3. Титаренко О. Б., Горобець Ю. О., Щипанський П. В., Власенко Є. В. Живучість угруповання зенітних ракетних військ в сучасних операціях: система поглядів. Повітряна міць України. 2024. № 1 (6). С. 49–55.

4. Радецький В. Г. та ін. Протиповітряна оборона у локальних війнах і збройних конфліктах. Київ : НАОУ, 2007. 254 с.

5. Городнов В. П. та ін. Моделирование боевых действий частей, соединений и объединений войск. Харьков : ВИРТА ПВО, 1987. 387 с.

6. Городнов В. П., Дробаха Г. А., Єрмошин М. О., Смірнов Є. Б., Ткаченко В. І. Моделювання бойових дій військ (сил) протиповітряної оборони та інформаційне забезпечення процесів управління ними (теорія, практика, історія розвитку) : монографія. Харків : ХВУ, 2004. 409 с.

7. Неупокоев Ф. К. Противовоздушный бой. Воениздат, 1989. 262 с.

8. Титаренко О. Б., Гогонянц С. Ю. Обґрунтування рекомендацій щодо підвищення живучості угруповання зенітних ракетних військ при відбитті удару засобів повітряного нападу противника. Труди університету. 2015. № 1 (128). С. 81–92.

9. Волювач С. А., Воронін В. В., Рисований О. М., Третяк В. Ф., Балакірева С. М. Удосконалення підходів щодо оцінювання показників живучості підрозділів зенітних ракетних військ. Системи озброєння і військова техніка. 2024. № 1 (77). С. 81–86.

10. Волков А. Ф. та ін. Методика визначення достатнього рівня ефективності бойових дій підрозділу ППО. Збірник наукових праць ХНУПС. 2021. № 4 (70). С. 7–14.

11. Єрмошин М. О. та ін. Підхід щодо оцінки ефективності бойових дій угрупування зенітних ракетних військ. Наука і техніка Повітряних Сил ЗС України. 2019. № 2 (35). С. 113–118.

12. Грідіна В. В., Кузьмін С. А., Малюга В. Г. Шляхи удосконалення методики оцінювання ефективності бойових дій зенітних ракетних військ. Наука і техніка Повітряних Сил ЗСУ. 2022. № 2 (47). С. 41–47.

13. Горбенко В. М., Власенко Є. В. Методичний підхід щодо оцінювання ефективності комплексу заходів забезпечення живучості угруповання зенітних ракетних військ в операції. Наука і техніка Повітряних Сил Збройних Сил України.

ГОНЧАР СЕРГІЙ ВІКТОРОВИЧ
кандидат технічних наук Національний університет цивільного захисту України

КРАПИВНИЙ ІЛЛЯ СЕРГІЙОВИЧ
здобувач вищої освіти
Національний університет цивільного захисту України

ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ВИЯВЛЕННЯ ФІШИНГОВИХ АТАК У ЗАХИЩЕНИХ МЕРЕЖАХ ДЕРЖАВНИХ ОРГАНІВ

У сучасних умовах стрімкого розвитку інформаційних технологій та активізації кібератак на об'єкти державного управління фішинг залишається одним із найбільш поширених і небезпечних методів несанкціонованого доступу до захищених інформаційних систем. За даними міжнародних організацій у сфері кібербезпеки, понад 90% успішних кібератак починаються саме з фішингових повідомлень, спрямованих проти співробітників державних органів. В умовах продовження збройного конфлікту з російською федерацією українські державні установи зазнають безпрецедентного тиску з боку хакерських угруповань, пов'язаних з ворожими спецслужбами, що підвищує актуальність пошуку ефективних технологічних рішень для протидії цим загрозам.

Фішингові атаки являють собою спроби зловмисників змусити користувачів розкрити конфіденційну інформацію - облікові дані, паролі, токени автентифікації - шляхом використання підроблених електронних листів, вебсайтів або повідомлень, що імітують легітимні джерела. Особливу небезпеку становлять цільові фішингові атаки (spear-phishing), які орієнтовані на конкретних посадових осіб і відрізняються високим рівнем персоналізації та складністю виявлення традиційними методами захисту.

Традиційні засоби протидії фішингу - сигнатурний аналіз, чорні списки URL-адрес, фільтрація за репутацією відправника - мають суттєві обмеження. Вони ефективні лише проти вже відомих загроз і неспроможні своєчасно реагувати на нові варіанти атак. Зловмисники постійно вдосконалюють техніки обходу таких засобів: використовують легітимні хмарні сервіси для розміщення фішингових сторінок, застосовують динамічну зміну URL-адрес та коротких посилань, а також генерують повідомлення з унікальним вмістом для обходу сигнатурних фільтрів. Це зумовлює необхідність переходу до адаптивних систем захисту на основі штучного інтелекту.

Застосування методів машинного навчання та штучного інтелекту відкриває принципово нові можливості для виявлення фішингових атак. Серед ключових технологій слід виділити кілька основних напрямів.

Перший напрям - аналіз природної мови (NLP). Алгоритми обробки природної мови аналізують текстовий зміст електронних листів, виявляючи характерні для фішингу мовні конструкції: надмірну терміновість, погрози наслідками, заклики до негайних дій, граматичні та стилістичні помилки. Моделі на основі трансформерних архітектур (BERT, GPT) дозволяють враховувати контекст повідомлення та виявляти смислові аномалії, що неможливо за допомогою простого ключового пошуку.

Другий напрям - аналіз поведінкових ознак та метаданих. Системи машинного навчання будують профілі нормальної поведінки для кожного користувача та відправника: типовий час відправлення листів, географічне розташування серверів, патерни взаємодії між адресатами. Будь-яке відхилення від встановленого профілю фіксується як підозрілий інцидент. Алгоритми класифікації, зокрема Random Forest та градієнтний бустинг, забезпечують високу точність виявлення аномалій навіть у зашифрованому трафіку.

Третій напрям - аналіз URL-адрес та вебсторінок. Рекурентні нейронні мережі (LSTM) аналізують структуру URL-адрес, виявляючи характерні для фішингу ознаки: використання схожих доменних імен (typosquatting), підозрілі субдомени, надмірну довжину адреси. Методи комп'ютерного зору застосовуються для порівняння зовнішнього вигляду підроблених сторінок з оригінальними ресурсами - навіть якщо вихідний код повністю змінений, візуальна схожість залишається характерною ознакою фішингу.

Практичний досвід впровадження ШІ-систем у державному секторі підтверджує їх значну ефективність. Агентство з кібербезпеки та безпеки інфраструктури США (CISA) використовує платформу на основі машинного навчання, яка дозволяє виявляти до 99,9% фішингових листів з рівнем хибних спрацьовувань менше 0,1%. Міністерство оборони Великобританії впровадило систему автоматизованого аналізу електронної пошти на базі нейронних мереж, що скоротило час реагування на фішингові інциденти з декількох годин до хвилин. Країни-члени НАТО активно обмінюються розвідувальними даними про фішингові кампанії через платформу Malware Information Sharing Platform (MISP), інтегровану з ШІ-інструментами для автоматизованого аналізу загроз.

Для України впровадження ШІ-технологій у захист державних інформаційних систем від фішингу є не лише технологічною необхідністю, але й стратегічним пріоритетом. Реалізація такого підходу передбачає кілька взаємопов'язаних кроків: по-перше, інтеграцію систем аналізу електронної пошти на базі машинного навчання у поштову інфраструктуру органів державної влади; по-друге, створення централізованої бази даних фішингових індикаторів компрометації з автоматичним оновленням через ШІ-аналіз; по-третє, розробку систем поведінкового аналізу користувачів для виявлення скомпрометованих облікових записів; по-

четверте, підготовку фахівців з кібербезпеки, здатних ефективно працювати з ШІ-інструментами захисту.

Окремої уваги заслуговує питання інтеграції вітчизняних розробок у сфері ШІ з міжнародними партнерами. В рамках співпраці з ЄС та НАТО Україна отримує доступ до передових технологій кіберзахисту, проте ефективне їх застосування потребує адаптації до специфіки українського інформаційного простору, зокрема врахування особливостей кириличних фішингових атак та національної нормативно-правової бази у сфері захисту інформації.

Таким чином, застосування штучного інтелекту для виявлення фішингових атак у захищених мережах державних органів є перспективним і необхідним напрямом розвитку системи кібербезпеки України. Комплексне використання технологій NLP, машинного навчання та комп'ютерного зору забезпечує суттєво вищий рівень виявлення загроз порівняно з традиційними методами, що є критично важливим в умовах постійного вдосконалення тактик кіберзловмисників. Впровадження відповідних рішень потребує системного підходу, що охоплює технологічну, організаційну та кадрову складові, а також тісну міжнародну співпрацю у сфері обміну даними про кіберзагрози.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Sahingoz O.K., Buber E., Demir O., Diri B. Machine learning based phishing detection from URLs. Expert Systems with Applications. 2019. Vol. 117. P. 345–357.

2. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 20.03.2026).

3. Basit A., Zafar M., Liu X., Javed A.R., Jalil Z., Kifayat K. A comprehensive survey of AI-enabled phishing attacks detection techniques. Telecommunication Systems. 2021. Vol. 76. P. 139–154.

ДАШКОВСЬКИЙ АНАТОЛІЙ ВІКТОРОВИЧ
ад'юнкт, Київський інститут Національної гвардії України

НАУКОВІ ПІДХОДИ ДО ПРОТИДІЇ ТЕРОРИЗМУ В СИСТЕМІ ДЕРЖАВНОЇ БЕЗПЕКИ

У сучасних умовах трансформації міжнародного безпекового середовища проблема протидії тероризму набуває особливої актуальності. Це зумовлено зростанням рівня глобальних загроз, розвитком гібридних форм протистояння, поширенням цифрових технологій та ускладненням викликів для системи державної безпеки. У Стратегії національної безпеки України серед пріоритетів державної політики визначено зміцнення національної стійкості, розвиток безпекових спроможностей держави та вдосконалення механізмів реагування на актуальні загрози [1]. У цьому контексті тероризм слід розглядати як один із чинників дестабілізації державного управління, що здатний негативно впливати на політичну стабільність, економічну безпеку та суспільну довіру до державних інституцій.

Правову основу протидії тероризму в Україні визначає Закон України «Про боротьбу з тероризмом», який установлює основні принципи державної політики у відповідній сфері, окреслює систему суб'єктів боротьби з тероризмом та передбачає механізми запобігання, виявлення і припинення терористичної діяльності [2]. Подальший розвиток державної системи реагування конкретизовано в Концепції боротьби з тероризмом в Україні, у якій акцентовано увагу на необхідності вдосконалення координації між державними органами, розвитку превентивних механізмів та адаптації національної системи безпеки до нових типів загроз [3].

На сучасному етапі розвитку безпекового середовища державна система протидії тероризму України функціонує в умовах суттєвого ускладнення характеру загроз, зумовленого