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

«До захисту допущено»
В.о. завідувача кафедри

_____ М.В.Грайворонський
(підпис)
“_____”_____2019 р.

Дипломна робота

на здобуття ступеня бакалавра

з напряму підготовки 6.170101 «Безпека інформаційних і комунікаційних систем»
на тему: Розпізнавання фішингових сайтів з використанням методів машинного навчання

_____

_____

Виконав (-ла): студент (-ка) 4 курсу, групи ФБ-51
(шифр групи)

Тернопольська Світлана Олександрівна
(прізвище, ім’я, по батькові) (підпис)

Керівник доцент Стьопочкіна І.В.
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Консультант _____ _____ _____
(назва розділу) (посада, вчене звання, науковий ступінь, прізвище, ініціали) (підпис)

Рецензент к.т.н., доц., доцент Жданова О.Г.
(посада, науковий ступінь, вчене звання, науковий ступінь, прізвище та ініціали) (підпис)

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.
Студент _____
(підпис)

Київ - 2019 року

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

Рівень вищої освіти – перший (бакалаврський)

Напрям підготовки 6.170101 «Безпека інформаційних і комунікаційних систем»

ЗАТВЕРДЖУЮ
В.о. завідувача кафедри
_____ М.В.Грайворонський
(підпис)
«___»_____2019 р.

ЗАВДАННЯ
на дипломну роботу студенту

Тернопольській Світлані Олександрівні
(прізвище, ім'я, по батькові)

1. Тема роботи: Розпізнавання фішингових сайтів з використаням методів машинного навчання,
науковий керівник роботи: Стьопочкіна Ірина Валеріївна, доцент,
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від «27» травня 2019 р. № 1414-с

2. Термін подання студентом роботи 10 червня 2019 р.

3. Вихідні дані до роботи

1. Попередні дослідження.
2. Програма роботи з даними WEKA.
3. Датасет з характеристиками.

4. Зміст роботи

1. Вивчити різні підходи до виявлення фішингових сайтів.
2. Відібрати характеристики, які можуть бути індикаторами того, що сайт є фішинговим.
3. Визначити ступінь важливості та інформативності даних характеристик при виявленні фішингових сайтів.
4. Проаналізувати, які алгоритми класифікації є найбільш придатними для розв'язання задачі розпізнавання фішингового сайту; розробити

відповідне програмне забезпечення та здійснити експериментальне дослідження.

5. За вибраними алгоритмами та результатами дослідження побудувати більш досконалу модель розпізнавання фішингового сайту.

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

Розпізнавання фішингових сайтів – презентація.

6. Дата видачі завдання 10.10.2019

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів дипломної роботи	Примітка
1	Отримання завдання	10.10.2019	
2	Збір інформації	01.02.2019	
3	Дослідження предметної області та існуючих рішень	10.04.2019	
4	Розробка плану роботи	15.04.2019	
5	Проведення експерименту з відбору характеристик	10.05.2019	
6	Проведення дослідження нової моделі класифікації	18.05.2019	
7	Оцінка результатів	23.05.2019	
8	Оформлення дипломної роботи	26.05.2019	
9	Отримання допуску до захисту	28.05.2019	

Студентка _____ Тернопольська С.О.
(підпис) (ініціали, прізвище)

Науковий керівник роботи _____ Стьопочкіна І.В.
(підпис) (ініціали, прізвище)

РЕФЕРАТ

Дана робота містить 67 сторінок, 22 ілюстрації, 21 таблицю, 24 джерела за переліком посилань.

Фішинг - це серйозна проблема безпеки в мережі, яка полягає в підробці справжніх веб-сайтів, щоб обдурити користувачів в Інтернеті і вкрасти їх конфіденційну інформацію. Задачу розпізнавання фішингових сайтів можна розглядати як типову проблему класифікації в інтелектуальному аналізі даних, коли класифікатор будується на певному наборі характеристик сайту. Існують суворі вимоги до визначення найкращого набору характеристик, які при правильному виборі підвищують точність прогнозування класифікаторів. У даній роботі досліджується вибір характеристик з метою визначення ефективного піднабору з точки зору точності класифікації, а так само дослідження точності розпізнавання фішингу новою схемою класифікатора побудованого на кількох стандартних. Порівнюються 3 відомі функції відбору ознак, щоб визначити найменший і точний набір функцій виявлення фішингу з використанням інтелектуального аналізу даних. Також розглядаються 6 алгоритмів класифікації даних: Naive Bayes, Decision Tree, Neural Network, Logistic Regression, k-nearest neighbours, Support Vector Machine. Експериментальні тести с відбором ознак були виконані з використанням методів Wrapper subset evaluation, Consistency subset evaluation і Correlation-based feature subset evaluation. Шість вишеперерахованих алгоритмів машинного навчання були треновані з різним набором характеристик, щоб показати переваги та недоліки процесу відбору функцій. Вдалося виявити кілька груп ознак з однаково хорошою точністю класифікації і відібрати 3 алгоритми із запропонованих шести для побудови нової схеми класифікації.

Ключові слова: соціальна інженерія, фішинг, фішинговий сайт, розпізнавання фішингових сайтів, відбір характеристик, класифікація, машинне навчання.

ABSTRACT

This work contains 67 pages, 22 illustrations, 21 tables, 24 sources in the list of links.

Phishing is a serious security problem on the Internet, which is considered as fake legitimate websites to deceive users on the Internet and steal their private information. Detection phishing websites can be considered as a typical classification problem in data mining, when the classifier is built on a specific set of website features. There are strict requirements for determining the best set of features, which, if chosen correctly, increase the accuracy of prediction of classifiers. This paper explores feature selection in order to determine the most effective subset from the point of view of classification accuracy, as well as research on the accuracy of phishing recognition with a new classifier scheme built on several standard ones. Three known feature selection methods are compared to determine the smallest and the most accurate phishing detection feature set using data mining. Here is also discussed 6 data classification algorithms: Naive Bayes, Decision Tree, Neural Network, Logistic Regression, k-nearest neighbors, Support Vector Machine. Experimental tests with feature selection were performed using the Wrapper subset evaluation, Consistency subset evaluation and Correlation-based feature subset evaluation methods. The six machine learning algorithms listed above were trained with a different set of features to show the advantages and disadvantages of the feature selection process. It was possible to find several groups of features with equally good classification accuracy and select 3 algorithms, from the six proposed, to build a new classification scheme.

Keywords: social engineering, phishing, phishing site, phishing website detection, feature selection, classification, machine learning.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

APWG	Anti-phishing working group, сервіс боротьби з фішингом
J48	Decision tree J48, дерево прийняття рішень J48
kNN	k-nearest neighbors, К найближчих сусідів
LR	Logistic regression, логістична регресія
MITB	Man in the browser, атака зловмисник в браузері
NB	Naïve Bayes, наївний Байєсівський метод
NN	Neural network, нейронна мережа
SMO	Sequential minimal optimization, послідовна мінімальна оптимізація

ВСТУП

Проблема атак соціальної інженерії в Інтернеті з кожним роком стає все більш розповсюдженою. Якщо говорити про організації, що мають конфіденційну інформацію таку як дані клієнтів, дані про співробітників, власні розробки, документацію і т.д., то з великою впевненістю можна сказати про те, що маючи захищену комп`ютерну систему всередині організації, не всі турбуються про витік інформації через своїх співробітників, а ті або через незнання або через неуважність стають жертвами соціальної інженерії.

У цій роботі буде розглянуто певний вид соціальної інженерії, який називається фішинг. Фішинг – це атака на основі соціальної інженерії, яка здійснюється через недоліки в кібербезпеки для обману користувачів з метою крадіжки їх логінів, паролів і грошових коштів. Техніки фішингу досить численні і складні, серед яких такі, які передбачають перехід за посиланням на зловмисний сайт.

Актуальність роботи

Оскільки фішинг є досить розповсюдженим явищем, то від нього потерпають як і підприємства так і звичайні люди, методи захисту від фішингу не є досконалими і завжди актуальним є пошук нових рішень в цій сфері. Мій пошук відбувається у сфері машинного аналізу даних, де все ще не існує досконалого, що означає точного і швидкого, алгоритму розпізнавання фішингових сайтів.

Мета і завдання дослідження

Метою дослідження є аналіз актуальних методів класифікації даних та відбору характеристик, притаманних фішинговим сайтам, побудова більш досконалої моделі класифікатора для розпізнавання фішингових сайтів, що буде прогнозувати з більш високою точністю чи є сайт фішинговим. Цей класифікатор буде тренований на знайденому піднаборі характеристик, які відібрані із загального списку.

Завдання дослідження:

1) вивчити різні підходи до виявлення фішингових сайтів.

2) відібрати характеристики, які можуть бути індикаторами того, що сайт є фішинговим;
3) визначити ступінь важливості та інформативності даних характеристик при виявленні фішингових сайтів.
4) проаналізувати, які алгоритми класифікації є найбільш придатними для розв'язання задачі розпізнавання фішингового сайту; розробити відповідне програмне забезпечення та здійснити експериментальне дослідження.
5) за вибраними алгоритмами та результатами дослідження побудувати більш досконалу модель розпізнавання фішингового сайту.

Об'єкт дослідження – фішингові сайти.

Предмет дослідження – методи машинного навчання для розпізнавання фішингових сайтів.

Наукова новизна одержаних результатів

В роботі запропоновано нову модель класифікації даних, яка є комбінацією декількох вже відомих та досить розповсюджених класифікаторів, це зроблено задля підвищення точності розпізнавання, а також сформовано набір характеристик, який є меншим за початковий, що збільшує швидкодію розпізнавання, при забезпеченні високого рівня точності.

Практичне значення одержаних результатів

Отриманий класифікатор є прототипом для подальшого створення програмних рішень для розпізнавання фішингових сайтів. Він, а також набір характеристик може бути впроваджений у антифішингові розширення для браузерів або інші інструменти боротьби з фішингом.

1 ФІШИНГ

1.1 Проблема фішингу

Виявлення фішингових сайтів надзвичайно складна і часозатратна проблема, що включає в себе багато різних факторів а критеріїв. На сьогоднішній день через високий рівень користування інтернетом через смартфон більшість комерційних та фінансових послуг надається сам через інтернет. Незважаючи на те, що інтернет забезпечує функціональну платформу для фінансових транзакцій користувачів, в той же час це не є абсолютно безпечним способом. Викрадення інформації або фішинг поширена проблема захисту інформації, що виконується через надсилання спаму або підроблених електронних листів. Цей тип атак передбачає отримання користувачем обманного листа, у якому міститься посилання на зловмисний веб-сайт, що в свою чергу призначений для збору інформації та персональних даних користувача. Фішингові атаки основані на розсиланні спаму – один з головних бар'єрів для розширення фінансової діяльності в інтернеті, що провокує великі збитки для фінансових та кредитних установ кожного року. Аналіз розсилки спаму та фішингових атак показує наявність деякого шаблону проведення атаки, але його складно розпізнати з першого погляду. Знаходження прихованих шаблонів фішингових атак є ефективним методом при розробці програмного забезпечення для запобігання атакам цього типу. Існує багато методів збору даних для вилучення потрібної інформації з різних невпорядкованих даних. Ця наука використовує різноманітні набори утиліт для збору даних, для аналізу даних, отриманих від попередніх атак щоб ідентифікувати типові шаблони атак і запобігти майбутнім вторгненням.

За останнє десятиліття кількість користувачів інтернету зросла в рази і продовжує зростати. Одна з причин такого зростання – це смартфони, вони дозволяють легко отримати доступ в інтернет, окрім інших переваг. У сучасному світі різні покоління смартфонів стають все більш популярними і поширеними, і використання інтернет протоколів стало невід'ємною частиною життя мільйонів

людей по всьому світу. З іншого боку, фінансові та бізнес-організації, банки, онлайн-магазини використовують інтернет платформи для надання своїх послуг. Проведення фінансових транзакцій через інтернет має ряд переваг, які включають в себе скорочення трафіку, зменшення забруднення повітря, економію часу і грошей і т.д. Однак, не дивлячись на всі переваги використання інтернет ресурсів для фінансових транзакцій і інтернет покупок, на жаль деякі користувачі можуть наражати на небезпеку фінансові операції інших і обманювати їх через фішингові атаки для крадіжки цінної інформації. Як багато користувачів використовують інтернет для розваги, так багато хто використовує для отримання грошей, помсти або розважаються, показуючи свої навички інтернет-обману. Таких людей називають хакери, крякери, зловмисники і т.п. Інтернет безпека – один з проломів в безпеці комп'ютерних систем. Крадіжка інформації або фішинг категоризується в сфері інформаційної безпеки. На сьогоднішній день, використання електронної пошти стало невід'ємною частиною життя, воно включає в себе офіційну, фінансову або особисту переписку. Поки такі кошти як електронна пошта має велику кількість функцій вони відіграють значну роль у крадіжці призначених для користувача даних. Один з типів електронних листів з якими користувачі стикаються майже щодня – спам-листи використовуються фішерами або хакерами для досягнення цілей таких як крадіжка інформації або реклама. Спам може розглядатися як засіб обману інтернет-користувачів в якому зловмисник представляється довіреною особою від організації або обіцяє виграш у лотереї або будь-який інший трюк, що змушує користувача перейти на підроблений сайт і ввести особисту інформацію у відповідне поле. Ретельний аналіз змісту цих листів або інтернет спаму показує що зловмисники використовують усталений поведінковий шаблон в написанні електронних листів згідно з яким вони рясніють граматичними помилками або часто зустрічаються такі слова як «допомога», «виграш», «віза» і т.п. Дані та інформація представлені в спамі і листах відправлених фішерами дають розуміння, яке потрібне для розпізнавання таких атак, старанний аналіз яких призведе до розвитку утиліт безпеки. Інтелектуальний аналіз даних – один з важливих методів для отримання прихованих шаблонів і

корисної інформації з величезної кількості невпорядкованих даних. Інтелектуальний аналіз даних включає різноманітні техніки для знаходження корисної інформації, такі як кластеризація, класифікація, дерево рішень, мережа Байєса, штучна нейронна мережа і машинне навчання.

1.2 Визначення «фішингу»

Фішинг – це атака на основі соціальної інженерії, яка здійснюється через слабкості в кібербезпеці для обману користувачів з метою крадіжки їх логінів, паролів і грошових коштів. Техніки фішингу досить численні і складні, серед яких такі, які спонукають користувача перейти за посиланням на зловмисний сайт. Не існує універсального визначення фішингу та досі їх існує велика кількість. Кількість і різноманітність визначень фішингу вказує на складність цього типу атак.

Згідно з сервісом PhishTank Company: фішинг – це спроба вкрасти інформацію про людину, використовуючи електронну пошту. Іноді фішингові атаки посилаються на сайти, які є підробкою реальних сайтів організацій, банків і у користувача складається враження, що він потрапив на реальний сайт цієї організації. [1]

Визначення від PhishTank покриває велику частину сценаріїв фішингових атак, але не завжди вірне. Це визначення обмежує фішингові атаки тільки крадіжкою персональних даних, а це не завжди так. Наприклад, зловмисник провокує жертву встановити шкідливу програму для атаки Man in the Browser (MITB), яка призводить до переказу грошей на банківський рахунок атакуючого, коли жертва авторизується в своєму банківському обліковому записі. Це все відбувається без отримання персональної інформації. Таким чином визначення від сервісу PhishTank не достатньо широко розкриває зміст поняття «фішинг».

Інше визначення звучить так: «Під фішинговою сторінкою розуміється будь-яка веб-сторінка, яка без дозволу заявляє, що діє від імені третьої сторони з метою

збити з пантелику користувачів в скоєнні дії, яку користувач може довіряти тільки справжньому агенту третьої сторони.» [2]

Це визначення є більш широким ніж попереднє в тому сенсі що мета зловмисника тепер не обмежена тільки крадіжкою персональної інформації. Але з іншого боку, це визначення обмежує фішингову атаку як таку, що діє завжди від імені третьої сторони. Наприклад, та ж зловмисна програма MITB, яку користувач встановить через перехід за безпечним посиланням (як йому здається) на свій комп'ютер під впливом фішера(це може бути, навіть, сайт з фільмами), може логуватися введення з клавіатури з метою крадіжки паролів. У цьому випадку атакуючий не стверджує що є 3-й стороною, а просто розсилає посилання на сайт.

Сервіс Anti-Phishing Working Group (APWG) описує фішинг як кримінальний механізм, який використовує як соціальну інженерію, так і технічні прийоми для крадіжки особистих даних користувачів і облікових даних фінансових рахунків. У схемах соціальної інженерії використовуються підроблені електронні листи, призначені для отримання повідомлень від законних підприємств і агентств, а так само для того, щоб змусити споживачів підробляти веб-сайти, які обманюють одержувачів в розголошенні фінансових даних, таких як імена користувачів і паролі. Схеми технічних прийомів впроваджують кримінальне програмне забезпечення на ПК для прямої крадіжки облікових даних, часто використовуючи системи для перехоплення імен користувачів і паролів в онлайн-акаунтах користувачів, а також для пошкодження локальної навігаційної інфраструктури, щоб дезорієнтувати споживачів на підроблених веб-сайтах (або автентичні веб-сайти через проксі-сервери, контрольовані фішером, використовувані для моніторингу і перехоплення натискань клавіш користувачами). [3]

Виходячи з усіх перерахованих вище визначень можна сказати що, по-перше, фішингова атака може відбуватися з будь-якого електронного каналу зв'язку, по-друге, атакуючий переконує жертву вчинити дії, і, по-третє, атакуючий отримує від цього особисту вигоду.

Таким чином формулювання поняття «фішинг» звучить так:

Фішинг - це комп'ютерна атака, яка передає людям повідомлення соціальної інженерії через електронні канали зв'язку, щоб переконати їх виконати певні дії в інтересах зловмисника.

1.3 Механізм фішингу

Механізм фішингу продемонстрований на рисунку 1.1.

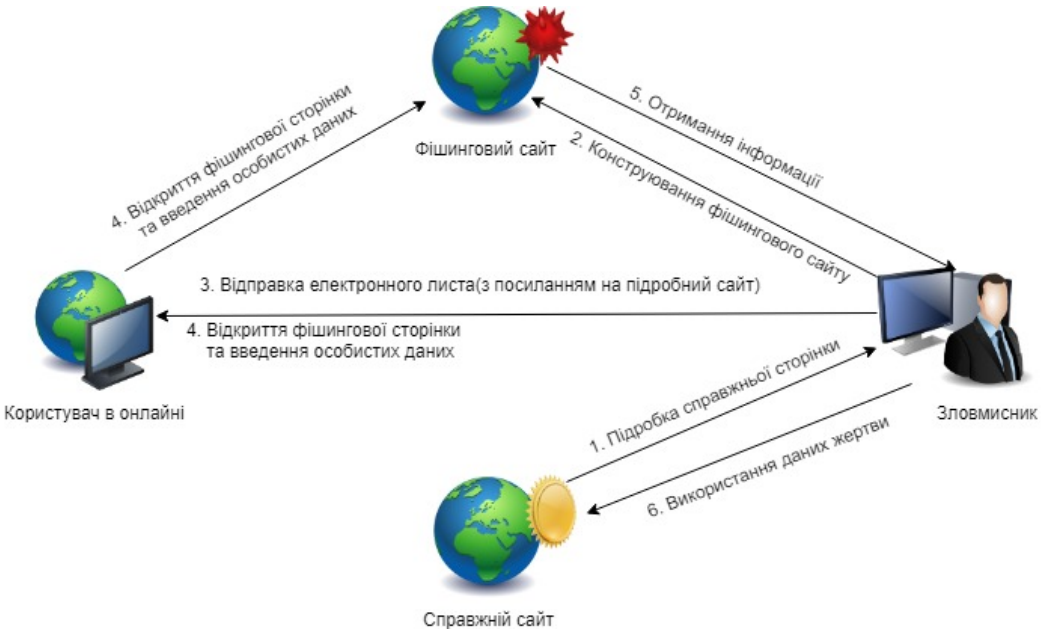

Рисунок 1.1 – Механізм фішингу

Підроблений сайт, який є майже точною копією справжнього завжди має поле для введення даних. Коли користувач вводить туди свої персональні дані і підтверджує дію, то ці дані відправляються прямо зловмисникові. Далі фішер витягує з них потрібні йому і використовує в своїх цілях.

Насамперед атакуючий збирає дані про організацію яку збирається підробляти. Він збирає детальну інформацію на сайті організації і потім використовує її щоб створити підробний сайт.

Другий крок атаки - це складання підробного електронного листа. До листа зловмисник прикріплює посилання на фішинговий сайт і розсилає його тисячам користувачів. У тому випадку якщо йде цілеспрямований фішинг, то розсилка іде кільком людям. Поширення шкідливого посилання відбувається не тільки за допомогою електронної пошти, для цього так само підходять блоги, форуми тощо.

Коли користувач відкриває підроблений сайт, він бачить на ньому форму для введення, теж підроблену, найчастіше його просять ввести свої логін і пароль. Він їх вводить, підтверджує і після цього зловмисник отримує доступ до даних жертви.

В кінцевому рахунку фішер використовує дані користувача в злочинних цілях, це може бути або крадіжка особистості, або використання кредитної картки для покупок тощо.

1.4 Життєвий цикл фішингових атак

Дослідження життєвого циклу фішингових атак може бути використано для розробки технік протидії фішингу. На рисунку 1.2 зображена блок-схема життєвого циклу фішингових атак.

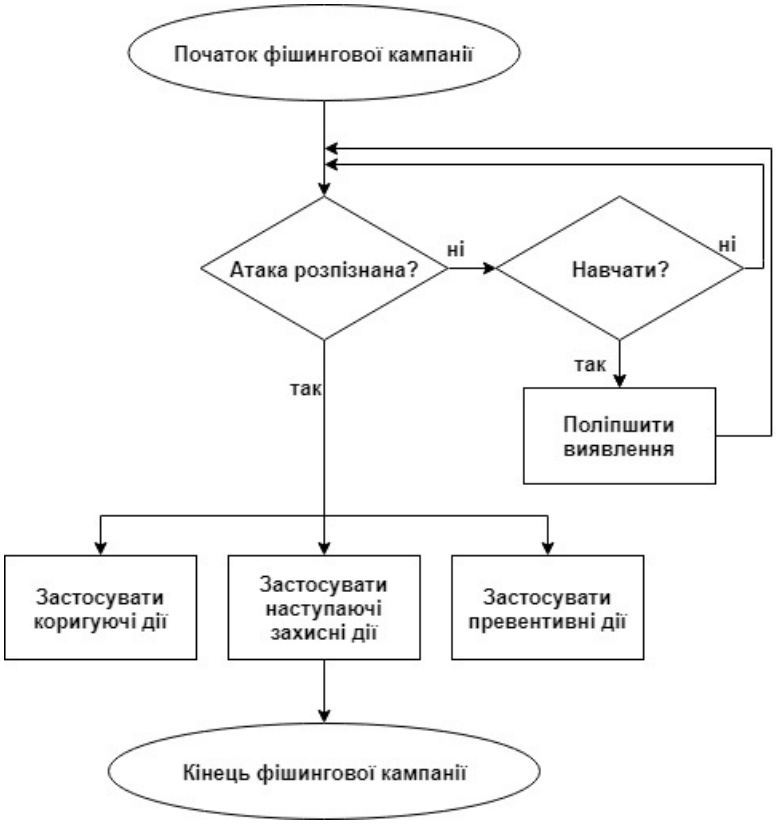

Рисунок 1.2 – Життєвий цикл фішинг-атаки

Коли фішингова атака тільки починається першим кроком до протидії є її виявлення. У виявленні фішингових атак існує 2 підходи: клієнтське програмне забезпечення кінцевого користувача і програми інформування користувачів. Здатність розпізнавати атаки вдосконалюється з часом шляхом навчання, це

навчання може бути проведено або за допомогою користувачів, або алгоритмами машинного навчання. Після виявлення атаки, є кілька шляхів протидії.

- Наступальний захист: в цьому випадку жертва фішингової атаки атакуватиме компанію, що запустила початкову атаку. Цей підхід частково корисний користувачам які вже відправили свої персональні дані зловмисникові.
- Корекція: в даному випадку користувач повідомляє про відповідний хостинг і видаляє сліди і файли, що залишилися після фішинг-атаки.
- Запобіжні заходи: в цьому підході користувач робить дії спрямовані на запобігання даних атак в майбутньому.

Всі перераховані вище методи працюють тільки якщо атака виявлена. Життєвий цикл фішингових атак має 3 етапи: ранній етап, середній етап і після фішінговий етап. На ранньому етапі фішер готується до атаки і складає повідомлення, яке розсилає жертвам. На середньому етапі жертви отримують обманні повідомлення і розкривають персональні дані і цінну інформацію. В кінцевому рахунку, на третій стадії крадіжка інформації здійснена. [4]

1.5 Види фішингу

1) *Spear phishing(направлений фішинг)*: цей вид фішингу має конкретного одержувача, групу одержувачів або організацію. Для виконання такої атаки фішер повинен зібрати якомога більше інформації про свої цілі, це може бути заплановане відрядження або замовлення з інтернет-магазину. Цільові атаки мають великий успіх, тому що вони ретельно підготовлені.

2) *Whaling*: атака націлена на керівника підприємства. Інформація від керівника буде завжди більш цінною ніж від звичайного співробітника. В даному випадку підроблений сайт має велику важливість, оскільки представляє певного клієнта організації. Найчастіше фішингових лист складається як суперечність з клієнтом або офіційна проблема, і має виглядати як справжнє бізнес-листування.

Атака адаптована для більш обмеженого застосування і найчастіше включає в себе деякі викривлені далекоглядні проблеми.

3) *Business email compromise(BEC)*: атака націлена на співробітників бухгалтерії і відділу фінансів, за допомогою шахрайських дій та з використанням електронної пошти, а також шахрайства з електронною поштою директора. Видаючи себе за значущих людей в компанії, начальника відділу або того ж генерального директора зловмисник провокує співробітників переводити гроші на несанкціоновані рахунки. Як правило, зловмисники компрометують обліковий запис електронної пошти керівника або фінансового директора, використовуючи різні методи. Зловмисник переховується і відстежує дії електронної пошти керівника протягом певного періоду часу, щоб дізнатися про процеси та процедури в компанії. Фактична атака приймає форму помилкового електронного листа, який виглядає так, як ніби воно прийшло з аккаунта керівника(скомпрометованого), відправленого тому, хто є постійним одержувачем. Лист здається важливим і терміновим, і він вимагає, щоб одержувач відправив банківський переказ на зовнішній або незнайомий банківський рахунок. Гроші в кінці-кінців потрапляють на банківський рахунок зловмисника.

4) *Clone phishing(фішинг-клонування)*: тип атаки при якій фішер клонує вихідне повідомлення, але вкладене в нього посилання замінює на зловмисне. Для цього використовується раніше перехоплене повідомлення і за шаблоном створюється точно таке ж, підробляється відправник. Можливо буде потрібно пояснення чому користувач отримав друге таке саме повідомлення, як правило такою причиною може бути повторна відправка оригіналу або оновлена версія.

5) *Gaming(ігроманія)*: ігри стали невід'ємною і поширеною частиною людського взаємодії. У Symatec провели оцінку ігрового простору і виявили, що 13% орієнтовані на застосунки. Ігри в яких відбувається комунікація гравців, як правило вимагають внесення кредитів для просування по рейтингу і використання деяких функцій. Кредити маються на увазі онлайн внески. Фішингові сайти ловлять клієнтів, пропонуючи неправдиві пропозиції безкоштовних кредитів, орієнтованих на ці ігрові програми.

6) *Live chat*: жертва вводиться в оману запрошенням в живий чат, наприклад на сайтах часто пропонують чат підтримки або питань, чат доданий зловмисником. Цей тип фішингу в основному відбувається на веб-сайті онлайн-банкінгу, де жертва відкриває підроблене вікно чату підтримки в реальному часі на сайті онлайн-банкінгу. Це додає сайту «реальності» і передбачає розкриття конфіденційної інформації жертвою.

7) *Vishing(телефонний фішинг)*: має на увазі використання телефону. Як правило, жертва отримує дзвінок з голосовим повідомленням, замаскованим під повідомлення від фінансової установи. Наприклад, повідомлення може попросити одержувача зателефонувати за номером і ввести дані свого облікового запису або PIN-код в цілях безпеки або в інших офіційних цілях. Проте, телефонний номер дзвонить прямо зловмисникові через службу передачі голосу по IP. Останнім часом злочинці стали дзвонити жертвам, прикидаючись технічною підтримкою Apple і надаючи користувачам номер для дзвінка, щоб вирішити «проблему безпеки».

8) *Pharming*: кібератака, призначена для перенаправлення трафіку сайту на інший, підроблений, сайт. Фармінг може проводитися або шляхом зміни файлу hosts на комп'ютері жертви, або шляхом використання вразливості в програмному забезпеченні DNS-сервера. DNS-сервери – це комп'ютери, що відповідають за перетворення імен Інтернету в їх реальні IP-адреси. Скомпрометовані DNS-сервери іноді називають «отруєними». Фармінг вимагає незахищеного доступу до цільового комп'ютера, наприклад, до зміни домашнього комп'ютера клієнта, а не корпоративного бізнес-сервера.

Вищенаведений перелік типів атак описаний згідно роботі [5].

1.6 Мотивація та мета фішингових атак

Головними мотивами зловмисників, що здійснюють фішингові атаки є [6]:

1. Отримання грошей: в цьому випадку, атакуючий намагається їх вкрасти з таких установ як банки або рахунки клієнтів

2. Приховати свою особу: деяким зловмисникам потрібно приховати свою особистість щоб довести до кінця згубні дії. Тому вони використовують вкрадені логіни і паролі і з їх допомогою намагаються приховати свою особистість під час інтернет-покупок, ігроманії, ображання дітей тощо.
3. Слава: багато користувачів використовують фішинг щоб домогтися популярності в кіберпросторі.

1.7 Статистика фішингових атак

Згідно зі звітом від сервісу Anti-Phishing Working Group(APWG) [3] за перший квартал 2019 року відсоток фішингу, націленого на Software-as-a-Service (SaaS) і послуги електронної пошти (Webmail), підскочив до 36% від усіх фішингових атак. Це значно вище, ніж в 4 кварталі 2018 року, де ця область становила всього 30% і 20,1% в 3 кварталі 2018 року. Фішинг в області SaaS і Webmail став найпоширенішим за цей період часу, вперше перевершивши фішинг в області платіжних послуг (payment).

Відсоток атак на хмарні сховища і сайти з файловими хостингами продовжував знижуватися, знизившись з 11,3% всіх атак в першому кварталі 2018 року до всього лише 2% в першому кварталі 2019 року. Більш наочно статистика продемонстрована на рисунку 1.3.

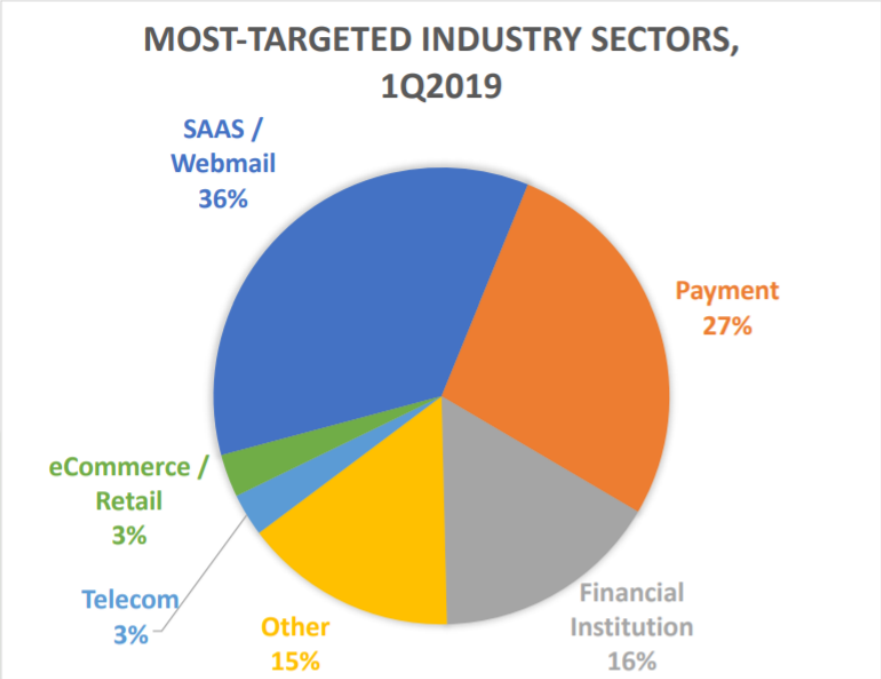

Рисунок 1.3 – Найбільш цільові галузі промисловості у 1 кварталі 2019 року

Загальна кількість фішингових сайтів, виявлених APWG в 1 кварталі, склало 180,768. Це було помітно в порівнянні з 138,328, зафіксованими в 4 кварталі 2018 року, і з 151,014, зафіксованими в 3 кварталі 2018 року. Дані представлені на рисунку 1.4.

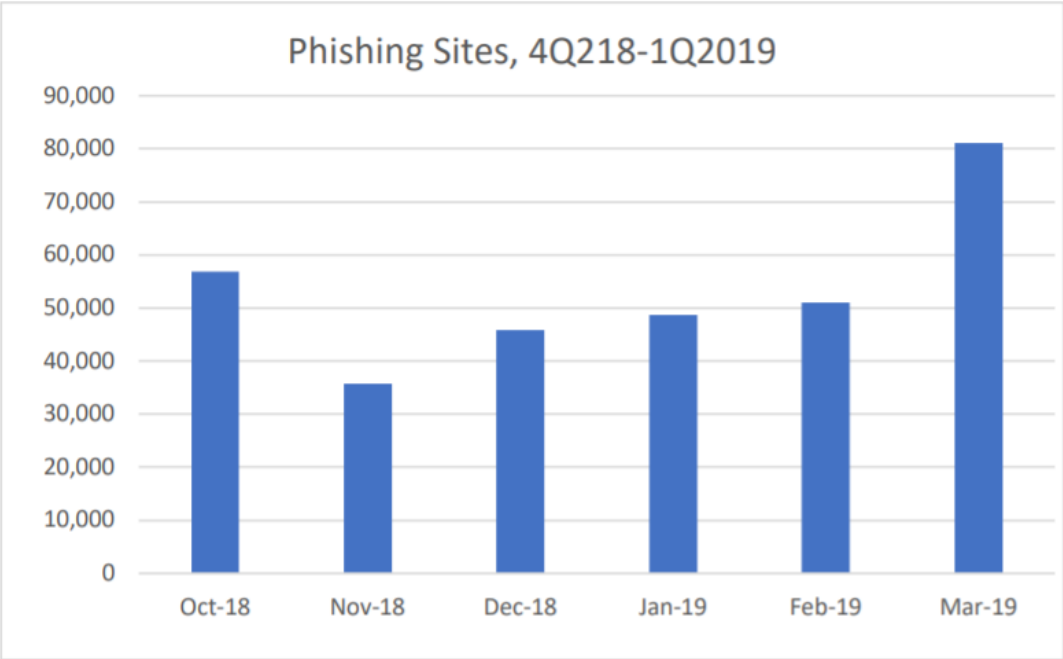

Рисунок 1.4 – Кількість фішингових сайтів за кінець 2018 і початок 2019

Учасник APWG PhishLabs відстежує кількість фішингових сайтів, захищених протоколом шифрування HTTPS. HTTPS особливо важливий на сайтах, які

пропонують онлайн-продажу або захищені паролем облікові записи. Вивчення HTTP на фішингових сайтах дає уявлення про те, як фішери обманюють інтернет-користувачів, налаштовуючи проти них функцію інтернет-безпеки (зазвичай за допомогою значка блокування протоколу HTTPS в адресному рядку браузера, щоб гарантувати користувачам, що сам домен «безпечний»). PhishLabs надає керовані служби безпеки, які допомагають організаціям захищатися від фішингових атак, спрямованих на їх співробітників і клієнтів.

«У першому кварталі 2019 року 58% фішингових сайтів використовували SSL-сертифікати, що значно більше в порівнянні з попереднім кварталом, де лише 46% використовували сертифікати», - сказав Джон Лакур, технічний директор PhishLabs. «Є дві причини, за якими ми бачимо більше. Зловмисники можуть легко створювати безкоштовні сертифікати DV (domain validated), і більше веб-сайтів використовують SSL в цілому. Все більше сайтів використовують SSL, тому що браузер попереджає користувачів, коли SSL не використовується. І велика частина фішингу розміщується на зламаних, законних сайтах». Більш детальна статистика зображена на рисунку 1.5.

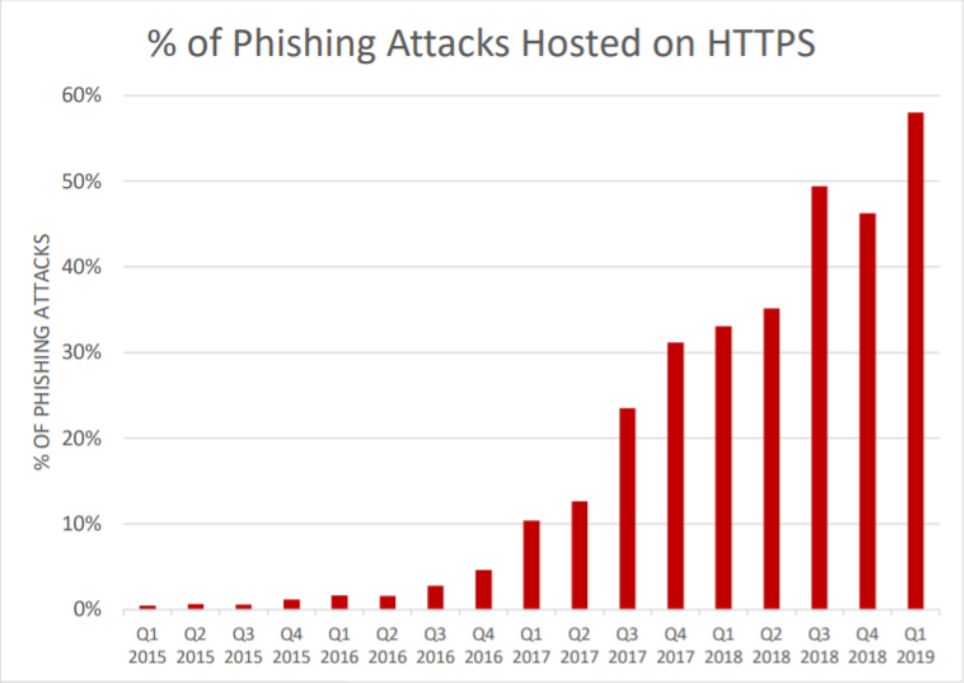

Рисунок 1.5 – Відсоток фішингових атак на HTTPS

Висновки з розділу 1

Дослідження фішингу як явища показало що це дуже розвинута область соціальної інженерії, оскільки фішинг має багато різновидів це: spear phishing, whaling, vishing, business email compromise, clone phishing, gaming, live chat, pharming. Фішинг застосовують у таких галузях як електронна пошта, прикладне програмне забезпечення, платіжні сервіси, фінансові установи тощо. Порівняно з 2018 роком відсоток фішингових атак у галузі електронної пошти помітно збільшився. Отже, проаналізувавши степінь загрози такого типу атак можна сказати, що першим і найважливішим кроком в антифішинговій кампанії є виявлення самої атаки, на цьому базуються три основні підходи до захисту від атак, які полягають у застосуванні запобіжних, наступальних та коригуючих заходів.

2 РОЗПІЗНАВАННЯ ФІШИНГОВИХ САЙТІВ

2.1 Підходи до розпізнавання фішингу

Є два основні підходи до розпізнавання фішингу: навчання користувачів і класифікація за допомогою програмних засобів [4].

1) *Навчання користувачів*: користувачів можна навчати для їх кращого розуміння природи фішингових атак, що в свою чергу приведе до коректного розпізнаванню фішингових і справжніх сайтів. Це протилежно категоризації в роботі [7], де навчання користувачів розглядається як запобіжний захід. Але навчання користувачів направлено на кінцеве виявлення цими користувачами фішингових атак, тому розглядається як підхід до розпізнавання.

2) *За допомогою програмних засобів*: цей підхід спрямований на більш точну класифікацію фішингових і справжніх сайтів та зменшення розриву виниклого через людську помилку або невігластво. Це важливий недолік, який необхідно вирішити, так як навчання користувачів обходиться дорожче ніж автоматична класифікація та не завжди представляється можливим. Наприклад, коли база користувачів дуже велика (PayPal, eBay, Amazon і т.д.).

Точність розпізнавання може бути поліпшена в процесі навчання класифікатора (будь то людина або ПЗ). У користувацького розпізнавання, якість може бути покращено шляхом накопичення знань кінцевим користувачем, навчаючись завдяки своєму онлайн-досвіду або за допомогою зовнішньої навчальної програми. У разі програмної класифікації, поліпшення може бути досягнуто в процесі тренування класифікатора побудованого на алгоритмах машинного навчання або поліпшенням правил виявлення в системі, побудованої на правилах.

Техніки розпізнавання можуть не тільки безпосередньо захистити користувачів від попадання в тенети зловмисників, але і допомогти в посиленні фішингових приманок щоб розмежувати фішинговий спам від не фішингового.

Розпізнавання фішинговою атаки – це відправна точка боротьби з фішингом. На рисунку 2.1 показана схема підходів до розпізнавання фішингових атак. Але слід пам'ятати, що жоден із способів захисту описаних в попередньому розділі не спрацює, тому що їх основою є те, що атака виявлена.

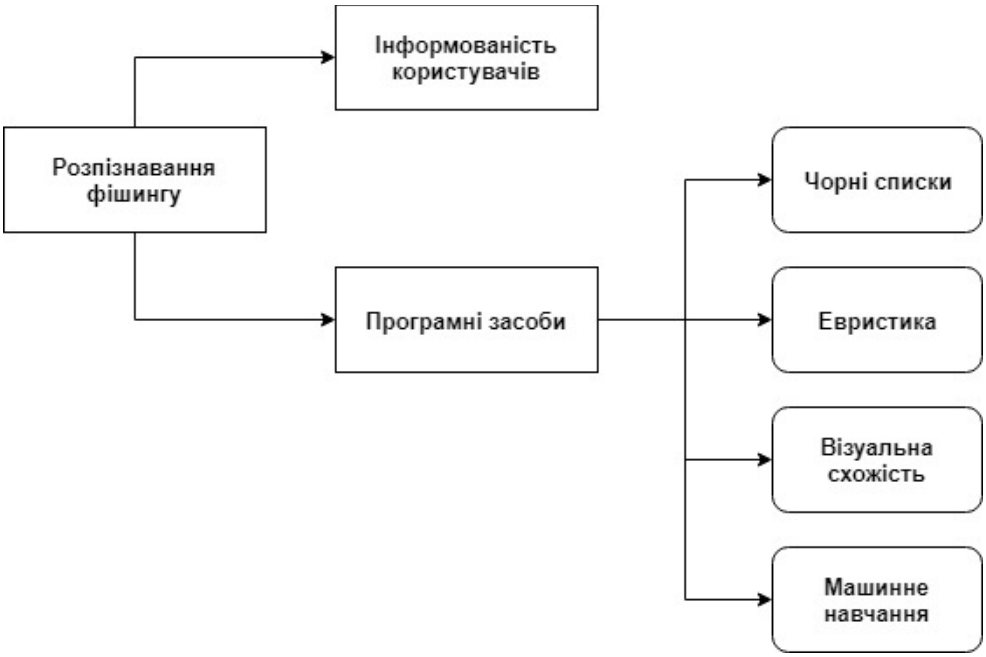

Рисунок 2.1 – Підходи до розпізнавання фішингової атаки

В рамках цієї роботи розглядається програмний підхід до виявлення фішингу, а більш детально машинне навчання.

2.2 Програмний підхід до розпізнавання

- *Чорні списки*

Під чорними списками маються на увазі регулярно оновлюванні списки, що містять інформацію про раніше виявлені фішингові URL, IP-адреси. Недоліком таких списків є їх неспроможність захисту від щойно створених фішингових сайтів, оскільки останні спочатку повинні бути виявлені і занесені в списки. Однак, чорні списки мають рейтинг неправильно розпізнаних менше ніж евристика [8]. Так само в роботі [8] чорні списки були визнані неефективними в виявленні нових сайтів і виявляли тільки 20% з них. Дослідження показало, що від 47% до 83% фішингових URL потрапили в чорні списки протягом 12 годин. Ця затримка є серйозною

проблемою, так як 63% фішингових кампаній згортається протягом перших 2-х годин.

Крім чорних є ще білі списки. На відміну від чорних, ці списки містять інформацію про надійні і перевірені URL-адреси. Вони можуть використовуватися для зниження рейтингу неправильно розпізнаних як фішинг (FP rate).

- *Евристика*

Фішингова евристика являє собою набір характеристик, які присутні в реальних фішингових атаках, але не завжди гарантовано мають місце в кожному окремому випадку атак. Якщо визначено набір загальних евристичних тестів, то він може бути застосований для виявлення щойно створених сайтів. У цьому перевага евристичного підходу перед чорними списками. Однак в цьому випадку існує ризик неправильної класифікації справжніх сайтів.

Програмне забезпечення може бути встановлено на стороні клієнта або сервера для перевірки корисних навантажень різних протоколів за допомогою різних алгоритмів. Це може бути HTTP, SMTP або будь-який інший протокол. Алгоритми можуть бути будь-яким механізмом для виявлення або запобігання фішингових атак.

Сучасні веб-браузери та поштові клієнти побудовані з механізмами захисту від фішингу, такими як евристичні тести з метою виявлення фішингових атак. Так само евристики виявлення фішингу можуть бути включені в антивіруси.

- *Візуальна схожість*

Метод розпізнавання заснований на зовнішньому вигляді фішингових сайтів, а не аналізі вихідного коду та інформації мережевого рівня. Фішингові сайти виглядають дуже схожими на оригінальні щоб ввести в оману користувача. В даному підході для прийняття рішення використовується набір характеристик текстового контенту, формат тексту, HTML теги, CSS, зображення і т.п. Йде порівняння підозрілого веб-сайту з відповідним перевіреним веб-сайтом, використовуючи різні функції, і якщо схожість перевищує попередньо визначене граничне значення, то сайт оголошується фішинговим.

Щоб уникнути виявлення фішингу, зловмисники зазвичай вставляють зображення, Flash, ActiveX і Java-аплет замість HTML-тексту. Підходи, засновані на візуальній подібності, можуть швидко виявляти такі вбудовані об'єкти, присутні на фішинговою веб-сторінці. Так само методи, засновані на візуальній схожості, використовують підпис для ідентифікації фішингових веб-сторінок. Підпис створюється шляхом використання загальних функцій всього сайту, а не однієї веб-сторінки. Таким чином, одного підпису досить для виявлення різних цільових веб-сторінок одного веб-сайту або різних версій веб-сайту. [9]

- *Машинне навчання*

Методи машинного навчання описані в наступному розділі. Вони розглядають виявлення фішингових атак як проблему класифікації документів або кластеризації, де моделі будуються з використанням переваг алгоритмів машинного навчання і класифікації, таких як k-Nearest Neighbors (kNN), J48, Машини опорних векторів (SVM), нейронні мережі, Наївний Байєсівський метод і Логістична регресія.

Таблиця 2.1 резюмує відомі утиліти для виявлення фішингу. [10]

Таблиця 2.1 – Поширені засоби виявлення фішингу

Утиліта	**Опис**	**Переваги**	**Недоліки**
GoldFish	Байєсівська фільтрація контенту	• Може бути натренований для кожного корустувача • Уникає помилкових спрацювань(FP)	• Нестійкий до техніки «байєсівського отруєння». • Можна обійти, трохи змінюючи слова
Браузери Site Adviser Netcraft	Чорні списки	Швидкий аналіз	• Повільне оновлення списків • Хибні спрацювання(FP)

Продовження таблиці 2.1

Утиліта	Опис	Переваги	Недоліки
SpoofGuard PwdHash	• Інтерговані в браузер рішення • Вивчає ознаки фішингу, такі як заплутані URL-адреси на веб-сторінках • Збільшує сповіщення • Метод евристики	• PwdHash запобігає крадіжці паролів • SpoofGuard захищає від неавторизованих IP та MAC-адрес.	• Ненадійність • Захоплений пароль можна використовувати на цільовому сайті
EarthLink toolbar	Комбінація евристики, користувацької оцінки та ручної перевірки	• Перевіряє інформацію про реєстрацію домену	• Не захищає від атак нульового дня
eBay tool	Евристика та чорні списки	• Захищає користувачів eBay	• Недоліки чорних списків

2.3 Методи розпізнавання з машинним навчанням

Під цим підходом мається на увазі використання автоматичних класифікаторів, побудованих на алгоритмах машинного навчання та інтелектуального аналізу даних. Дані класифікатори працюють на стороні сервера і визначають клас переданої сторінки за набором характеристик.

У таблиці 2.2 представлена порівняльна характеристику автоматизованих методів розпізнавання [11].

Таблиця 2.2 – Порівняльна характеристика класифікаторів

Алгоритм	**Основний принцип**	**Потрібність навчання**	**Переваги**	**Недоліки**
Naïve Bayes	• Кожен параметр класифікованих даних розглядається незалежно від інших параметрів класу. • Побудовано на теоремі Байеса. • Дозволяє передбачити клас використовуючи ймовірність.	Цей метод потребує навчання, оскільки алгоритм використовує розмічений набір даних для побудови таблиці.	• Алгоритм складається з простої арифметики (множення і ділення) • Швидке обчислення • Добре працює з великими розмірами	• Покладається на припущення незалежності і буде погано працювати, якщо це припущення не буде виконано
LR	• Використовує лінійне рівняння з незалежними показниками для передбачення значення. • У центрі аналізу перебуває задача оцінки шансів на подію.	Цей метод потребує навчання	• Легко інтерпретовані результати • Модель є функціональною при прогнозуванні двійкових даних	• Потрібно більше статистичних припущень перед застосуванням • Більш функціонально зі змінними, які мають лінійну залежність, ніж комплексну • Точність прогнозування чутлива до повноти вхідних даних

Продовження таблиці 2.2

Алгоритм	**Основний принцип**	**Потрібність навчання**	**Переваги**	**Недоліки**
J48	• Алгоритм будує класифікатор в формі дерева рішень. • У кожній точці блок-схеми ставиться питання про значимість тієї чи іншої ознаки, і в залежності від цих ознак екземпляри потрапляють в певний клас. • Реалізує алгоритм Quinlan C4.5 • Будує дерева рішень на основі маркованих навчальних даних, використовуючи ідею ентропії даних	Цей метод потребує навчання, тут тренувальний набір даних розмічується класами.	• Проста інтерпретація • Висока швидкість роботи • Вихідні дані легко розуміються людиною	• Схильність до перенавчання • Можливі проблеми з діагональними межами рішення
Neural Network	• Організовано як розташування взаємопов'язаних нерозпізнаних одиниць (нейронів) • З'єднання використовуються для відправки сигналів від одного нейрона до іншого.	Цей метод потребує навчання	• Дуже гнучкий, може бути використаний для задач регресії і класифікації • Можуть бути треновані з будь-якою кількістю вхідних даних	• Вимагають великих обчислювальних ресурсів • Збільшена тривалість роботи • Природа «чорного ящика»

Продовження таблиці 2.2

Алгоритм	Основний принцип	Потрібність навчання	Переваги	Недоліки
	• З'єднання мають вагу, щоб поліпшити транспортування серед нейронів.		• Після навчання прогнози досить швидкі	•
kNN	• Не параметризований контрольований метод машинного навчання • Для класифікації екземпляру використовуються клас k найближчих сусідніх екземплярів	Цей метод потребує навчання, оскільки kNN необхідний розмічений набір даних	• Легкий в розумінні • Легко реалізується • Залежно від вибору дистанційної метрики, kNN може показувати досить точні результати	• Може бути дуже ресурсозатратним • Зашумлені дані можуть «зіпсуваи» kNN-класифікацію • Характеристики з великою кількістю значень можуть впливати на дистанційну метрику, по відношенню до характеристик з меншою кількістю значень • Вимагає більше місця, ніж активні класифікатори
SMO	• Алгоритм з групи Support Vector Machine (SVM) • Використовує гіперплощину, щоб класифікувати дані по 2 класам	Цей метод потребує навчання	• Може вирішити проблеми QP (Quadratic Programming)	• Необхідність вибору ядра • Погана интерпретованість

Продовження таблиці 2.2

Алгоритм	Основний принцип	Потрібність навчання	Переваги	Недоліки
	• На верхньому рівні SVM виконує ті ж операції, що і J48 • Самостійно визначає функцію гіперплощини		• Виконує аналогічно логістичної регресії при лінійному розподілі • Добре працює з нелінійним кордоном в залежності від використовуваного ядра	

2.4 Огляд існуючих рішень

В роботі [12] автори використовували інформацію домену про посилання для розпізнавання фішингових сторінок. Одною з переваг їхнього методу було використання інформації про домен для виявлення фішингових сайтів, оскільки ця важлива характеристика не враховувалася в інших анти-фішингових методах. У цьому запропонованому методі в першу чергу витягувалися всі прямі і непрямі посилання на обраний сайт. Далі, використовуючи вихідний код сторінки, всі домени пов'язані з прямими посиланнями витягувалися і поміщалися в набір S1. Потім непрямі посилання витягувалися і поміщалися в набір S2, після цього обидва набори об'єднувалися і витягувалися тільки загальні домени, з яких згодом, за допомогою DNS пошуку, витягувалися IP-адреси цих доменів. Результат дослідження показує, що accuracy, FP, FN, TN і TP запропонованого методу 99.62, 0.32, 0.5, 99.5 і 99.67 відсотків. Не дивлячись на такі переваги як точність і виявлення сторінок в їх методі, залежність цього методу від різних зовнішніх

методів типу DNS-пошуку і пошукових систем може вплинути на його ефективність.

В роботі [13] автори запропонували новий метод виявлення атак з використанням асоціативної класифікації як методу інтелектуального аналізу для класифікації даних. Використовуючи PHP-сценарій, вони зібрали інформацію з 601 легальних сайтів і 752 фішингових. Вони використовували 16 ключових характеристик для розпізнавання атак. Автори роботи розрахували частоту появи кожної з 16 характеристик на фішингових сторінках. Наприклад, частота використання на фішингових сайтах IP-адреси в URL становить 20.5 відсотків.

У ще одній роботі [14] автор досліджує різні методи відбору характеристик з метою вибрати такий набір характеристик, на якому можна побудувати добре прогнозовані класифікатори з використанням інтелектуального аналізу даних. Так само він досліджує чи може малий набір характеристик бути не менш ефективним при побудові добре прогнозованого класифікатора. Для цього автор використовує 2 алгоритму машинного навчання: дерево рішень C4.5 і введення правил IREP. Для відбору характеристик використовується приріст інформації (Information Gain) і симетрична невизначеність. В результаті експерименту ефективність і продуктивність обох методів відбору характеристик була однаковою. Було відібрано 11 характеристик, які в подальшому привели до побудови високоточного класифікатора. Дві головні характеристики – це «Сертифікат SSL» і «URL якоря». Алгоритм IREP був здатний генерувати керовані класифікатори в порівнянні з деревом прийняття рішень. Точність прогнозування зі зменшенням кількості характеристик впала всього на 1.02% і 1.23% в алгоритмах C4.5 і IREP відповідно.

На відміну від попередньої роботи, в дослідженні [15] для відбору ознак використовувався метод Wrapper-based feature selection (WBFS). Цей метод використовує індуктивний класифікатор для оцінки підмножини характеристик. WBFS зазвичай дає найбільш ефективні характеристики, встановлені для цього конкретного виду класифікатора. Тому в цій роботі WBFS використовувався для вибору найбільш впливових характеристик, які можна використовувати для відмінності фішингу від справжніх веб-сайтів. Для порівняння характеристики

також відбиралися за допомогою методів Information Gain (IG) і Principal component analysis (PCA). Результати експерименту показали, що кращі результати були у алгоритмів kNN і Random Forest при відборі ознак методами WBFS і IG, їх точність дорівнює 0,971 і 0,973 відповідно, для всіх інших алгоритмів при відборі методом WBFS, точність була строго вище.

В роботі [16] автори провели дослідження точності і чутливості 4 алгоритмів класифікації, це Bayesian Network, NNet, SVM і Decision Tree. Їх завданням було знайти, з цих 4, найефективніший для розпізнавання фішингових сайтів. В результаті кращим алгоритмом став NNet.

Так само порівняльну оцінку алгоритмів Naïve Bayes, Support Vector Machine (SVM), Neural Net (NN), Random Forest (RF), IBK lazy classifier and Decision Tree (J48) провів автор роботи [17] за його результатами найточнішими стали RF і kNN з показником accuracy вище 97%.

Новий алгоритм класифікації розробив автор роботи [18], цей алгоритм заснований на раніше відомому алгоритмі PRISM і представляє його поліпшену версію. Результати експерименту підтверджують, що число правил запропонованого способу виявлення фішингу зростає і показують, що зберігається помилково позитивний і помилково негативний показник близько 0,1%, що є досить низьким. Експерименти продемонстрували здійсненність і ефективність використання цього методу класифікації в реальних додатках з великими базами даних. Запропонований алгоритм точно розпізнав майже 87% фішингових сайтів.

У дослідженні [19] запропонована модель, яка може визначити, чи є сайт фішингових чи ні. Використовується шість різних алгоритмів класифікації, заснованих на машинному навчанні, які називаються Naive Bayes, J48, SVM, Logistic Regression, Neural Network і ледачий класифікатор IBK з 92,7846%, 95,11%, 96,57%, 96,3%, 93,85%, 93,4039% точності класифікації відповідно. Співвідношення тренувального і тестового набору даних становить 70-30. Мета моєї роботи – розширити їх дослідження щоб підвищити точність класифікації за допомогою цих алгоритмів.

В роботі [20] було обговорено ряд антифішингових панелей інструментів і запропонована системна модель для боротьби з фішинг-атакою. Запропонована антифішингова система заснована на розробці плагіна для веб-браузера. Працездатність пропонованої системи вивчається за допомогою трьох різних алгоритмів класифікації збору даних: RF, kNN, Bayesian Classificator (BC). Щоб оцінити пропоновану антифішингову систему для виявлення фішингових веб-сайтів, 7690 законних веб-сайтів і 2280 фішингових веб-сайтів були зібрані з офіційних джерел, таких як база даних APWG і PhishTank. Після аналізу алгоритмів інтелектуального аналізу даних на фішингових веб-сторінках було виявлено, що байесовский алгоритм дає швидкий результат і дає більш точні результати, ніж інші алгоритми.

2.5 Алгоритм розпізнавання фішингового сайту

Огляд рішень з готових робіт по різним підходам до розпізнавання фішингових сайтів дозволив визначити ефективний підхід до вивчення цього питання за допомогою технік інтелектуального аналізу даних і методів машинного навчання. Алгоритм має чітку структуру і послідовність дій. Спочатку досліджується точність розпізнавання фішингових сайтів з повним набором характеристик. Але оскільки витяг характеристик досить довга робота і вимагає багато часу, має сенс скоротити кількість характеристик, якщо це не суттєво позначиться на точності прогнозування, що і є предметом дослідження в даній роботі. Також підвищити точність прогнозування можливо за рахунок вдалої комбінації декількох класифікаторів, це буде представлено в останній частині дослідження. На рисунку 2.2 представлена поетапна схема реалізації процесу.

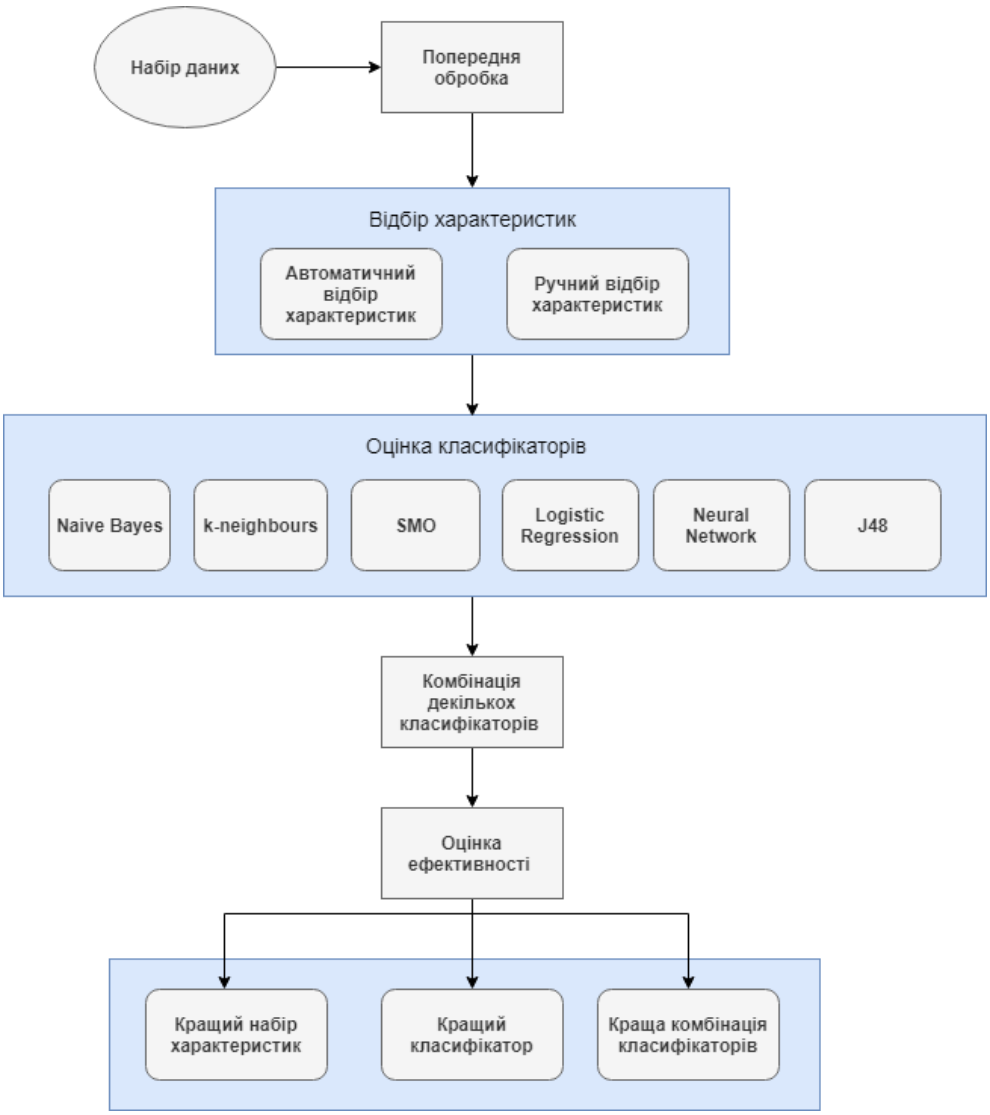

Рисунок 2.2 – Процес розпізнавання фішингового сайту

2.6 Попередня обробка

На етапі попередньої обробки виконується насамперед збір даних. Так щоб спростити роботу використовується набір даних з уже витягнутими характеристиками. Вони представлені у вигляді матриці, з колонками, що відповідають за кожну з 30 характеристик, а рядки представляють наявність тієї або іншої характеристики в дослідженому екземплярі набору. Значення характеристики може бути представленим трьома числовими значеннями: 1 – надійний, 0 – підозрілий, -1 – фішинг. Остання колонка набору даних відповідає за кінцевий розподіл екземпляру на фішинг чи ні, представлена тільки двома

значеннями: 1 і -1. Список характеристик представлений 4 групами розділеними за належністю характеристики до тієї чи іншої частини веб-сторінки. Перша група складається з характеристик адресного рядка і знаходиться в таблиці 2.3. Друга складається з аномальних характеристик і представлена в таблиці 2.4. Третя група містить характеристики HTML і JavaScript, і продемонстрована в таблиці 2.5. Четверта описує характеристики домену, в таблиці 2.6. Характеристики взяті з роботи [21], також у цій роботі доведена їх ефективність та впливовість в прогнозуванні фішингових та легітимних веб-сайтів.

Таблиця 2.3 – Характеристики адресного рядка

Назва характеристики	**Опис**
Using the IP Address	IP адреса використовується замість доменного імені, іноді трансформується у шістнадцятковий вигляд
Long URL	Фішери можуть використовувати довгу URL адресу щоб приховати підозрілу частину
Using URL Shortening Services “TinyURL”	Скорочення URL-адреси - це метод у "Всесвітній павутині", в якому URL може бути значно меншим за довжиною і привести до необхідної веб-сторінки. Це досягається за допомогою "HTTP Redirect" на короткому доменному імені, яке посилається на веб-сторінку з довгим URL
URL’s having “@” Symbol	Використання @ призводить до того що браузер ігнорує все що було до @, а справжня адреса йде за цим символом
Redirecting using “//”	Наявність у URL "//" означає що користувач буде перенаправлений на інший сайт
Adding Prefix or Suffix Separated by (-) to the Domain	Дефіс рідко використовується у перевірених адресах
Sub Domain and Multi Sub Domains	URL може мати не більше 2 суб-доменів, це домен першого рівня(країни) та другого рівня
HTTPS (Hyper Text Transfer Protocol with Secure Sockets Layer)	Наявність SSL сертифкату, його довіреність для вік
Domain Registration Length	Основано на тому що фішинговий сайт живе короткий період часу

Продовження таблиці 2.3

Назва характеристики	**Опис**
Favicon	Графічне зображення, що асоціюється з певною веб-сторінкою
Using Non-Standard Port	Характеристика є корисною у перевірці чи працює певна служба(наприклад HTTP) на сервері
The Existence of “HTTPS” Token in the Domain Part of the URL	Фішери можуть додавати "HTTPS" до доменної частини

Таблиця 2.4 – Аномальні характеристики

Назва характеристики	**Опис**
Request URL	Перевіряє чи завантажуються медіа ресурси з того ж домену
URL of Anchor	Якір - це елемент, визначений тегом <a>. Ця характеристика рахується як попередня
Links in <Meta>, <Script> and <Link> tags	Звичайні веб-сайти використовують теги <Meta>, щоб запропонувати метадані про документ HTML; <Script> теги для створення клієнтського сценарію; і теги <Link> для отримання інших веб-ресурсів. Очікується, що ці теги пов'язані з тим доменом що і веб-сторінка
Server Form Handler (SFH)	SFH, які містять порожній рядок або "about: blank", вважаються сумнівними, оскільки слід вживати дії щодо поданої інформації. Крім того, якщо доменне ім'я в SFH відрізняється від доменного імені веб-сторінки, це показує, що веб-сторінка підозріла.
Submitting Information to Email	Веб-форма дозволяє користувачеві подавати свою особисту інформацію, яка спрямовується на сервер для обробки. Фішер може перенаправити інформацію користувача на його особисту електронну пошту. З цією метою можна використовувати мову скриптів на сервері, наприклад, функцію "mail ()" в PHP. Ще однією функцією на стороні клієнта, яка може бути використана для цієї мети, є функція "mailto:"
Abnormal URL	Перевіряється за допомогою WHOIS бази даних

Таблиця 2.5 – Характеристики HTML та JavaScript

Назва характеристики	**Опис**
Website Forwarding	Скільки разів веб-сайт був перенаправлений
Status Bar Customization	Фахівці можуть використовувати JavaScript для показу підробленої URL-адреси в рядку стану для користувачів. Щоб витягти цю функцію, ми повинні викопати вихідний код веб-сторінки, зокрема подію "onMouseOver", і перевірити, чи вона вносить будь-які зміни у рядок стану.
Disabling Right Click	Фішери використовують JavaScript, щоб вимкнути функцію правої кнопки миші, так що користувачі не можуть переглядати та зберігати вихідний код веб-сторінки.
Using Pop-up Window	Просить користувачів надати персональну інформацію у вспливаючому вікні
IFrame Redirection	Використання Iframe вказує на фішинг

Таблиця 2.6 – Характеристики домену

Назва характеристики	**Опис**
Age of Domain	Співставляється з базою WHOIS, якщо вік менше 6 місяців - фішинг
DNS Record	Немає запису DNS для домену
Website Traffic	Вимірюється популярність сайту через визначення кількості відвідувачів і кількості сторінок що вони відвідали
PageRank	Рейтинг від 0 до 1, вказує наскільки важлива сторінка в інтернеті
Google Index	Чи індексується сторінка у google
Number of Links Pointing to Page	Чим більше сторінок посилається на дану тим більша імовірність що сторінка перевірена
Statistical-Reports Based Feature	Чи немає сайту у списку фішингових які збирає спеціальний сервіс, наприклад PhishTank

2.7 Відбір характеристик

Для відбору характеристик використовується два різних шляхи, це ручний відбір і автоматизований. Алгоритм відбору представлений на рисунку 2.3.

Рисунок 2.3 – Відбір характеристик

Ручний відбір характеристик – це відбір відповідно до чотирьох груп описаних вище, що ґрунтується на структурі веб-сторінки. Таким чином згенеровано 9 піднаборів характеристик і надалі досліджувати їх працездатність. Дані піднабори представлені в таблиці 2.7.

Таблиця 2.7 – Групи ручного відбору характеристик

Група характеристик	***Кількість характеристик***
Всі характеристики	30
Характеристики адресного рядка	12
Аномальні характеристики	6
Характеристики HTML & JS	5

Продовження таблиці 2.7

Група характеристик	***Кількість характеристик***
Характеристики домену	7
Всі характеристики крім хар. адресного рядка	18
Всі характеристики крім аномальних	24
Всі характеристики крім HTML & JS	25
Всі характеристики крім доменних	23

Автоматизований відбір характеристик проводиться з використанням трьох алгоритмів відбору характеристик та відповідно генерує три групи ознак. Використовувалися наступні алгоритми:

- Consistency subset evaluator, який оцінює значимість піднабору характеристик за рівнем узгодженості значень класу, коли навчальні екземпляри проектуються на підмножину характеристик. Узгодженість будь-якої підмножини ніколи не може бути нижче, ніж у повного набору характеристик, тому звичайною практикою є використання цього оцінювача піднаборів в поєднанні з випадковим або вичерпним пошуком, який шукає найменшу підмножина з узгодженістю, рівній узгодженості повного набору ознак. [22]
- Wrapper subset evaluator оцінює набори характеристик, використовуючи схему навчання. Перехресна перевірка використовується для оцінки точності схеми навчання для набору атрибутів. [23]
- Correlation-based feature subset evaluator оцінює значимість підмножини характеристик, з огляду на індивідуальну прогностичну здатність кожної функції, а також ступінь надмірності між ними. [24]

Таблиця 2.8 показує яку техніку відбору і які алгоритми пошуку використовувалися, а також кількість відібраних ознак.

Таблиця 2.8 – Групи автоматичного відбору характеристик

Метод відбору	**Метод пошуку**	**Кількість характеристик**
Consistency subset evaluation	Greedy Stepwise	23
Wrapper subset evaluation	Best First	19
Correlation-based feature subset evaluation	Greedy Stepwise	9

Характеристики, що входять в кожну з груп представлені у додатку А.

2.8 Оцінка классифікаторів

Були обрані 6 найпоширеніших алгоритмів класифікації для тренування і тестування точності прогнозування фішингових сайтів на обраних групах характеристик. Причиною вибору саме цих алгоритмів стали їх різноманітні стратегії тренування моделі класифікації і побудови правил і різні механізми навчання і тестування, список алгоритмів наведено нижче. Кожен з алгоритмів є представником одного з класів машинних методів навчання і класифікації.

- Naïve Bayes
- Neural Network
- C4.8(Дерево прийняття рішень)
- K-nearest neighbors(kNN)
- Sequential minimal optimization(SMO)
- Logistic Regression(LR)

Для оцінки класифікаторів машинного навчання, які використовуються для прогнозування фішингових веб-сайтів, використовувалася 10-кратна перехресна перевірка. При 10-кратної перехресній перевірці набір даних ділиться на 10 непересічних наборів даних однакового розміру. Кожен набір даних потім використовується в якості тестового набору даних, а решта 9 наборів даних об'єднуються і використовуються в якості навчального набору даних для

тренування класифікатора. Потім цей процес запускається 10 разів. Точність розраховується для кожного прогону. Таким чином, остаточна точність навчання із цього набору даних є середнім значенням 10 точності для всіх прогонів.

2.9 Нова модель классифікації

Алгоритм прогнозування збудований на комбінації декількох класифікаторів полягає в наступному: вибираються три класифікатора з найвищою точністю прогнозування та мінімальні часом витраченим на побудову моделі, потім будується схема наведена на малюнку 2.4, в якій 2 з алгоритмів виносять свій прогноз по заданому екземпляру є сайт фішингових або перевіреним, якщо прогноз збігається, то екземпляру присвоюється відповідний результат, якщо прогноз відрізняється, то в справу вступає третій класифікатор і вже він остаточно визначає до якого класу належить екземпляр.

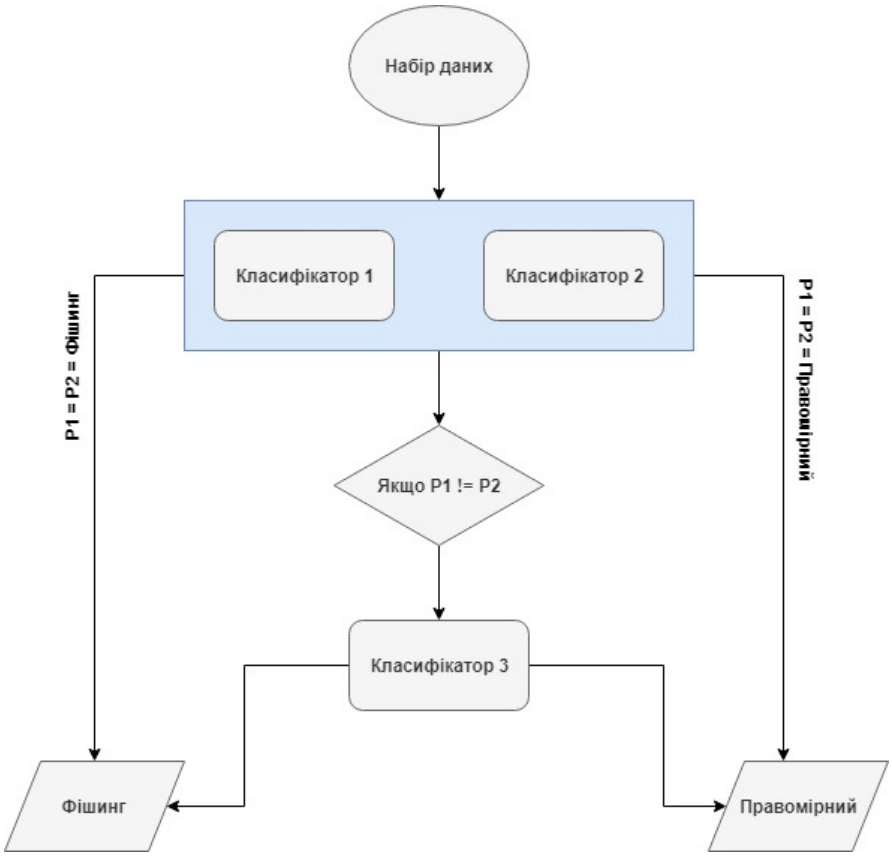

Рисунок 2.4 – Модель класифікатора

Висновки з розділу 2

У цьому розділі розглянуто методи розпізнавання фішингових сайтів, які полягають у пошуку візуальної схожості між справжнім та підробним сайтом, евристичні закономірності, які прослідковуються у багатьох екземплярах, але не гарантовано присутні у всіх, метод чорних та білих списків, який має важливий недолік, що при такому підході не можливо виявити щойно створений сайт, оскільки його немає у списках, а також методи машинного навчання, на яких зосереджено найбільше уваги. Розглянуто популярні популярні готові програми розпізнавання фішингу, це і прикладні програми і розширення для браузерів, самі браузери, які працюють за методом чорних списків. Більшість цих засобів побудовано на методах евристики і чорних списках, тому мають недоліки згаданих підходів, машинні методи є більш точними, але складнішими в реалізації.

До розглянутих машинних методів відносяться Logistic regression, J48(Decision tree), Naïve Bayes, Neural Network, k-nearest neighbors та SMO. Кожен з методів має свої переваги і недоліки, а також мають різний принцип дії, це дозволить відшукати групу методів, які найбільш ефективні в даній конкретній ситуації. Слід зазначити, що було проведено досить багато досліджень порівняння методів машинного навчання для задачі класифікації фішингових сайтів, але мало досліджень відбору характеристик сайтів.

Також у розділі 2 мною запропоновано підхід до знаходження ефективної моделі класифікатора, що розпізнає фішингові сайти з покращеною точністю. Підхід має декілька основних етапів. На першому відбулася попередня обробка даних, що складається зі збору даних, тобто формування датасету, а також витягнення характеристик и представлення їх у матричному вигляді. Другий етап – це відбір характеристик, полягає у пошуку піднабору характеристик за яких точність розпізнавання майже не зміниться. Далі відбулася оцінка класифікаторів, для пошуку найефективнішого, і на завершення побудовано модель з 3 найкращих класифікаторів з поліпшеною точністю розпізнавання. Результати представлені у розділі 3.

3 АНАЛІЗ РЕЗУЛЬТАТІВ ДОСЛІДЖЕННЯ

3.1 Інструментарій та набір даних

Для роботи був використаний набір даних, що містить 11055 екземплярів, з яких 6157 надійних і 4898 фішингових. Дані отримані з сервісу UCI Machine Learning Repository. Витяг характеристик вбудовано в даний датасету, в якому кожен сайт представлений як вектор характеристик, а колонки показують приналежність сайту до одного з двох класів. Приклад частини датасету продемонстрований на рисунку 3.1.

Файл з даними був конвертований в формат ARFF для зручного використання в програмі WEKA. WEKA – це набір алгоритмів машинного навчання використовуються для глибокого аналізу даних, так само дана програма містить інструментарій для задач початкової обробки даних, задач регресії, класифікації, кластеризації та візуалізації. Алгоритми можуть бути застосовані безпосередньо, тобто з наявного набору, або отримані з коду на мові Java. Так само WEKA підходить для розробки нових схем машинного навчання.

ıg_IP_Ad	JRL_Lengt	rtining_Ser	ng_At_Syr	_slash_red	refix_Suffi	g_Sub_Do	Lfinal_Sta	registeratic	Favicon	port	TTPS_toke
-1	1	1	1	-1	-1	-1	-1	-1	1	1	-1
1	1	1	1	1	-1	0	1	-1	1	1	-1
1	1	0	1	1	-1	-1	-1	-1	1	1	-1
1	1	0	1	1	-1	-1	-1	1	1	1	-1
1	-1	0	1	1	-1	1	1	-1	1	1	1
-1	-1	0	1	-1	-1	1	1	-1	1	1	-1
1	-1	0	1	1	-1	-1	-1	1	1	1	1
1	1	0	1	1	-1	-1	-1	1	1	1	-1
1	-1	0	1	1	-1	1	1	-1	1	1	-1
1	-1	1	1	1	-1	-1	1	-1	1	1	1

Рисунок 3.1 – Вигляд датасету

3.2 Критерії оцінки

Кілька експериментів були приведені в різних сценаріях, експеримент і результат оцінювалися з використанням декількох вимірювань, порівнювалися результати декількох експериментів і були виведені результати.

Першим критерієм є accuracy (3.1). Це показник кількості коректних прогнозів, отриманих в результаті запуску моделі на тестовому наборі даних і наступному порівнянні результатів в фактичними, що знаходяться в датасеті. Але у цього критерію є один мінус, якщо набір даних незбалансований, то в рамках одного класу точність може бути високою, а інший визначається досить погано.

$$\text{Accuracy} = \frac{\text{TP+TN}}{\text{TP+FP+TN+FN}} \tag{3.1}$$

У свою чергу precision (точність) (3.2) і recall (повнота) (3.3) є критеріями, використовуваними для оцінки в більшій частині алгоритмів витягу інформації. Точність системи в межах класу – це частка екземплярів, дійсно належать даному класу щодо всіх документів, які система віднесла до цього класу. Повнота системи – це частка знайдених класифікатором екземплярів, що належать класу відносно всіх екземплярів цього класу в тестовій вибірці.

$$Precision = \frac{TP}{TP+FP} \tag{3.2}$$

$$Recall = \frac{TP}{TP+FN} \tag{3.3}$$

Значення TP, FP, TN, FN знаходяться в confusion matrix (матриця неточностей), показаної в таблиці 3.1.

Таблиця 3.1 – Confusion matrix

	Классифіковано як фішинг	Классифіковано як надійний
Насправді фішинг	TP	FN
Насправді надійний	FP	TN

True Positive(TP): кількість фішингових сторінок ідентифікованих як фішинг.
False Positive(FP): кількість надійних сторінок ідентифікованих як фішинг.
False Negative(FN): кількість фішингових сторінок ідентифікованих як надійні.
True Negative(TN): кількість правомірних сторінок ідентифікованих як надійні.

3.3 Результати оцінки відбору характеристик

В ході експерименту розраховуються вищезгадані метрики для кожного набору характеристик отриманого в результаті ручного та автоматичного відбору. Крім цього, оцінюється вплив кожної групи на кінцевий результат. В кінцевому підсумку, отримані результати порівнюються з результатами отриманими при оцінці на наборі з усіх характеристик щоб рекомендувати найкращий підхід до відбору ознак. Критерієм відбору в даному випадку є так само розмір набору ознак. Насамперед розрахунки були проведені для набору з усіх характеристик. Результати представлені в таблиці 3.2 і на рисунку 3.2.

Таблиця 3.2 – Результати тесту для всіх характеристик

Алгоритм	Accuracy	Precision	Recall
Naïve Bayes	92,980	0,930	0,930
Neural Network	96,900	0,969	0,969
J48(c4.8)	95,870	0,959	0,959
kNN	97,180	0,972	0,972
SMO	94,030	0,940	0,940
Logistic Regression	93,990	0,940	0,940

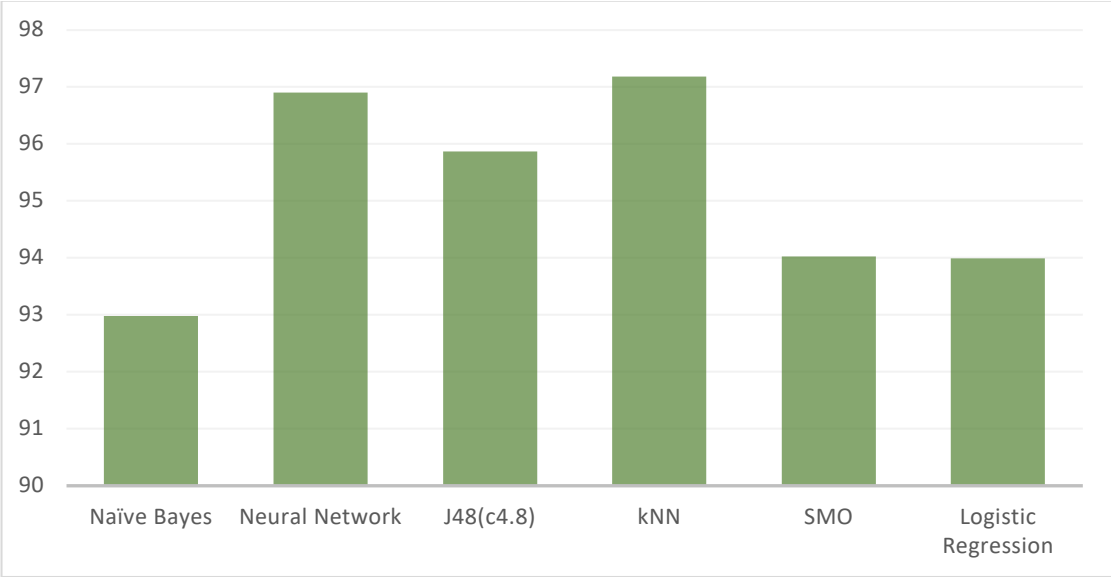

Рисунок 3.2 – Accuracy для всіх характеристик

Результати показують кращі оцінки за всіма трьома параметрами у алгоритмів Neural Network і kNN, які дорівнюють відповідно 96,9 і 97,18. А найгірший результат показує алгоритм Naïve Bayes з результатом 92,98.

Далі розглядаються тільки характеристики адресного рядка, результати представлені в таблиці 3.3 і на рисунку 3.3.

Таблиця 3.3 – Результати тесту для характеристик адресного рядка

Алгоритм	Accuracy	Precision	Recall
Naïve Bayes	89,792	0,898	0,898
Neural Network	90,742	0,908	0,907
J48(c4.8)	90,385	0,904	0,904
kNN	90,837	0,909	0,908
SMO	89,815	0,899	0,898
Logistic Regression	89,765	0,898	0,898

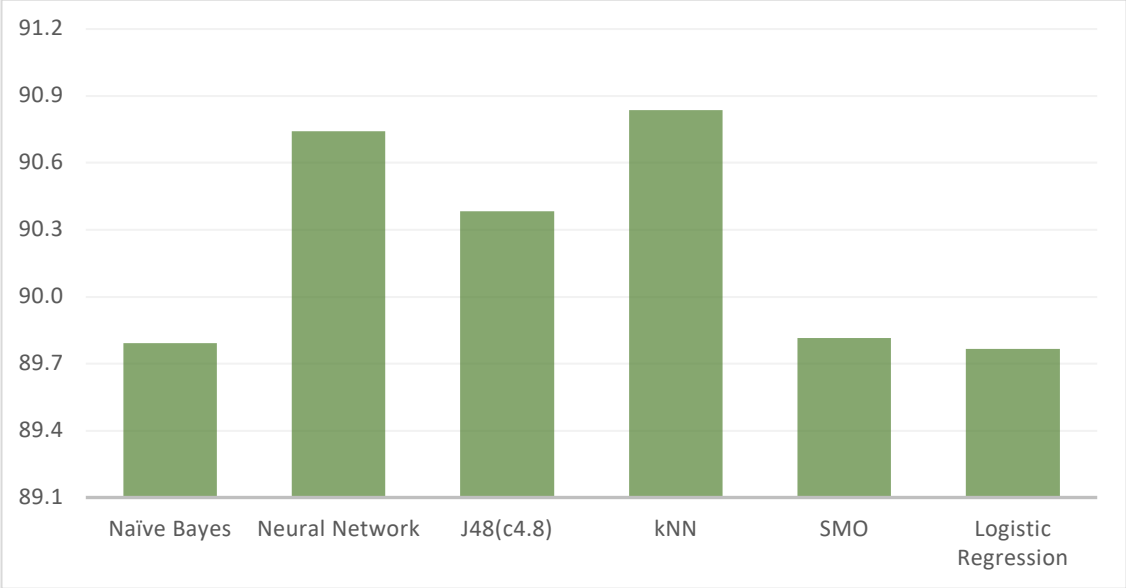

Рисунок 3.3 – Accuracy для характеристик адресного рядка

За результатами видно, що показники впали на 6,5% для алгоритму kNN і на 3,4% для Naïve Bayes, який і в цей раз показує найгірші результати. Так само зберігається тенденція показувати кращий результат у алгоритмів Neural Network і kNN.

Далі розглядаються тільки характеристики аномальні характеристики, результати представлені в таблиці 3.4 і на рисунку 3.4.

Таблиця 3.4 – Результати тесту для аномальних характеристик

Алгоритм	Accuracy	Precision	Recall
Naïve Bayes	87,024	0,879	0,870
Neural Network	87,445	0,880	0,874
J48(c4.8)	87,309	0,879	0,873
kNN	87,191	0,875	0,872
SMO	84,731	0,877	0,847
Logistic Regression	87,187	0,880	0,872

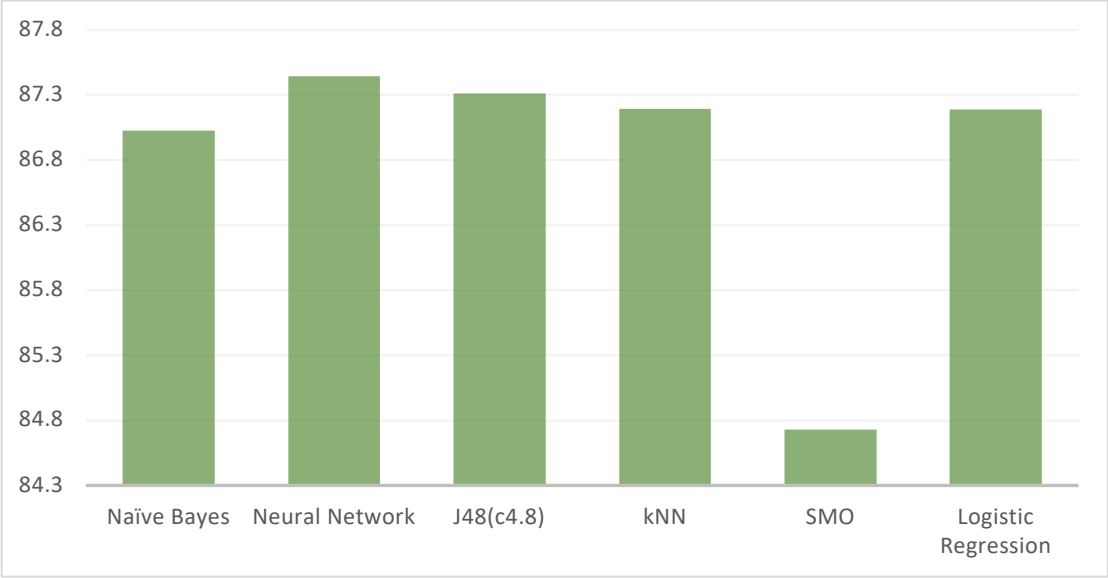

Рисунок 3.4 – Accuracy для аномальних характеристик

За отриманими даними видно що результати тільки погіршилися, а найменш точним алгоритмом виявився SMO. Точність прогнозування впала на 10% для kNN та Neural Network. Тому однозначно можна сказати що цей набір характеристик не підходить для використання у подальшому.

Далі розглядаються тільки характеристики HTML і JS, результати представлені в таблиці 3.5 і на рисунку 3.5.

Таблиця 3.5 – Результати тесту для характеристик HTML и JS

Алгоритм	Accuracy	Precision	Recall
Naïve Bayes	56,101	0,573	0,561
Neural Network	55,789	0,629	0,558
J48(c4.8)	57,137	0,654	0,571
kNN	57,210	0,652	0,572
SMO	55,694	0,557	0,557
Logistic Regression	56,178	0,556	0,562

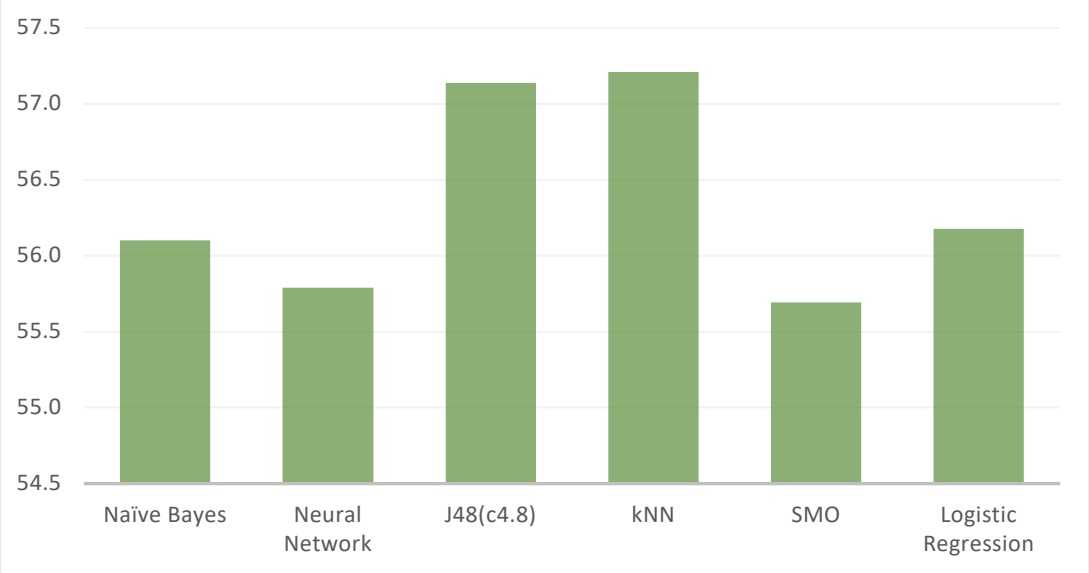

Рисунок 3.5 – Accuracy для характеристики HTML та JavaScript

Показники впали на 41% що свідчить про повну непридатність даного набору ознак для використання в подальшому. Але варто зазначити, що найкращі результати в цей раз продемонстрували алгоритми kNN і J48.

Далі розглядаються тільки характеристики домену, результати представлені в таблиці 3.6 і на рисунку 3.6.

Таблиця 3.6 – Результати тесту для характеристик домену

Алгоритм	Accuracy	Precision	Recall
Naïve Bayes	70,927	0,709	0,709
Neural Network	73,641	0,737	0,736
J48(c4.8)	74,170	0,741	0,742
kNN	74,545	0,745	0,745
SMO	69,787	0,701	0,698
Logistic Regression	71,646	0,716	0,716

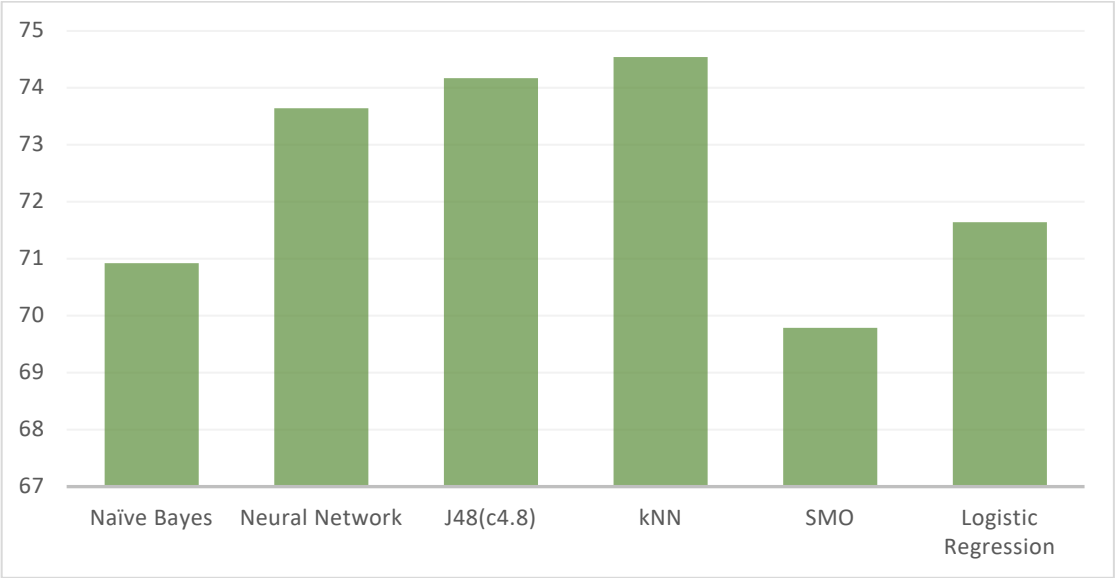

Рисунок 3.6 – Accuracy для характеристик домену

В даному випадку кращі показники всього лише в районі 74%, що не є підходящим варіантом для прогнозування фішингу. Алгоритм kNN все ще показує кращий результат.

Далі розглядаються всі характеристики за винятком характеристик адресного рядка, результати представлені в таблиці 3.7 і на рисунку 3.7.

Таблиця 3.7 – Результати тесту для всіх характеристик крім характеристик адресного рядка

Алгоритм	Accuracy	Precision	Recall
Naïve Bayes	87,626	0,879	0,876
Neural Network	91,524	0,916	0,915
J48(c4.8)	91,361	0,916	0,914
kNN	92,583	0,926	0,926
SMO	88,209	0,892	0,882
Logistic Regression	88,621	0,889	0,886

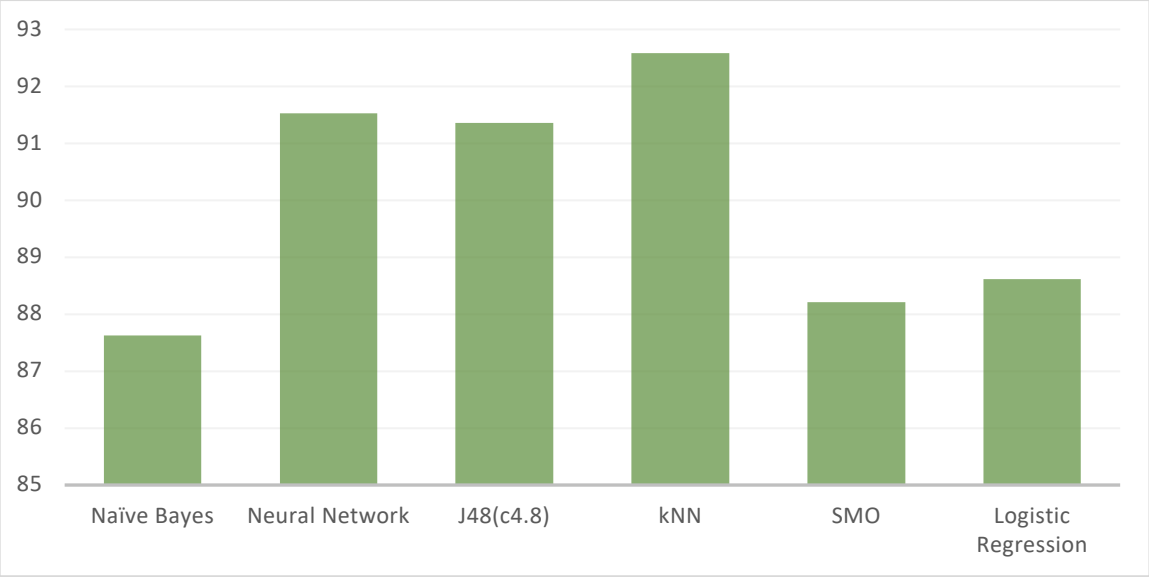

Рисунок 3.7 – Accuracy для всіх характеристик крім хар. адресного рядка

Результати показали що найкраща точність досягнута алгоритмом kNN 92,583 і недалеко від нього пішли Neural Network і J48 (c4.8) з різницею всього в 1%. Показники в загальному впали на 4,7%. Порівняно з вищерозглянутими наборами цей має поки найкращий результат.

Далі розглядаються всі характеристики за винятком аномальних характеристик, результати представлені в таблиці 3.8 і на рисунку 3.8.

Таблиця 3.8 – Результати тесту для всіх характеристик крім аномальних характеристик

Алгоритм	Accuracy	Precision	Recall
Naïve Bayes	90,204	0,902	0,902
Neural Network	93,781	0,938	0,938
J48(c4.8)	93,152	0,932	0,932
kNN	94,568	0,946	0,946
SMO	89,815	0,899	0,898
Logistic Regression	91,28	0,913	0,913

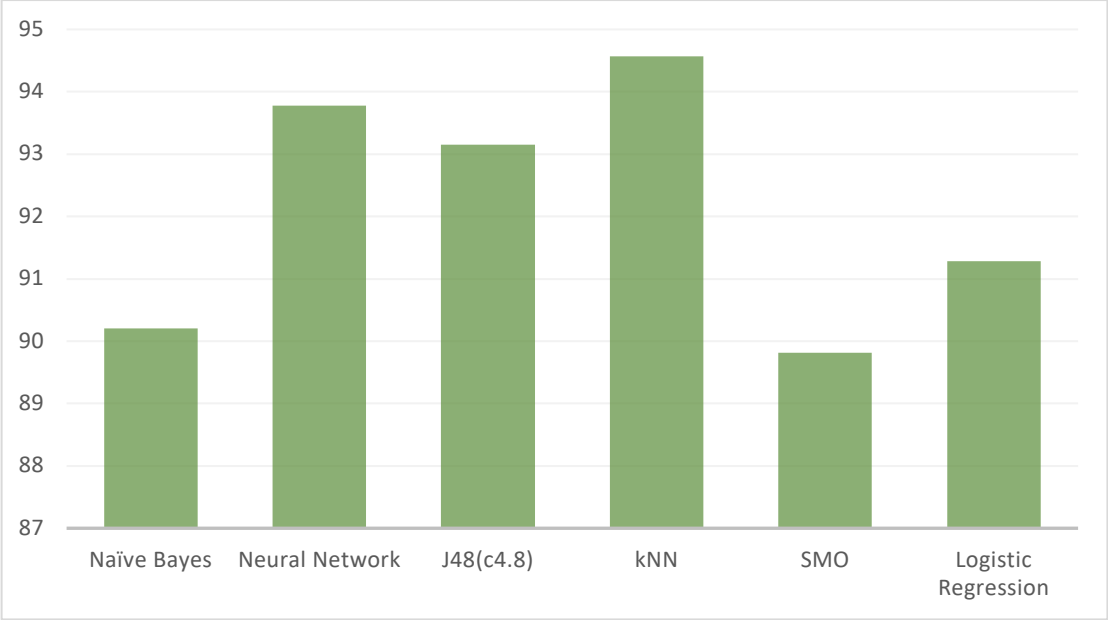

Рисунок 3.8 – Accuracy для всіх характеристик крім аномальних

Показники цього набору впали на 2,7%, це гарний результат, в лідерах залишаються алгоритми Neural Network, kNN і J48 (c4.8).

Далі розглядаються всі характеристики за винятком характеристик HTML і JS, результати представлені в таблиці 3.9 і на рисунку 3.9.

Таблиця 3.9 – Результати тесту для всіх характеристик крім характеристик HTML і JS

Алгоритм	Accuracy	Precision	Recall
Naïve Bayes	92,962	0,93	0,93
Neural Network	96,662	0,967	0,967
J48(c4.8)	95,889	0,959	0,959
kNN	97,087	0,971	0,971
SMO	93,853	0,939	0,939
Logistic Regression	93,731	0,937	0,937

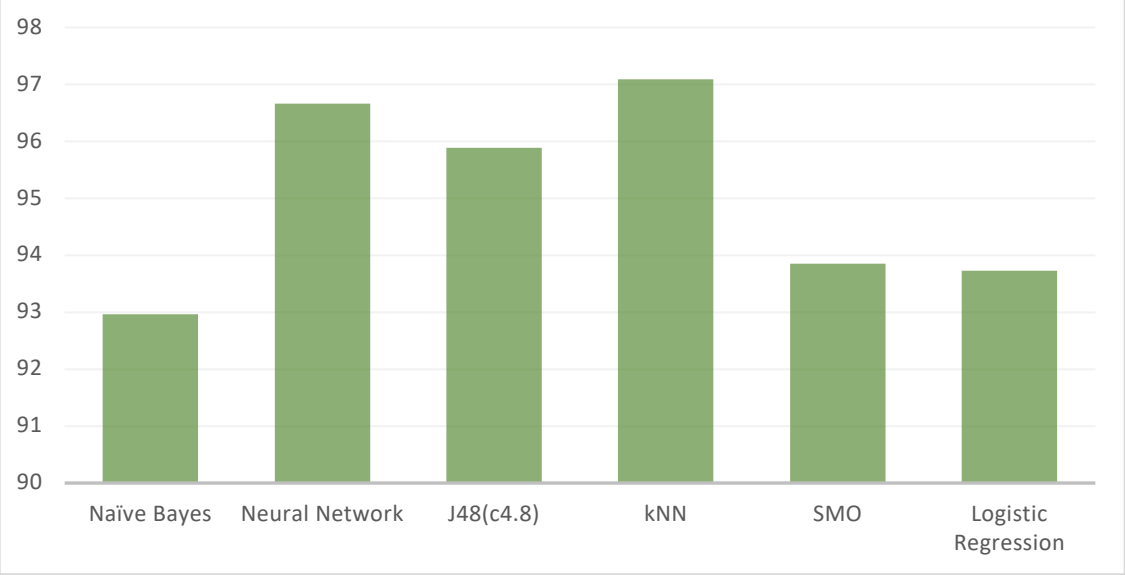

Рисунок 3.9 – Accuracy для всіх характеристик крім HTML & JS

Показники впали менш ніж на 1%, цей набір однозначно можна використовувати для прогнозування фішингових сайтів. Набір складається з 25 показників.

Далі розглядаються всі характеристики за винятком характеристик домену, результати представлені в таблиці 3.10 і на рисунку 3.10.

Таблиця 3.10 – Результати тесту для всіх характеристик крім характеристик домену

Алгоритм	Accuracy	Precision	Recall
Naïve Bayes	92,741	0,928	0,927
Neural Network	94,627	0,946	0,946
J48(c4.8)	94,496	0,945	0,945
kNN	94,984	0,95	0,95
SMO	91,714	0,917	0,917
Logistic Regression	93,162	0,932	0,932

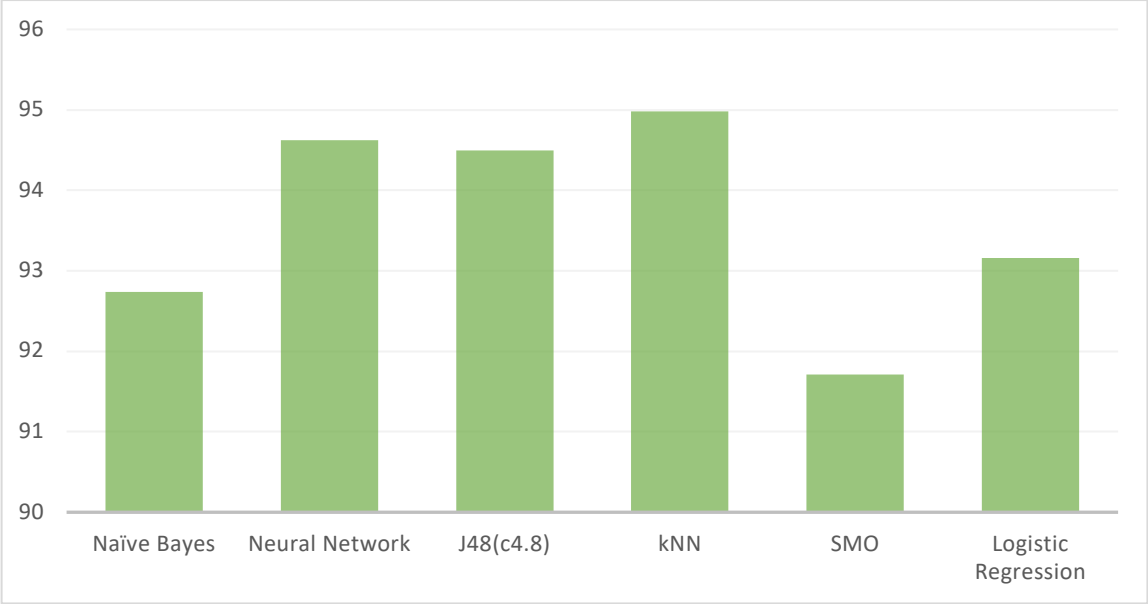

Рисунок 3.10 – Accuracy для всіх характеристик крім доменних

Точність результатів впала на 2-3%, цей набір є конкурентоспроможним у завданні розпізнання фішингових сайтів. Набір включає в себе 23 характеристики.

Підбиваючи підсумки в дослідженні вручну відібраних наборів кращі показники представили такі набори як:

• Всі характеристики крім HTML і JS (показники впали менш ніж на 1%)

• Всі характеристики крім доменних (показники впали менш ніж на 3%)

Найточнішими алгоритмами класифікації виявилися kNN і Neural Network, не на багато відстав результат J48. Найгіршими показали себе Naïve Bayes і SMO.

Далі розглядаються набори автоматично відібраних ознак. Результати дослідження всіх трьох груп представлені в таблиці 3.11 і на рисунку 3.11.

Таблиця 3.11 – Результати тесту accuracy для автоматично відібраних груп

Алгоритм	Група 1(cfs)	Група 2(consistency)	Група 3(wraper)
Naïve Bayes	92,668	92,899	92,474
Neural Network	94,491	96,662	95,884
J48(c4.8)	94,315	95,803	95,984
kNN	94,387	97,078	96,314
SMO	92,587	93,939	92,75
Logistic Regression	93,211	93,917	93,424

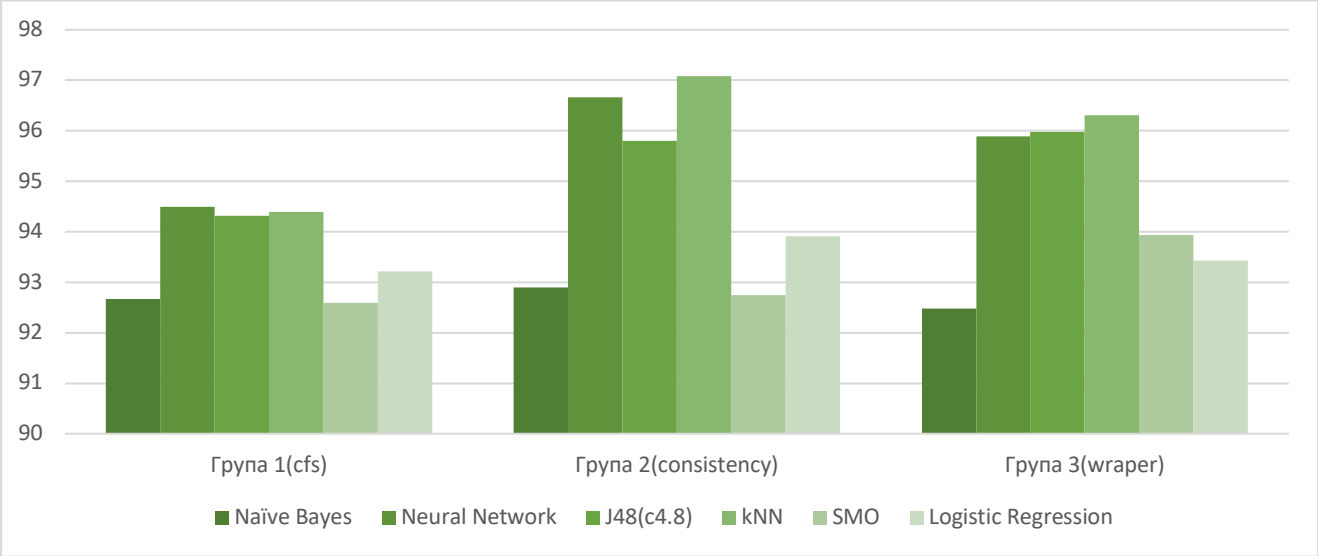

Рисунок 3.11 – Accuracy для автоматично відібраних груп

Згідно з одержаними результатами, розрахунки параметра accuracy показали, що найточнішим для виявлення фішингових сайтів є другий набір характеристик, він складається з 23 ознак і був отриманий методом Consistency subset evaluation, його найкраща точність дорівнює 97,078, а найгірша 92,899, що менш ніж на 0,5% нижче точності прогнозування з набором з усіх характеристик. Група складається з 23 ознак. Не далеко пішла третя група ознак, отриманих методом Wrapper subset evaluation і складається з 19 показників. Кращий результат в цьому піднаборі 96,314, а найгірший 92,474. Показники впали менш ніж на 1%, це означає, що

піднабір можна використовувати для передбачення фішингових сайтів. Група складається з 19 ознак. У першої групи ознак показники найгірші з усіх трьох, але обсяг групи всього 9 характеристик. Кращий результат в цій групі дорівнює 94,491, а найгірший 92,587, в порівнянні з початковим набором характеристик, точність прогнозування впала на менш ніж на 3% для кращого результату, а для гіршого майже не змінилася.

У таблиці 3.12 представлені зведені результати кращих груп ручного відбору та груп автоматичного відбору.

Таблиця 3.12 – Результати тесту accuracy для кращих відібраних груп

Алгоритм	Автоматичний відбір			Ручний відбір		Всі
	Група 1(cfs)	Група 2(consistency)	Група 3(wraper)	Всі крім доменних	Всі крім HTML & JS	
Naïve Bayes	92,668	92,899	92,474	92,741	92,962	92,980
Neural Network	94,491	96,662	95,884	94,627	96,662	96,900
J48(c4.8)	94,315	95,803	95,984	94,496	95,889	95,870
kNN	94,387	97,078	96,314	94,984	97,087	97,180
SMO	92,587	93,939	92,75	91,714	93,853	94,030
Logistic Regression	93,211	93,917	93,424	93,162	93,731	93,990
Кількість характеристик	9	23	19	23	25	30

З таблиці 3.12 видно, що результати групи «1 автоматична» і «все крім доменних» майже рівні з відзнакою 0,1-0,5, але оскільки група 1 складається всього з 9 ознак, її, очевидно, використовувати краще. Також видно схожість результатів 2-ї групи і групи «все крім HTML & JS», вони відрізняються на 0,01-0,2. Для наочності результатів демонструється графік на малюнку 3.12.

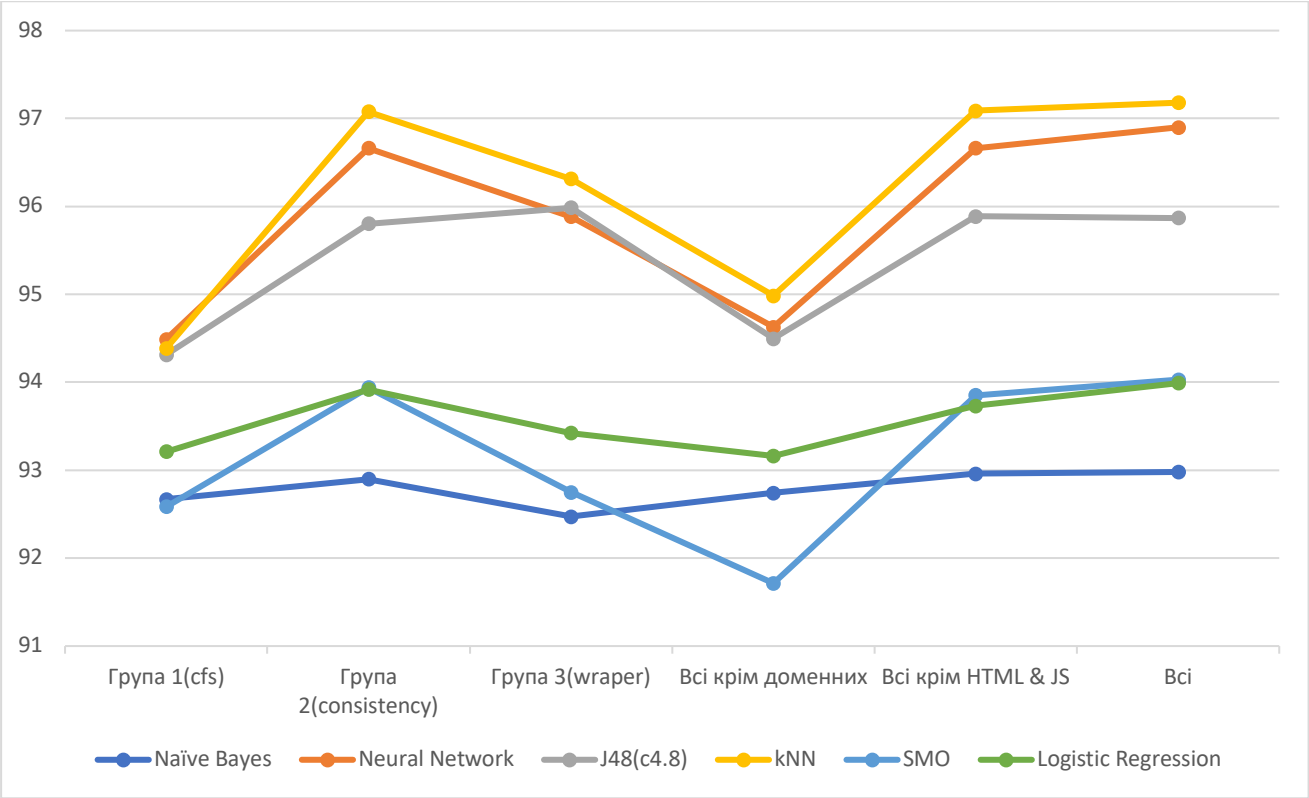

Рисунок 3.12 – Accuracy для кращих відібраних груп

3.4 Результати побудови комбінованої моделі

Метою дослідження так само була побудова комбінованої моделі класифікаторів, яка дозволила б з більшою точністю і акуратністю визначати фішингові сайти. Виходячи з вищенаведеного експерименту кращі результати показували kNN, Neural Network і Decision tree (J48), в порядку зменшення точності. Ще одним важливим критерієм відбору класифікаторів є його час роботи, так час витрачений на побудову моделі kNN одно 0,02 секунди, на побудову Neural Network 164,36 секунд і на побудову Decision tree (J48) - 0,21 секунда. Для прискорення роботи моделі замість Neural Network взяти наступний за ефективністю алгоритм - це Logistic Regression. Час побудови моделі, основаної на цьому алгоритмі - 1,07 секунди. Таким чином для побудови комбінованої моделі класифікаторів обрано алгоритми kNN, LR і J48. Код алгоритму моделі знаходиться у додатку Б.

Для оцінки роботи моделі було взято 5 груп характеристик, що мали найкращі результати у попередньому дослідженні, а також початковий набір. Результати оцінки accuracy представлені у таблиці 3.13.

Таблиця 3.13 – Результати тесту accuracy для комбінації класифікаторів

Група характеристик	Max accuracy до	Max accuracy після	% покращення
Група 1(cfs)	94,491	95,564	1,14
Група 2(consistency)	97,078	98,102	1,05
Група 3(wraper)	96,314	97,022	0,74
Всі крім доменних	94,984	95,78	0,84
Всі крім HTML & JS	97,087	98,34	1,29
Всі	97,18	98,766	1,63

В ході експерименту було встановлено, що завдяки новій схемі класифікації спостерігається покращення таких параметрів як accuracy, precision та recall. В таблиці 3.13 наведені результати тільки тесту accuracy, оскільки не має значної різниці між цим показником та двома іншими. Встановлене підвищення accuracy в межах 0,74 – 1,63%.

Також слід зазначити, що від зміни положення кожного з трьох класифікаторів результат не змінюється. Зріст показників для кожної з груп зображено на рисунку 3.13.

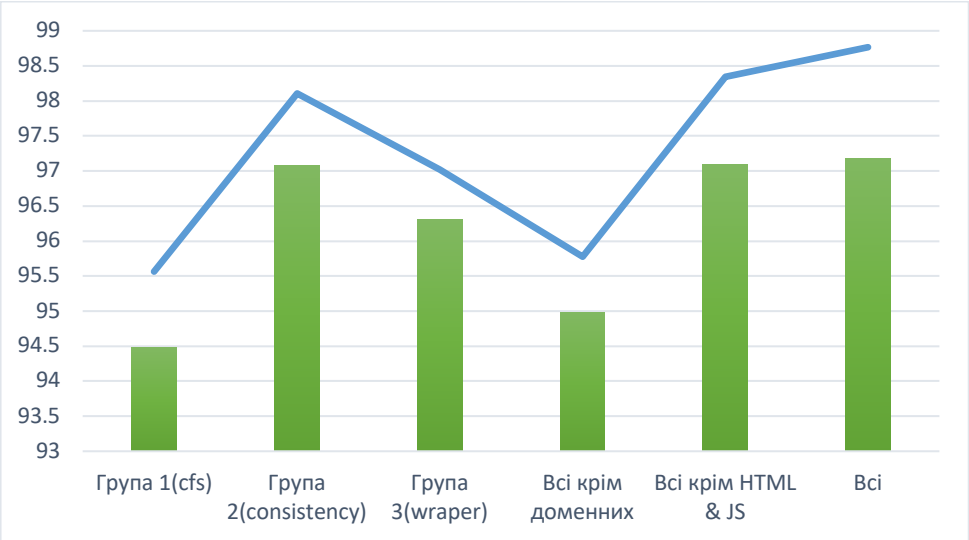

Рисунок 3.13 – Зміна accuracy для запропонованої моделі

Висновки з розділу 3

В розділі 3 були проведені експерименти щодо пошуку найкращого класифікатора, найкращого піднабору характеристик та кращої комбінації класифікаторів. Результати оцінювались з точки зору трьох показників точності, це accuracy, precision та recall, а також враховувався час побудови моделі при відборі класифікаторів для подальшого використання у комбінованій моделі. За наведеними результатами можна зробити такі висновки:

1) Серед розглянутих груп характеристик ручного відбору найкращі результати продемонструвала група характеристик, де не враховувалися характеристики HTML&JavaScript, група містить 25 характеристик. Серед груп автоматичного відбору найкращі результати продемонструвала група відібрана методом Consistency subset evaluator, група складається з 23 характеристик. Різниця у результатах між цими двома наборами дуже незначна, складає 0,01% для найкращого алгоритму(kNN) та 0,06% для найгіршого(NB). Враховуючи кількість ознак у групі, а це впливає на швидкість роботи, найкращою обрано групу 2(consistency). Слід зазначити, що група 1(cfs) має найбільшу швидкодію, оскільки у групі лише 9 ознак.
2) Найкращим класифікатором для цього завдання виявився kNN, з максимальною точністю 97,18%.
3) Щодо нової моделі класифікації, побудованої на простих алгоритмах класифікації kNN, LR, J48, точність розпізнавання виросла у середньому на 1,11%. Також було з’ясовано, що порядок класифікаторів у моделі не впливає на точність прогнозування. Найбільший показник має перевірка на всіх характеристиках зі значенням accuracy 98,766%.

ВИСНОВКИ

Фішингові сайти стали великою проблемою за останні роки. Фішинг - це комп'ютерна атака, яка передає людям повідомлення соціальної інженерії через електронні канали зв'язку, щоб переконати їх виконати певні дії в інтересах зловмисника. Саме таке означення фішингу найбільш повно і точно описує цей вид соціальної інженерії. Існує багато технік розпізнавання фішингових сайтів, але такі недоліки як низька точність, контент може бути таким самим як і на справжньому сайті, тому не розпізнається, рівень розпізнавання невисокий.

У цьому дослідженні:

1) Було вивчено та проаналізовано різні підходи до виявлення фішингових сайтів, встановлено, що вони базуються на навчанні користувачів або використанні програмних засобів (тут підходи поділяються на евристику, чорні списки, візуальну схожість та машинне навчання).
2) Проаналізовано готові програмні продукти для розпізнавання фішингу, їх принцип дії та недоліки, більшість побудована на чорних списках, які не розпізнають щойно створені фішингові сайти.
3) Вивчено актуальні методи класифікації та відбору характеристик за допомогою алгоритмів машинного навчання.
4) Відібрано характеристики, які можуть бути індикаторами того, що сайт є фішинговим, за двома підходами, ручний відбір та автоматичний, було сформовано 11 груп для подальшого дослідження обраними алгоритмами класифікації.
5) Визначено ступінь важливості та інформативності даних характеристик при виявленні фішингових сайтів.
6) Проаналізовано які алгоритми класифікації є найбільш придатними для розв’язання задачі розпізнавання фішингового сайту.
7) Розроблено відповідне програмне забезпечення та здійснено експериментальне дослідження.

8) Запропоновано нову модель класифікації даних, яка є комбінацією декількох вже відомих та досить розповсюджених класифікаторів, яка відрізняється від існуючих покращеною точністю розпізнавання.

Практична цінність результатів полягає у можливості використання отриманого класифікатору для подальшого створення програмних рішень для розпізнавання фішингових сайтів. Він, а також набір характеристик може бути впроваджений у антифішингові розширення для браузерів або інші інструменти боротьби з фішингом.

ПЕРЕЛІК ДЖЕРЕЛ І ПОСИЛАНЬ

1. PhishTank [Електронний ресурс] – Режим доступу до ресурсу: https://www.phishtank.com/what_is_phishing.php
2. C. Whittaker. Large-scale automatic classification of phishing pages [Електронний ресурс] / C. Whittaker, B. Ryner, M. Nazif. – 2013. – Режим доступу до ресурсу: https://research.google.com/pubs/archive/35580.pdf
3. Phishing Activity Trends Report, 1st Quarter 2019 [Електронний ресурс]. – 2019. – Режим доступу до ресурсу: http://docs.apwg.org/reports/apwg_trends_report_q1_2019.pdf
4. Khonji M. Phishing Detection: A Literature Survey [Електронний ресурс] / M. Khonji, Y. Iraqi, A. Jones. – 2015. – Режим доступу до ресурсу: https://www.researchgate.net/publication/256841808_Phishing_Detection_A_Literature_Survey
5. Dakpa T. Study of Phishing Attacks and Preventions [Електронний ресурс] / T. Dakpa, P. Augustine. – 2017. – Режим доступу до ресурсу: https://pdfs.semanticscholar.org/6fb2/13dabcf9c3c30acba3b2e241e5531b0c9a98.pdf
6. Yu W. A phishing vulnerability analysis of web based systems [Електронний ресурс] / W. Yu, S. Nargundkar, N. Tiruthani. – 2015. – Режим доступу до ресурсу: http://ieeexplore.ieee.org/abstract/document/4625681/
7. Abu-Nimeh S. A Comparison of Machine Learning Techniques for Phishing Detection [Електронний ресурс] / S.Abu-Nimeh, D. Nappa, X. Wang, S. Nair. – 2017. – Режим доступу до ресурсу: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.114.1242&rep=rep1&type=pdf
8. Sheng S. An Empirical Analysis of Phishing Blacklists [Електронний ресурс] / S. Sheng, G. Warner, L. Cranor. – 2009. – Режим доступу до ресурсу: https://www.researchgate.net/publication/228932769_An_Empirical_Analysis_of_Phishing_Blacklists
9. Kumar Jain A. Phishing Detection: Analysis of Visual Similarity Based Approaches [Електронний ресурс] / A. Kumar Jain, B. Gupta. – 2017. – Режим доступу до

ресурсу: https://www.researchgate.net/publication/312205924_Phishing_Detection_Analysis_of_Visual_Similarity_Based_Approaches

10. Anti-Phishing Services: Pros and Cons [Електронний ресурс] – Режим доступу до ресурсу: https://resources.infosecinstitute.com/category/enterprise/phishing/phishing-countermeasures/anti-phishing-services-pros-and-cons/
11. Top 10 algorithms in data mining [Електронний ресурс] / X.Wu, V. Kumar, J. Quinlan, Z. Zhou. – 2017. – Режим доступу до ресурсу: https://www.researchgate.net/publication/29467751_Top_10_algorithms_in_data_mining
12. Ramesh G. An efficacious method for detecting phishing webpages through target domain identification [Електронний ресурс] / G. Ramesh, I. Krishnamurthi, K. Kumar – Режим доступу до ресурсу: https://github.com/secdr/sec-paper/blob/master/Phishing/An%20efficacious%20method%20for%20detecting%20phishing%20webpages%20through%20target%20domain%20identification.pdf
13. Abdelhamid N. Phishing detection based Associative Classification data mining [Електронний ресурс] / N. Abdelhamid, A. Ayesh, F. Thabtah. – 2014. – Режим доступу до ресурсу: https://www.researchgate.net/publication/262111701_Phishing_detection_based_Associative_Classification_data_mining
14. Al-diabat M. Detection and Prediction of Phishing Websites using Classification Mining Techniques [Електронний ресурс] / Mofleh Al-diabat. – 2016. – Режим доступу до ресурсу: https://www.researchgate.net/publication/306124393_Detection_and_Prediction_of_Phishing_Websites_using_Classification_Mining_Techniques
15. Ali W. Phishing Website Detection based on Supervised Machine Learning with Wrapper Features [Електронний ресурс] / Waleed Ali. – 2017. – Режим доступу до ресурсу: https://www.researchgate.net/publication/320131222_Phishing_Website_Detection_based_on_Supervised_Machine_Learning_with_Wrapper_Features_Selection

16. Abdeyazdan M. Detecting Internet Phishing Attacks Using Data Mining Methods [Електронний ресурс] / M. Abdeyazdan, A. Ali Rayat. – 2016. – Режим доступу до ресурсу: http://iieng.org/images/proceedings_pdf/E0816003.pdf
17. Islam M. Phishing Websites Detection Using Machine Learning Based Classification Techniques [Електронний ресурс] / M. Islam, N. Chowdhury. – 2013. – Режим доступу до ресурсу: https://www.researchgate.net/publication/269032183_Detection_of_phishing_URLs_using_machine_learning_techniques
18. Jabri R. Phishing Websites Detection Using Data Mining Classification Model [Електронний ресурс] / Riad Jabri. – 2015. – Режим доступу до ресурсу: https://www.researchgate.net/publication/282408351_Phishing_Websites_Detection_Using_Data_Mining_Classification_Model
19. Tiwari P. International Journal of Engineering Research &Technology [Електронний ресурс] / P. Tiwari, R. Singh. – 2015. – Режим доступу до ресурсу: https://www.ijert.org/
20. Gupta D. Comparison of classification algorithms to detect phishing web pages using feature selection and extraction [Електронний ресурс] / Dr. Rajendra Gupta. – 2016. – Режим доступу до ресурсу: https://pdfs.semanticscholar.org/fccd/8ff23734a1947d3efc14d3df9863a5efac6c.pdf
21. Mohammad R. An assessment of features related to phishing websites using an automated technique [Електронний ресурс] / R. Mohammad, F. Thabtah, L. McCluskey. – 2012. – Режим доступу до ресурсу: https://www.researchgate.net/publication/261081735_An_assessment_of_features_related_to_phishing_websites_using_an_automated_technique
22. ConsistencySubsetEval [Електронний ресурс] – Режим доступу до ресурсу:http://weka.sourceforge.net/doc.stable/weka/attributeSelection/ConsistencySubsetEval.html
23. WrapperSubsetEval [Електронний ресурс] – Режим доступу до ресурсу: http://weka.sourceforge.net/doc.stable/weka/attributeSelection/WrapperSubsetEval.html
24. CfsSubsetEval [Електронний ресурс] – Режим доступу до ресурсу: http://weka.sourceforge.net/doc.stable/weka/attributeSelection/CfsSubsetEval.html

ДОДАТОК А

Характеристика	Група1(cfs)	Група2(consistency)	Група3(wrapper)
Using the IP Address		■	■
Long URL		■	■
Using URL Shortening Services “TinyURL”		■	■
URL’s having “@” Symbol		■	
Redirecting using “//”			
Adding Prefix or Suffix Separated by (-) to the Domain	■	■	■
Sub Domain and Multi Sub Domains	■	■	■
HTTPS (Hyper Text Transfer Protocol with Secure Sockets Layer)	■	■	■
Domain Registration Length		■	
Favicon			
Using Non-Standard Port			■
The Existence of “HTTPS” Token in the Domain Part of the URL		■	
Request URL	■	■	■
URL of Anchor	■	■	■
Links in <Meta>, <Script> and <Link> tags	■	■	■
Server Form Handler (SFH)	■	■	
Submitting Information to Email		■	■
Abnormal URL			
Website Forwarding		■	
Status Bar Customization			■
Disabling Right Click			
Using Pop-up Window		■	■
IFrame Redirection			■
Age of Domain		■	■
DNS Record		■	■
Website Traffic	■	■	■
PageRank		■	■
Google Index	■	■	
Number of Links Pointing to Page		■	■
Statistical-Reports Based Feature		■	

ДОДАТОК Б

```
import weka.core.jvm as jvm
import weka.core.serialization as serialization
from weka.classifiers import Classifier
from weka.core.converters import Loader
from weka.core.classes import Random
from sklearn.metrics import accuracy_score
jvm.start()

loader = Loader(classname="weka.core.converters.ArffLoader")
data = loader.load_file("../all.arff")
data.class_is_last()
train, test = data.train_test_split(70.0, Random(1))

J48 = Classifier(jobject = serialization.read("../J48.model"))
IBk = Classifier(jobject = serialization.read("../IBk.model"))
Logistic = Classifier(jobject = serialization.read("../Logistic.model"))

pred_J48 = []
pred_IBk = []
pred_Logistic = []

actual = []
for index, inst in enumerate(test):
      pred = J48.classify_instance(inst)
      actual.append(inst.get_string_value(inst.class_index))
      pred_J48.append(inst.class_attribute.value(int(pred)))

for index, inst in enumerate(test):
      pred = IBk.classify_instance(inst)
      pred_IBk.append(inst.class_attribute.value(int(pred)))

for index, inst in enumerate(test):
      pred = Logistic.classify_instance(inst)
      pred_Logistic.append(inst.class_attribute.value(int(pred)))

MultiClass =[]
for i in range(0,len(test)):
   if pred_Logistic[i] == pred_IBk[i]:
      MultiClass.append(pred_Logistic[i])
   else:
      MultiClass.append(pred_J48[i])

print(accuracy_score(actual,MultiClass))
```