DOI 10.31891/2307-5732-2023-327-5-231-236
УДК 005.21:005.8:004.8.

БОХОНЬКО ОЛЕКСАНДР
Хмельницький національний університет
ЛИСЕНКО СЕРГІЙ
Хмельницький національний університет
https://orcid.org/0000-0001-7243-8747

МЕТОДИ ВИЯВЛЕННЯ КІБЕРАТАК СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

З розвитком сучасних технологій Інтернет став ключовим для обміну різноманітною інформацією та комунікацій. Як наслідок, подібна еволюція принесла децентралізований доступ до даних та інформації через обмін файлами за допомогою платформ, зокрема таких як соціальні мережі, які як правило, не є досить захищеними.

Роботу присвячено проблемі кібератак соціальної інженерії. Це кібератаки, які здійснюють маніпулювання користувачами, змушуючи їх розкривати конфіденційну інформацію, виконувати певні дії, що призводять до зламування діючих систем безпеки. Подібні кібератаки часто використовують людську психологію, довіру та відсутність пильності з метою отримання несанкціонованого доступу до мереж, систем або даних. Таким чином, конфіденційність користувачів Інтернету завжди під загрозою. Серед злочинів у сфері кібербезпеки атаки соціальної інженерії є найпотужнішим інструментом, який використовують зловмисники.

Масштабні кібератаки із застосуванням соціальної інженерії можуть мати далекосяжні наслідки, що виходять за межі окремих жертв або організацій. Наприклад, кібератаки на об'єкти критичної інфраструктури, державні системи або комунальні підприємства можуть порушити надання основних послуг, поставити під загрозу громадську безпеку або підірвати довіру в суспільстві.

Жертвами таких атак стали багато транснаціональних корпорацій і компаній, інформаційних агентств і навіть урядові установи цілих держав. Зловмисники отримують доступ до інформації, націлюючись на окремих осіб, але в більшості випадків їхньою основною метою є організації з якими такі особи мають певні зв'язки.

У статті представлено спробу виявлення кібератак соціальної інженерії. Під час дослідження використано чотири алгоритми машинного навчання (decision tree, random forest, K-nearest neighbor, and extreme gradient boosting). Аналіз зосереджено на даних, зібраних з мережевих хостів, які можуть слугувати індикаторами потенційних кібератак соціальної інженерії. Емпіричні результати продемонстрували високу точність виявлення.

Ключові слова: соціальна інженерія; кібератаки; виявлення; мережевий хост; кібербезпека

BOHONKO OLEKSANDR, LYSENKO SERGII
Khmelnytskyi National University, Khmelnytskyi, Ukraine

SOCIAL ENGINEERING ATTACKS DETECTION APPROACH

With the development of modern technologies, the Internet has become the key to the exchange of various information and communications. As a result, such an evolution has brought decentralized access to data and information through file sharing through platforms, in particular such as social networks, which are generally not sufficiently secure.

The work is devoted to the problem of social engineering cyberattacks. These are cyberattacks that manipulate users, forcing them to disclose confidential information, to perform certain actions that lead to breaking existing security systems. Such cyberattacks often exploit human psychology, trust, and lack of vigilance to gain unauthorized access to networks, systems, or data. Thus, the privacy of Internet users is always at risk. Among cyber security crimes, social engineering attacks are the most powerful tool used by criminals.

Large-scale social engineering cyberattacks can have far-reaching consequences beyond individual victims or organizations. For example, cyberattacks on critical infrastructure, government systems, or utilities can disrupt the provision of essential services, endanger public safety, or undermine public trust.

Many transnational corporations and companies, news agencies and even government institutions of entire countries became victims of such attacks. Criminals gain access to information by targeting individuals, but in most cases, their main target is organizations with which such individuals have certain ties.

The article presents an attempt to detect social engineering cyberattacks. Four machine learning algorithms (decision tree , random forest , K- nearest neighbor , and extreme gradient boosting). The analysis focuses on data collected from network hosts that can serve as indicators of potential social engineering cyberattacks. Empirical results demonstrated high detection accuracy.

Keywords: Social Engineering; Cyber Attacks; Detection; Network host; Cybersecurity

Вступ

Сьогодні кібератаки соціальної інженерії можуть завдати значної шкоди окремим особам, організаціям і навіть суспільству. Основними потенційними наслідками та збитками, які можуть виникнути в результаті кібератак соціальної інженерії є фінансові втрати, витік даних, крадіжка персональних даних, скомпрометовані системи, репутаційні збитки, порушення операційної діяльності, правові та регуляторні наслідки, психологічний та емоційний вплив, розповсюдження шкідливого програмного забезпечення та програм-вимагачів. Кібератаки соціальної інженерії часто спрямовані на те, щоб обманом змусити людей розкрити конфіденційну фінансову інформацію або переказати гроші на шахрайські рахунки. Жертви можуть зазнати прямих фінансових збитків, включаючи несанкціоновані транзакції, крадіжку особистих даних або шахрайські покупки. Кібератаки соціальної інженерії можуть призвести до витоку даних, коли викрадають конфіденційну інформацію, таку як особисті дані, облікові дані для входу в систему або фінансові дані. Це може мати серйозні наслідки, включаючи крадіжку особистих даних, несанкціонований доступ до облікових записів або шкоду репутації [1-3].

Кібератаки соціальної інженерії можна розділити на дві групи: технічні (Vishing, Phishing, Spear Phishing, Spam Email, Interesting Software, Popup Window, Baiting, Tailgating, and Waterholing) та нетехнічні (pretexting, face-to-face interaction, shoulder surfing, quid pro quo attacks, diversion theft attacks, reverse social engineering, authoritative voice, spying, technical expert, support stuff, smudge attack).

Мета дослідження - розроблення нового методу виявлення кібератак соціальної інженерії. Кібератаки соціальної інженерії передбачають маніпулювання людьми з метою розкриття конфіденційної інформації, виконання певних дій або компрометації систем безпеки.

Відомі методи виявлення кібератак соціальної інженерії

У науковій літературі існує велика кількість підказок для вирішення цієї проблеми. У статті [4] розглядаються методології, що застосовуються у фішингових кібератаках. Її основна мета - сприяти професійному обговоренню фішингових кібератак, підвищити обізнаність громадськості про тактику фішингу та сприяти навчанню щодо цих типів кібератак. Дослідження [5] показують, що соціальна інженерія може бути автоматизована в багатьох випадках, що дозволяє її широкомасштабну реалізацію. Як наслідок, соціальна інженерія стала значною загрозою у віртуальних спільнотах. Визнаючи важливість інформаційної безпеки для розвитку бізнесу, ця стаття надає всебічний огляд кібератак соціальної інженерії на соціальні мережі, а також принципів, що лежать в їх основі, і різних типів таких кібератак. У дослідженні [6] автори пропонують стратегії і тактики кампаній з охорони здоров'я для протидії кібератакам соціальної інженерії. Ці стратегії включають телевізійну рекламу, фізичні інформаційні брошури та дискусії в соціальних мережах. Однак дуже важливо, щоб ці методи кампанії були підкріплені відповідною і достатньою освітою. Одне з обмежень цього дослідження полягає в тому, що воно ґрунтується на якісному дослідженні, якому бракує емпіричної перевірки. У дослідженні [7] вивчався зв'язок між рисами особистості та її вразливістю до соціальної інженерії в контексті соціальних мереж. Щоб заповнити цю прогалину, в дослідженні було представлено інноваційну модель для прогнозування вразливості користувачів, яка враховує різні аспекти їхніх характеристик. Запропонована в статті модель враховує взаємодію між різними факторами, пов'язаними з соціальними мережами, такими як рівень залученості користувача в мережу, мотивація використання мережі та компетентність у боротьбі з мережевими загрозами. У статті [8] представлено етичний аналіз соціальної інженерії в тестуванні на проникнення. Робота описує фундаментальні принципи функціонування соціальної інженерії. У [9] було створено фреймворк «людина як сенсор безпеки», який було практично реалізовано за допомогою Cogni-Sense, прототипу програми для Microsoft Windows. Cogni-Sense має на меті надати користувачам можливість проактивно виявляти та повідомляти про семантичні кібератаки соціальної інженерії, спрямовані на них. Кіберзлочинці користуються можливістю запускати кібератаки соціальної інженерії, використовуючи шкідливі URL-адреси, що поширюються електронною поштою або текстовими повідомленнями в соціальних мережах [10]. У роботі [11] автори розробили та валідували методику вилучення даних, необхідних для проведення ефективних фішингових кібератак, з відкритих наукових джерел. Автори запропонували використовувати автоматизовані скрипти для перевірки автентичності зібраних даних перед розгортанням і для автоматизації процесу розсилки в обхід алгоритмів виявлення спаму. У статті [12] представлено модель виявлення з використанням методів машинного навчання, яка передбачає поділ набору даних на навчальні та тестові набори. Такий метод дозволив зафіксувати характерні риси тексту електронної пошти та інші особливості, що уможливило ефективну класифікацію на фішингові та нефішингові атаки. У роботі [13] автори розробили метод виявлення атак соціальної інженерії під назвою Anti-Social Engineering Tool ASsET, який виявляє атаки на основі семантичного змісту розмови. Даний метод здійснює обробку природної мови, щоб визначити, чи міститься значення шахрайського підпису в розмові. Дослідниками було зібрано набір даних про телефонне шахрайство, на основі реальних прикладів шахрайства. Даний метод виявлення атак соціальної інженерії зміг з високою точністю відрізнити шахрайські та нешахрайські дзвінки. У роботі [14] автори розробили метод виявлення шахрайства в транскрибованих телефонних розмовах за допомогою лінгвістичних особливостей. Запропонований метод використовує синтаксичну та семантичну інформацію транскрипції, щоб виділити певні лінгвістичні маркери. Дослідниками продемонстровано результати на основі реальних даних за допомогою простих, надійних і зрозумілих класифікаторів, таких як: Naive Bayes, Decision Tree, Nearest Neighbours, та Support Vector Machines. У роботі [15] представлено метод аналізу голосового трафіку в телефонних мережах на основі алгоритмів машинного навчання, з метою виявлення шахрайства. Починаючи з необробленого набору даних, який включає інформацію про дату виклику, номер адресата, тривалість і номер абонента, дослідниками було досить ефективно виявлено шахрайські дзвінки на ранніх стадіях. У статті [16] представлено огляд методів виявлення та аналізу шахрайства або спаму на основі штучного інтелекту. Запропоновано новий метод виявлення телефонних шахрайських викликів, який досягає високої точності. Для даного методу було використано набір даних реальних шахрайських викликів. Результати демонструють, що метод досяг високої точності у виявленні зловмисних дзвінків і ідентифікації потенційних ознак шахрайства чи спаму. Аналіз дзвінків про шахрайство також дозволив зрозуміти тактику та методи, які використовують шахраї, які можна використати для розробки контрзаходів. У статті [17] пропонується метод машинного навчання, заснований на розпізнаванні голосу, на основі обробки природної мови «ScamBlk». Аудіо дзвінка використовується як вхідний сигнал і транскрибується в текстову форму, яка додатково обробляється та передається в модель машинного навчання. У моделі машинного навчання використовується комплексний підхід, який розгортає пакетування послідовної моделі довгострокової мережі короткочасної пам’яті та лінійної моделі машини

опорних векторів для класифікації шахрайських фраз у телефонній розмові. Запропонований метод є кращим за інші методи машинного навчання, його точність визначено на рівні 97,08%.

Аналіз показав, що існують різні підходи до виявлення кібератак соціальної інженерії, які мають певні недоліки та обмеження. Усунення цих недоліків вимагає розроблення нових методів виявлення, включаючи постійне вдосконалення технологій, навчання користувачів і розробку більш досконалих і адаптивних методів виявлення, які можуть ефективно протистояти зловмисникам, що використовують соціальну інженерію.

Метод виявлення кібератак соціальної інженерії

Запропоновано новий метод до виявлення кібератак соціальної інженерії. Дослідження включає етапи навчання та виявлення. Розглянемо кроки етапу навчання: побудова знань шляхом аналізу характеристик, які можуть припустити існування кібератак соціальної інженерії на хостах мережі; представлення інформації про кібератаки у вигляді набору векторів ознак. Етап виявлення складається з наступних етапів: моніторинг системних подій в хостах мережі; збір характеристик і виділення функцій з хосту мережі, які потенційно можуть означати існування кібератаки соціальної інженерії на цей хост та побудова вектору ознак з цих атрибутів; формування векторів ознак з використанням даних, отриманих від хостів мережі; виконання класифікації об'єктів з використанням алгоритмів машинного навчання шляхом використання отриманих векторів ознак для віднесення досліджуваного об'єкту до конкретного класу кібератак; локалізація хоста мережі, який піддається атаці.

Для прийняття рішення метод використовує алгоритми машинного навчання: Decision Trees (DT), Random Forest (RF), K-Nearest Neighbors (KNN), Extreme Gradient Boosting (XGBoost).

Побудова знань на основі ознак кібератак соціальної інженерії

Позначимо кібератаки соціальної інженерії, які підлягають виявленню, як множину *A*, $\mathrm{a} = \{\mathrm{a_m}\}_{\mathrm{m=1}}^{\mathrm{N_a}}$, $\mathrm{a_1}$– атака типу вішинг; $\mathrm{a_2}$ – атака типу фішинг; $\mathrm{a_3}$– атака типу grooming; $\mathrm{a_4}$ – атака типу клонування профілю; $\mathrm{a_5}$ – атака типу пошук у смітнику; $\mathrm{a_6}$ – атака типу tailgating; $\mathrm{a_7}$ – атака типу file masquerade; $\mathrm{a_8}$ – атака типу baiting; $\mathrm{a_9}$ – атака типу scareware or pop-up windows; $\mathrm{a_{10}}$ – атака типу water-holing; $\mathrm{a_{11}}$ – атака типу троянська пошта; $\mathrm{a_{12}}$ – атака типу spear фішинг; $\mathrm{a_{13}}$ – атака типу спам; $\mathrm{a_{14}}$ – атака типу цікаве програмне забезпечення; $\mathrm{a_{15}}$ – атака типу обман; $\mathrm{a_{16}}$ - атака типу - pretexting ; $\mathrm{a_{17}}$ атака типу - face – to – face interaction; $\mathrm{a_{18}}$ атака типу - shoulder surfing; $\mathrm{a_{19}}$ атака типу - quid pro quo attacks; $\mathrm{a_{20}}$ атака типу - diversion theft attacks; $\mathrm{a_{21}}$ - атака типу - piggybacking or tailgating or trailing & pretending; $\mathrm{a_{22}}$ - атака типу - reverse social engineering; $\mathrm{a_{23}}$ - атака типу – технічний експерт; $\mathrm{a_{24}}$ - атака типу - support stuff; $\mathrm{a_{25}}$ - атака типу - smudge attack.

Позначимо ознаки B, які можуть вказувати на кібератаки соціальної інженерії як набір [13-17]:

$$B = \left\{b_{a_j}\right\}_{a_j=1}^{N_B}, \tag{2}$$

де N_B– кількість ознак щодо a_jтипу кібератаки; b_{a_1}– сукупність дій, спрямованих хакерами на отримання конфіденційної інформації від користувачів (таких як PIN-коди, одноразові паролі) шляхом здійснення телефонних дзвінків; b_{a_2}– сукупність дій хакерів, спрямованих на розсилку повідомлень, які містять модифіковану інформацію, але при цьому можуть бути візуально дуже схожі на легітимні та офіційні джерела; b_{a_3} – сукупність дій хакерів, спрямованих на поєднання хакерами інформаційних технологій (SMS, електронна пошта, телефон) з психологічними методами. Дії хакерів спрямовані на отримання інформації про потенційних жертв педофілії; b_{a_4} – сукупність дій хакерів, спрямованих на використання загальнодоступної інформації із соціальної мережі з метою створення клону особистого профілю користувача; b_{a_5} – сукупність дій хакерів, спрямованих на збір та використання документів чи іншої інформації, видаленої до «кошика» з певного ресурсу на жорсткому диску користувача; b_{a_6} – сукупність дій хакерів, спрямованих на незаконне отримання персональних даних співробітників певної організації; b_{a_7} – сукупність дій зловмисників, спрямованих на встановлення шкідливого програмного забезпечення у файли, які знаходяться як на ПК користувача, так і на зовнішніх носіях. Дії хакерів призводять до того, що користувач запускає шкідливі програми під час використання звичайних файлів у роботі; b_{a_8} – сукупність дій, що використовуються хакерами для кібератаки за допомогою електронних носіїв, заражених шкідливим програмним забезпеченням у фізичній формі (USB-накопичувачі); b_{a_9} – сукупність дій/функцій, у яких хакери використовують спливаючі вікна у вікнах або браузерах, які з'являються на моніторі, коли користувач виконує певну дію на комп'ютері. Хакери встановлюють певні скрипти або коди на сторінках, які можуть генерувати спливаючі вікна, налаштовані на потенційних і цільових жертв; $b_{a_{10}}$ – сукупність дій/функцій, спрямованих хакерами на злом веб-сайтів з високим рівнем відвідуваності з метою впровадження на них шкідливого програмного забезпечення або троянських програм; $b_{a_{11}}$ – сукупність дій хакерів, спрямованих на розповсюдження шкідливих програм електронною поштою, при цьому подібні листи виглядають цілком безпечно; $b_{a_{12}}$– сукупність дій хакерів, спрямованих на викрадення конфіденційної інформації у конкретної жертви, де хакери збирають всю необхідну інформацію про діяльність потенційної жертви, аналізують її та маскуючи під добре відомі користувачеві речі, здійснюють кібератаку з метою отримання незаконного доступу до облікового запису користувача чи іншої конфіденційної інформації; $b_{a_{13}}$ – сукупність дій хакерів, спрямованих на

надсилання потенційним жертвам величезної кількості електронних листів з рекламною інформацією та потенційно шкідливим контентом у систему користувача; $b_{a_{14}}$ – сукупність дій хакерів, спрямованих на аналіз та визначення контенту програмного забезпечення, цікавого для більшості користувачів, з метою розміщення неправдивих посилань на цей контент в мережі Інтернет; $b_{a_{15}}$– сукупність дій хакерів з поширення неправдивої інформації (фейків) в Інтернет-просторі. Хакери спонукають жертву відвідати сайт або перейти за посиланням, що призводить до зараження системи вірусами; $b_{a_{16}}$– сукупність дій хакерів, спрямованих на використання інформації із вільним доступом. На основі отриманих даних, хакери контактують із потенційною жертвою в результаті чого жертва розголошує конфіденційну інформацію. Контакт відбувається у формі живого спілкування; $b_{a_{17}}$– сукупність дій хакерів, спрямованих на проведення зустрічей із потенційною жертвою (віч-на-віч) з метою визначення психологічних особливостей або слабкостей людини. Далі шахраї вдаються до маніпуляції жертвою та спонукають надати певного роду допомогу чи розкрити фізичний доступ до конфіденційної інформації; $b_{a_{18}}$– сукупність дій хакерів, спрямованих на незаконне використання доступу або паролю користувачів соціальної інженерії які не мають або мають дуже слабкі знання та навички з питань безпеки; Дії зловмисників полягають в підгляданні конфіденційної інформації через плече жертви; $b_{a_{19}}$– сукупність дій хакерів, спрямованих на отримання взаємної вигоди від наданої послуги на підставі умовної угоди, яка укладається із потенційної жертвою. Після виконання своєї частини угоди, хакери вимагають від людини розкриття важливої інформації або щось інше; $b_{a_{20}}$– сукупність дій хакерів, спрямованих на зміну фактичної адреси місця доставки товару, в програмному забезпеченні кур'єрської служби через яку потенційна жертва здійснила замовлення доставки товару; $b_{a_{21}}$– сукупність дій хакерів, спрямованих на незаконне заволодіння персональними даними працівників певної організації. Хакери здійснюють спостереження за обраним співробітником організації та маючи конфіденційну інформацію, використовують її для незаконного входження в систему організації, обминувши її систему безпеки; $b_{a_{22}}$– сукупність дій хакерів, спрямованих на моделювання ситуації, при якій користувач стикається з із штучно створеними хакерами проблемами в програмному забезпеченні користувача. Таким чином, хакери змушують потенційну жертву звертатися за допомогою. При наданні допомоги у відновленні роботи системи, хакери встановлюють незаконне програмне забезпечення для можливості отримання в подальшому адміністративного доступу через комп'ютер потенційної жертви; $b_{a_{23}}$– це множина дій та методів хакерів в результаті яких зловмисникам вдається видати себе за технічного працівника організації. Хакери вводять в оману потенційну жертву та під виглядом надання технічної підтримки клієнту, отримують незаконний доступ до персональних даних користувача або іншої конфіденційної інформації; $b_{a_{24}}$– це множина дій та методів хакерів в результаті яких зловмисниками створюється ілюзія контакту жертви із службою підтримки певної організації. Хакерами застосовуються різні методи контакту із потенційною жертвою. В результаті таких дій, хакери отримують доступ до конфіденційної інформації жертви; $b_{a_{25}}$– сукупність дій хакерів, спрямованих на збір інформації яку залишають пальці рук користувачів на сенсорних пристроях у формі плям. Зловмисниками збирається конфіденційна інформація, типу паролів чи PIN-кодів, на підставі аналізу візерунків залишених плям.

Усі згадані раніше функції кібератаки утворюють знання колекції векторів ознак $X = \{x_k\}_{k=1}^{N_X}$, де кожен із векторівx_k описує кібератаку соціальної інженерії та поведінку законних користувачів,N_X – кількість векторів ознак. Використання отриманих від мережевих хостів ознак представлено як вектори ознак.

Збір характеристик і виділення функцій з хосту мережі, які потенційно можуть означати існування кібератаки соціальної інженерії на цей хост, і побудова вектора ознак із цих ознак. Цей етап методу включає моніторинг системних подій мережевих хостів з метою збору ознак, які можуть вказувати на наявність кібератак. Після цього зібрана інформація передається до класифікаторів для подальшого аналізу інформації.

Характеристики, які можуть вказувати на наявність соціальних кібератак на хостах мережі, отримуються з даних, зібраних на попередньому етапі , і підлягають аналізу. За результатом аналізу робиться висновок про наявність або відсутність нападу. Як засоби класифікації згадуються алгоритми машинного навчання, де об'єктами класифікації є вектори x_kознак , отримані в результаті аналізу системних подій хостів мережі. Результатом класифікації є значення приналежності u_{ik}вектора ознак x_kдо кожного класу i. Приналежність вектора ознак x_k визначає до якого класу *i* відноситься тип кібератаки соціальної інженерії.

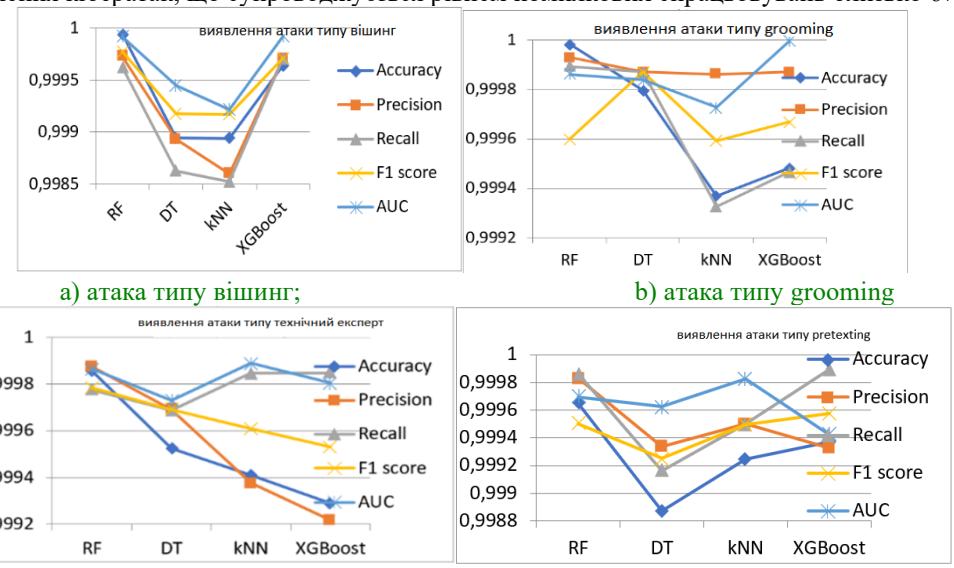
Експериментальні дослідження

Для оцінки ефективності запропонованого методу було проведено серію експериментів. У цих експериментах використовувалися набори даних [18-22], що містять приклади зловмисної поведінки. У цих експериментах було задіяно 50 мережевих хостів, на яких було виконано (змодельовано) кожен з 15 типів кібератак. Кожен експеримент тривав 24 години.

Запропонований метод включав чотири алгоритми машинного навчання (decision tree, random forest, K-nearest neighbor, extreme gradient boosting), щоб порівняти їхні можливості виявлення. Всі алгоритми були навчені та протестовані на наборі даних з відсотковим співвідношенням навчання та тестування 75% та 25%.

Як середовище виявлення було використано фреймворк BotGRABBER, який використовує бібліотеку scikit-learn [23], а конфігурація кожного використаного алгоритму машинного навчання залежить від

відповідного набору параметрів алгоритму. У дослідженні найвищий рівень виявлення показав Random Forest. Результати для чотирьох різних типів кібератак показані на рисунку 1. Ці результати показали приблизно 99% точність виявлення кібератак, що супроводжується рівнем помилкових спрацьовувань близько 6%.



a) атака типу вішинг; b) атака типу grooming

c) атака типу технічний експерт; d) атака типу pretexting

Рис. 1. Результати виявлення кібератак з використанням decision tree, random forest, K-nearest neighbor, and extreme gradient boosting MLA для: a) атаки типу вішинг; b) атики типу grooming; c) атаки типу технічний експерт; d) атаки типу pretexting.

Висновки

Запропоновано інноваційний метод виявлення кібератак соціальної інженерії технічного та нетехнічного типу. Цей метод передбачає використання чотирьох алгоритмів машинного навчання: decision tree, random forest, K-nearest neighbor та extreme gradient boosting. Запропонована методика складається з двох основних етапів: навчання та виявлення.

Дослідження зосереджене на даних, зібраних з мережевих хостів, які потенційно можуть вказувати на наявність кібератаки соціальної інженерії. Емпіричні результати показали вражаючу точність виявлення - близько 99%, у поєднанні з рівнем помилкових спрацьовувань близько 6%.

Література

1. Brabin D., Bojjagani S. A Secure Mechanism for Prevention of Vishing Attack in Banking System. *2023 International Conference on Networking and Communications (ICNWC) Chennai*, India. 2023. https://doi: 10.1109/icnwc57852.2023.10127561.

2. Ameen R.M., Sarab M.H. Review of Smishing Detection Via Machine Learning. *Iraqi Journal of Science*. 2023. vol. 64, № 8, pp. 4244-4259. https://doi: 10.24996/ijs.2023.64.8.42.

3. Ruwa F. Abu Hweidi, Derar Eleyan. Social Engineering Attack Concepts, Frameworks, and Awareness: A Systematic Literature Review. *International Journal of Science and Engineering Invention* (*IJSEI*). 2022. vol. 08. https://doi.org/10.23958/ijsei/vol08-i02/226.

4. Alghenaim M.F., Bakar N.A.A., Rahim F.A. Awareness of Phishing Attacks in the Public Sector: Review Types and Technical Approaches. Proceedings of the 2nd International Conference on Emerging Technologies and Intelligent Systems. *ICETIS 2022. Lecture Notes in Networks and Systems*. Springer. 2023. vol. 584. pp 616–629. https://doi.org/10.1007/978-3-031-25274-7_54.

5. Chetioui K., Bah B., Alami A.O., Bahnasse A. Overview of Social Engineering Attacks on Social Networks. *Procedia Computer Science*. 2022. Vol. 198. pp. 656-661. https://doi.org/10.1016/j.procs.2021.12.302.

6. Abe N., Soltys M. Deploying health campaign strategies to defend against social engineering threats. *Procedia Computer Science*. 2019. vol. 159, pp. 824–831, https://doi.org/10.1016/j.procs.2019.09.241.

7. Albladi S.M., Weir G.R.S. Predicting individuals' vulnerability to social engineering in social networks. *Cybersecurity*. 2020. article number 7. https://doi.org/10.1186/s42400-020-00047-5.

8. Hatfield J. Virtuous Human Hacking: The Ethics of Social Engineering in Penetration-Testing. *Computers and Security*. 2019. vol. 83. pp. 354–366. https://doi.org/10.1016/j.cose.2019.02.012.

9. Heartfield R., Loukas G. Detecting semantic social engineering attacks with the weakest link: Implementation and empirical evaluation of a human-as-a-security-sensor framework. *Computers & Security*. 2018. Vol. 76. pp. 101-127. https://doi.org/10.1016/j.cose.2018.02.020.

10. Saleem R.A., Madhubala R., Rajesh N., Shaheetha L., Arulkumar N. Survey. *Malicious URL Detection Techniques. 6th International Conference on Trends in Electronics and Informatics (ICOEI). Tirunelveli, India*. 2022. pp. 778-781. https://doi: 10.1109/ICOEI53556.2022.9777221.

11. Marusenko R., Sokolov V., Bogachuk I. Method of Obtaining Data from Open Scientific Sources and Social Engineering Attack Simulation. Artificial Systems for Logistics Engineering. ICAILE 2022. Lecture Notes on Data Engineering and Communications Technologies. *Springer*. 2022. vol. 135. https://doi.org/10.1007/978-3-031-04809-8_53.

12. Mughaid A., AlZu'bi S., Hnaif A. An intelligent cyber security phishing detection system using deep learning techniques. *Cluster Comput*. 2022. vol. 25, pp. 3819–3828. https://doi.org/10.1007/s10586-022-03604-4.

13. Derakhshan Ali, Harris Ian G., Behzadi Mitra. Detecting Telephone-based Social Engineering Attacks using Scam Signatures. *Матеріали семінару ACM 2021 з аналізу безпеки та конфіденційності.* 2021. pp.67–73 https://doi.org/10.1145/3445970.3451152.

14. Bajaj N., Constance T.G., Rajwadi M., Wall J., Moniri M., Glackin C., Cannings N., Woodruff C., Laird J. Fraud detection in telephone conversations for financial services using linguistic features. *33rd Conference on Neural Information Processing Systems (NeurIPS 2019), AI for Social Good Workshop, Vancouver, Canada*. 2019.https://doi.org/10.48550/arXiv.1912.04748.

15. Department of Computer of Information TechnologyUniversity of Galati, Romania. Using machine learning algorithms to detect frauds in telephone networks. *University of Galati Fascicle III*. 2020. vol. 43. № 3. https://doi.org/10.35219/eeaci.2020.3.03.

16. Malhotra S., Arora G., Bathla R. Detection and Analysis of Fraud Phone Calls using Artificial Intelligence. *2023 International Conference on Recent Advances in Electrical, Electronics & Digital Healthcare Technologies (REEDCON) New Delhi, India*. 2023. https://doi:10.1109/reedcon57544.2023.10150631.

17. Nandakumar M., Nachiappan R., Sunil A.K, Neves J.C., Proença H.P., Sathiyanarayanan M. ScamBlk: A Voice Recognition-Based Natural Language Processing Approach for the Detection of Telecommunication Fraud. *Springer. Lecture Notes in Networks and Systems book series (LNNS)*. 2022. vol. 394. https://doi.org/10.1007/978-981-19-0604-6_47.

18. Lansley M., Mouton F., Kapetanakis S., Polatidis N., SEADer++: social engineering attack detection in online environments using machine learning. *J. Inf. Telecommun*. 2020. vol. 4. № 3. pp. 346 – 362, https://doi: 10.1080/24751839.2020.1747001.

19. Catal C., Giray G., Tekinerdogan B., Kumar S., Shukla, S. Applications of deep learning for phishing detection: a systematic literature review. *Knowledge and Information Systems*. 2022. Vol.64(6), pp. 1457-1500.

20. Al-Khateeb M., Al-Mousa M., Al-Sherideh A., Almajali D., Asassfeha M., Khafajeh H. Awareness model for minimizing the effects of social engineering attacks in web applications. *International Journal of Data and Network Science*. Vol. 20237(2), pp. 791-800.

21. Rifat N., Ahsan M., Chowdhury M., Gomes R. BERT against social engineering attack: Phishing text detection. *2022 IEEE International Conference on Electro Information Technology.* IEEE. 2022. pp. 1-6.

22. Wang Z., Ren Y., Zhu H., Sun L. Threat detection for general social engineering attack using machine learning techniques. arXiv preprint *arXiv*:2203.07933. 2022.

23. Lysenko S., Bobrovnikova K., Savenko O., Kryshchuk A., BotGRABBER: SVM-Based Self-Adaptive System for the Network Resilience Against the Botnets' Cyberattacks. *Communications in Computer and Information Science*. 2019, pp. 127-143. ISSN: 1865-0929.