DOI 10.15276/imms.v13.no3-4.266
УДК 004.056.53

Informatics and Mathematical Methods in Simulation
Vol.13 (2023), No. 3-4, pp. 266-274

МЕТОД ВИЯВЛЕННЯ ФІШИНГОВИХ QR-КОДІВ ІЗ ЗАСТОСУВАННЯ МАШИННОГО НАВЧАННЯ

А.В. Касаяні, Н.І. Кушніренко, О.В. Троянський, В.В. Подуфалов

Національний університет «Одеська політехніка»
1 Шевченка пр., Одеса, 65044, Україна
e-mail: infsec2011@gmail.com

На сьогоднішній день існує багато інструментів, які можуть виявляти та блокувати шкідливі посилання, які ведуть до фішингових сайтів або зловмисного програмного забезпечення. Проте більшість з них поки не здатні перевіряти шкідливі QR-коди, і це дає зловмисникам можливість активно використовувати їх в атаках. Фішинг з використанням QR-кодів дуже схожий на інші форми фішингу. Ця атака спрямована на маніпулювання користувачами та отримання від них особистої інформації, такої як облікові дані для входу чи фінансова інформація. Суть фішингу з використанням QR-кодів не нова. Основна відмінність полягає в тому, що в цьому випадку QR-код використовується для перенаправлення жертви на шкідливий веб-сайт. Метою даної роботи є підвищення безпеки користувачів у цифровому середовищі шляхом розробки та впровадження методу виявлення фішингових QR-кодів з використанням машинного навчання. У роботі проведено аналіз методів та засобів протидії фішингу та атакам через QR-коди, який дозволив визначити напрямки розробки та основні завдання дослідження. Розроблений метод включає в себе аналіз особливих ознак посилання та його тексту за допомогою мовно моделі, на основі яких навчався та тестувався алгоритм машинного навчання. Створений метод виявлення фішингових QR-кодів значно підвищує безпеку користувачів у використанні QR-кодів. Аналіз ефективності розробленого методу показав результат у понад 90% точності виявлення. Метод виявлення фішингових QR-кодів, розроблений у рамках цієї роботи, може бути успішно впроваджений в діяльність різних організацій, включаючи підприємства та установи. Цей метод надає можливість зменшити ризики фішингових атак через QR-коди, що призводить до підвищення безпеки для співробітників. Результати даної роботи можуть бути використані при подальших дослідженнях, розробках у сфері кібербезпеки та боротьби з фішинговими атаками через QR-коди.

Ключові слова: фішинг, QR-код, машинне навчання, кібербезпека, мовна модель.

Вступ. Питання фішингу в сучасному інтернет-середовищі визначається як одна з найбільш поширених та серйозних загроз для безпеки користувачів та організацій. Фішинг є методом соціальної інженерії, який заснований на обмані та маніпуляціях з метою здобуття конфіденційної інформації, фінансових ресурсів або доступу до цифрових активів.

Особливу увагу слід звернути на фішингові атаки, які використовують QR-коди. Зараз QR-коди широко використовуються у рекламі, маркетингу та логістиці, і ця популярність робить їх привабливими для зловмисників. Вони можуть створювати фішингові QR-коди, які виглядають легітимними, але насправді ведуть до шахрайських веб-сайтів або завантажують шкідливе програмне забезпечення на пристрої користувачів.

Використання фішигових QR-кодів стало серйозним викликом для кібербезпеки і призвело до поганих наслідків для багатьох людей та компаній. Ось деякі відомі приклади цих атак [1]:

– паркувальні квитки у Китаї: У Китаї шахраї розміщали підроблені паркувальні квитки з QR-кодами на автомобілях. QR-коди надавали зручну можливість оплати за допомогою мобільних телефонів. Однак, фактично, це були шахрайські схеми, що призводили до фінансових втрат;
– мобільний банкінг в Нідерландах: У Нідерландах зловмисники використовували легальні функції мобільних банківських додатків для обману клієнтів. Вони використовували QR-коди, щоб провести фішингові атаки та вимагали конфіденційну інформацію;
– фальшиві електронні листи в Німеччині: У Німеччині злочинці використовували QR-коди у фальшивих електронних листах, щоб вести клієнтів системи електронного банкінгу на шкідливі веб-сайти, прикидаючись перевіркою політики конфіденційності;
– фішингові атаки в Техасі: В Техасі зловмисники приклеювали шкідливі QR-коди до міських паркоматів. Жертви, скануючи ці коди, потрапляли на фейкові фішингові сайти і вводили свої кредитні картки, стаючи об'єктом фінансового шахрайства.

Ці приклади свідчать про різноманітність атак, які використовують QR-коди для здійснення злочинних дій. З цим явищем пов'язані серйозні загрози для інтернет-безпеки, і важливо бути обережними при взаємодії з QR-кодами, особливо якщо вони надійшли від невідомих джерел. Це робить проблему фішингу через QR-коди актуальною та вимагає розробки ефективних методів виявлення цих атак.

На теперішній час існує багато методів для виявлення фішингових посилань, які використовують машинне навчання [2 - 4]. Вони мають високий рівень ефективності, але не пропонують боротьбу з фішинговими атаками через QR-коди, які все частіше становляться загрозою для підприємств та окремих користувачів. Тому було вирішено розробити метод, що застосовується саме для виявлення фішингу у QR-кодах. Розроблений метод містить у собі механізм аналізу тексту посилання за допомогою мовної моделі. Його ефективність порівняна або навіть перевищує ефективність інших методів.

Мета і задачі дослідження. Метою даної роботи є підвищення безпеки користувачів у цифровому середовищі шляхом розробки та впровадження методу виявлення фішингових QR-кодів з використанням машинного навчання. Для досягнення поставленої мети необхідно розв'язати такі завдання:

– аналіз предметної області – вивчення методів та засобів протидії фішингу, зокрема в контексті використання QR-кодів;
– розробка теоретичної основи виявлення фішингових QR-кодів;
– вибір методу машинного навчання;
– реалізація та тренування моделі машинного навчання для виявлення фішингових QR-кодів;
– тестування розробленого методу та аналіз ефективності.

Основна частина. Фішинг – це вид кіберзлочинності, який спрямований на отримання конфіденційної інформації від користувачів Інтернету шляхом імітації довірливих джерел або осіб [5]. Фішингові атаки спираються на соціальну інженерію та мають на меті обман цільових користувачів для отримання їхніх особистих даних, таких як паролі, номери кредитних карт та іншої фінансової інформації.

Соціальна інженерія відіграє ключову роль у фішингу, оскільки вона визначає ефективність атаки. В основі фішингу лежить психологічний вплив на жертву, який допомагає атакуючому переконати жертву надавати конфіденційну інформацію чи виконувати вказівки. Соціальна інженерія допомагає атакуючому створити обманливу ситуацію та надати вигляд довіри та легітимності атаки. Це може включати в себе імітацію офіційних логотипів, листів, повідомлень або веб-

сайтів, а також створення обманливих сценаріїв, які спонукають жертву до виконання дій на користь атакуючого [6].

Розглянемо основні види фішингу з якими можуть зіткнутися користувачі у Інтернет мережі [7 - 8]:

- фішинг через QR-коди (QR Code Phishing);
- голосовий фішинг (Vishing);
- фішинг через клонування (Clone Phishing);
- фішинг через соціальні мережі (Social Media Phishing);
- фішинг через смс-повідомлення (Smishing);
- фішинг через електронну пошту (Email Phishing);
- фішинг атака «злий двійник» (Evil Twin Phishing);
- китобійний фішинг (Whaling);
- цільовий фішинг (Spear Phishing).

QR-коди, або Quick Response Codes, є двовимірними штрих-кодами, які стали надзвичайно популярними в останні десятиріччя. Вони забезпечують ефективний спосіб кодування і передачі інформації, і використовуються в різних сферах, від маркетингу до логістики та медицини. QR-коди створені для швидкого і зручного зчитування інформації за допомогою сучасних мобільних пристроїв. Вони мають специфічну структуру, що дозволяє кодувати багато типів даних, включаючи текст, веб-посилання, контактну інформацію, географічні координати та багато інших.

Інформація, що зберігається в QR-коді, може приймати різні форми, але найчастіше вона є простим веб-посиланням. Наприклад, в операційній системі iOS додаток «Камера» автоматично розпізнає QR-коди і пропонує відкрити веб-сторінку за посиланням, що в них міститься. Основна інформація, яку слід мати на увазі щодо QR-кодів, полягає в тому, що вони часто служать як звичайні посилання на веб-сторінки і це має важливий вплив на питання кібербезпеки.

QR-коди, як зручний і поширений спосіб передачі інформації, стали привабливим знаряддям для зловмисників, які прагнуть використовувати їх для фішингових атак. Процес функціонування таких атак представлений на рисунку 1.

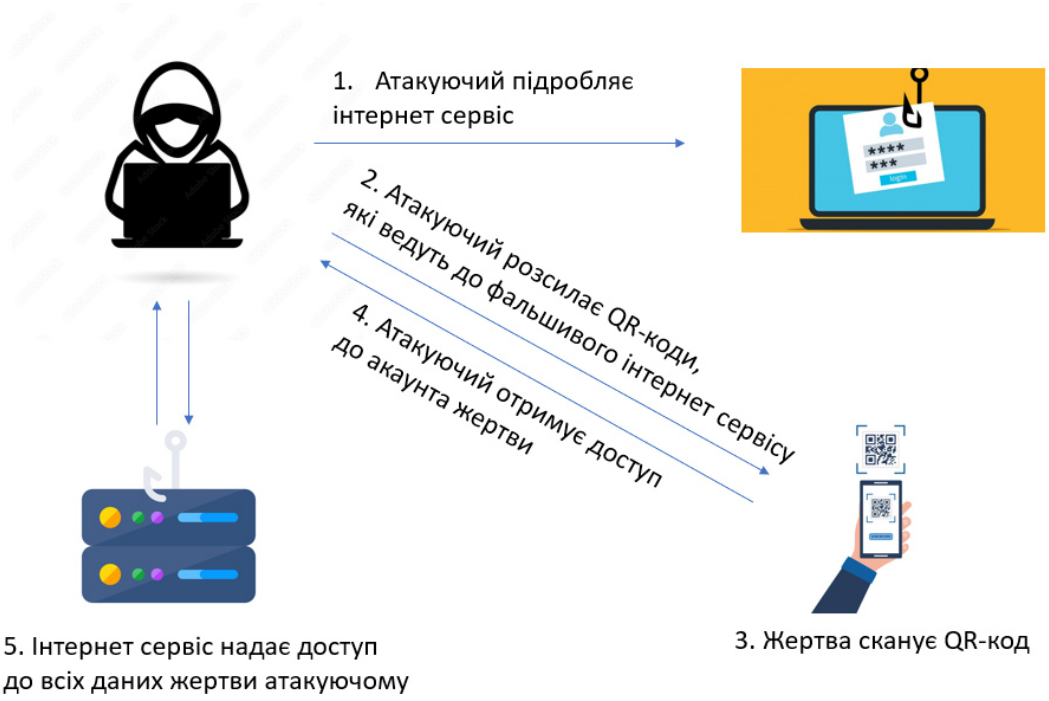

Рис.1. Фішингова атака із використанням QR-коду

QR-коди широко використовуються в різних галузях промисловості, спрощуючи процеси для торгівлі, розважальних закладів і ресторанів. Однак ця популярність не робить користувачів імунними до фішингових атак. Кіберзлочинці використовують QR-коди разом із обманливими повідомленнями, щоб змусити людей розголошувати конфіденційну та особисту інформацію. Підроблені QR-коди часто направляють жертв на фальшиві веб-сайти, де збираються конфіденційні дані, такі як номери кредитних карток. За допомогою цих викрадених даних хакери можуть отримати контроль над особою жертви і спричинити фінансовий хаос через несанкціоновані витрати з кредитної картки. Виявлення шкідливого QR-коду та захист від потенційних загроз надзвичайно важливі в цифровому середовищі.

Коли йдеться про QR-коди, важливо розрізняти їх різновиди, такі як фізичний QR-код та цифровий QR-код, оскільки обидва можуть бути використані в атаках фішингу, але мають свої особливості. Поговоримо про кожен з типів більш докладно.

Фізичний QR-код представляє собою візуальний штрихкод, який можна надрукувати чи нанести на поверхню. Такі QR-коди можуть бути підробленими чи розміщеними на несподіваних об’єктах, викликаючи замішання та підвищуючи ймовірність виникнення фішингових сценаріїв. У випадку фізичного QR-коду прикладом атаки є наклеювання підроблених кодів на фізичні об’єкти, такі як паркомати або продукти у магазинах.

Цифровий QR-код, навпаки, зберігається та розповсюджується в електронному форматі але також може бути розпізнаний за допомогою камери смартфона або іншого пристрою. Цифрові QR-коди можуть використовуватися на шахрайських інтернет сторінках, у смс-повідомленнях або в листах електронної пошти, що намагаються імітувати легітимні повідомлення від банків чи відомих компаній.

Особливості обох видів QR-кодів свідчать про необхідність пильності та обережності користувачів при взаємодії з ними, особливо в ситуаціях, де може виникнути підозра щодо їхнього походження чи наміру. Ось декілька аспектів, які варто врахувати для виявлення шахрайських QR-кодів [9]:

- перевірка джерела;
- перевірка URL-адреси;
- дизайн QR-коду;
- наявність механізму автентифікація;
- наявність запиту конфіденційної інформації;
- наявність надмірно щедрих пропозицій;
- використання програм сканування QR-кодів із вбудованими функціями захисту від фішингових атак;
- використання антивірусів та іншого корисного програмного забезпечення для захисту від шахрайства;
- регулярне оновлення програмного забезпечення безпеки;
- використання двухфакторної автентифікації.

Також слід підкреслити вразливість компаній та корпоративних спільноти до фішингових атак. Зростаюча поширеність шахрайства через QR-коди підкреслює критичну потребу компаній у посиленні свого захисту. Підсумовуючи, зручність QR-кодів не повинна приховувати постійну загрозу фішингових атак. Підприємства мають активно навчати свій персонал, створюючи пильну корпоративну спільноту, здатну вчасно розпізнавати та запобігати шахрайству. Шляхом навчання з кібербезпеки та використання спеціалізованого програмного забезпечення, організації можуть ефективно захищати себе від потенційних небезпек, забезпечуючи постійну безпеку своїх операцій та даних.

Як було зазначено вище, у QR-кодах найбільш поширеною формою інформації є веб-посилання, яке часто використовується для спрощеного доступу до веб-ресурсів. Також, у контексті кібербезпеки, важливо зауважити, що аналіз цього посилання є критичним етапом у виявленні можливих фішингових атак, оскільки саме воно приховує шкідливий вміст, спрямований на шахрайські цілі. При ретельному аналізі структури та джерела посилання, можливо виявити потенційно небезпечні QR-коди та запобігти їх шкідливому впливу.

Першим етапом на шляху до виявлення фішингових QR-кодів є декодування посилання та його подальший аналіз. Для виявлення потенційних вразливостей або ознак фальшивості, необхідно ретельно розглянути всі частини посилання, яке міститься в QR-коді. Цей процес включає дослідження протоколу передачі даних, доменних імен, шляху до ресурсу, параметрів запиту та інших метаданих.

Особливі ознаки у веб-посиланнях є ключовими компонентами аналізу. Ці параметри дозволяють виявляти певні відмінності та характеристики, які є типовими для підозрілих або потенційно шкідливих посилань.

У таблиці 1 наведено перелік особливих ознак посилання, обраних для методу виявлення фішингу.

Таблиця 1

Особливі ознаки посилання

Особливі ознаки адресної строки	Кількість двійних скісних рисок «//»
	Наявність IP-адреси безпосередньо у посиланні
	Наявність символу собака «@»
	Довжина посилання
	Наявність букв не латинського алфавіту
	Використання захищеного протоколу
Особливі ознаки домену	Кількість днів до закінчення терміну дії домена
	Кількість днів з моменту реєстрації домену
	Наявність піддомену

Перейдемо безпосередньо до алгоритмів машинного навчання. Машинне навчання може включати розробку моделі, яка навчається на певних тренувальних даних та використовується для обробки даних з метою передбачення результату. Для даної задачі будемо розглядати та порівнювати дві моделі машинного навчання: нейронні мережі та дерева рішень.

Наступний крок це аналіз тексту посилання за допомогою мовної моделі. Мовні моделі представляють собою складні математичні або комп'ютерні структури, що навчаються розуміти та генерувати мовленнєві зразки. Їхньою основною метою є розуміння мови, виявлення закономірностей у тексті та здатність створювати нові мовні вислови. Ці моделі базуються на великій кількості даних – текстах, документах, великих корпусах мовленнєвих матеріалів.

Головним поняттям при обробці природної мови є векторні відображення. Векторні відображення – це числові представлення слів або текстових фрагментів у векторному просторі. Сутність векторних відображень полягає в тому, що вони є словами чи текстом у формі, зрозумілими для комп’ютера, в якій відображена семантична та синтаксична інформація. Вектори відображення розташовані у таких просторах, де схожі слова або фрази розміщені близько одне до одного, відображаючи їхні семантичні відносини. Це дозволяє створити систему класифікації, яка здатна виявляти вирази або ключові ознаки, що вказують на можливу загрозу кібербезпеці.

Таким чином з тексту посилання ми отримуємо його числове представлення у вигляді вектору, який далі буде використовуватися як додаткові вхідні дані для алгоритму машинного навчання.

Блок-схема загального алгоритму виявлення фішингових QR-кодів представлена на рисунку 2.

Глибокий аналіз створеного методу виявлення фішингових QR-кодів спрямований на оцінку його ефективності. Він включає докладний аналіз результатів тестування, що охоплює точність та надійність новаторського підходу до виявлення підроблених QR-кодів. Мета цього аналізу – визначити потенційні можливості та обмеження запропонованого методу в контексті протидії фішинговим атакам.

Ефективність моделей у машинному навчанні, особливо в задачах бінарної класифікації, часто оцінюється за допомогою матриці помилок (Confusion Matrix). Ця матриця – ключовий інструмент для подальшої оцінки моделі, що дозволяє визначити різні показники, такі як точність, чутливість, специфічність та інші.

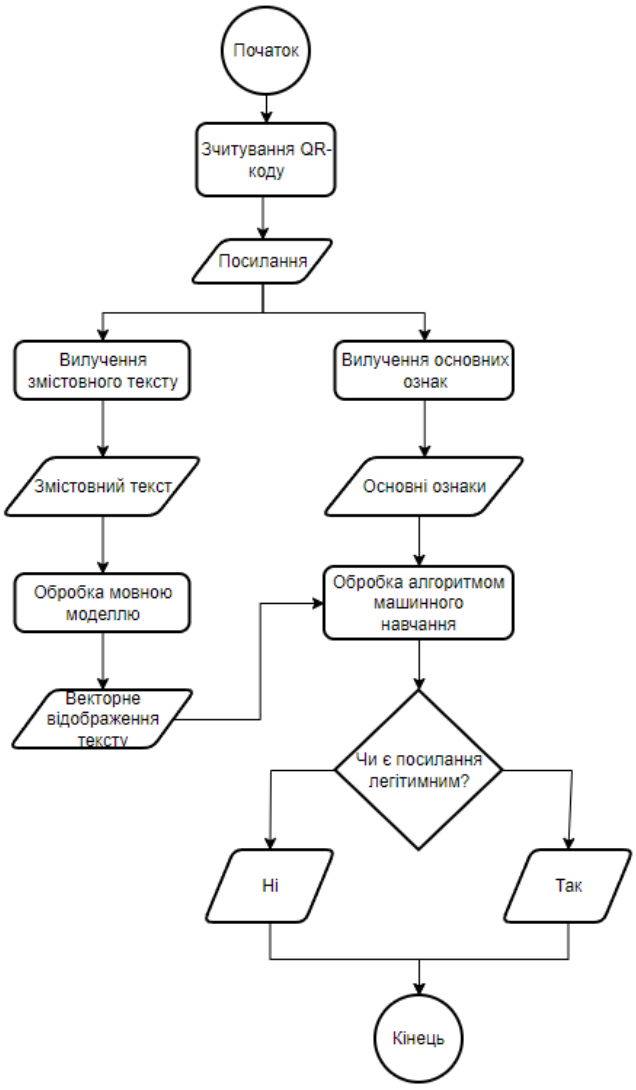

Рис.2. Блок-схема алгоритму аналізу QR-коду на предмет фішингу

Для обраних алгоритмів машинного навчання були розраховані матриці помилок, які у виді діаграм представлені на рисунку 3. Набір даних складався з 50000 посилань, з яких випадково обрані 70% були використані для тренування, а решта для тестування. Перші розрахунки були отримані лише з використанням аналізу особливих ознак посилання. При подальшій розробці алгоритму було

вирішено впровадити мовну модель, яка значно підвищила ефективність розпізнавання.

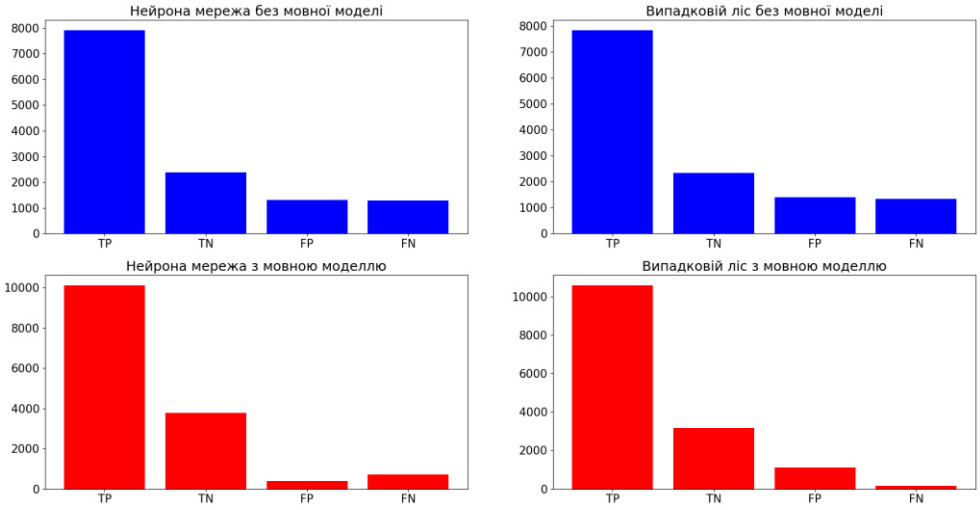

Рис.3. Діаграми значень матриці помилок

Отримавши матрицю помилок, ми переходимо до розрахунків ключових метрик ефективності моделі в бінарній класифікації. Зазвичай на основі цієї матриці визначаються такі показники, як [10]:

- точність (accuracy);
- влучність (precision);
- повнота (recall);
- специфічність (specificity);
- F-міра (F-score).

Кожен з цих показників відображає різні аспекти ефективності моделі в контексті конкретного завдання класифікації. Аналіз цих метрик надає глибше розуміння того, як добре модель пристосовується до розпізнавання певних класів, а також дозволяє здійснити порівняння з іншими моделями чи підходами до вирішення задачі.

Для розрахування цих метрик використовують наступні формули [10]:

$$Acurracy = \frac{TP + TN}{TP + TN + FP + FN},$$

$$Precision = \frac{TP}{TP + FP},$$

$$Recall = \frac{TP}{TP + FN},$$

$$Specificity = \frac{TN}{TN + FP}.$$

Після розрахунку основних метрик, таких як точність, влучність чутливість та специфічність, можна розрахувати F-міру (F-score). F-міра є комбінованою метрикою, що об’єднує влучність і чутливість моделі в одне числове значення. Формула розрахунку F-міри [10]:

$$F\text{-}score = 2 * \frac{Precision * Recall}{Precision + Recall}$$

Ця метрика надає комплексну оцінку ефективності моделі, враховуючи як правильність класифікації позитивних прикладів (чутливість), так і уникнення помилкових класифікацій позитивних та негативних прикладів (точність). Цей показник допомагає здійснити більш об’єктивне порівняння моделей та визначити їхню загальну ефективність у вирішенні задачі класифікації.

Для оцінки ефективності розробленого методу були побудовані графіки які відображають значення всіх вище перерахованих метрик ефективності. У рамках поставленої задачі розпізнавання фішингових QR-кодів ці графіки відображають порівняльну характеристику як алгоритмів машинного навчання так і самого методу до та після впровадження мовної моделі. Результати аналізу за метриками ефективності представлені на рисунку 4.

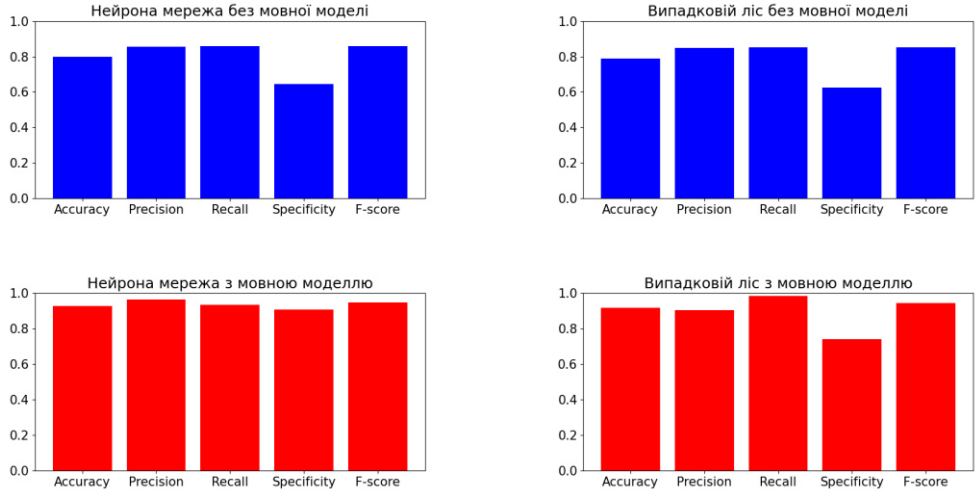

Рис.4. Діаграми значень метрик ефективності

Висновки. В роботі проведено аналіз фішингу та засобів для його виявлення та запобігання, а також надано важливе уявлення про загрозу, яку це питання складає у сучасному цифровому світі.

Розроблено метод виявлення фішингу в QR-кодах, який базується на аналізі особливих ознак посилання та його контенту з використанням технологій машинного навчання та мовних моделей. Проведено аналіз ефективності запропонованого методу. Отримані результати дають понад 90% точності у виявленні фішингових QR-кодів. Аналіз особливих ознак посилань, зокрема параметрів URL-адрес, структури посилання, структури домену тощо, дозволив створити модель, яка з високою точністю розпізнає потенційні фішингові посилання. Також, аналіз текстової інформації з QR-кодів за допомогою мовних моделей дав змогу виявити відмінності у способі побудови фішингових текстів посилання.

Отже, це дослідження має важливе теоретичне та практичне значення. Розроблений метод може бути використаний для покращення безпеки користувачів при взаємодії з QR-кодами, а також впроваджений у захисне програмне забезпечення мобільних пристроїв або сервісів, що виявляють потенційно шкідливі посилання та QR-коди.

Список літератури

1. Cloudav. 11 типов фишинга и их примеры из реальной жизни. URL: https://www.cloudav.ru/mediacenter/tips/types-of-phishing/
2. Mridha K., Hasan J., Ghosh A., Saravanan D. Phishing. URL Classification Analysis Using ANN Algorithm. *2021 IEEE 4th International Conference on Computing, Power and Communication Technologies* (GUCON) URL:https://www.researchgate.net/publication/355861339_Phishing_URL_Classification_Analysis_Using_ANN_Algorithm
3. Bouijij H., Berqia A. Machine Learning Algorithms Evaluation for Phishing URLs Classification. *2021 4th International Symposium on Advanced Electrical and Communication Technologies (ISAECT).*

URL:https://www.researchgate.net/publication/357813273_Machine_Learning_Algorithms_Evaluation_for_Phishing_URLs_Classification
4. Nagasunder R., Pawar B., Rao P. Detection of Phishing URL using Machine Learning. 2021. URL: https://norma.ncirl.ie/5100/1/nagasunderraopawarbaburaopawar.pdf
5. Termin. Фішинг — що це таке, суть, визначення, види та приклади фішингу. URL: https://termin.in.ua/fishynh/
6. Radiosvoboda. Соціальна інженерія: як шахраї використовують людську психологію в інтернеті. URL: https://www.radiosvoboda.org/a/socialna-inzhenerija-shaxrajstvo/29460139.html
7. Trendmicro. What Are the Different Types of Phishing. URL: https://www.trendmicro.com/en_us/what-is/phishing/types-of-phishing.html
8. Adlam S. Hidden Scams: Could QR Code Actually Be a Phishing Attack URL: https://gridinsoft.com/blogs/qr-code-phishing-attack/
9. Loyality company. How To Protect Your Business From QR Code Phishing Attacks. URL: https://www.linkedin.com/pulse/how-protect-your-business-from-qr-code-phishing-attacks/
10. Geeksforgeeks. Confusion Matrix in Machine Learning. URL: https://www.geeksforgeeks.org/confusion-matrix-machine-learning/

METHOD FOR DETECTING PHISHING QR CODES USING MACHINE LEARNING

A. Kasaiani, N. Kushnirenko, O. Troyanskiy, V. Podufalov

National Odesa Polytechnic University
1, Shevchenko Ave., Odesa, 65044, Ukraine
e-mail: infsec2011@gmail.com

Today, there are many tools that can detect and block malicious links that lead to phishing sites or malware. However, most of them are not yet capable of validating malicious QR codes, and this gives attackers the opportunity to actively use them in attacks. Phishing using QR codes is very similar to other forms of phishing. This attack aims to manipulate users and obtain personal information from them, such as login credentials or financial information. Essence of phishing using QR codes is not new. The main difference is that in this case, a QR code is used to redirect the victim to a malicious website. The purpose of this work is to increase the security of users in the digital environment by developing and implementing a method for detecting phishing QR codes using machine learning. The work analyzed the methods and means of countering phishing and attacks through QR codes, which made it possible to determine the directions of development and the main tasks of the research. Developed method includes the analysis of special features of the link and its text using a language model, on the basis of which the machine learning algorithm was trained and tested. The created method of detecting phishing QR codes significantly increases the safety of users in the use of QR codes. Analysis of the effectiveness of the developed method showed a result of more than 90% detection accuracy. The method of detecting phishing QR codes, developed within the framework of this work, can be successfully implemented in the activities of various organizations, including enterprises and institutions. This method provides an opportunity to reduce the risks of phishing attacks through QR codes, resulting in increased security for employees. The results of this work can be used in further research, development in the field of cyber security and combating phishing attacks through QR codes.

Keywords: phishing, QR code, machine learning, cybersecurity, language model.