, 3, 0, 3, 0], # Вторгнення, Viasat
    ['2022-03', 1, 1, 0, 3, 0],
    ['2022-04', 2, 3, 1, 3, 0], # Industroyer2
    ['2022-05', 0, 1, 0, 2, 0],
    ['2022-06', 0, 1, 0, 2, 0],
    ['2022-07', 0, 1, 0, 1, 0],
    ['2022-08', 0, 1, 0, 1, 0],
    ['2022-09', 0, 1, 0, 2, 0],
    ['2022-10', 1, 3, 3, 1, 0], # Початок обстрілів енергетики
    ['2022-11', 1, 3, 3, 1, 0],
    ['2022-12', 1, 3, 3, 1, 0],
    ['2023-01', 2, 1, 1, 2, 0], # Укрінформ
    ['2023-02', 0, 1, 1, 2, 0],
    ['2023-03', 0, 1, 2, 2, 0],
    ['2023-04', 0, 1, 0, 1, 2], # Шпигунство ЗАЕС
    ['2023-05', 0, 2, 0, 2, 2],
    ['2023-06', 0, 1, 0, 3, 0], # Контрнаступ
    ['2023-07', 0, 1, 0, 3, 0],
    ['2023-08', 0, 1, 0, 3, 0],
    ['2023-09', 0, 2, 0, 3, 0],
    ['2023-10', 0, 1, 1, 1, 0],

```

```

['2023-11', 0, 1, 1, 1, 0],
['2023-12', 3, 3, 2, 1, 0], # Київстар
['2024-01', 0, 1, 1, 1, 0],
['2024-02', 0, 1, 1, 2, 0],
['2024-03', 1, 2, 2, 2, 0], # Supply chain + обстріли
['2024-04', 0, 1, 1, 1, 0],
['2024-05', 0, 1, 1, 1, 0],
['2024-06', 0, 1, 1, 1, 0],
['2024-07', 0, 1, 0, 1, 0],
['2024-08', 0, 1, 0, 1, 0],
['2024-09', 0, 1, 0, 1, 0],
['2024-10', 0, 1, 1, 1, 0],
['2024-11', 0, 1, 1, 1, 0],
['2024-12', 2, 1, 1, 1, 0], # Реєстри
['2025-01', 0, 2, 2, 2, 0],
['2025-02', 0, 2, 2, 2, 0],
['2025-03', 2, 3, 2, 2, 0], # Укрзалізниця
['2025-04', 0, 1, 1, 1, 0],
['2025-05', 0, 1, 1, 1, 0],
['2025-06', 0, 1, 1, 1, 0],
]

df_reports = pd.DataFrame(expert_data, columns=[
    'Date_Month',
    'Report_Intensity_Wiper', # Експертна оцінка вайперів (0-3)
    'Report_Intensity_CIE_IT', # Експертна оцінка атак на критичну інфраструктуру (0-
3)
    'Trigger_Missile_Strike', # Тригер: Ракетні обстріли (0-3)
    'Trigger_Military_Ops', # Тригер: Військові операції (0-3)
    'Trigger_Political_Event' # Тригер: Політика (0-3)
])
df_reports.set_index('Date_Month', inplace=True)

print("Об'єднання даних...")
final_dataset = df_monthly.join(df_reports, how='outer').fillna(0)
final_dataset = final_dataset.astype(int) # Все в цілі числа

final_dataset['TARGET_NextMonth_CIE_High'] =
(final_dataset['Report_Intensity_CIE_IT'].shift(-1) > 1).fillna(0).astype(int)

final_dataset['TARGET_NextMonth_Wiper_High'] =
(final_dataset['Report_Intensity_Wiper'].shift(-1) > 1).fillna(0).astype(int)

avg_phishing = final_dataset['Count_Phishing'].mean()
final_dataset['TARGET_NextMonth_Phishing_Spike'] =
(final_dataset['Count_Phishing'].shift(-1) > avg_phishing).fillna(0).astype(int)

output_file = 'final_thesis_dataset.csv'
final_dataset.to_csv(output_file)

print(f"Готово! Фінальний датасет збережено у '{output_file}'")
print("\n--- Перші 5 рядків ---")
print(final_dataset.head())
print("\n--- Останні 5 рядків ---")
print(final_dataset.tail())

```

Додаток В

```
import pandas as pd
from mlxtend.frequent_patterns import apriori, association_rules

def load_and_process_data(filepath):
    """
    Завантаження та попередня обробка даних для аналізу TP-правил.
    """
    try:
        df = pd.read_csv(filepath)
        print(f"[INFO] Датасет '{filepath}' успішно завантажено. Розмір: {df.shape}")
    except FileNotFoundError:
        print(f"[ERROR] Файл '{filepath}' не знайдено. Спочатку виконайте скрипт з пункту 3.1.")
        return None

    # Визначаємо змінні, які будуть брати участь у пошуку правил
    # X (Antecedents): Події-тригери (поточний місяць)
    triggers = [col for col in df.columns if 'Trigger_' in col]

    # Y (Consequents): Цільові атаки (наступний місяць)
    targets = [col for col in df.columns if 'TARGET_' in col]

    cols_to_analyze = triggers + targets

    # Бінаризація даних:
    # Алгоритм Apriori вимагає 0 або 1. Якщо подія відбулася (значення > 0), ставимо
    1. df_binary = df[cols_to_analyze].applymap(lambda x: 1 if x > 0 else 0)

    return df_binary, triggers, targets

def mine_tp_rules(df_binary, min_support=0.05, min_lift=1.0, max_lift=1.7):
    """
    Пошук часових імовірнісних правил (TP-rules) за допомогою алгоритму Apriori.
    """
    print(f"[INFO] Пошук частих наборів (min_support={min_support})...")
    frequent_itemsets = apriori(df_binary, min_support=min_support, use_colnames=True)

    if frequent_itemsets.empty:
        print("[WARNING] Частих наборів не знайдено. Зменшіть min_support.")
        return pd.DataFrame()

    print(f"[INFO] Генерація правил (lift діапазон: {min_lift}-{max_lift})...")
    rules = association_rules(frequent_itemsets, metric="lift",
min_threshold=min_lift)

    rules = rules[rules['lift'] <= max_lift]

    return rules

def filter_and_format_rules(rules, triggers, targets):
    """
    Фільтрація правил, щоб залишити тільки логічні конструкції 'Тригер -> Атака'.
    """
```

```

# Допоміжна функція для перевірки вмісту правила
def is_valid_rule(row):
    # Ліва частина (antecedents) має містити ТІЛЬКИ тригери
    is_trigger_only = all(item in triggers for item in row['antecedents'])
    # Права частина (consequents) має містити ТІЛЬКИ цільові атаки
    is_target_only = all(item in targets for item in row['consequents'])
    return is_trigger_only and is_target_only

# Застосовуємо фільтр
valid_rules = rules[rules.apply(is_valid_rule, axis=1)].copy()

valid_rules['support'] = valid_rules['support'].round(3)
valid_rules['confidence'] = valid_rules['confidence'].round(3)
valid_rules['lift'] = valid_rules['lift'].round(3)

# Сортування: спочатку за Lift (сила зв'язку), потім за Confidence (надійність)
valid_rules = valid_rules.sort_values(by=['lift', 'confidence'], ascending=[False,
False])

return valid_rules

if __name__ == "__main__":

    input_file = 'cert_ua_calibrated_dataset.csv'

    # 2. Обробка
    data, trigger_cols, target_cols = load_and_process_data(input_file)

    if data is not None:
        all_rules = mine_tp_rules(data, min_support=0.05, min_lift=1.01, max_lift=1.7)

        # 4. Фільтрація та форматування
        final_tp_rules = filter_and_format_rules(all_rules, trigger_cols, target_cols)

        # 5. Вивід результатів
        print(f"\n[RESULT] Знайдено {len(final_tp_rules)} валідних TP-правил.")
        print("\nТОП-10 Правил для включення в Розділ 3.2:")

        # Виводимо колонки, необхідні для таблиці в дипломній роботі
        display_cols = ['antecedents', 'consequents', 'support', 'confidence', 'lift']
        print(final_tp_rules[display_cols].head(10).to_string(index=False))

        # 6. Збереження у CSV для додатків
        final_tp_rules.to_csv('tp_rules_results.csv', index=False)
        print("\n[INFO] Повний список правил збережено у 'tp_rules_results.csv'")

```