МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМ. В. ДАЛЯ
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА ЕЛЕКТРОНІКИ
КАФЕДРА КОМП'ЮТЕРНИХ НАУК ТА ІНЖЕНЕРІЇ

До захисту допускається
Завідувач кафедри
_____ Скарга-Бандурова І.С.
«____»_____ 2019 р.

МАГІСТЕРСЬКА РОБОТА

НА ТЕМУ:

Інформаційна технологія виявлення шахрайства в банківській системі

Освітньо-кваліфікаційний рівень "Магістр"
Спеціальність 122 – "Комп'ютерні науки"

Науковий керівник роботи:	_____ (підпис)	О.І. Рязанцев (ініціали, прізвище)
Консультант з охорони праці:	_____ (підпис)	Я.О. Критська (ініціали, прізвище)
Студент:	_____ (підпис)	Д.О. Знаменський (ініціали, прізвище)
Група:		КН-17дм

Сєвєродонецьк 2019

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ВОЛОДИМИРА ДАЛЯ

Факультет Інформаційних технологій та електроніки
Кафедра Комп'ютерних наук та інженерії
Освітньо-кваліфікаційний рівень магістр
Напрям підготовки "Комп'ютерні науки"
(шифр і назва)
Спеціальність 122 – "Комп'ютерні науки"
(шифр і назва)

ЗАТВЕРДЖУЮ:

Завідувач кафедри _____
_____ І.С. Скарга-Бандурова
«_____» _____2019 р.

ЗАВДАННЯ
НА МАГІСТЕРСЬКУ РОБОТУ СТУДЕНТУ

Знаменському Дмитру Олександровичу
(прізвище, ім'я,по батькові)

1. Тема роботи Інформаційна технологія виявлення шахрайства в банківській системі керівник проекту (роботи) к.т.н., проф. Рязанцев О.І.

(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом вищого навчального закладу від " _ " _ 2018 року №
2. Строк подання студентом проекту (роботи) 12.01.2019
3. Вихідні дані до проекту (роботи) матеріали науково-дослідницької практики

4.Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)Аналіз існуючих систем, створення інформаційної технології виявлення шахрайства в банківських системах, питання охорони праці, екологія.
5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслеників)
Презентація доповіді.

6. Консультанти розділів проекту (роботи)

Розділ	Прізвище, ініціали та посада П.І.Б. консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці	Критська Яна Олександрівна		

7. Дата видачі завдання 18.10.2018

Керівник _____
(підпис)

Завдання прийняв до виконання _____
(підпис)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Найменування етапів дипломного проекту (роботи)	Термін виконання етапів проекту (роботи)	Примітка
1	Огляд проблеми.	18.10.2018 – 16.11.2018	
2	Дослідження існуючих засобів захисту в банківських системах.	17.11.2018 – 22.11.2018	
3	Реалізація алгоритмів та моделі.	23.11.2018 – 28.11.2018	
4	Проведення експерименту та огляд результатів	29.11.2018 – 07.12.2018	
5	Розгляд питань охорони праці та основних напрямків їх дотримання.	08.12.2018 – 12.12.2018	
6	Оформлення пояснювальної записки.	13.12.2018 – 20.12.2018	
7	Оформлення презентації роботи	21.12.2018 – 24.12.2018	
8	Підготовка та подання магістерської роботи до захисту	07.01.2019 – 16.01.2019	

Студент _____ Знаменський Д.О.
(підпис) (прізвище та ініціали)

Науковий керівник _____ Рязанцев О.І.
(підпис) (прізвище та ініціали)

АННОТАЦИЯ

Знаменский Д.А. Информационная технология обнаружения мошенничества в банковской системе.

Целью данной магистерской аттестационной работы является разработка аналитического ядра выявления мошеннических действий в платежных операциях банковской системы. Данный сервис преследует цель снизить денежные потери от преступных действий.

Ключевые слова: банкинг, мошенничество, информационная технология, банковскя система.

АНОТАЦІЯ

Знаменський Д.А. Інформаційна технологія виявлення шахрайства в банківській системі.

Метою даної магістерської атестаційної роботи є розробка аналітичного ядра виявлення шахрайських дій в платіжних операціях банківської системи. Даний сервіс має на меті знизити грошові втрати від злочинних дій.

Ключові слова: банкінг, шахрайство, інформаційна технологія, банківська система.

THE ABSTRACT

Znamensky D.A. Information technology of fraud detection in the banking system.

The purpose of this master's attestation work is to develop analytic core for detecting fraudulent actions in the payment transactions of the banking system. This service aims to reduce the monetary losses from criminal acts.

Key words: banking, fraud, information technology, banking system.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

SMS – Short Message Service
SSL – Secure Sockets Layer
SVM – Support Vector Machine
REST – Representational State Transfer

ВСТУП

Актуальність теми. Історія впровадження всесвітніми банками електронних грошей починає свій розвиток з 1918 року, коли Федеральний Резервний Банк США зробив перший в світі валютний переказ за допомогою телеграфу. З тих пір організації в банківській сфері розробляли і впроваджували все більш оптимізовані способи безготівкового переказу грошей, проте якісний стрибок стався після появи всесвітньої мережі Інтернет. Саме тоді переказ грошей за допомогою банківської системи придбав характерні риси, які якісно відрізняють його від готівкового переказу.

Сьогодні, будь-яка людина в будь-який час маючи свій електронний рахунок може оплатити послугу, не виходячи з квартири. Простота спричинила за собою масовість, що не пройшло повз уваги інтернет шахраїв. Знаходження програмних вразливостей в системі, викрадення персональніих даних, оплата зі зламаних рахунків це невеликий перечень злочинів, пов'язаних з банківськими системами.

У роботі розглядаються основні аспекти злочинів у банківській сфері, огляд наявних засобів захисту і створення інформаційної технології, здатної визначати махінації з переведенням безготівкових грошей в інтернеті.

Мета і задачі дослідження. Аналіз та вибір найбільш оптимальних засобів та методів для створення інформаційної технології.

Об’єкт дослідження – процес моніторингу грошових операцій на банківському рахунку.

Предмет дослідження – методи виявлення шахрайства в банківських системах.

Методи дослідження. Під час дослідження застосовувались аналітичні алгоритми аналізу.

Наукова новизна одержаних результатів.

- запропонований метод виявлення інтернет злочинства в банківських системах, в якому аналізуються данні о грошових переказах;
- запропонована модель виявлення інтернет злочинства в банківських системах, яка має поліпшити якість функціонування банківської системи.

Практичне значення одержаних результатів. Побудова інформаційної технології для виявлення електронного шахрайства для використання в сфері банкінгу.

РОЗДІЛ 1
АНАЛІЗ ВИМОГ ТА ПОСТАНОВА ЗАДАЧІ

1.1 Загальна характеристика пробелеми

На даний момент можна виділити найголовнішу невирішену задачу в сфері кібербезпеки, і суть цієї проблеми полягає в захисті персональних даних користувача в банківських системах. Як показує практика, більшість людей мають свої електронні банківські рахунки за допомогою яких вони оплачують послуги в мережі Інтеренет.

Питанню електронної безпеки банківської системи присвячено багато наукових праць, зокрема роботи видатних зарубіжних дослідників В. Ойккена (V. Oyken), Я. Корнаі (Y. Kornay), І. Шумперт (I. Shympert), Е. Уткіна (E. Utkin) та ін., але це питання й досі залишається відкритим.

У 2017 р. З.Р. Абдєева опублікувала наукову статтю[1], в якій перерахувала основні види шахрайства в банківській сфері, програмні засоби для боротьби з вірусними атаками на систему електронних грошей, та перспективи розвитку сервісів онлайн транзакцій.

В статті виділені наступні види фальсифікацій з електронними грошима в банківській системі:

- ризик дублювання технічного пристрою (електронного гаманця або жорсткого диска комп'ютера);
- ризик зміни або дублювання звернень або програм;
- ризик зміни повідомлень;
- риск викрадення;
- ризик відмови операцій.

Для попередження викрадення особистих даних пропонується використовувати:

- протокол SSL;
- перевірку CVV2 / CBK2-кодів;
- список паролей, роздрукований у вигляді чека з банкомату, який необхідно зберігати для підтвердження майбутніх операцій.

У 2018 році Юсупова О.А. опублікувала роботу[2], в якій проаналізувала проблеми інформаційної безпеки в сфері інтернет банкінгу. Виявляється, що за даними одного з провідних міжнародних компаній Group-IB, з кожним роком спостерігається збільшення цільових атак (DDoS-атаки6, спам тощо) на банківські організації. Як випливає з дослідження, найбільш поширеним способом впливу мошенників на банківські рахунки

клієнтів протягом п'яти років залишалося відправлення на поштові адреси або мобільні телефони спам повідомлення, що містять посилання на шкідливий програмний код. Від дій порушників постраждали навіть такі компанії, як «Сколково-Нанотех» та «Тройка Венчур Кепітал», а в платіжній системі «Ківі» було зафіксовано втрату на сумму близько 40 млн. грн.

Цілих О.Н опублікував роботу [3], в якій з'ясував, що найбільш важлива інформація, яку намагаються роздобути шахраї, це данні про залишки коштів на рахунку, інформація про грошові перекази, та інформація про систему захисту банку. Як наслідок, введення нових і сучасних засобів захисту від шахраїв - пріоритет для всіх банківських установ і головне завдання в сфері безпеки.

У зв'язку з такими величезними грошовими втратами виникає питання встановлення вимог до безпеки банківської системи.

Розглянемо суть поняття кібебезпека. Дотримуватися кібербезпеки в мережі Інтернет означає, що ті особисті дані, які находяться на базі електронного ресурсу, доступні тільки для певного кола осіб, відповідального за роботу системи, можливість доступу для сторонніх осіб обмежена, що нівелює можливість втрати даних без злому системи.

1.) Інформаційні ресурси системи захищені, якщо до них є доступ тільки у певного системою кола осіб.

2.) Коло осіб, які мають доступ до певної інформації в системі не може бути розширено без реєстрації користувача в системі.

У банківській системі електронних платежів, присутня перевірка особистих даних того хто запитує доступ і перевірка для чого запитується цей доступ. Іншими словами в разі збою, злому або втрати даних стороння особа, яка може бути потенційним шахраєм отримує доступ до особистої інформації користувачів системи. Так само є два типи загроз - ті, які надходять від сторонніх осіб, і ті, які надходять від самих працівників банківської системи. У разі якщо стався збій в роботі системи, втрата даних, але до цього не причетні ні працівники ні сторонні особи, причина збою можлива в аппартаних неполадках обладнання, некоректно праюючого серверного обладнання, обриви з'єднань, перепади напруги що можуть вплинути на випадкові помилки в системі. Так само до таких причин можна віднести обставини природного характеру, землетруси, повені, пожежі, при яких можливо як часткове пошкодження системи, так і повне її знищення.

Особисті дані користувачів системи можуть стати доступні стороннім особам через:

- отримання доступу до даних під час відправки їх на сервер;
- редагування даних (відсилання особі фішингових повідомлення нібито від імені адміністратора сисеми з пропозицією вказати логін і пароль);

- відправка співробітнику системи повідомлення від імені потенційної жертви;
- технічний злом;
- аппаратний злом;
- підроблена реєстрація;
- помилка в обладнанні.

Можна виділити наступні найбільш відомі види інтернет-шахрайства пов’язані з користувачами банківських систем в інтернеті:

- фішинг;
- вішинг;
- спам;
- Ddos-атаки;
- кардінг;
- скіммінг;
- клікфрод.

Фішинг – вид інтернет-злочину, ціллю якого є одержати персональні дані користувача. Сюди можна прирахувати викрадення паролів, номерів банківських карток, рахунків та іншої персональної інформації. Фішинг представляє з себе підроблене повідомлення, що прийшов на скриньку від банків, провайдерів, та інших інстанцій про те, що з якоїсь причини адресанту негайно треба предоставити або оновити персональні дані. Причини бувають різні, це може бути втрата даних, або помилка в системі .

Атаки фішерів стають все більш комплексними, тому що використовуються алгоритми соціальної інженерії. Але у кожному разі користувача намагаються налякати, придумати негайний привід для того, щоб він відправив свої особисті дані. Як правило, ці звістки мають в собі загрозу, нзокрема те, що буде заблокований рахунок у випадку ігноруванням адресантом вимог, представлених у повідомленні. Майже завжди як причина, по якій жертва повиненна відправити персональну інформацію, шахраї називають потребою покращити антифішингові сервіси (“якщо ви хочете забезпечити собі захист від фішингу, увійдіть на цей сайт та авторизуйтесь”). Приклад фішингового повідомлення зображений на рисунку 1.1.

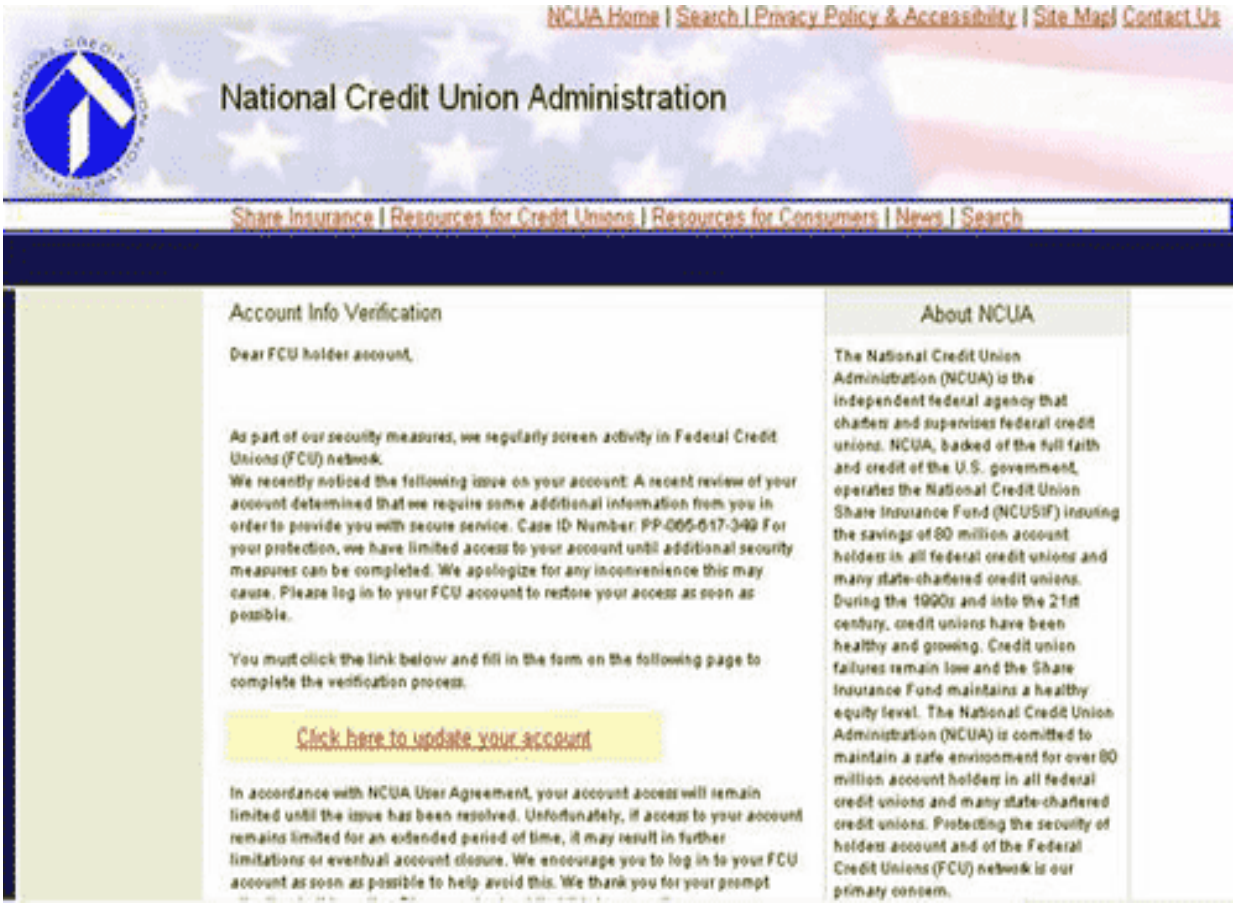


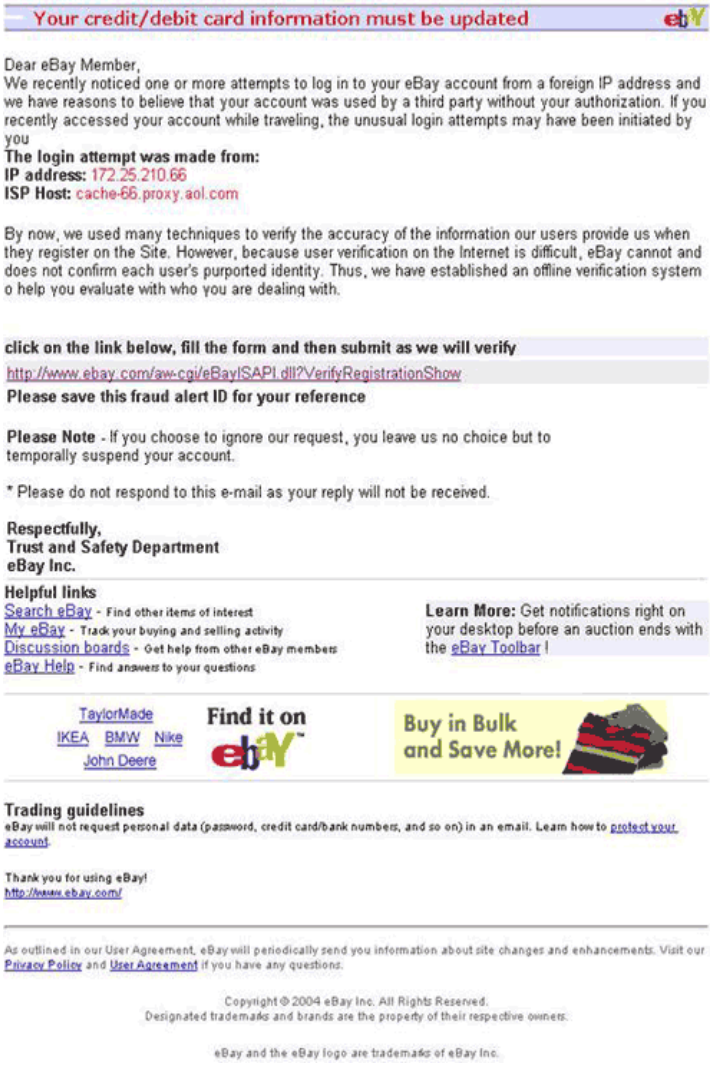
Рисунок 1.1 – Зразок фішингового сайту

Фішингові сайти, майже завжди, функціонують короткий проміжок часу (приблизно 3 - 4 днів). По причині того, що антифішингові системи доволі оперативно отримують данні про чергові загрози, шахраї змушені створювати все нові і нові сайти. Ці сайти мають однаковий візуальний стиль – він повторює оригінальний офіційний сайт, під який пробують підмінити свій сайт фішери. Перейшовши на шахрайский сайт, людина вбиває у відповідні поля персональну інформацію, а далі фішери одержують пароль в кращому разі від його електронної пошти, а в гіршому разі – до його банківського рахунку. Однак не всі шахраї самі знімають фінанси з картки жертв. Річ у тім, що транзакція віртуальних коштів у готівку складно зробити на практиці, до того ж шахрая, який це робить, простіше зловити і завести на нього справуі. Так що, зберігши персональну інформацію, багато шахраїв розсилаюсть за кошти їх другим шахраям, які, щодо себе, мають безпечні методи переведення в готівку коштів з зломаних рахунків. Першочергові жертви даного виду шахрайства – банківські системи та електронні платіжні системи. У підсумку фішери

бажають взнати ту персональну інформацію, котра допоможе їм отримати доступ до фінансів.

Ще один часто зустрічаючийся вид викрадення персональних даних від електронної скриньки – наведена інформація може використовуватися тими, хто розповсюджує віруси. Показовою рисою фішингових повідомлень є високорівнева якість підробленого сайту. Жертві надходить повідомлення з лого банку чи сайту, який на вигляд в точності такий же як реальне лого. Не знаючи про реальний хід справи жертва натискє на посилання та заходить не на офіційний сайт, а на підробний сайт, зроблений з найкращою схожістю. Ще однією прийом шахраїв є посилання, на вигляд найблизько співпадаючі з URL вихідних сайтів. В результаті навіть дуже уважна людина може не помітити те, що у рядку вводу пошуковика показується посилання цілком і повністю відмінне від справжнього посилання сайту. Дані шахрайскі посилання також мають місце бути, але створені вони для того, щоб провести саму недосвідчену людину. Такі повідомлення завжди починаються з IP-адреси, хоча офіційні компанії вже здавна не відсилають такого типу листи. По цій причині шахрайскі URL в багатьох випадках схожі на офіційнії. Ці адреси в багатьох випадках містять в собі назву офіційного URL, яке змінене іншими словами (к приміру, замість www.stiedu.com користувачеві відображається адреса www.stiedui.com). Крім того часто використовуваний фішинговий метод – адреси з крапкою натомість слеша, на вигляд дуже схожі на офіційні посилання (наприклад, www.stiedu.com/student.register замість www.stiedu.com/studentl/register).

Ще в тексті листа може показуватись посилання на офіційний сайт, проте справжній URL, на який вона посилається, буде другим. Пильність жертви знижується тим, що в повідомленні може бути багато інших посилань, що бть вести на справжній сайт, але головне посилання, за яким жертві необхідно пройти та ввести свої персональні дані, приводить на фішинговий сайт (рис. 1.2).



Your credit/debit card information must be updated

Dear eBay Member,
We recently noticed one or more attempts to log in to your eBay account from a foreign IP address and we have reasons to believe that your account was used by a third party without your authorization. If you recently accessed your account while traveling, the unusual login attempts may have been initiated by you
The login attempt was made from:
IP address: 172.25.210.66
ISP Host: cache-66.proxy.aol.com

By now, we used many techniques to verify the accuracy of the information our users provide us when they register on the Site. However, because user verification on the Internet is difficult, eBay cannot and does not confirm each user's purported identity. Thus, we have established an offline verification system o help you evaluate with who you are dealing with.

click on the link below, fill the form and then submit as we will verify
http://www.ebay.com/aw-cgi/eBayISAPI.dll?VerifyRegistrationShow
Please save this fraud alert ID for your reference

Please Note - If you choose to ignore our request, you leave us no choice but to temporally suspend your account.

* Please do not respond to this e-mail as your reply will not be received.

Respectfully,
Trust and Safety Department
eBay Inc.

Helpful links
Search eBay - Find other items of interest
My eBay - Track your buying and selling activity
Discussion boards - Get help from other eBay members
eBay Help - Find answers to your questions

Learn More: Get notifications right on your desktop before an auction ends with the eBay Toolbar !

TaylorMade
IKEA BMW Nike
John Deere
Find it on eBay
Buy in Bulk and Save More!

Trading guidelines
eBay will not request personal data (password, credit card/bank numbers, and so on) in an email. Learn how to protect your account.

Thank you for using eBay!
http://www.ebay.com/

As outlined in our User Agreement, eBay will periodically send you information about site changes and enhancements. Visit our Privacy Policy and User Agreement if you have any questions.

Copyright © 2004 eBay Inc. All Rights Reserved.
Designated trademarks and brands are the property of their respective owners.

eBay and the eBay logo are trademarks of eBay Inc.

Рисунок 1.2 – Зразок фішингового листу

У рідких випадках персональні дані користувача просять ввести безпосередньо в посланні. Очевидно що справжнє повідомлення від банку ніколи не буде мати такого прохання

Вішинг – популярне мережеве шахрайство, суть якого полягає в повідомленні користувачів будь-якої платіжної системи на електронну скриньку начебто від банка або його служби безпеки з пропозицією повідомити номери своїх банківських рахунків, паролі і так далі. В такому разі посилання в листі веде на шахрайський сайт, де і проходить викрадення персональних даних. Після цього сайт видаляється через декілька годин, і вислідити хто його автор в інтернеті фактично неможливо. Методи викрадення даних на перший вигляд, майже однакові, однак у вішингу в електронному повідомленні автори листа потребують зателефонувати на вказаний номер. Коли людина звонить на цей номер, її

просять сказати свою персональну інформацію. Шахрая, який звонить з даного номера знайти дуже складно, так як з розповсюдженням інтернет-телефонії, виклик на міський номер телефона скоріш за все буде автоматично переадресований у довільну точку нашої планети на неіснуючий номер. Так як людина, яка позвонила на шахрайский номер телефона про це не знає, цим вдало користуються злочинці. Згідно даним від Secure Computing, злочинці програмують бота, який постійно набирає номери телефонів в вказаному регіоні і, коли на виклик відповідають, проводиться наступне:

- автовідповідач говорить, що рахунок чи банківська картка зламані, та повідомляє що треба негайно передзвонити за певним номером;аппаратний злом;
- коли жертва набрала вказаний номер, автовідповідач говорить, що людина має зробити звірку інформації та набрати 16-значний код картки з телефону, коли пароль введен, шахрай здобуває усю необхідну інформацію;
- за допомогою такого дзвінка, можна взнати будь-яку інформацію, наприклад пін-код, номер іншого рахунку тощо.

Спам – масове розповсюдження повідомлень рекламного чи іншого характеру особам, які не висловили бажання її одержувати. Перш за все поняття «спам» відноситься до рекламних електронних повідомлень.Слово «спам» почало використовуватися з 1994 року, коли рекламні фірми почали надсилати в групах новин Usenet, дискусійних листах, гостьових книгах інформацію, що не має ніякого відношення до заданої тематики, або повідомлення, яке є прямою рекламою (Рис. 1.3).

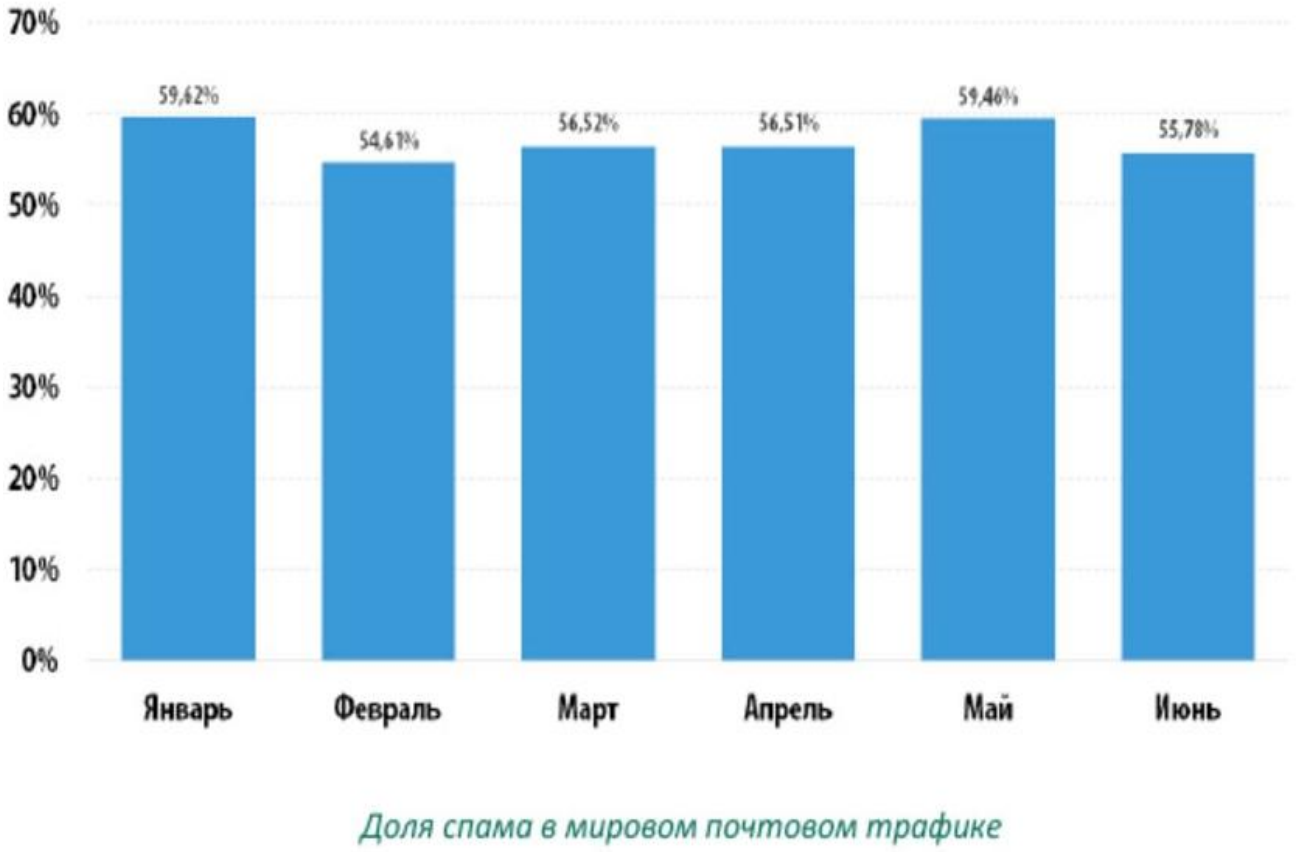


Рисунок 1.3 – Доля спама в електронних повідомленнях

Найбільший потік спаму поширюється через електронну пошту (e-mail). Станом на 2016 рік потік спаму в загальному трафіку електронної пошти становить близько 65% за даними Cisco Systems. Спамери збирають e-mail адреси за допомогою спеціального бота або вручну (рідко), використовуючи веб-сторінки, конференції Usenet, списки розсилок, електронні дошки оголошень, гостьові книги, чати тощо. Такі програми-роботи здатні зібрати за годину тисячі адрес і створити з них базу даних для подальшого розсилання на них спаму.

Деякі компанії займаються тільки збором адрес, а бази потім продають. Деякі компанії продають спамерам e-mail адреси своїх клієнтів, що замовили в них товари чи послуги електронною поштою. Приклад спам листа зображений на рисунку 1.4.

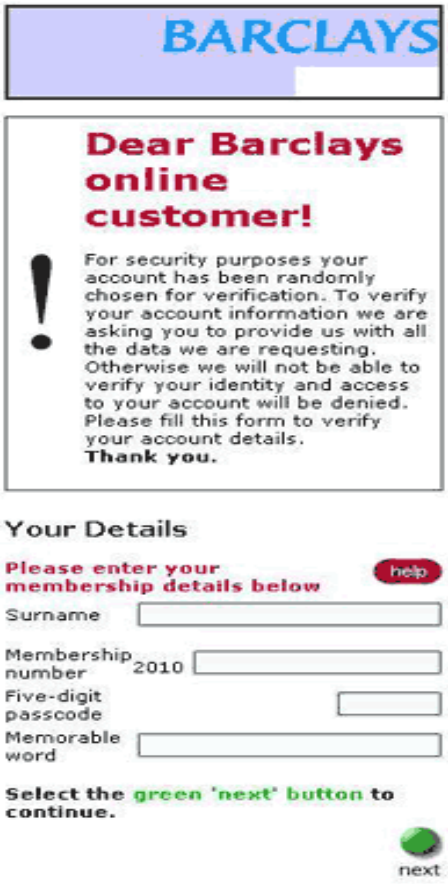


Рисунок 1.4 – Приклад спам листа

Ddos – атака – атака на інформаційну систему з цілью перетворити їїі ресурси на такі, котрі будуть недоступними користувачам, для яких інформаційна система була створена.

Одним із найпопулярнійших алгоритмів атаки є відправка до атакованого комп'ютера або серверу велику множину зовнішніх запитів (які не несуть смислове навантаження), що стає причиною того, що атакований компьютер не має змоги відповісти на запити, або відповідає з великими затримками, так що робота з ним стає неможливою. Підсумувавши, злам системи компьютера робиться як з примусом атакованої системи до зупинки виконання команд програмного забезпечення або до витрат наявних ресурсів, через що система не може продовжувати працювати . DoS-атаки діляться на локальні та віддалені. До локальних відносяться різні експлойти: форк-бомби і програми, що відкривають по мільйону файлів або запускають якийсь циклічний алгоритм, який навантажує пам'ять та процесорні ресурси.

Для локальної DoS атаки необхідно мати, або якимось чином отримати доступ до атакованої машини на рівні, що буде достатнім для захоплення ресурсів. Віддалені DoS-атаки поділяються на два види:

- Віддалена експлуатація помилок в ПЗ з метою довести його до неробочого стану
- flood - посилка на адресу жертви величезної кількості безглуздих (рідше — осмислених) пакетів.

У першому випадку потік пакетів займає весь пропускний канал і не дає машині, що атакується, можливості обробляти легальні запити. У другому — ресурси машини захоплюються за допомогою багаторазового і дуже частого звернення до якого-небудь сервісу, що виконує складну, ресурсоємну операцію. Це може бути, наприклад, тривале звернення до одного з активних компонентів (скрипту) web-сервера. Сервер витрачає всі ресурси машини на обробку запитів, що атакують, а користувачам доводиться чекати.

Кардінґ – вид інтернет злочинства, при якому виконуються дії з використанням електронної картки, яка не активована або не зареєстрована її власником. Данні для активації платіжних карток найчастіше знаходять на пошкоджених серверах онлайн-сервісів, платіжних систем, а також з домашніх комп'ютерів використовуючи для цього шахрайські програми, наприклад Trojan або Worm. Як приклад, одним з найбільших шахрайств в рамках картингу можна назвати злам всесвітнього процесингу банківських карток Worldpay та викрадення з використанням цього способу персональної інформації приблизно на 10 мільйонів доларів США. У грудні 2016 р. упо цьому ділу були пред'явлені звинувачення хакерській групі, в якої були громадяни СНД.

Скіммінг – це метод зчитування даних карти з використанням спеціалізованого пристрою який називається скімер. Шахраї зчитують усі дані з магнітної смуги карти, зчитують PIN-код з використанням веб-камери та накладок на клавіатуру, встановлену на банківських автоматах. Втратити свої персональні дані за методикою скіммінгу можна не тільки знімаючи гроші, а й заносячи гроші в термінал в магазинах. Для зчитування даних злочинці які працюють в магазині, сервісі, і т.д. використовують портативні скімери або прилади, вбудовані до терміналу (рис 1.5).

Рисунок 1.5. – Схема скіммінгу банкомата

Клікфрод – це вид злочинства у мережі, що представляє собою ложні кліки з переходом на шахрайский сайт користувачем, не зацікавленим у цьому посиланні. Може виконуватись за допомогою запрограмованих скриптів що генерують натискання користувачем на рекламне оголошення. Не попадатись на техніку клікфорд можуть лише розробники цих же сайтів. (Рис. 1.6).

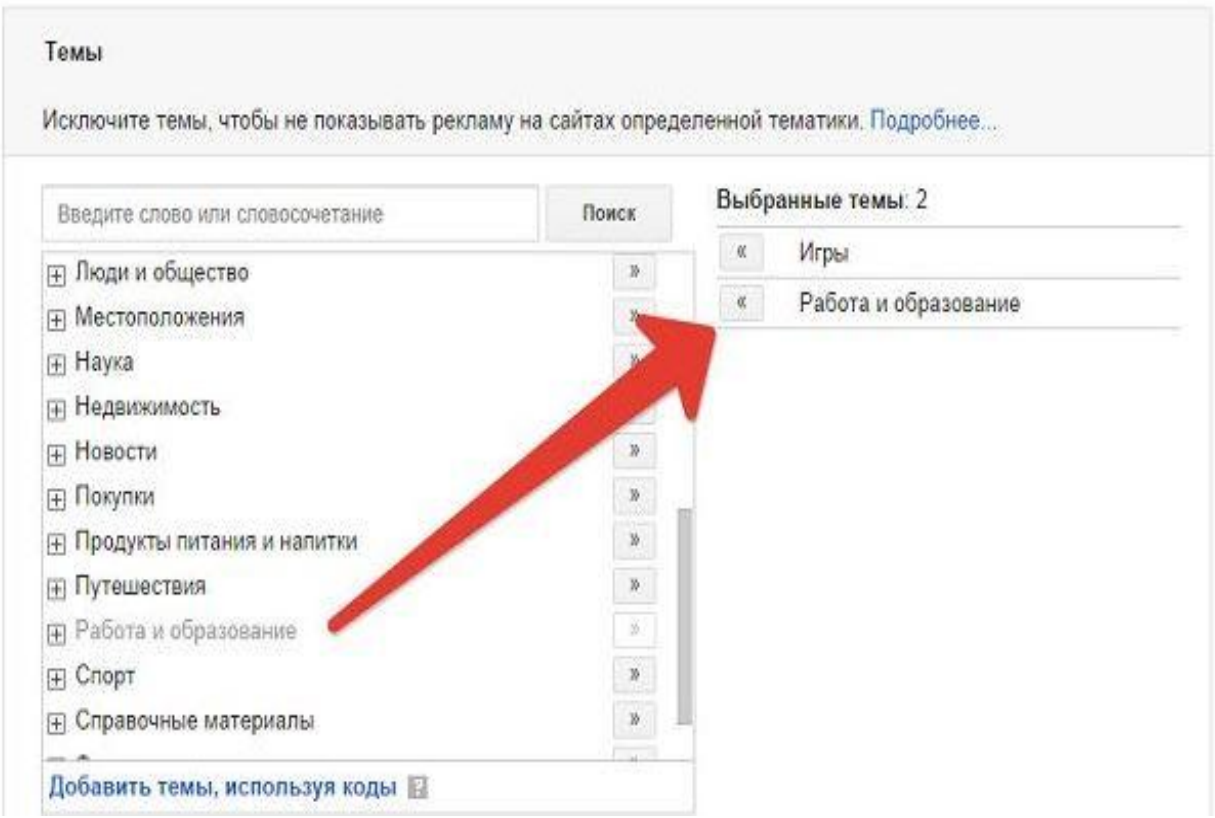


Рисунок 1.6 – Плагін на пошуковик для боротьби з клікфордом

Ознаки клікфрода:

- велика кількість переходів з однієї IP-адреси;
- велика кількість відвідувачів, які швидко залишають сайт;
- висока кількість переходів на сайтах певного партнера;
- зниження рівня конверсії при збільшенні кількості переходів;
- збільшення кількості переходів на всі ключові слова.

На рисунку 1.7 зображен графік відвідуваності сайта, на якому чітко видно, що в один з днів кількість відвідувачів зросла в декілька десятків разів. Це результат роботи шахраїв, які використовують техніку клікфорда.

Рисунок 1.7 – Графік роботи техніки клікфорда

Фармінг – це модифікований різновид фішингу (рис.1.8). Основна ідея фармінгу у тому, що на персональному комп’ютері будь-якої особи замінюються файли та атрибути файлів, що змінюють алгоритм роботи персонального комп’ютера при доступі до сайту у мережі інтернет.

В результаті всі дії злочинців призводять до того, що персональний комп’ютер починає виконувати запрогрмований шахраями набір команд. Користувач шукає у пошуковику гарантовано вірну адресу сайту де він буває регулярно, але у результаті виконання злочинних команд комп’ютер переходить на іншу адресу, яку заздалегідь ввів злочинець.

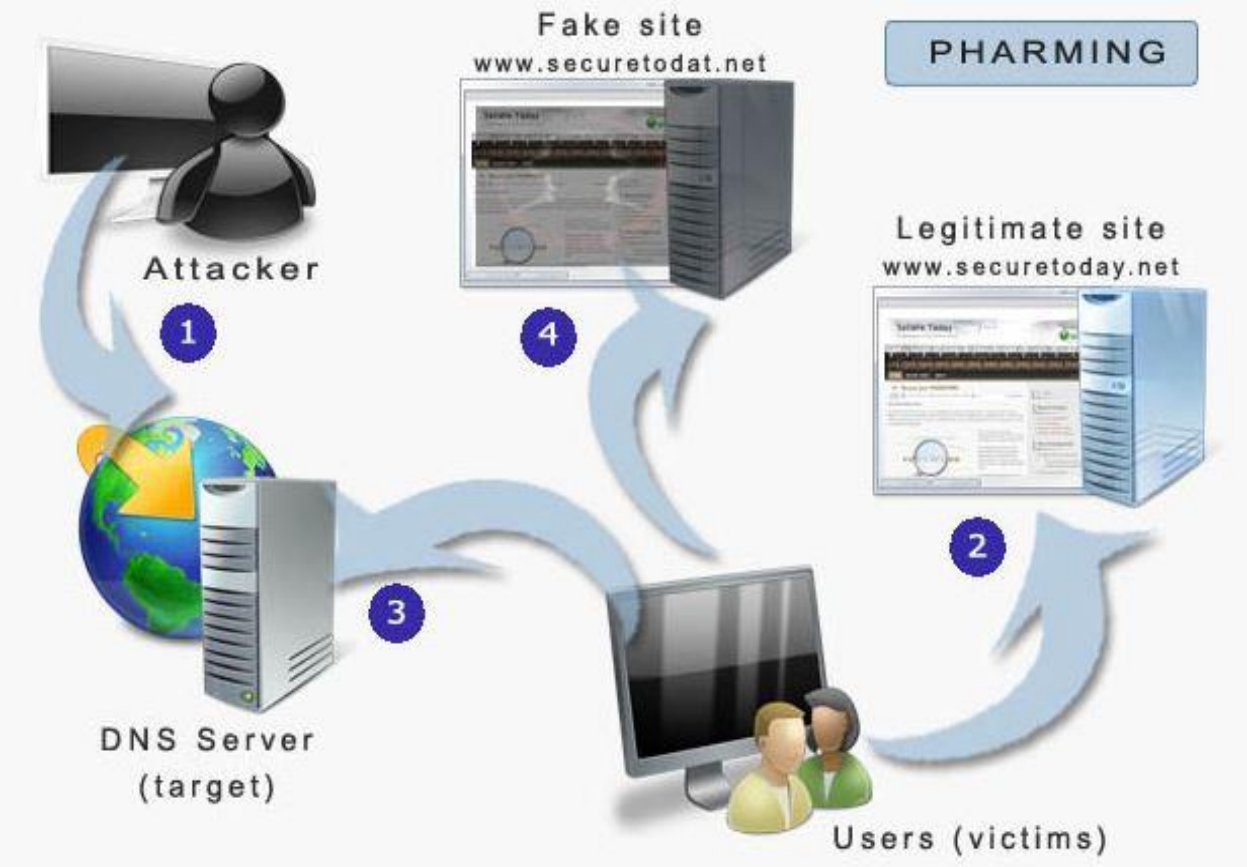


Рисунок 1.8 – Схема шахрайства з використанням фармінгу

1.2 Аналіз програмних засобів для боротьби з шахрайством

1.2.1 Pay Online

Роздивимось систему моніторингу, яку використовує програма PayOnline для виявлення шахрайства в банкінгу. Натискаючи кнопку “Оплатити” спрацьовує система захисту PayOnline. На данному етапі система володіє двома персональними інформаційними пакетами данних: інформацією про даний одноразовий платіж та інформацією про профіль корустувача банка, на якому проводятся операції з оплатою. Програма не тільки аналізує операцію з грошима, але і отримує інформацію, поповнюючи свою базу даних.

Методи, за якими працює інформаційна система, дозволяє виявити багато факторів:

- розмір оплати;
- рейтинг банківської карти;

– рейтинг користувачів даного банку.

Грошовий переказ проходить моніторинг на підставі даних факторів з присвоєнням рейтингу, який повідомляє про наявність злочинних дій. Існують три категорії рейтингів. “Зелений” відзначає грошову операцію з малою ймовірністю виявлення злочинних дій. “Жовтим” рейтингом позначаються операції, в яких вирогідність виявлення шахрайської операції більше середнього, та для отримання платежу будуть необхідні додаткові перевірки. “Червоною” відмічаються ті дії, які найбільш усього походять на злочинні, і при їх виконанні необхідно буде зробити підтвердження даних користувча банка.

Схема роботи зображена на рисунку 1.9.

Рисунок 1.9 – Алгоритм виявлення шахрайства в PayOnline

Механіхм валідації представлен на рисунку 1.10. З “зеленими” операціями виконується наступне: платник робить оплату карткою. Сума операції не буде більшою за середній ліміт банка. Система безпеки банка присвоює операції «зеленій» рейтинг. Далі грошова операція потрапляє на авторизацію в системі 3D Secure. В разі, якщо картка не

зареєстрована в базі даних паролів або банк яких згенерував картку не підтримує цю систему, запит на проходження цієї оплати буде переадресований в систему банку традиційним способом. Рейтинг «жовтого» кольору присвоюється оплатам із середньою та більш за середню можливістю виникнення злочинних дій. Наприклад, в системі одного регіону проводиться грошова операція банківською картою, яка зареєстрована в іншому регіоні. Під час оплати клієнт банка знаходиться не в тому регіоні де знаходиться банк-емітент.

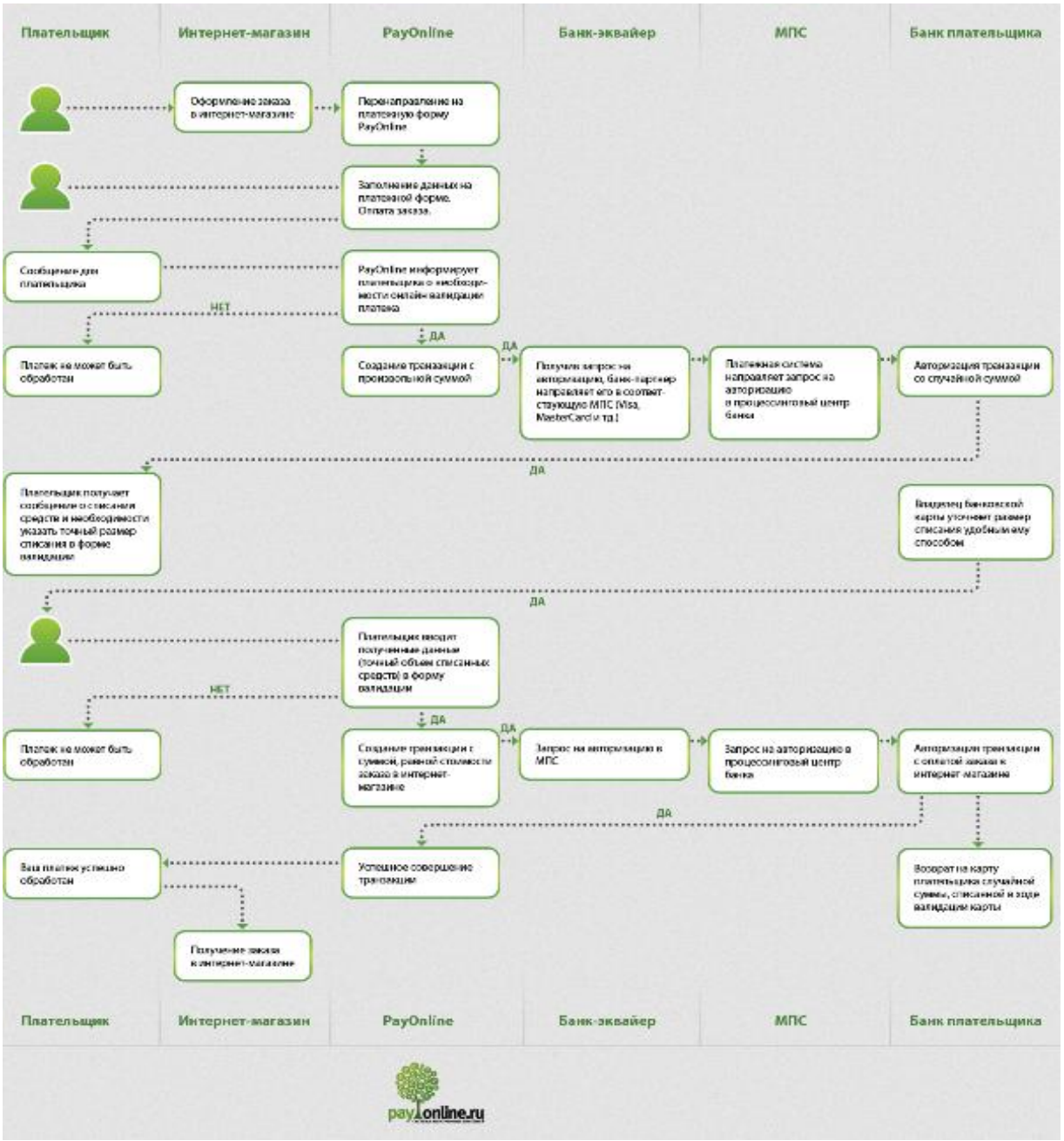


Рисунок 1.10 – Механізм валідації платежу PayOnline

Система дає грошовій операції “жовтий” рейтинг, і для її роботи потребуються додаткові дії користувача. В тому разі, якщо карта працює на 3D Secure, то грошовій переклад буде зареєстрован з використанням SMS - пароля. В тому разі, коли користувач не має змоги зробити авторизації операції даним способом, його дії будуть автоматично переадресовані на перевірку через систему Інтернет. Цей метод працює наступним чином: банк знімає суми від одного до десяти гривень з картки клієнта. Після проведення цієї операції користувач отримує данні про розмір списаних з його карти грошей та вказує їх на сторінці сервісного центру. Особистість клієнта банку буде підтверджена коли він зазначить суму коштв, котрі були зписані з його рахунку. Якщо сума була введена невірно, операція блокується.

“Червоний” рейтинг система безпеки PayOnline дає грошовим переказам з високим рівнем вирогідності виникнення злочинних дій. Якщо грошова операція виконується карткою, яка зроблена в іншому регіоні, відмінному від регіону користувача, а розмір грошової операції відрізняється від розміру загального середнього значення переказу грошей в данній системі.

У разі якщо грошові операції з використанням даної банківської картки раніше не робились через сервісний центр, система контролю дасть операції «червоний» рейтинг і переведе її в ручний.режим Даний платіж буде переадресований на контроль співробітникам системи PayOnline. Для аутентифікації клієнта банка буде необхідне паспортне підтвердження особистості з фотографією банківської карти Після надання цих даних грошова операція переходить отримує зелений рейтинг, авторизується і переадресовується на сервіс банку. Підозрілі дії, які не пройшли перевірку співробітниками банка, не реєструються системою щоб уникнути вирогідості виникнення злочинних операцій.

1.2.2 Cyber Plat

Компанія CyberPlat запропонуавала інструментальний засіб для виявлення злочинців в системах онлайн транзакцій. У відповідності від вказаних інструкцій система може виконувати моніторинг платіжних операцій, що виконуються в банківській системі, які використовуюсть сервіс CyberPlat. Коли програмній засіб виявив злочинні дії система посилає аварійні сигнали, які надходять власнику картки у вигляді повідомлень на телефон або за допомогою електронної скриньки. Одночасно на сайті банківської системи генерується виділений червоним месседж, який вказує клієнтові на блокування транзакції.

Побачивши алерт повідомлення від системи CyberPlat, співробітникам банківській системі надається лістинг усіх платежів, зроблених за останній час, та у разі підозрілих дій шахрайскі елементи блокуються. Данний варіант вирішення проблеми шахрайства має значні переваги, бо власник картки має широкий та гнучкий спектр користувальницьких налаштувань, таких як розмір однієї транзакції, кількістна межа транзакцій, часовий проміжок опрацьовування грошових переказів.

У червні 2017 року компанія CyberPlat створила та почала налаштовувати до роботи сервіс по контролю за інтернет злочинністю в банковській сфері. Данна система аналізує емісійні ризики, в якості доповнення до наявних на той день EMV технології та можливістю відправляти повідомлення на сотові телефони клієнтів банка в разі виявлення шахрайства з їх грошовими операціями.

Запропонований сервіс вирахунку емісійних відхилень дає можливість структурам в банківській системі проводити моніторинг карток, які знаходяться в локальній мережі системи, так і в глобальній системі, наприклад в такій як MasterCard Worldwide. Можливості, які предоставляє данна технологія моніторингу дають змогу створювати інструкції для аналізу грошових переказів, та проводити моніторинг грошових переказів в режимі онлайн з втручанням співробітників банківської системи для виявлення шахрайских дій.

1.3 Аналіз протоколів захисту для боротьби з шахрайством

1.3.1 3D Secure

3D Secure - протокол захисту, суть роботи якого полягає в додатковому контролі введених даних клієнта банку при здійсненні оплати через електронний рахунок.

Перший этап контролю: перевірка ID карти, ПІБ власника, термін використання карти. Другий етап перевірки: система запитує власнику контрольний код, який відправляється йому службою моментальних повідомлень (SMS) на його сотовый телефон. Клієнт також має можливість отримати цей пароль на свою електронну пошту, або зберегти в системі (рис. 1.11).

Рис. 1.11 – Схема проведення грошової операції 3D Secure

Загальня схема роботи 3D Secure представлена на малюнку 1.12:

Рис. 1.12 Схема обробки грошової операції 3D Secure

1.3.2 SET

SET (Secure Electronic Transaction) - Протокол безпеки в мережі Інтернет, створений спільно компаніями VISA і MasterCard в 1996 році. Є набором інструкцій для здійснення безпечного електронного грошового переказу. Система захисту SET обазіруется на фундаментальних криптографічних алгоритмах RSA і DES.

Система ініціалізує шифрування на базі двосторонніх ключів - серверного та клієнтського, що дозволяє уникнути дешифрування коду сторонньою особою, крім

власника даного ключа. Крім того технологія SET дозволяє застосовувати електронні цифрові підписи до даних, для доступу до яких використовуються цифрові сертифікати власників карт і банківської системи. В даному сертифікаті з використанням закритого ключа сертифікації закодований відкритий ключ конкретного учасника грошової операції з використанням хеш – коду.

Його робота полягає в генерації хеш-коду з атрибутами платежу такими як сума грошової операції, ПІБ клієнта, ID рахунку з якого проводяться операції, ID гаманця куди будуть надходити кошти, чек-сума та так далі. Коли дана операція буде направлена на виконання банківською системою, система відправляє на сайт (сайт торгівельної площадки,тощо) данні з параметрами і хеш-кодом.

Сайт декодуючи хеш-код операції на своїй стороні аналізує його на відповідність хеш-коду, який був сгенерований банківською системою і якщо хєш-коди співпадають грошова операція буде оброблена, в іншому разі система аналізує, що переказ грошей міг бути пошкоджений шахраями з послідуючим редагуванням. Алгоритм генерації хеш-коду операції відомий як торгівельній площадці, яка використовує послуги банка так і цьому банку. До того ж при генерації хеш-коду робиться контрольний шифр, який є одноразовим, отже якщо шахрай взнав алгоритм генерації коду, без данних о контрольній сумі, зловмистник не зможе сгенерувати вірний хеш-код.

Контрольна сума знаходиться на сервері кліента банківської системи та на сервері самої банківської системи. Для генерації цього коду використовують багато методів хешування, нприклад SHA або MD4.

Процес обробки та аналізу грошової операції з використанням хеш-коду:

- сервер відправляє дані для виконання переказу грошей в системі;
- система аналізує дані для організації платежу визначивши дані клінта;
- якщо дані клієнта виявлені на сервері проводиться виконання грошової операції та відправка на сайту результат виконання запиту та хеш-код, в якому є набір атрибутів операції та контрольний шифр;
- сайт звіряє хеш-код;
- в разу збіжності хеш-коду грошова операція вважається завершеною.

До плюсів цього алгоритму можно віднести те, що хєш-коди є тільки у клієнта банківської системи та у самої системи. В разі зміни лише одного атрибута система блокує грошовий переказ.

Система SET проводить перверірку транзакції по атрибутам. Платіжна карта є складовою частиною банківської системи тому її перевірка має виконуватись не менш ретельно ніж грошові перекази. В системі генерується база даних яка позначається як

чорний список. В цій базі данних може знаходитись будь який атрибут грошового переказу, який набув підозрілого характеру. Під час проведення грошової операції система перевіряє атрибути операції на наявність у чорному списку.

Якщо будь який атрибут занесен у чорний список, операція блокується. Перелік атрибутів має наступний вигляд:

Основні атрибути платіжної картки:

- географічне положення банку, що генерував картку;
- наявність банківської картки у червоному списку;
- чек-суми грошових операцій;
- періодичність платіжних операцій з картки;
- наявність аккаунта користувача банківської картки у червоному списку.

Данний метод захисту даних користувачів банківської системи використовується в разі, коли безпека рахунку клієнта не може бути забезпечена іншим способом. До такого заходу зі сторони банка може привести викрадення банківської картки, її пароля, якщо клієнт банка загубів картку або якщо карткою заволодів злочинець. В такому разі клієнту банка надається можливість відправити повідомлення, отримавши яке система негайно зупиняє роботу рахунка та гаманця, в результаті чого робота з ними стає неможливою. Цей метод має стовідсоткову гарантію працездатності, тому його використовуюсть усі наявні на сьогоднішній день системи.

В разі, коли власник картки оновив пароль та рахунок, система автоматчно їх розблокує, та клієнт зможе приступити до роботи.

1.4 Постанова наукової задачі та обгрунтування методики дослідженнь

Результати проведеного аналізу моделей, методів й інструментальних засобів показали, що у відомих роботах використовується дуже коштовне програмне забезпечення. Задачі, пов'язані з самоповчающимися автоматичними технологіями не розглядались.

Для виконання поставленої задачі доцільно використовувати програмний продукт Microsoft Azure. З плюсів даної віддаленої структури можна відзначити мінімальні грошові витрати завдяки низькому навантаженні на технічне забезпечення сервера. Так само наявність комплексних засобів розробки та управління для моніторингу, контролю і захисту віддалених ресурсів дозволяє гарантувати як якість послуг, так і швидкість їх виконання.

1.5 Висновки до розділу 1

У цьому розділі було проведеного аналіз моделей, методів та інструментальних засобів для боротьби з інтернет шахрайством.

Був зроблен висновок, що наявні на сьогодні засоби виявлення шахрайства дуже коштовні, та не мають належний рівень автоматизації, тому для виконання поставленої задачі доцільно використовувати програмний продукт Microsoft Azure.

РОЗДІЛ 2
АНАЛІЗ ФУНКЦІОНАЛЬНОСТІ ІНФОРМАЦІЙНОЇ ТЕХНОЛОГІЇ

2.1 Загальні положення

Високі темпи розвитку онлайн платежів і повсюдне використання банківських карт, які дозволяють здійснювати оплату через мережу Інтернет, змушують фахівців в області IT-безпеки розробляти нові і більш комплексні способи захисту приватної інформації в банківських системах, так як поширеність і популярність онлайн платежів підвищують інтерес шахраїв до даної галузі, в результаті заради крадіжки коштів вони намагаються тим чи іншим способом роздобути дані про карту користувача.

Серед країн, які найбільш схильні до шахрайства в сфері онлайн платежів можна виділити США, Китай, РФ, а також провідні країни Європейського союзу, в яких нараховується найбільша кількість незаконних операцій з віртуальними грошовими коштами. Збиток від таких дій в 2017 році оцінюється в 1.5 млрд доларів, з них на Україну припадає 3 млн. доларів, що в рамках нашої країни є серйозним ударом по економіці.

Платіжна карта - електронний пристрій у вигляді в установленому правовому полі пластикової або подібного формату карти, яка застосовується для організації переказу фінансів з рахунку користувача банківської системи для оплати вартості послуг і покупок, переведення фінансів з одного рахунку на інший, отримання електронних грошей в готівковому вигляді за допомогою банкоматів, а також вчинення інших дій, встановлених конкретним договіром.

Існують три методи оплати через банківські карти: дебетовий метод, дебетово-кредитний метод а також кредитний метод.

Дебетовий метод надає можливість здійснювати грошові операції із застосуванням платіжної картки в межах залишку грошових коштів, наявних на його рахунку.

При використанні дебетово-кредитної схеми клієнт виконує грошові операції із застосуванням банківської картки в межах залишку грошових коштів, що знаходяться на його рахунку, а якщо їх не вистачає або грошей немає - за рахунок виданого банком кредиту.

Кредитна схема дозволяє виконувати клієнтам банківської системи грошові операції із застосуванням платіжної картки за рахунок електронних грошей, виданих йому банком на кредитній основі.

Феномен інтернет-шахрайства поширюється в більшості випадків на банківські картки та рахунки в системі, тому дані елементи є головними об'єктами контролю системи виявлення шахрайства

На рисунку 2.1 приведена загальна схема здійснення переказу віртуальних грошей через мережу Інтернет при безготівковій оплаті.

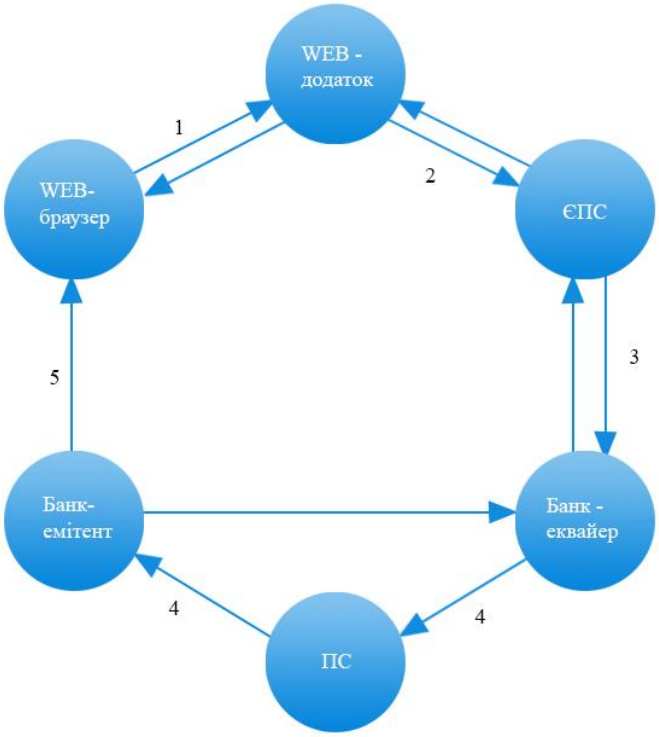


Рисунок 2.1 – Загальня схема переказу електронних коштів

На рисунку 2.1 можна побачити, що від втрати персональних даних на будь-якому з етапів переказу електронних грошей ризикують відразу всі її сторони. Банк ризикує втратити не тільки прибуток, але й дові ру клієнтів, що негативно позначиться на зростанні попиту його послугами.

Виходячи з цього, технологія, що дозволяє заздалегідь визначати крадіжку даних клієнтів банку є не простою примхою, а необхідністю, умовою, за якої банк зможе отримувати прибуток зі своєї роботи та залучати нових клієнтів.

2.2 Опис функцій системи

В рамках роботи інформаційної системи слід виділите те, що сама система є серверною частиною, а результат обробки запиту відправляється на клієнтську частину.

При роботі з клієнтською стороною сервер повинен виконати наступні функції:

- вказати API клієнтській стороні для взаємодії з системою;
- відправити звіт про підсумок обробки транзакції клієнтській стороні;
- зберігти звіт про роботу.

Основним критерієм якості системи виявлення шахрайства є те, що вона повинна вірно розпізнавати підозрілу активність на банківській картці користувача, як наслідок помилкові спрацьовування є неприпустимими.

Серед головних атрибутів, які свідчать про підозрілі дії можна виділити помилково введені користувачем дані, а також кількість спроб їх введення.

2.3 Перевірка валідності платіжних даних

Суть роботи аналогічних системи полягає в тому, що якщо дані користувача потрапили хоч в один з видів підозрілих дій, у відношенні даної особи будуть проведені додаткові перевірки.

Наприклад, якщо спроба зняти гроші з рахунку була проведено з країни, яка не обслуговується даним банком, або якщо було зроблено велику кількість запитів з будь-якої мережевої адреси, дані потрапляють в категорію підозрілих, і особа, яка використовує їх буде підлягати додатковим перевіркам.

Як показує практика, перевірити чи дійсно дані були введені неправильно в шахрайських цілях або ж це випадковість дуже складно.

Однак, головна мета - визначення відповідності операцій шахрайству на початкових стадіях, адже зниження кількості обчислювальних операцій дозволить використовувати менші апаратні потужності сервера, а також дозволить не навантажувати зайвими даними програмний засіб, модель або систему.

Для цього потрібно проаналізувати, чи не занесена картка в чорний список в банківській системі, перевірити її алгоритмом обчислювання контрольної суми номера карти відповідно до стандарту ISO / IEC 7812, а також довідатися чи не прострочена вона.

В мережі Інтернет пропонується велика кількість методів наукового дослідження, здатних визначити чи є транзакція підозрілою. Однак більшість з них вимагають великих

обчислювальних потужностей, а кількість чітко визначених підозрілих транзакцій залишає бажати кращого.

У даній роботі для визначення, чи є зняття грошей з рахунку шахрайської операцією будуть застосовані нейромережі, які мають вивичати як поточні так і ранні операції на картці клієнта. Для цього буде використовуватись та тесуватись наступні методи: двухклассова регресія, метод опорних векторів, метод нейронних мереж

2.4 Огляд функціональності платформи Microsoft Azure

Для реалізації поставленої задачі буде використовуватись сервіс Microsoft Azure. З плюсів даної віддаленої структури можна відзначити мінімальні грошові витрати завдяки низькому навантаженню на технічне забезпечення сервера.

Наявність комплексних засобів розробки та управління для моніторингу, контролю і захисту віддалених ресурсів дозволяє гарантувати як якість послуг, так і швидкість їх виконання.

Переваги сервісу Microsoft Azure:

- низькі грошові витрати;
- конфіденційність - забезпечення доступності інформації тільки для тих, хто має відповідні повноваження (авторизовані користувачі);
- доступність - забезпечення доступу до інформації авторизованим користувачам коли це необхідно;
- відповідність стандарту Payment Card Industry Data Security Standard;
- стабільність в роботі;
- випадках окремо;
- адаптивність;
- можливість підключення системи до програмного продукту Microsoft Visual Studio.

Процес роботи з Azure ML складається з наступних кроків, показаних на рисунку 2.2.

Рисунок 2.2 – Процес роботи в Azure Studio

Виділимо головні можливості системи Azure:

- дані завантажуються з використанням документів CSV, TSV, а також в форматі HDFS, таблиці SQL Azure. Також їх можна імпортувати з стандартних таблиць в середовищі Microsoft Azure та з web-сайту;
- для того щоб провести аналіз набору завантажених даних, в середовищі присутні модулі, що використовуються для експортування даних, модулі аналізу вхідних даних. У середовищі розробки є доступ до візуалізації імпортуваних даних.
- для того щоб створити та редагувати ознаку треба застосовувати блоки масштабування і функціональні перетворення, угрупування цифрових характеристик, двійкове кодування категоріальних функцій.
- для того щоб створити модель застосовуються наступні алгоритми: класифікації, регресії, рекомендацій і кластерізації. Недавно введений алгоритм «Learning with Counts», робить можливим вилучення знань з 1000 Гб даних методом вирішення завдань класифікації і регресії з використанням нейронних мереж і дерев прийняття рішень. Алгоритми машинного навчання автоматично масштабуються в залежності

від обсягів даних. Наприклад, можна працювати з пакетом скриптів R, і мовою програмування Python.

- для того щоб тестувати і перевіряти роботу алгоритмів є можливість використовування методів розділення даних (випадкове, з розшаруванням), а також є можливість використання крос-валідації та глобальної метрики.

Microsoft Azure має наступний набір сервісів:

- web-роль - веб-ролі потрібні для того щоб надавати веб-сервер для служб з метою завантаження веб-додатків. Веб-ролі дають можливість завантажувати веб-додатки з подальшим масштабуванням обчислювальних ресурсів;
- worker-роль - додаток, створений для того, щоб виконувати несинхронні, довготривалі і постійні в часі завдання у фоновому режимі. Відділення таких процесів на два додатка та розміщення інтерфейсної частини в веб-ролі уможливлюють якнайкраще оптимізувати логіку сервісу;
- web Sites - веб-сайти які використовують мову Java, PHP, і т.д. Відкриваються за нетривалий час завдяки технологіям FTP, Mercurial і Dropbox. Обмежену версію можна використовувати в безкоштовному режимі. Перебуваючи в такому режимі обчислювальні ресурси діляться між сайтами, проте є можливість збільшити число примірників і перемкнути веб-сайт в стан резервування ресурсів. З липня 2014 року послуга Web Sites підтримує редаговані сертифікати SSL як за адресою, так і на базі Server Name Indication;
- таблиці - використовуються сервісами, які оперують великими обсягами інформації та мають необхідність в структуруванні цих даних;
- черги - створюють надійний канал обміну даними між сервісами;
- BLOB-об'єкт - сама легка можливість сберігати великі обсяги неструктурованої інформації, наприклад текстові документи, аудіозаписи, зображення;
- SQL (реляційна база даних) - це віддалена від користувача служба бази даних, створена на базі SQL Server;
- SQL Data - віддалений сервіс синхронізації інформації, що дає можливість використовувати як односторонню, так і двосторонню синхронізацію. За допомогою сервісу Data Sync можна досить просто пересилати інформацію між SQL та Azure;
- SQL Reporting - сервіс дає можливість інтегрувати в програму Windows Azure функцію роботи зі звітами. На даний момент сервіс зупинена;

- SQL Federations - ця функція дає можливість більш просто масштабувати інформацію в базі даних, оптимізує її по безлічі вузлів. Це дає можливість користувачеві оплачувати конкретно ті ресурси системи, якими він оперує.
- backup - даний сервіс дає можливість зберігати резервні копії на сервері Windows Server. Microsoft Azure підтримує резервні копіїї даних в системах на базі Windows Server 2008 \ 2012. Доступно інкрементальне резервне копіювання даних;
- azure files - даний сервіс дозволяє звертатися до сховища Azure Storage як до мережного ресурсу, що дає можливість отримувати класичний доступ до інформації з віртуальних машин через мережевий канал.

2.5 Структура системи

Структура розроблюваного сервісу представлена на рисунку 2.3.

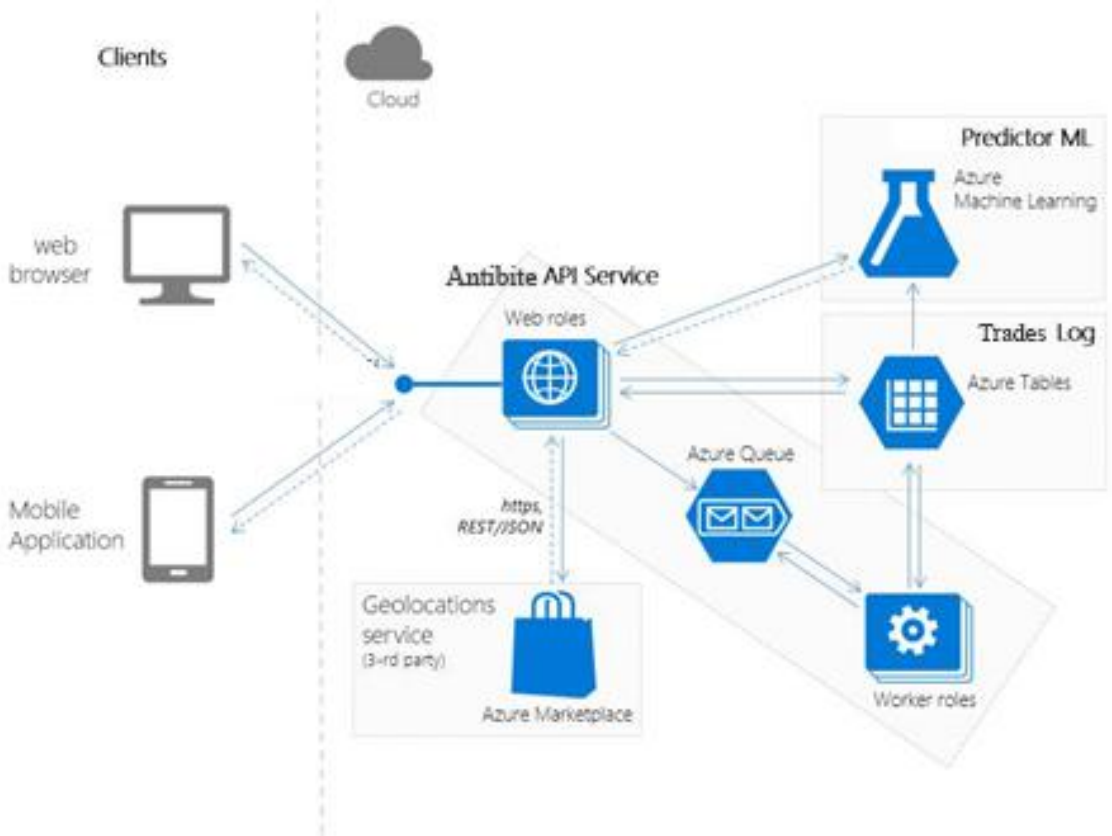


Рисунок 2.3 – Структура системи

Система складається з наступних компонентів:

- Antibite API Service – REST-сервіс, що дає API доступ для роботи з сервісом Predictor ML;
- Predictor ML - сервіс для виявлення підозрілої активності на банківському рахунку, в основі якого лежать самоповчающиєся нейромережі;
- Trades Log - сховище даних про фінансові операції. З точки зору споживачів система виявлення шахрайства виглядає як сервіс, до якого можна звернутися через протокол HyperText Transfer Protocol Antibite.

Процес аналізу вхідних даних показаний на рисунку 2.4, в ньому продемонстровані всі оперції які відбуваються при перевірці платежу на підозрілу активність.

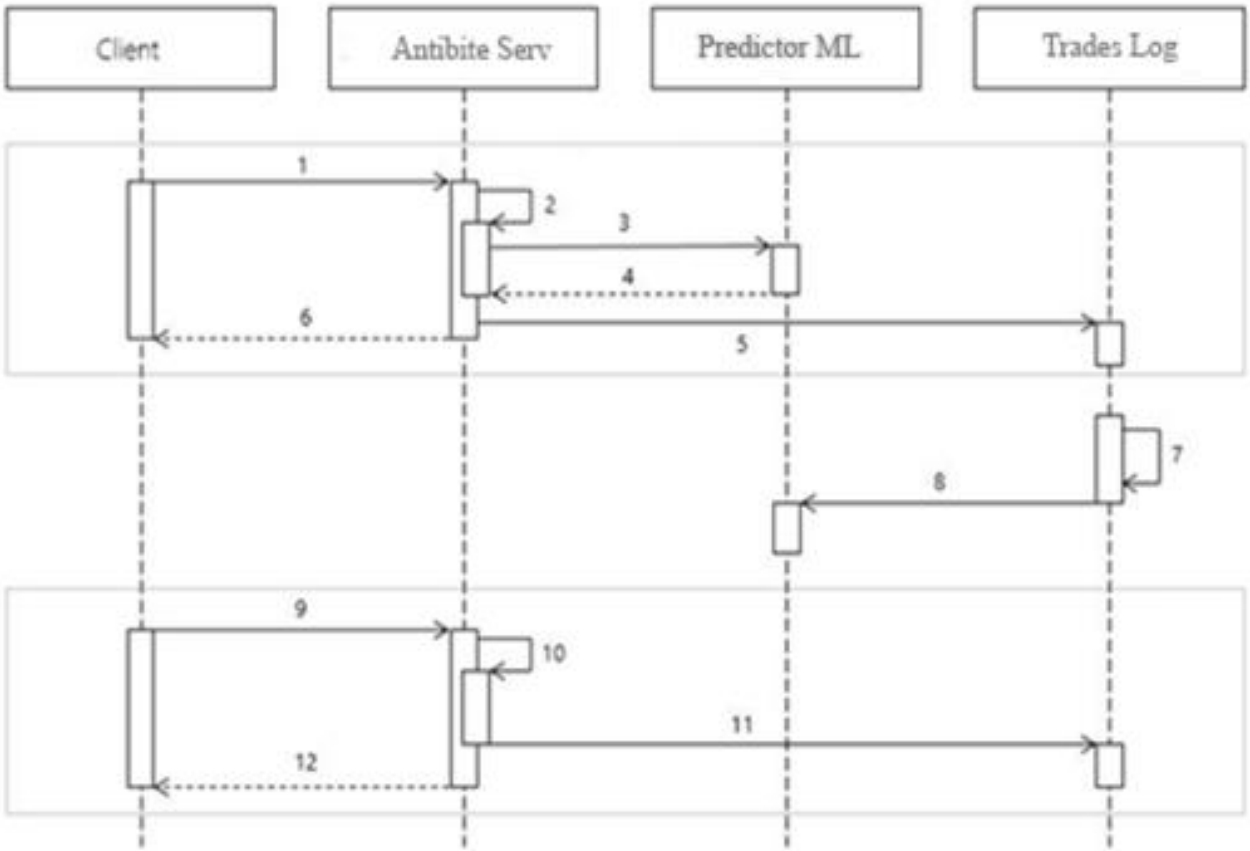


Рисунок 2.4 – Схема перевірки грошової операції

На першому етапі клієнтська частина сервісу передає дані про транзакцію на сервер Antibite API Service, на другому етапі проходить конвертація даних. На третьому етапі проходить передача даних для аналізу на предмет шахрайських операцій в службу

Predictor ML. Після цього серверна частина повертає відповідь(4), проходить збереження даних(5) та надання результату аналізу клієнтові(6).

Система працює наступним чином: клієнт відправляє дані, які потім приймає Antibite API Serviceer (серверна частина). На серверній частини дані перетворюватися в об'єкт предметної області, проводиться звернення до служб позиціонування від Azure для того щоб визначити, з якого міста та країни був відправлений запит на проведення грошової операції.

Далі проводиться перевірка на правильність введених особистих даних, потім вся особиста інформація про користувача та його картки кодується в довільній довжини бітовий рядок. Після цього дані відсилаються в модуль передачі даних Data Transfer Object, який відсилає запит на сервіс Predictor ML а в результаті обробки запиту сервісом Predictor ML результат передається на сервіс Trades Log.

Щоб уникнути ті випадки, коли система видала клієнтові один результат грошової операції, а звіт по ній не збігається з даними в самій операції, клієнту доступна функція оновлення даних по грошовій операції (кроки 9 – 12). Така функція передає дані які аналізується в службі Predictor ML, в наслідок чого заносяться в модуль черг Azure Queue та відправляються до сховища даних про фінансові операції яке представлене у вигляді таблиці даних середовища Azure.

Сховище даних про фінансові операції використовує дві таблиці даних:

- таблицю з даними про переказ грошей Trades Log: ідентифікаційний код переказу грошей, клієнта, номінал;
- таблицю з даними TradesStats, в якій вказано кількість грошових переказів з даної карти, з яких географічних місць був здійснений платіж, час запиту, кількість шахрайських операцій.

На останніх етапах обробки запиту йде перенавчання нейромережі. В результаті навчальна вибірка містить в собі інформацію зі сховища даних про фінансові операції, так як там зберігаються дані з грошових переказів і їх результатах.

Перенавчання виконується за заданим часом, по досягненню певної кількості вхідних даних, та по досягненню конкретної колькості некоректних результатів аналізу.

У даній роботі проводиться навчання 3 моделі, застосовуючи логит - регресію, SVM, а також регресійне дерево. В результаті з трьох моделей експерементальним шляхом буде знайдена і використана максимально точна модель. У підсумку ця модель буде завантажена в форматі REST, і перевірена на працездатність клієнтською стороною.

2.6 Складнощі при розробці

2.6.1 Вимоги до відповідості міжнародним стандартам

PCISS - стандарт збереження даних в банківськіх системах, створений радою безпеки в інтернет-сфері Payment Card Industry Security Standards Council, прийнят на використання провідними платіжними сервісами світу, такими як Visa, MasterCard, і т.д. PCISS пропонує до використання перечень основних вимог з підтримки збереження особистої інформації власників банківських карт, котра знаходиться, зберігається та редагується в інформаційних системах банку. Використання даних правил щодо дотримання вимог стандарту встановлює комплексний підхід до організації безпеки інформації в банківських системах.

2.6.2 Вимоги до банківської системи

Вихід з ладу інформаційної системи гарантовано призведе до збою в роботі банківської системи в цілому, спричинить за собою тимчасовий відтік капіталу і зниження рейтингу банку.

Виходячи з цього першочерговим важливістю при розробці такої системи є безперебійного її роботи і надійності в заощадження оперується інформації. Для обслуговування даної системи потрібна наявність следущих спеціальностей:

- співробітник, що відповідає за консультацію в області банкінгу, онлайн транзакцій, законодавчі аспекти в області;
- програміст: вносить правки в систему, налагоджує при її збої;
- фахівець в області аналізу даних;
- менеджер: курація проекту.

2.7 Висновки до розділу 2

У цьому розділі був проведений аналітичний огляд поставленої задачі, запропоновані структурні схеми роботи розроблюваної інформаційної технології, проведен огляд складнощів при розробці та вимоги.

Наступним кроком стане розробка інформаційної технології на базі платформи Microsoft Azure.

РОЗДІЛ 3
РОЗРОБКА ІНФОРМАЦІЙНОЇ ТЕХНОЛОГІЇ

3.1 Побудова моделі

В результаті проведення аналітичного огляду поставленної задачі, була зроблена схема (рис 3.1), згідно якої буде проходити експеримент в середовищі Microsoft Azure.

Рисунок 3.1 – Загальня схема

Вхідними даними, котрими буде оперувати система виступатиме сховище даних, яке включає в себе 2 таблиці: перша таблиця з даними о грошових переказах TransactionsData а друга таблиця з статистичними даними TransactionsStats.

Так на даному етапі обробки імпортується дві таблиці в контейнери Import Data (рис 3.2).

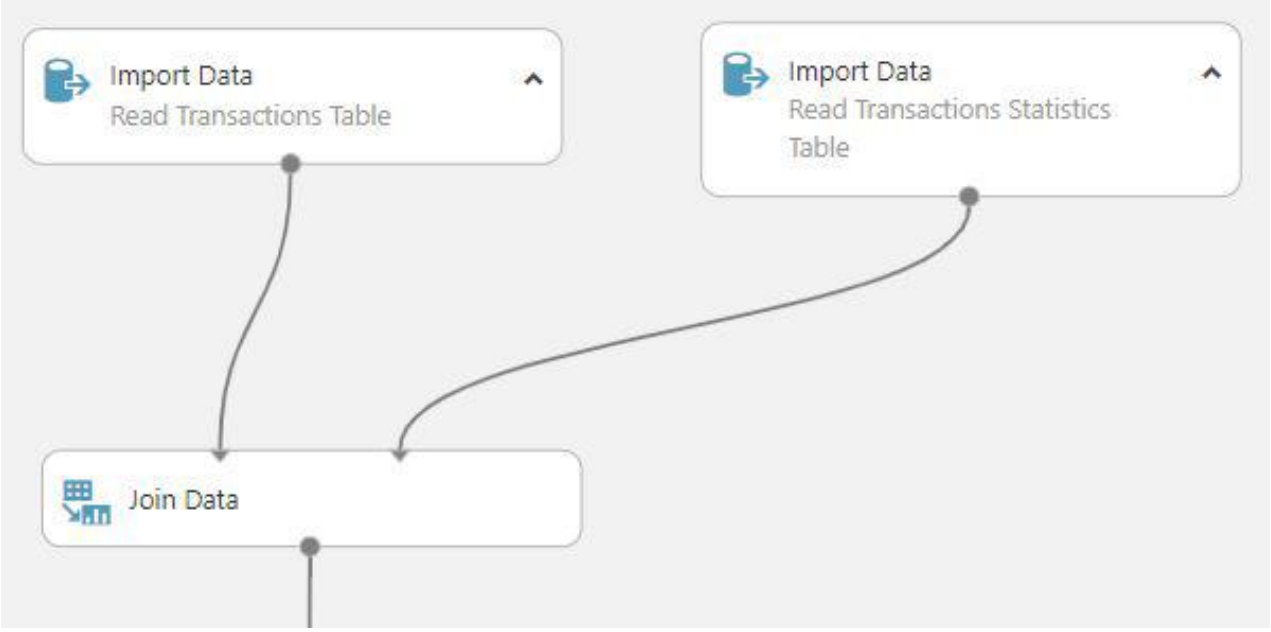


Рисунок 3.2 - Елемент управлінням даних Import Data.

Далі використовуємо функцію Join Data для цих двох таблиць. Використовуючи контейнер редагування інформації в редакторі мета інформації виставимо тип вхідних даних, виділимо ряд label, далі вкажемо тип даних: номінальні (рис. 3.3).

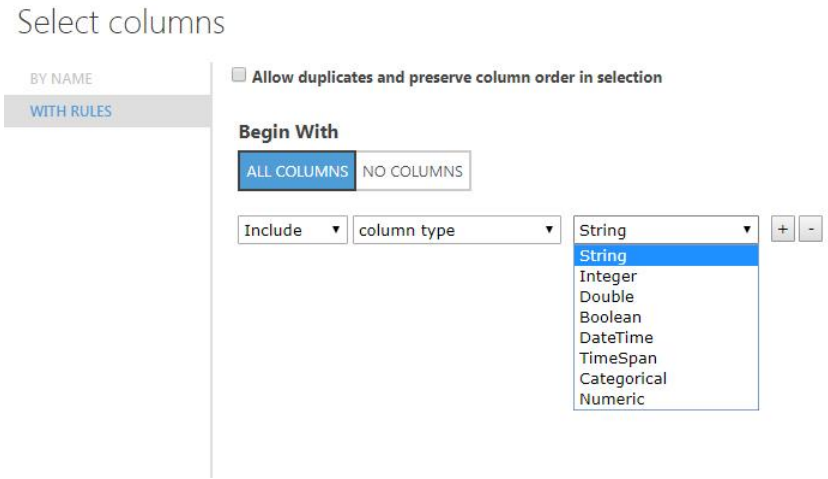


Рисунок 3.3 - Вибір типу даних

Дані, отримані з таблиці в деяких випадках можуть мати не вписані значення. Якщо географічне розташування клієнта дізнатися не вдається, то цей рядок залишається порожнім. Для того щоб пропусків не було, використовуємо елемент редагування інформації Clean Missing Data.

Використовуючи елемент Clean Missin Data (рис. 3.4) зітремо дані які стосуються ПІБ власника карти, кількість переведених грошей, так як ці дані мають характер явно неправдивих, а точніше додають шум в нейромережу.

Далі видаляємо зайві поля у вибірці за допомогою елемента Remove Duplicate Rows (рис. 3.5): місце проживання клієнта (потрібно порівняти тільки місце, з якого була здійснена транзакція), код та ПІБ власника карти.

Рисунок 3.4 - Елемент редагування даних cean Missing Data

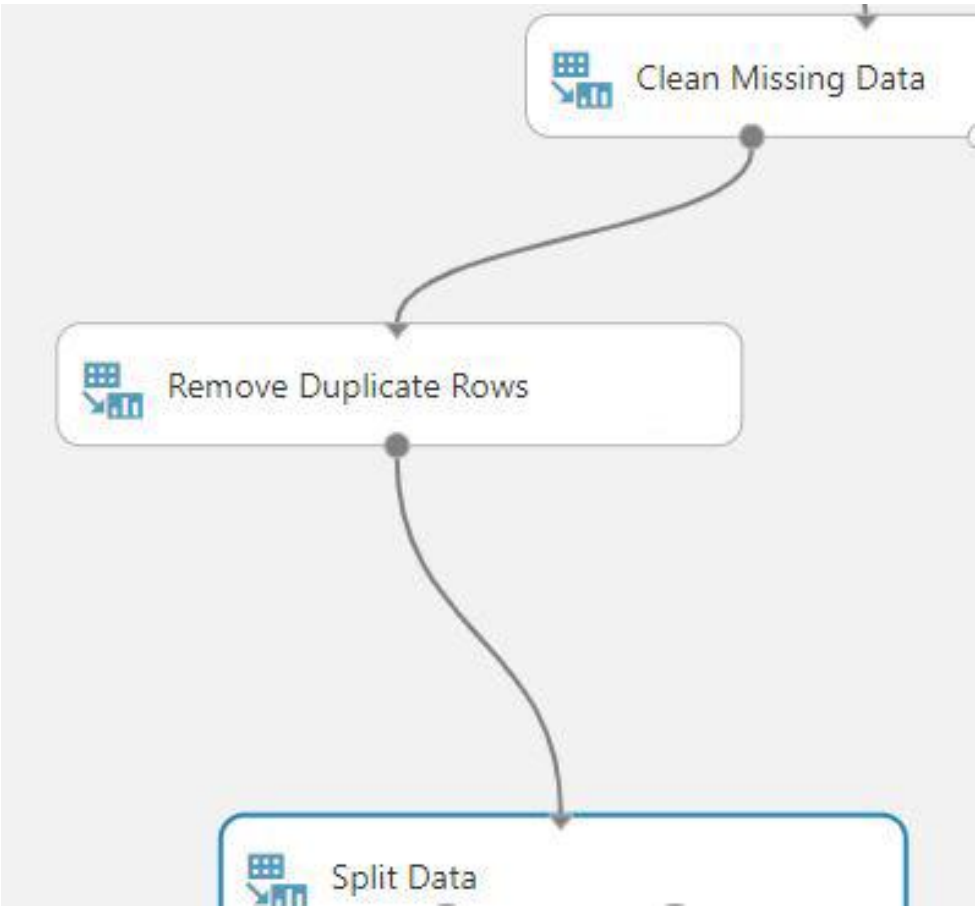


Рисунок 3.5 - Елемент Remove Duplicate Rows

Відсортуємо вхідну інформацію на навчальну і тестову. Визначимо максимально правильну пропорцію інформації в навчальній вибірці та пробній. Елемент Split (рис.3.6) перемістив 60% загальної кількості інформації в навчальний вибір, в навантаження запустив змішану інформацію (покажчик рандомізованого поділу) при конвертації в піднабори даних.

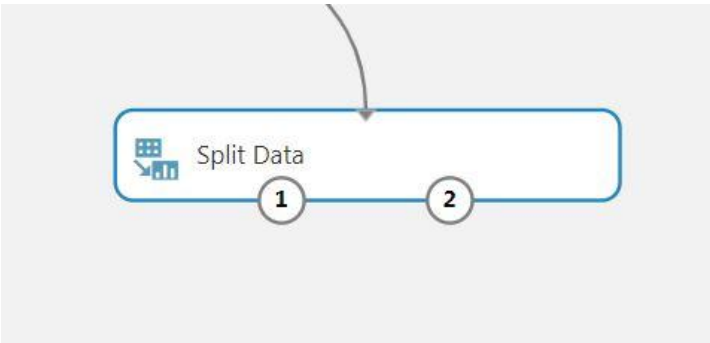


Рисунок 3.6 - Елемент управления Split

На наступному етапі побудови моделі вибираємо алгоритм аналізу даних та підключаємо до нього модуль побудови моделі Train Model. На рисунку 3.7 представлен алгоритм логічної регрессії Two Class Boosted Decion.

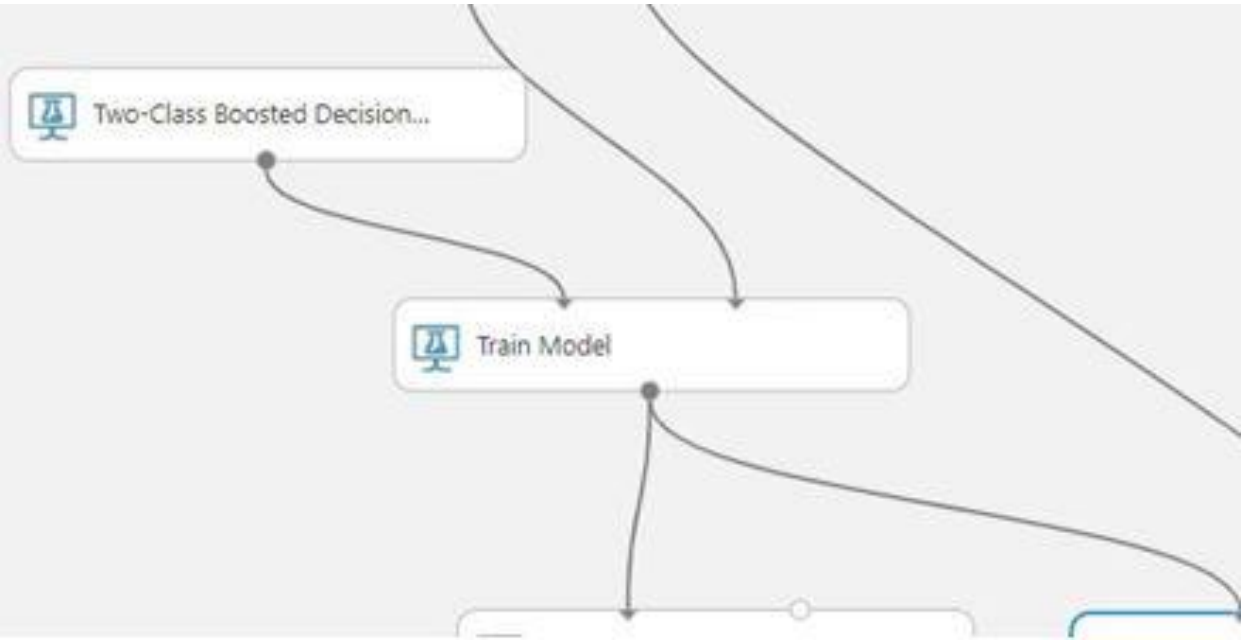


Рисунок 3.7 - Елемент Two Class Boosted Decion

На фінальному етапі проходить вибір моделі, для цього використовується модуль Evaluate model (рис. 3.8).

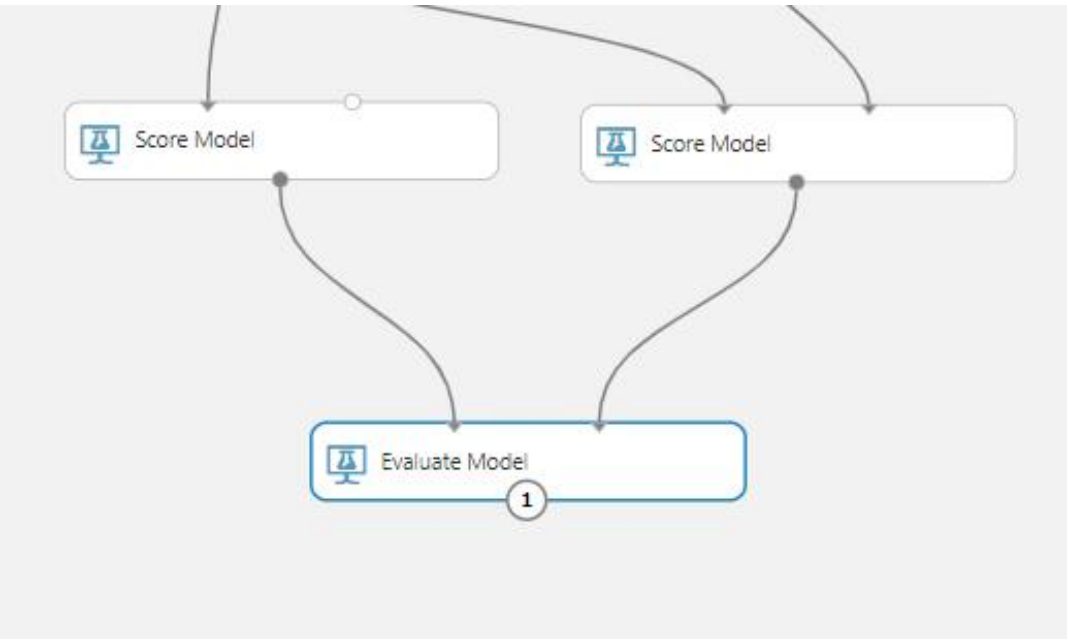


Рисунок 3.8 - Елемент Evaluate Model

Загальний вид побудованої моделі представлений на рисунку 3.9.

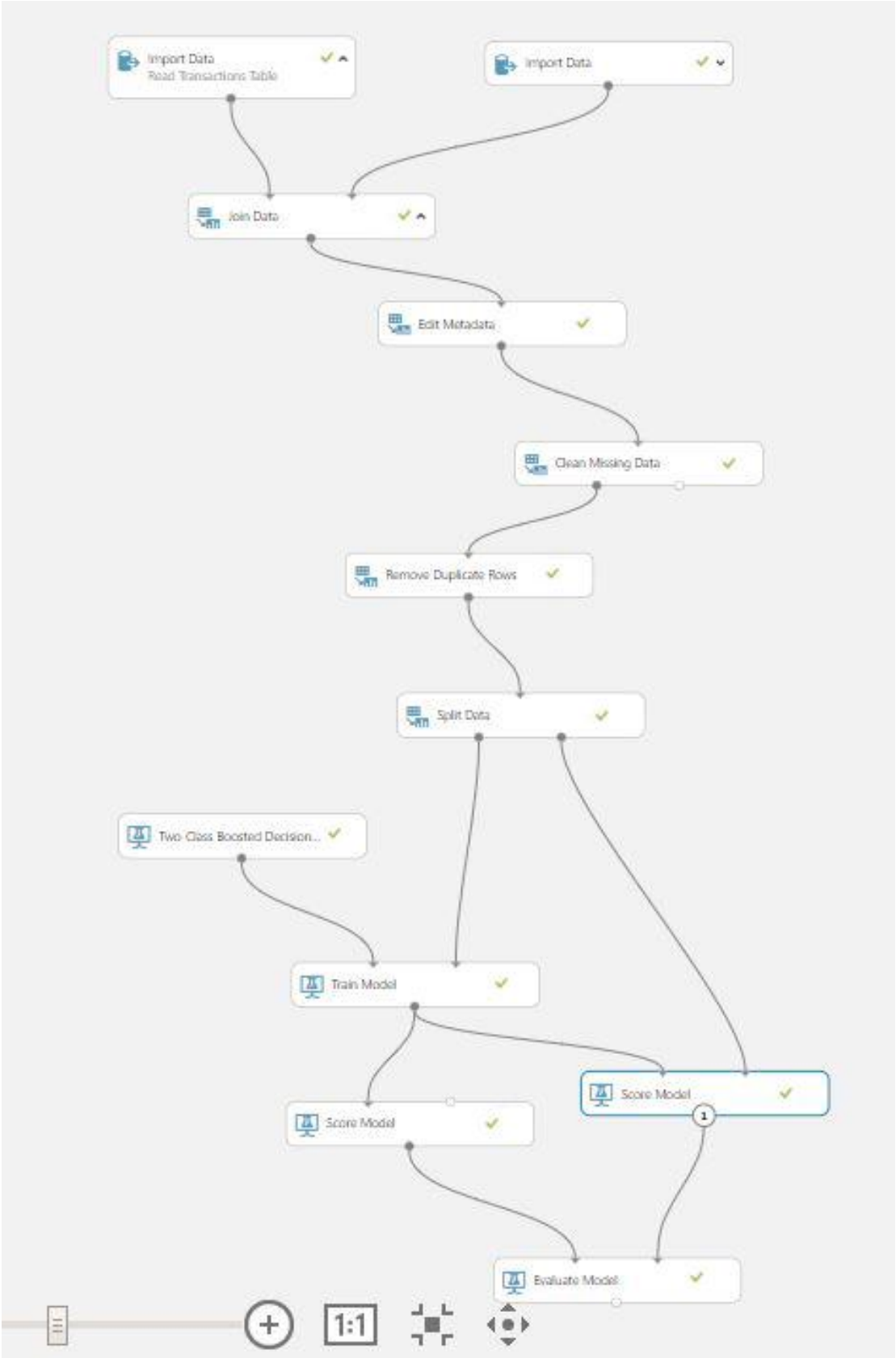


Рисунок 3.9 – Загальний вигляд моделі

Активуємо методи класифікації щоб переконається в якому разі надійшла найкраща відповідь на тестовій вибірці. На жаль, немає ніяких гарантій що навантаження на CPU буде однаковим при тестовому запуску та при пробному

Для того щоб уникнути втрат в продуктивності і точності, потрібно перевіряти, який з методів працює краще, який гірше, відредагувати метод і повторити процес навчання. Робота над помилками закінчується коли розробник досягає бажаної точності.

Azure ML дає можливість використовувати в одному проекті величезну кількість алгоритмів навчання. Завдяки цьому на етапі розробки можна дізнатися яка якість роботи кожного з використовуваних алгоритмів для того щоб взнати, який саме краще використовувати для поставленої мети. В даному проекті застосовуються наступні методи: логічна регресія, метод опорних векторів, регресійне дерево.

Додаткова можливість яка дозволяє підвищити продуктивність системи - налаштування методу машинного навчання, застосовуючи максимально можливу кількість нпараметрів наявних в параметрах системи. В нашій моделі в методі логічної регресії було використано фіксуване число дерев і відгалужень, яке потрібно було моделювати. У методі двухкласового розподілу вказано фіксована кількість використовуваних вузлів, кількості ітерацій навчання та вихідної ваги.

На фінальній стадії роботи був побудований графік, що виводить інформацію з контейнера редагуання оціночної моделі, для чого була використана функція Visualize для всіх трьох методів (рис 3.10 – 3.12).

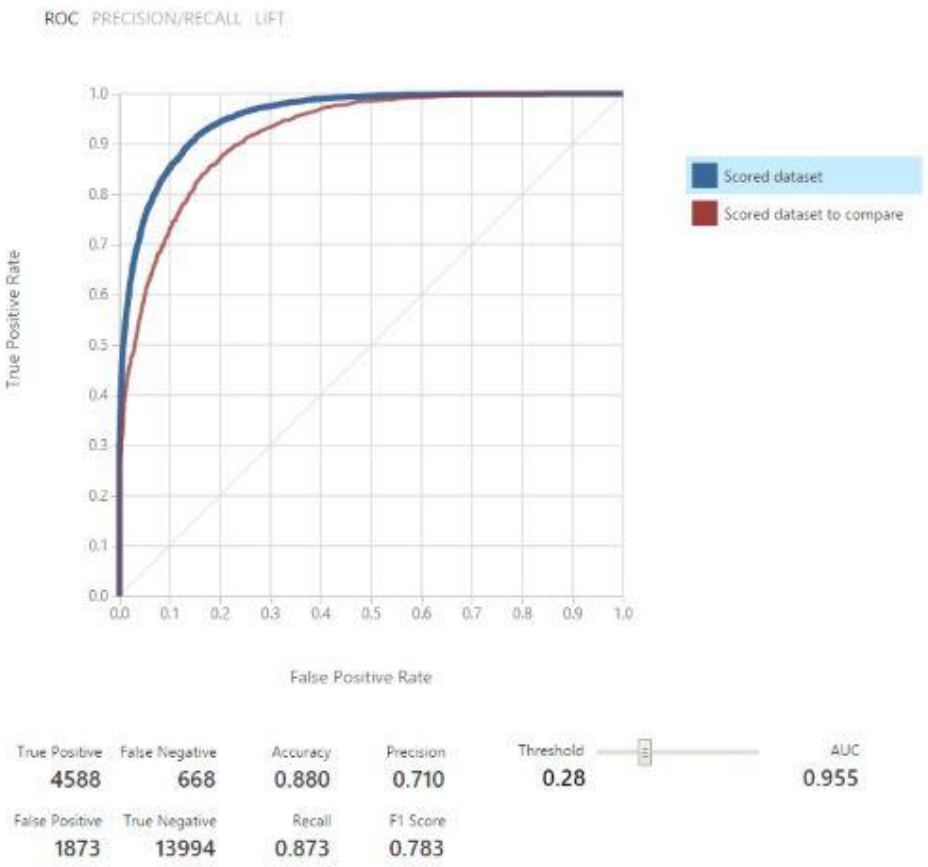


Рисунок 3.10 – ROC графік для методу логічної регрессії

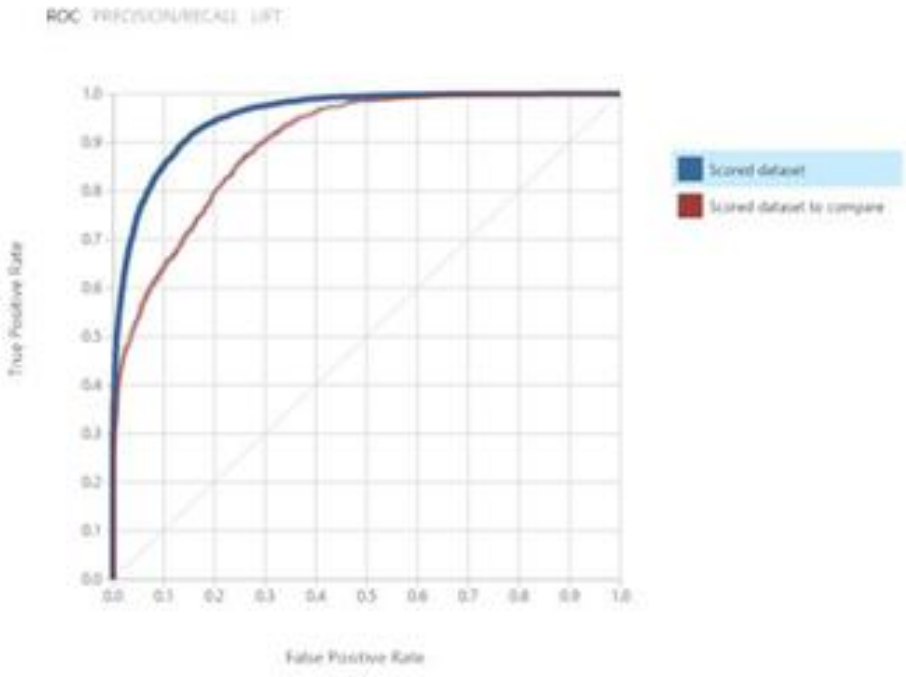


Рисунок 3.11 – ROC графік для методу опорних векторів

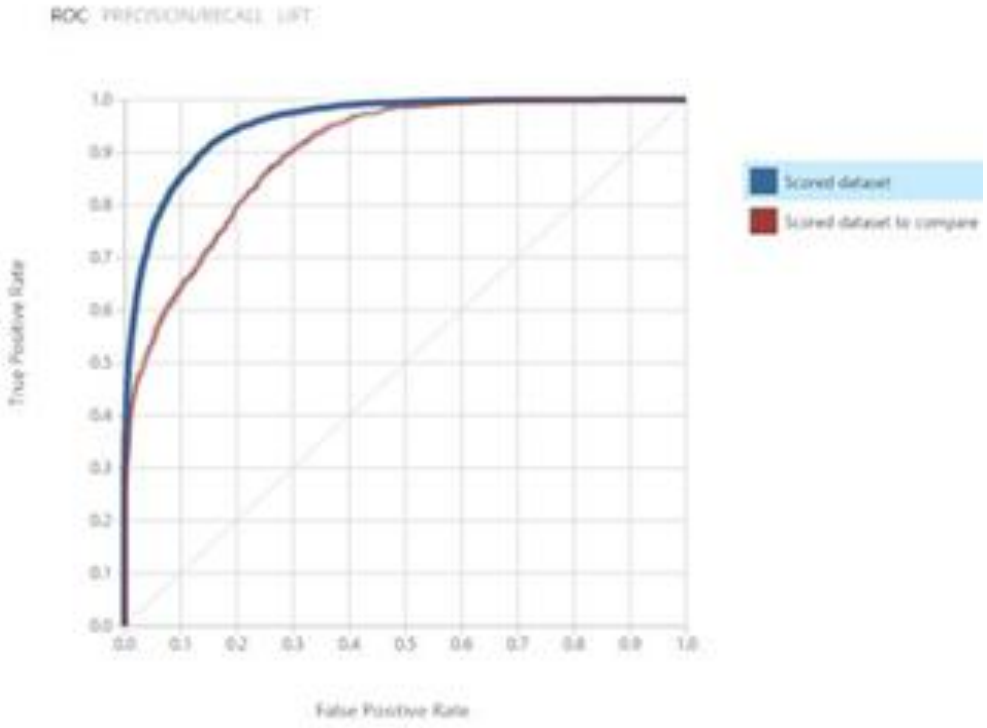


Рисунок 3.12 – ROC графік для методу регресійного дерева

У оціночної матриці передбачення, вираховуються дані точності використовуваних в роботі методів. Для аналізу слід вибрати той метод, який за показником AUC має найбільшу наближеність до значення 1.

Так само, слід проаналізувати параметр AUC по відношенню до параметру Threshold. У даній роботі значення цього параметра дуже важливе, так як збитки від самих грабежів банківських карт (False Positive) більше в рази, ніж від платежів, випадково ідентифікованих як шахрайські операції (False Negative).Для цього потрібно вказати Threshold значення, більше або менше вихідного (0.5).

При виборі найкращого методу для ініціалізації найточнішою моделі виявлення шахрайських операцій, потрібно взяти до уваги, що прийняття рішення для деяких використаних методів можливо відтворити, в той час як для інших не можна. Це буде корисно, в разі якщо потрібно дізнатися, чому по певшому етапі роботи система прийняла те чи інше рішення, з якої конкретно причини платіжна операція була ідентифікована як шахрайська. В даному випадку кращий реультат продемонстрував метод на базі логічної регресії.

3.2 Підключення web-сервісу

Зробивши всі необхідні перевірки, провівши підготовку експерименту Microsoft Azure, завантажуємо його в якості стандартної веб-служби Azure. Використовуючи веб-службу розробники можуть надсилати інформацію моделі, де, в свою чергу буде проходити аналіз інформації, що надійшла і відсилання назад своїх прогнозів.

Для цього скористаємося функцією Deploy Web Service (рис 3.13). Веб-служба буде створена, внаслідок чого з'явиться панель її візуалізації.

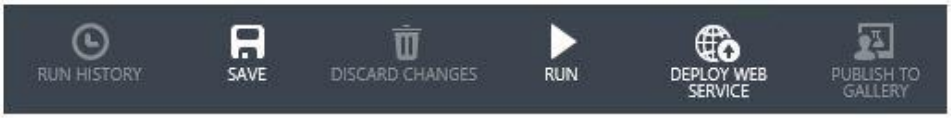


Рисунок 3.13 - Функція Deploy Web Service

Використовуючи будь-яку мову програмування, що надає можливість відправляти HTTP запит і отримувати відповідь можна підключитися до служби веб-служби машинного навчання. в нашому випадку ми будемо використовувати мову програмування C #.

3.3 Розробка додатка

Створимо програму, яка працює з Azure ML в ролі кінцевого сервісу. На першому кроці створюємо новий проект універсального застосування Windows. Для цього в Visual Studio натискаємо File -> New -> Project ... У вікні заходимо в категорію Windows в списку натискаємо на Blank App (Universal Windows). Називаємо проект AF System і приступаємо до роботи.

Скористаємося кодом написаним мовою C# та за допомогою нього викличемо систему виявлення шахрайських операцій.

```
private async Task<RequestStatistics> InvokePredictorService(TransactionInfo
transactionInfo, TransactionStatistics transactionStatistics)
{
    Contract.Requires<ArgumentNullException>(transactionInfo != null);
    Contract.Requires<ArgumentNullException>(transactionStatistics != null);

    var statistics = new RequestStatistics();
```

```
    var watch = new Stopwatch();

    using (var client = new HttpClient())
    {
        var scoreRequest = new
        {
            Inputs = new Dictionary<string, StringTable>() {
                {
                    "transactionInfo",
                    new StringTable()
                    {
                        ColumnNames = new []
                        {
                            #region Column name list
                        },
                        Values = new [,]
                        {
                            {
                                #region Column value list
                            }
                        }
                    }
                },
            },
            GlobalParameters = new Dictionary<string, string>()
        };

        client.DefaultRequestHeaders.Authorization = new
AuthenticationHeaderValue("Bearer",
ConfigurationManager.AppSettings["FraudPredictorML:ServiceApiKey"]);
        client.BaseAddress = new
Uri("https://ussouthcentral.services.azureml.net/workspaces/<workspace_id>/servic
es/<service_id>/execute?api-version=2.0&details=true");

        watch.Start();

        HttpResponseMessage response = await client.PostAsJsonAsync("",
scoreRequest);
        if (response.IsSuccessStatusCode)
            await response.Content.ReadAsStringAsync();

        statistics.TimeToResponse = watch.Elapsed;
        statistics.ResponseStatusCode = response.StatusCode;
        watch.Stop();
    }

    return statistics;
}
```

Отримаємо наступний запит:

```
POST
https://ussouthcentral.services.azureml.net/workspaces/<workspace_id>/services/<s
ervice_id>/execute?api-version=2.0&details=true HTTP/1.1
Authorization: Bearer <api key>
Content-Type: application/json; charset=utf-8
Host: ussouthcentral.services.azureml.net
/* другие заголовки */
```

```
{
   "Inputs": {
   "transactionInfo": {
   "ColumnNames": [
       "PartitionKey",
       "RowKey",
       "Timestamp",
       "CardId",
       "CrmAccountId",
       "MCC",
       "MerchantId",
       "TransactionAmount",
       "TransactionCreatedTime",
       "TransactionCurrency",
       "TransactionId",
       "TransactionResult",
       "CardExpirationDate",
       "CardholderName",
       "CrmAccountFullName",
       "TransactionRequestHost",
       "PartitionKey (2)",
       "RowKey (2)",
       "Timestamp (2)",
       "CardsCountFromThisCrmAccount1D",
       "CardsCountFromThisCrmAccount1H",
       "CardsCountFromThisCrmAccount1M",
       "CardsCountFromThisCrmAccount1S",
       "CardsCountFromThisHost1D",
       "CrmAccountsCountFromThisCard1D",
       "FailedPaymentsCountByThisCard1D",
       "SecondsPassedFromPreviousPaymentByThisCard1D",
       "PaymentsCountByThisCard1D",
       "HostsCountFromThisCard1D",
       "HasHumanEmail",
       "HasHumanPhone",
       "IsCardholderNameIsTheSameAsCrmAccountName",
       "IsRequestCountryIsTheSameAsCrmAccountCountry",
       "TransactionDayOfWeek",
       "TransactionLocalTimeOfDay"
       /* значения прочие предикторы */
       ],
   "Values": [
       [
       "990",
       "f31f64f367644b1cb173a48a34817fbc",
       "2019-15-1T20:54:28.6508575Z",
       "349567471",
       "10145",
       "32",
       "990",
       "136.69",
       "2019-15-1T20:54:28.6508575Z",
       "840",
       "f31f64f367644b1cb173a48a34817fbc",
       null,
       "2019-15-1T23:44:28.6508575+03:00",
       "640ab2bae07bedc4c163f679a746f7ab7fb5d1fa",
       "640ab2bae07bedc4c163f679a746f7ab7fb5d1fa",
       "20.30.30.40",
       "990",
       "f31f64f367644b1cb173a48a34817fbc",
```

```
        "2019-03-15T20:54:28.6508575Z",
        "2",
        "1",
        "0",
        "0",
        "0",
        "0",
        "1",
        "2",
        "0",
        "0",
        "true",
        null,
        "true",
        "true",
        "Monday",
        "Morning"
        /* значения прочих предикторов */
        ]
    ]
    }
    },
    "GlobalParameters": { }
    }
```

Відповідь web-сервісу Azure ML:

```
HTTP/1.1 200 OK
Content-Length: 1619
Content-Type: application/json; charset=utf-8
Server: Microsoft-HTTPAPI/2.0
x-ms-request-id: f8cb48b8-6bb5-4813-a8e9-5baffaf49e15
Date: Sun, 15 Jan 2019 20:44:31 GMT
{
    "Results": {
       "transactionPrediction": {
       "type": "table",
       "value": {
       "ColumnNames": [
           "PartitionKey",
           "RowKey",
           "Timestamp",
           "CardId",
           "CrmAccountId",
           "MCC",
           "MerchantId",
           "TransactionAmount",
           "TransactionCreatedTime",
           "TransactionCurrency",
           "TransactionId",
           /* значения прочие предикторы */
           "Scored Labels",
           "Scored Probabilities"
           ],
       "Values": [
           [
           "990",
```

```
            "f31f64f367644b1cb173a48a34817fbc",
            "2019-15-1T20:54:28.6508575Z",
            "349567471",
            "10145",
            "32",
            "990",
            "136.69",
            "2019-15-1T20:54:28.6508575Z",
            "840",
            "f31f64f367644b1cb173a48a34817fbc",
            /* значения прочих предикторов */
            "Success",
            "0.779961256980896"
            ]
        ]
        }
        }
    }
}
```

3.3 Тестування системи на працездатність

Працездатність системи перевірялась засобами Microsoft Azure, для чого був використаний віртуальний комп'ютер, який був умовно розташований в аналогічному регіоні, що й сервіс виявлення шахрайства.

Після чого було дане навантаження в 16 тисяч запитів.

```
/// <summary>
/// Entry point
/// </summary>
public void Main()
{
    var client = new PredictorMLClient();

    RequestsStatistics invokeParallelStatistics = client.InvokeParallel(1024,
22);
    LogResult(invokeParallelStatistics);

    RequestsStatistics invokeAsyncStatistics = client.InvokeAsync(1024).Result;
    LogResult(invokeAsyncStatistics);
}

private static void LogResult(RequestsStatistics statistics)
{
    Contract.Requires<ArgumentNullException>(statistics != null);

    Func<double, string> format = d => d.ToString("F3");

    Log.Info("Results:");
    Log.Info("Min: {0} ms", format(statistics.Min));
    Log.Info("Average: {0} ms", format(statistics.Average));
    Log.Info("Max: {0} ms", format(statistics.Max));
    Log.Info("Count of failed requests: {0}", statistics.FailedRequestsCount);
}
```

```
/// <summary>
/// Client for PredictorML web-service
/// </summary>
public class PredictorMLClient
{
/// <summary>
/// Async invocation of method
/// </summary>
/// <param name="merchantId">Merchant id</param>
/// <exception cref="ArgumentOutOfRangeException"><paramref
name="merchantId"/></exception>
public async Task<RequestsStatistics> InvokeAsync(int merchantId)
{
    Contract.Requires<ArgumentOutOfRangeException>(merchantId > 0);

    IEnumerable<TransactionInfo> tis = null; IEnumerable<TransactionStatistics>
tss = null;

    // upload input data
    Parallel.Invoke(
        () => tis = new TransactionsInfoRepository().Get(merchantId),
        () => tss = new TransactionsStatisticsRepository().Get(merchantId)
    );

    var inputs = tis
        .Join(tss, ti => ti.TransactionId, ts => ts.TransactionId, (ti, ts) =>
new { TransactionInfo = ti, TransactionStatistics = ts })
        .ToList();

    // send requests
    var statistics = new List<RequestStatistics>(inputs.Count);
    foreach (var input in inputs)
    {
        RequestStatistics stats = await
InvokePredictorService(input.TransactionInfo,
input.TransactionStatistics).ConfigureAwait(false);
        statistics.Add(stats);
    }

    // return result
    return new RequestsStatistics(statistics);
}


/// <summary>
/// Parallel invocation of method (for load testing purposes)
/// </summary>
/// <param name="merchantId">Merchant id</param>
/// <param name="degreeOfParallelism">Count of parallel requests</param>
/// <exception cref="ArgumentOutOfRangeException"><paramref
name="merchantId"/></exception>
/// <exception cref="ArgumentOutOfRangeException"><paramref
name="merchantId"/></exception>
public RequestsStatistics InvokeParallel(int merchantId, int degreeOfParallelism)
{
    Contract.Requires<ArgumentOutOfRangeException>(merchantId > 0);
    Contract.Requires<ArgumentOutOfRangeException>(degreeOfParallelism > 0);
```

```
    IEnumerable<TransactionInfo> tis = null; IEnumerable<TransactionStatistics>
tss = null;

    // upload input data
    Parallel.Invoke(
        () => tis = new TransactionsInfoRepository().Get(merchantId),
        () => tss = new TransactionsStatisticsRepository().Get(merchantId)
    );
    var inputs = tis
                    .Join(tss, ti => ti.TransactionId, ts => ts.TransactionId,
(ti, ts) => new { TransactionInfo = ti, TransactionStatistics = ts })
                    .ToList();

    // send requests
    var statistics = new List<RequestStatistics>(inputs.Count);
    for (int i = 0; i < inputs.Count; i = i + degreeOfParallelism)
    {
        var tasks = new List<Task<RequestStatistics>>();
        for (int j = i; j < i + degreeOfParallelism; j++)
        {
            if (inputs.Count <= j) break;

            var input = inputs[j];
            tasks.Add(InvokePredictorService(input.TransactionInfo,
input.TransactionStatistics));
        }
        Task.WaitAll(tasks.ToArray());

        statistics.AddRange(tasks.Select(t => t.Result));
    }

    // return result
    return new RequestsStatistics(statistics);
}

 /* other members */
}
```

В результаті цього маємо наступні показники:

- кращий час отримання результату: 432.575 millisecond;
- гірший час отримання результату: 1466.718 millisecond;
- середній час отримання результату: 543.726 millisecond;
- кількість опрацьованих звернень: 14542;
- кількість неопрацьованих зернень: 874.

3.4 Програмні обмеження

Основною перевагою розробленої інформаційної системи в рівній мірі як і головним недоліком є віддалена платформа Microsoft Azure. В рамках системних обмежень даної платформи можна задати ряд питань, наприклад скільки даних можна передати

одночасно платформі, і який розмір одного пакета даних є максимально допустимим, так як ця інформація не вказується розробниками і знайти її не видається можливим.

Важливо розуміти що швидкість передачі інформації від веб-вузла Predictor ML повинна бути максимально велика, однак в разі затримок яким чином можна підняти швидкість передачі даних невідомо

3.5 Рекомендації

Дана інформаційна технологія виявлення шахрайства в банківській системі дає виключно рекомендаційний характер оцінки платежів, залишаючи право фінального вердикту за компетентними співробітниками банка. Для того щоб якісно зберігати особисті дані в системі необхідний комплексний підхід, тривала історія здійснення платежів власниками карт, використовувати різні підходи до усунення програмних вразливостей. Перевірка транзакцій повинна проходити за рахунок великих знань і отриманих даних в області, моделі і методи, одна з яких була предлажена в роботі, дповинні постійно оновлюватися та вдосконалюватися.

3.6 Висновки до розділу 3

У цьому розділі було запропоновано та розроблено модель на основі сервісу Microsoft Azure, яка здатна відслідковувати шахрайські дії на банківській карті користувача.

Були запропоновані методи віришення задачі та побудовані графіки, що виводять інформацію о процесі виявлення підозрілих операцій згідно з вибраним методом, та вибран найбільш оптимальний з них.

Результати роботи повністю відповідають поставленій меті.

РОЗДІЛ 4
ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ. ЕКОЛОГІЯ

В даному розділі проведено аналіз потенційних небезпечних та шкідливих виробничих факторів, причин пожеж. Розглянуті заходи, які дозволяють забезпечити гігієну праці і виробничу санітарію. На підставі аналізу розроблені заходи з техніки безпеки та рекомендації з пожежної профілактики.

Завданням даного проекту бакалавра було «Інформаційна технологія виявлення шахрайства в банківській системі». Так як в процесі проектування виконувалось у домашніх умовах, то аналіз потенційно небезпечних і шкідливих виробничих чинників виконується для робочого місця, з використанням персонального комп'ютера на якому буде виконуватись дослідження.

4.1 Загальні питання з охорони праці

Умови праці на робочому місці, безпека технологічних процесів, машин, механізмів, устаткування та інших засобів виробництва, стан засобів колективного та індивідуального захисту, що використовуються працівником, а також санітарно-побутові умови повинні відповідати вимогам нормативних актів про охорону праці. В законі України «Про охорону праці»[**Ошибка! Источник ссылки не найден.**] визначається, що охорона праці - це система правових, соціально-економічних, організаційно-технічних, санітарно-гігієнічних і лікувально-профілактичних заходів та засобів, спрямованих на збереження життя, здоров'я і працездатності людини у процесі трудової діяльності.

4.1.1 Правові та організаційні основи охорони праці

Основним організаційним напрямом у здійсненні управління в сфері охорони праці є усвідомлення пріоритету безпеки праці і підвищення соціальної відповідальності держави, і особистої відповідальності працівників.

Державна політика в галузі охорони праці визначається відповідно до Конституції України Верховною Радою України і спрямована на створення належних, безпечних і здорових умов праці, запобігання нещасним випадкам та професійним захворюванням. Відповідно до статті 3 Закону України «Про охорону праці» [7] (далі – Закону) законодавство про охорону праці складається з Закону, Кодексу законів про працю України [22], Закону України "Про загальнообов'язкове державне соціальне страхування від нещасного випадку на виробництві та професійного захворювання, які спричинили втрату працездатності" [23] та прийнятих відповідно до них нормативно-правових актів, норм міжнародного договору (ратифіковані Конвенції і Рекомендації МОТ, директиви Європейської Ради).

4.1.2 Організаційно-технічні заходи з безпеки праці

В організації/підприємстві проводиться навчання і перевірка знань з питань охорони праці відповідно до вимог Типового положення про порядок проведення навчання і перевірки знань з питань охорони праці, затвердженого наказом Держнаглядохоронпраці України від 26.01.2005 N 15, зареєстрованого в Міністерстві юстиції України 15.02.2005 за N 231/10511 [9].

Обов’язковими вимогами враховане наступне:

– не слід допускати до роботи осіб, що в установленому порядку не пройшли навчання, інструктаж та перевірку знань з охорони праці, пожежної безпеки та цих Правил.

– на підприємстві/організації, де експлуатуються ЕОМ з відео дисплейними терміналами (ВДТ) і периферійними пристроями (ПП), розробляється інструкція з охорони праці відповідно до Положення про розробку інструкцій з охорони праці, затвердженого наказом Держнаглядохоронпраці від 29.01.98 N 9, зареєстрованого в Міністерстві юстиції України 07.04.98 за N 226/2666 [10].

– ознайомлення з правилами безпеки праці, одержання відповідних інструктажів засвідчується у журналі інструктажів.

4.2 Аналіз стану умов праці

Робота над створенням локальної комп'ютерної мережі проходить в побутовому приміщенні. Для даної роботи достатньо однієї людини, для якої надано робоче місце зі стаціонарним комп'ютером.

4.2.1 Вимоги до приміщення

Геометричні розміри приміщення зазначені у таблиці 4.1.

Таблиця4.1 – розміри робочого місця

Параметр	Значення
Довжина, м	3
Ширина, м	5
Висота, м	2,5
Площа, $м^2$	15
Об'єм, $м^3$	37,5

Згідно до санітарних норм мікроклімату виробничих приміщень [13] розмір площі для одного робочого місця оператора персонального комп'ютера має бути не менше 6 кв. м, а об'єм – не менше 20 куб. м. Отже, дане приміщення цілком відповідає зазначеним нормам.

4.2.2 Вимоги до організації робочого місця

При порівнянні відповідності характеристик робочого місця нормативним основні вимоги до організації робочого місця [**Ошибка! Источник ссылки не найден.**] (табл. 4.2) і відповідними фактичними значеннями для робочого місця, констатуємо повну відповідність.

Таблиця 4.2 – Характеристика робочого місця

Найменування параметра	Фактичне значення	Нормативне значення
Висота робочої поверхні, мм	750	680 ÷800
Висота простору для ніг, мм	730	не менше 600
Ширина простору для ніг, мм	660	не менше 500

Глибина простору для ніг, мм	700	не менше 650

Продовження таблиці 4.2

Найменування параметра	Фактичне значення	Нормативне значення
Висота поверхні сидіння, мм	470	400 ÷500
Ширина сидіння, мм	400	не менше 400
Глибина сидіння, мм	400	не менше 400
Висота поверхні спинки, мм	600	не менше 300
Ширина опорної поверхні спинки, мм	500	не менше 380
Радіус кривини спинки в горизонтальній площині, мм	400	400
Відстань від очей до екрану дисплея, мм	800	700 ÷800

У кабінеті є електрична мережа з напругою 220 В, яка створює небезпеку ураження електричним струмом. ПК та периферійні пристрої можуть бути джерелами електромагнітних випромінювань, аерозолів та шкідливих речовин (часток тонеру, оксидів нітрогену та озону).

За ступенем пожежної безпеки приміщення належить до категорії В. Кабінет оснащений переносним вуглекислотним вогнегасником ВВК-5 .

Наявна аптечка для надання долікарської допомоги, а також у кабінеті роблять вологе прибирання та щоденно провітрюють приміщення.

4.2.3 Навантаження та напруженість процесу праці

За фізичним навантаженням робота відноситься до категорії легкі роботи (Іа), її виконують сидячи з періодичним ходінням. Щодо характеру організування виконання дипломної роботи, то він підпадає під нав’язаний режим, оскільки певні розділи роботи необхідно виконати у встановлені конкретні терміни. За ступенем нервово-психічної напруги виконання роботи можна віднести до ІІ – ІІІ ступеня і кваліфікувати як помірно напружений – напружений за умови успішного виконання поставлених завдань.

Роботу за дипломним проектом визнано, таку, що займає 50% часу робочого дня та за восьмигодинної робочої зміни рекомендовано встановити додаткові регламентовані перерви тривалістю 15 хв через кожну годину роботи;

4.3 Виробнича санітарія

На підставі аналізу небезпечних та шкідливих факторів при виробництві (експлуатації), пожежної безпеки можуть бути надалі вирішені питання необхідності забезпечення працюючих достатньою кількістю освітлення, вентиляції повітря, організації заземлення, тощо.

4.3.1 Аналіз небезпечних та шкідливих факторів при розробці виробу

Аналіз небезпечних та шкідливих виробничих факторів виконується у табличній формі (табл. 4.3). Роботу, пов'язану з ЕОП з ВДТ, у тому числі на тих, які мають робочі місця, обладнані ЕОМ з ВДТ і ПП, виконують із забезпеченням виконання, які встановлюють вимоги безпеки до обладнання робочих місць, до роботи із застосуванням ЕОМ з ВДТ і ПП. Переважно роботи за проектами виконують у кабінетах чи інших приміщеннях, де використовують різноманітне електрообладнання, зокрема персональні комп’ютери (ПК) та периферійні пристрої. Основними робочими характеристиками персонального комп'ютера є:

- робоча напруга U = +220В +-5%;
- робочий струм I = 2А;
- споживана потужність P = 600 Вт.

Таблиця 4.3 – Аналіз небезпечних і шкідливих виробничих факторів

Небезпечні і шкідливі виробничі фактори	Джерела факторів (види робіт)	Нормативні документи
Фізичні		
- підвищена температура поверхонь обладнання	експлуатація ЕОМ, серверного обладнання для роботи	[13]
- підвищена або знижена вологість повітря	-//-	[13]
- підвищена або знижена рухливість повітря	-//-	[24]
- підвищений рівень напруги електричної мережі	-//-	[**Ошибка! Источник ссылки не**

		найден.] [17]
- підвищений рівень статичної електрики	-//-	[**Ошибка! Источник ссылки не найден.**]
- підвищена напруженість електромагнітного поля	-//-	[17]

Продовження таблиці 4.3

Небезпечні і шкідливі виробничі фактори	Джерела факторів (види робіт)	Нормативні документи
- недостатність природного світла	порушення умов праці (вимог до приміщень)	[20]
- недостатнє освітлення робочої зони	порушення гігієнічних параметрів виробничого середовища	[20]
Психофізиологічні		
-нервово-психічна перевантаження	Розумова робота над проектом	[14] [**Ошибка! Источник ссылки не найден.**]
- фізичні (статичне – сидіння)	порушення умов праці та організації робочого часу	[14]

Робочі місця мають відповідати вимогам Державних санітарних правил і норм роботи з візуальними дисплейними терміналами електронно-обчислювальних машин, затверджених постановою Головного державного санітарного лікаря України від 10.12.98 [14]. За умов роботи з ПК виникають наступні небезпечні та шкідливі чинники: несприятливі мікрокліматичні умови, освітлення, електромагнітні випромінювання, забруднення повітря шкідливими речовинами (джерелом, яких можуть бути: принтер, сканер та інші джерела виділення багатьох хімічних речовин - напр., озону, оксидів азоту та аерозолів високодисперсних частинок тонера), шум, вібрація, електричний струм, електростатичне поле, напруженість трудового процесу та інше.

4.3.2 Пожежна безпека

Небезпека розвитку пожежі на обчислювальному центрі обумовлюється застосуванням розгалужених систем електроживлення ЕОМ, вентиляції і кондиціювання. Небезпека загоряння пов'язана з особливістю комп'ютерів – із значною кількістю щільно

розташованих на монтажній платі і блоках електронних вузлів і схем, електричних і комутаційних кабелів, резисторів, конденсаторів, напівпровідникових діодів і транзисторів. Надійна робота окремих елементів і мікросхем в цілому забезпечується тільки в певних інтервалах температури, вологості і при заданих електричних параметрах. При відхиленні реальних умов експлуатації від розрахункових можуть виникнути пожежонебезпечні ситуації.

Для гасіння пожеж в офісному приміщенні пропонується використовувати порошкові або вуглекислотні вогнегасники, так як вони є універсальними.

4.3.3 Електробезпека

На робочому місці виконуються наступні вимоги електробезпеки: ПК, периферійні пристрої та устаткування для обслуговування, електропроводи і кабелі за виконанням та ступенем захисту відповідають класу зони за ПУЕ (правила улаштування електроустановок), мають апаратуру захисту від струму короткого замикання та інших аварійних режимів. Лінія електромережі для живлення ПК, периферійних пристроїв і устаткування для обслуговування, виконана як окрема групова три- провідна мережа, шляхом прокладання фазового, нульового робочого та нульового захисного провідників. Нульовий захисний провідник використовується для заземлення (занулення) електроприймачів. Штепсельні з'єднання та електророзетки крім контактів фазового та нульового робочого провідників мають спеціальні контакти для підключення нульового захисного провідника. Електромережа штепсельних розеток для живлення персональних ПК, укладено по підлозі поруч зі стінами відповідно до затвердженого плану розміщення обладнання та технічних характеристик обладнання. Металеві труби та гнучкі металеві рукави заземлені. Захисне заземлення включає в себе заземлюючих пристроїв і провідник, який з'єднує заземлюючий пристрій з обладнанням, яке заземлюється - заземлюючий провідник.

4.4 Гігієнічні вимоги до параметрів виробничого середовища

4.4.1 Мікроклімат

Мікроклімат робочих приміщень – це клімат внутрішнього середовища цих приміщень, що визначається діючої на організм людини з'єднанням температури, вологості, швидкості переміщення повітря. В даному приміщенні проводяться роботи, що

виконуються сидячи і не потребують динамічного фізичного напруження, то для нього відповідає категорія робіт Іа. Отже оптимальні значення для температури, відносної вологості й рухливості повітря для зазначеного робочого місця відповідають нормам [13] і наведені в табл. 4.4.

Таблиця 4.4 – Норми мікроклімату робочої зони об’єкту

Період року	Категорія робіт	Температура *С°*	Відносна вологість %	Швидкість руху повітря, м/с
Холодна	легка-1 а	22 - 24	40 – 60	0,1
Тепла	легка-1 а	23 - 25	40 – 60	0,1

Дане приміщення обладнане системами опалення, кондиціонування повітря або припливно-витяжною вентиляцією. У приміщенні на робочому місці забезпечуються оптимальні значення параметрів мікроклімату: температури, відносної вологості й рухливості повітря у відповідності до [13]. Рівні позитивних і негативних іонів у повітрі мають відповідати [13]. Для забезпечення оптимальних параметрів мікроклімату в приміщенні проводяться перерви в роботі співробітників, з метою його провітрювання. Існують спеціальні системи кондиціонування, які забезпечують підтримання в приміщенні балансу оптимальних параметрів мікроклімату.

Контроль параметрів мікроклімату в холодний і теплий період року здійснюється не менше 3-х разів на зміну (на початку, середині, в кінці).

4.4.2 Освітлення

У проекті, що розробляється, передбачається використовувати суміщене освітлення. У світлий час доби використовуватиметься природне освітлення приміщення через віконні отвори, в решту часу використовуватиметься штучне освітлення. Штучне освітлення створюється газорозрядними лампами.

Розрахунок освітлення

Для виробничих та адміністративних приміщень світловий коефіцієнт приймається не менше -1/8, в побутових – 1/10:

$$S_b = \left(\frac{1}{5} \div \frac{1}{10}\right) \cdot S_n \qquad (4.1)$$

де S_b – площа віконних прорізів, м^2;

S_n – площа підлоги, м^2.

$S_n = a \cdot b = 5 \cdot 3 = 15$ м^2,

$S = 1/10 \cdot 15 = 1{,}5$ м^2.

Приймаємо 1 вікно площею S=1,5 м^2.

Світильники загального освітлення розташовуються над робочими поверхнями в рівномірно-прямокутному порядку. Для організації освітлення в темний час доби передбачається обладнати приміщення, довжина якого складає 3 м, ширина 5 м, світильниками ЛПО2П, оснащеними лампами типа ЛБ (дві по 40 Вт) з світловим потоком 3200 лм кожна.

Розрахунок штучного освітлення виробляється по коефіцієнтах використання світлового потоку, яким визначається потік, необхідний для створення заданої освітленості при загальному рівномірному освітленні. Розрахунок кількості світильників n виробляється по формулі (5.2):

$$n = \frac{E \cdot S \cdot Z \cdot K}{F \cdot U \cdot M}, \qquad (4.2)$$

де E – нормована освітленість робочої поверхні, визначається нормами – 300 лк;

S – освітлювана площа, м^2; S = 15 м^2;

Z – поправочний коефіцієнт світильника (1,1 для люмінесцентних ламп);

K – коефіцієнт запасу, що враховує зниження освітленості в процесі експлуатації – 1,5;

U – коефіцієнт використання, залежний від типу світильника, показника індексу приміщення і т.п. – 0,575

M – число люмінесцентних ламп в світильнику – 2;

F – світловий потік лампи – 3200лм (для ЛБ-40-2).

Підставивши числові значення у формулу (5.2), отримуємо:

$$n = \frac{300 \cdot 15 \cdot 1{,}1 \cdot 1{,}5}{3200 \cdot 0.575 \cdot 2} = 2{,}018$$

Приймаємо освітлювальну установку, яка складається з 2-х світильників, які складаються з 2-х люмінесцентних ламп загальною потужністю 40 Вт, напругою – 220 В.

4.4.3 Вентилювання

У приміщенні, де знаходяться ЕОМ, повітрообмін реалізується за допомогою природної організованої вентиляції. Цей метод забезпечує приток потрібної кількості свіжого повітря, що визначається в СНіП.

Також має здійснюватися провітрювання приміщення, в залежності від погодних умов, тривалість повинна бути не менше 10 хв. Найкращий обмін повітря здійснюється при наскрізному провітрюванні.

4.5 Заходи з організації виробничого середовища та попередження виникнення надзвичайних ситуацій

Відповідно до санітарно-гігієнічних нормативів та правил експлуатації обладнання наводимо приклади деяких заходів безпеки.

1) Заходи безпеки під час експлуатації персонального комп'ютера та периферійних пристроїв передбачають:

- правильне організування місця праці та дотримання оптимальних режимів праці та відпочинку під час роботи з ПК;

- експлуатацію сертифікованого обладнання;

- дотримання заходів електробезпеки;

- забезпечення оптимальних параметрів мікроклімату;

- забезпечення раціонального освітлення місця праці (освітленість робочого місця не перевищувала 2/3 нормальної освітленості приміщення);

- облаштовуючи приміщення для роботи з ПК, потрібно передбачити припливно-витяжну вентиляцію або кондиціювання повітря:

а) якщо об'єм приміщення 20 м^3, то потрібно подати не менш як 30 м^3/год повітря;

б) якщо об'єм приміщення у межах від 20 до 40 м^3, то потрібно подати не менш як 20 м^3/год повітря;

в) якщо об'єм приміщення становить понад 40 м^3, допускається природна вентиляція, у випадку, коли немає виділення шкідливих речовин.

- зниження рівня шуму та вібрації:

а) у джерелі виникнення, шляхом застосування раціональних конструкцій, нових матеріалів і технологічних процесів;

б) звукоізолювання устаткування за допомогою глушників, резонаторів, кожухів, захисних конструкцій, оздоблення стін, стелі, підлоги тощо;

в) використання засобів індивідуального захисту).

2) Заходи безпеки під час експлуатації інших електричних приладів передбачають дотримання таких правил:

- постійно стежити за справним станом електромережі, розподільних щитків, вимикачів, штепсельних розеток, лампових патронів, а також мережевих кабелів живлення, за допомогою яких електроприлади під'єднують до електромережі;

- постійно стежити за справністю ізоляції електромережі та мережевих кабелів, не допускаючи їхньої експлуатації з пошкодженою ізоляцією;

- не тягнути за мережевий кабель, щоб витягти вилку з розетки;

- не закривати меблями, різноманітним інвентарем вимикачі, штепсельні розетки;

- не підключати одночасно декілька потужних електропристроїв до однієї розетки, що може викликати надмірне нагрівання провідників, руйнування їхньої ізоляції, розплавлення і загоряння полімерних матеріалів;

- не залишати включені електроприлади без нагляду;

- не допускати потрапляння всередину електроприладів крізь вентиляційні отвори рідин або металевих предметів, а також не закривати їх та підтримувати в належній чистоті, щоб уникнути перегрівання та займання приладу;

- не ставити на електроприлади матеріали, які можуть під дією теплоти, що виділяється, загорітися (канцелярські товари, сувенірну продукцію тощо).

Від ураження струмом застосовують різні електричні захисні засоби:

а) Ізолюючі – ізолюють людини від струмоведучих або заземлених частин, а так-же від землі. Вони діляться на основні та додаткові.

б) Основні – володіють ізоляцією, здатної довго витримувати робоче напругу електроустановки і тому ними дозволяється стосуватися струмоведучих частин, знаходячи-трудящих під напругою.

в) Запобіжні – володіють ізоляцією нездатною витримати робоча напруга електроустановки, і тому вони не можуть самостійно захищати людину від ураження струмом під цим напругою. Їх значення - посилити захисні дії основних і ізолюючих засобів, разом з якими вони повинні застосовуватися, при чому при використання основних захисних засобів достатньо застосування одного запобіжного захисного засобу.

4.6 Розрахунок захисного заземлення

Згідно з класифікацією приміщень за ступенем небезпеки ураження електричним струмом [17], приміщення в якому проводяться всі роботи відноситься до першого класу (без підвищеної небезпеки). Під час роботи використовуються електроустановки з напругою живлення 36 В, 220 В, та 360 В. Опір контуру заземлення повинен мати не більше 4 Ом.

Послідовність розрахунку:

1) Визначається необхідний опір штучних заземлювачів $R_{шт.з.}$:

$$R_{шт.з.} = \frac{R_Д \cdot R_{пр.з.}}{R_{пр.з.} - R_Д}; \quad (4.3)$$

де $R_{пр.з.}$ – опір природних заземлювачів; $R_д$ – допустимий опір заземлення. Якщо природні заземлювачі відсутні, то $R_{шт.з.} = R_д$.

Підставивши числові значення у формулу (5.3), отримуємо:

$$R_{шт.з.} = \frac{4 \cdot 40}{40 - 4} \approx 4 Ом$$

2) Опір заземлення в значній мірі залежить від питомого опору ґрунту ρ, Ом·м. Приблизне значення питомого опору глини приймаємо ρ = 40 Ом·м (табличне значення).

3) Розрахунковий питомий опір ґрунту, $\rho_{розр}$, Ом·м, визначається відповідно для вертикальних заземлювачів $\rho_{розр.в}$, і горизонтальних $\rho_{розр.г}$, Ом·м за формулою:

$$\rho_{розр.} = \psi \cdot \rho \quad (4.4)$$

де ψ – коефіцієнт сезонності для вертикальних заземлювачів і кліматичної зони з нормальною вологістю землі, приймається для вертикальних заземлювачів $\rho_{розр.в}$ = 1,7 і горизонтальних $\rho_{розр.г}$ = 5,5 Ом·м.

$$\rho_{розр.в} = 1,7 \cdot 40 = 68 Ом \cdot м$$

$$\rho_{розр.в} = 5,5 \cdot 40 = 220 Ом \cdot м$$

4) Розраховується опір розтікання струму вертикального заземлювача $R_в$, Ом, за (4.).

$$R_B = \frac{\rho_{розр.в}}{2 \cdot \pi \cdot 1_B} \cdot \left(\ln \frac{2 \cdot l_B}{d_{CT}} + \frac{1}{2} \cdot \ln \frac{4 \cdot t + l_B}{4 \cdot t - l_B} \right), \quad (4.5)$$

де $l_в$ – довжина вертикального заземлювача (для труб – 2 − 3 м; $l_в$ = 3 м);

$d_{ст}$ – діаметр стержня (для труб – 0,03 − 0,05 м; $d_{ст}$ = 0,05 м);

t – відстань від поверхні землі до середини заземлювача, яка визначається за ф. (5.6):

$$t = h_E + \frac{l_E}{2}, \tag{4.6}$$

де $h_в$ – глибина закладання вертикальних заземлювачів (0,8 м); тоді

$$t = 0,8 + \frac{3}{2} = 2,3 \text{ м};$$

$$R_в = \frac{68}{2 \cdot \pi \cdot 3} \cdot \left(\ln \frac{2 \cdot 3}{0,05} + \frac{1}{2} \cdot \ln \frac{4 \cdot 2,3 + 3}{4 \cdot 2,3 - 3} \right) = 18,5 \text{ Ом}$$

1) Визначається теоретична кількість вертикальних заземлювачів n штук, без урахування коефіцієнта використання $\eta_в$:

$$n = \frac{2R_E}{R_Д} = \frac{2 \cdot 18,5}{4} = 9,25 \quad , \tag{4.7}$$

І визначається коефіцієнт використання вертикальних електродів групового заземлювача без врахування впливу з'єднувальної стрічки $\eta_в = 0,57$ (табличне значення).

2) Визначається необхідна кількість вертикальних заземлювачів з урахуванням коефіцієнта використання $\eta_в$, шт:

$$n = \frac{2 \cdot R_E}{R_Д \cdot \eta_E} = \frac{2 \cdot 18,5}{4 \cdot 0,57} \approx 16, \tag{4.8}$$

3) Визначається довжина з'єднувальної стрічки горизонтального заземлювача $l_с$, м:

$$l_C = 1,05 \cdot L_B \cdot (n_B - 1), \tag{4.9}$$

де $L_в$ – відстань між вертикальними заземлювачами, (прийняти за $L_в$ = 3м);
$n_в$ – необхідна кількість вертикальних заземлювачів.

$$l_с = 1,05 \cdot 3 \cdot (16 - 1) \approx 48 \text{ м}$$

Визначається опір розтіканню струму горизонтального заземлювача (з'єднувальної стрічки) $R_г$, Ом:

$$R_г = \frac{\rho_{розр.г}}{2 \cdot \pi \cdot l_c} \cdot \ln \frac{2 \cdot l_c^2}{d_{см} \cdot h_г}, \tag{4.10}$$

де $d_{см}$ – еквівалентний діаметр смуги шириною b, $d_{см} = 0{,}95b$, $b = 0{,}15$ м;

$h_г$ – глибина закладання горизантальних заземлювачів (0,5 м);

$l_с$ – довжина з'єднувальної стрічки горизонтального заземлювача $l_с$, м

$$R_г = \frac{220}{2 \cdot \pi \cdot 48} \cdot \ln \frac{2 \cdot 48^2}{0{,}95 \cdot 0{,}15 \cdot 0{,}5} = 8{,}1 \text{ Ом}$$

4) Визначається коефіцієнт використання горизонтального заземлювача $\eta_{с.}$ відповідно до необхідної кількості вертикальних заземлювачів $n_в$.

Коефіцієнт використання з'єднувальної смуги $\eta_с = 0{,}3$.

Розраховується результуючий опір заземлювального електроду з урахуванням з'єднувальної смуги:

$$R_{заг.} = \frac{R_E \cdot R_г}{R_E \cdot \eta_c + R_г \cdot n_E \cdot \eta_E} \le R_д, \qquad (4.11)$$

Висновок: дане захисне заземлення буде забезпечувати електробезпеку будівлі, так як виконується умова: $R_{заг} < 4$ Ом, а саме:

$$R_{заг} = \frac{18{,}5 \cdot 8{,}1}{18{,}5 \cdot 0{,}3 + 8{,}1 \cdot 16 \cdot 0{,}57} = 1{,}9 \le R_д$$

При виникненню пожеж при роботі на ПЕОМ від таких можливими джерел запалювання як:

– іскри і дуги коротких замикань;

– перегрів провідників, резисторів та інших радіодеталей ПЕОМ, від тривалої перевантаження та наявність перехідного опору;

– іскри при розмиканні і розмиканні ланцюгів;

– розряди статичної електрики;

– необережному поводженню з вогнем, а також вибухи газо-повітряних і паро-повітряних сумішей.

4.7 Екологія та охорона навколишнього середовища

Діяльність за темою магістерської роботи, а саме: Дослідження ефективності ядер процесорів з спеціалізованими функціональними пристроями в процесі її виконання впливає на навколишнє природнє середовище і регламентується нормами діючого

законодавства: Законом України «Про охорону навколишнього природного середовища»[25], Законом України «Про забезпечення санітарного та епідемічного благополуччя населення»[26], Законом України «Про відходи»[27], Законом України «Про охорону атмосферного повітря»[28], Законом України «Про захист населення і територій від надзвичайних ситуацій техногенного та природного характеру»[29], Водний кодекс України[30].

В процесі діяльності дослідження за допомогою ПК виникають процеси поводження з відходами ІТ галузі. Нижче надано перелік відходів, що утворюються в процесі роботи:

- Відпрацьовані люмінесцентні лампи - I клас небезпеки
- Акумулятор для джерел безперебійного живлення – III клас безпеки
- Змінні носії інформації - IV клас небезпеки
- Макулатура - IV клас небезпеки
- Побутові відходи - IV клас небезпеки

Зберігання відходів та їх утилізація виконується згідно до вимог Державних санітарних правил і норм ДСанПіН 2.2.7.029 [15].

4.8 Висновки до розілу 4

В результаті проведеної роботи було зроблено аналіз умов праці, шкідливих та небезпечних чинників, з якими стикається робітник. Було визначено параметри і певні характеристики приміщення для роботи над запропонованим проектом написаному в кваліфікаційній роботі, описано, які заходи потрібно зробити для того, щоб дане приміщення відповідало необхідним нормам і було комфортним і безпечним для робітника.

Приведені рекомендації щодо організації робочого місця, а також важливу інформацію щодо пожежної та електробезпеки. Були наведені розміри приміщення та наведено значення температури, вологості й рухливості повітря, необхідна кількість і потужність ламп та інші параметри, значення яких впливає на умови праці робітника, а також – наведені інструкції з охорони праці, техніки безпеки при роботі на комп’ютері.

ВИСНОВКИ

В результаті роботи була створено аналітичне ядро інформаційної технології виявлення шахрайства в банківських системах з використанням аналітичні алгоритми аналізу. Дана система оперує інформацією як поточною, так і отриманої за певну кількість часу, на базі цього приймає рішення про підозрілі дії під час проведення платежу.

Варто визнати що дана система є раннім прототипом, і згодом буде поліпшуватися і модернізуватися, будуть додаватися нові компоненти. На даний момент ця розробка не може конкурувати з світовими аналогами, однак дуже низька стартова ціна роблять її актуальною.

ПЕРЕЛІК ПОСИЛАНЬ

[1] Абдєева З.Р. Информационная безопасность и информационные технологии в банковской сфере / ДонНУЭТ им. Михаила Туган-Барановского. Секция «Современные информационные технологии», подсекция 1. 2013.

[2] Yusupova O.A. Финансовый мониторинг в Украине (организационно-правовые аспекты). Симферополь, 2010.

[3] Цілих О.Н. Инновационная деятельность в банковской сфере. Электронные инновации // Молодой ученый. 2013. № 9. С. 269–275.

4 Ярочкин В.И. Информационная безопасность [Текст]: учебник / В.И. Ярочкин; 2-е изд. – М.: Академический Проект; Гаудеамус, 2004. – 544 с.

5 Симаков М.Н. V Съезд директоров по информационной безопасности / М.Н. Симаков. – Москва, 2012

[6] Поздеева И.А. Актуальные вопросы дистанционного банковского обслуживания с использованием интернет-технологий // Проблемы современной экономики. 2013. № 2. С. 150–154.

[7] Закон України «Про охорону праці».

[8] НПАОП 0.00.-1.28-10 «Правил охорони праці під час експлуатації електронно-обчислювальних машин»;

[9] НПАОП 0.00-4.12-05 «Типове положення про порядок проведення навчання і перевірки знань з питань охорони праці»;

[10] НПАОП 0.00-4.15-98 «Положення про розробку інструкцій з охорони праці»;

[11] НПАОП 40.1-1.01-97 «Правила безпечної експлуатації електроустановок»;

[12] НАПБ Б.02.005-2003 Типове положення про інструктажі, спеціальне навчання та перевірку знань з питань пожежної безпеки на підприємствах, в установах та організаціях України;.

[13] ДСН 3.3.6.042-99 «Санітарні норми мікроклімату виробничих приміщень» ;

[14] ДСанПіН 3.3.2.007-98 «Правила і норми роботи з візуальними дисплейним терміналами електронно-обчислювальних машин»;

[15] ДСанПіН 2.2.7.029 Гігієнічні вимоги щодо поводження з промисловими відходам та визначення їх класу небезпеки для здоров'я населення

[16] ГОСТ 12.1.044-89 «ССБТ. Вогнестійкість. Номенклатура показників і методи ї визначення»;

[17] ГОСТ 12.1.030-81 «Електробезпека. Захисне заземлення, занулення».

[18] ГОСТ 12.1.006-84 «ССБТ. Електромагнітні поля радіочастот»;

[19] ГОСТ 13109-97 «Електрична енергія. Сумісність технічних засобів. Норми якост електричної енергії в системах електропостачання загального призначення»;

[20] ДБН В.2.5-28:2015 «Державні Будівельні Норми України. Природне і штучн освітлення»;

[21] НАПБ Б.03.002-2007 «Норми визначення категорій приміщень, будинків т зовнішніх установок за вибухопожежною та пожежною небезпекою».

[22] Кодекс законів про працю України.

[23] Закону України "Про загальнообов'язкове державне соціальне страхування ві нещасного випадку на виробництві та професійного захворювання, які спричинил втрату працездатності.

[24] ДСН 3.3.6.037-99 Санітарні норми виробничого шуму, ультразвуку та інфразвуку.

[25] Закон України «Про охорону навколишнього природного середовища».

[26] Закон України «Про забезпечення санітарного та епідемічного благополучч населення».

[27] Законом України «Про відходи».

[28] Законом України «Про охорону атмосферного повітря».

[29] Законом України «Про захист населення і територій від надзвичайних ситуаці техногенного та природного характеру».

[30] Водний кодекс України.

Додаток А.
Комп'ютерна презентація

Рисунок А.1 – Презентація. Титульний аркуш

Рисунок А.2 – Презентація. Банківська система

Рисунок А.3 – Презентація. Види шахрайства

Рисунок А.4 – Презентація. Наявні програмні засоби для боротьби з шахрайством

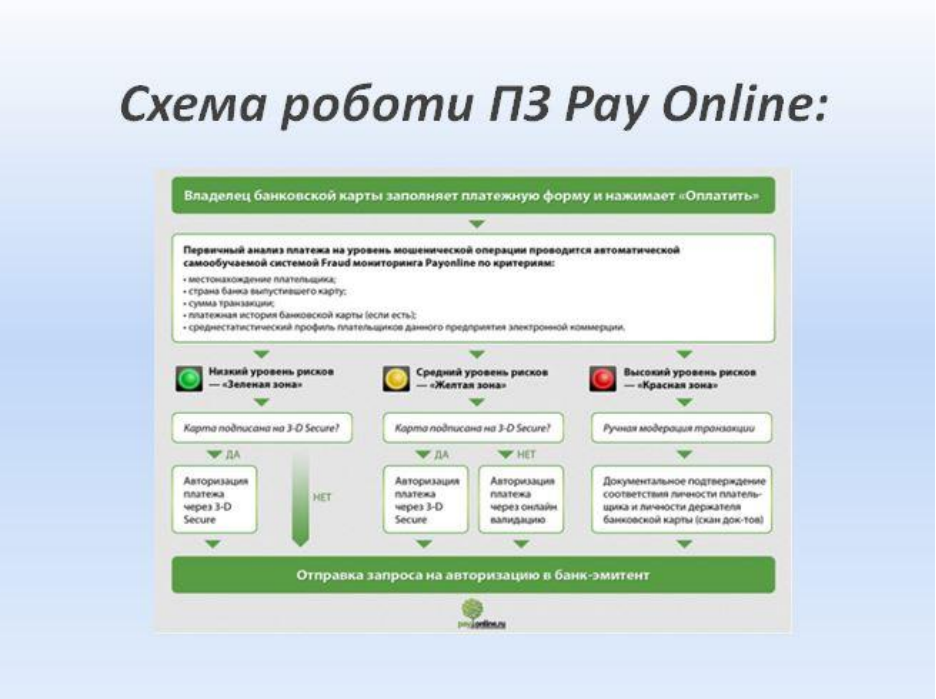


Рисунок А.5 – Презентація. Схема роботи програмного засобу Pay Online

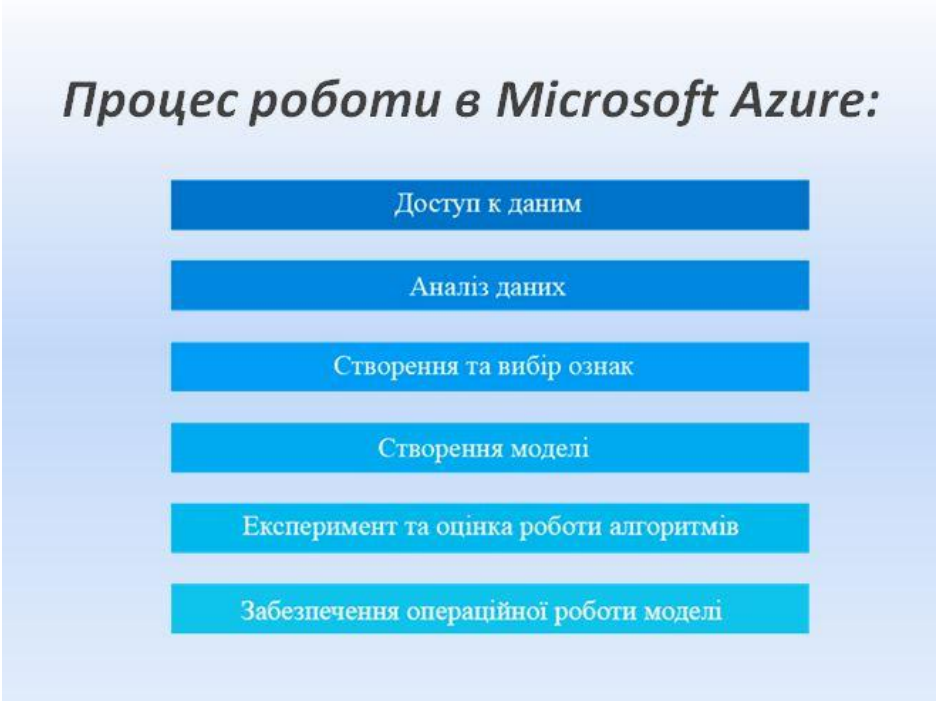


Рисунок А.6 – Презентація. Процес роботи в Microsoft Azure

Рисунок А.7 – Презентація. Структура системи

Рисунок А.8 – Презентація. Схема перевірки транзакці

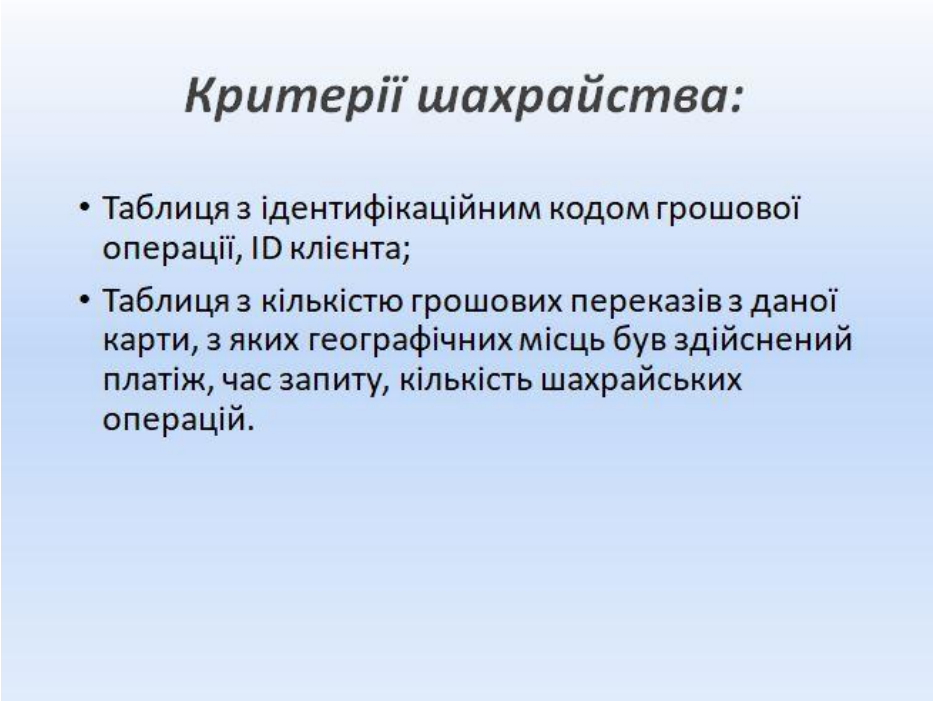


Рисунок А.9 – Презентація. Критерії шахрайства

Рисунок А.10 – Презентація. Побудований експеримент

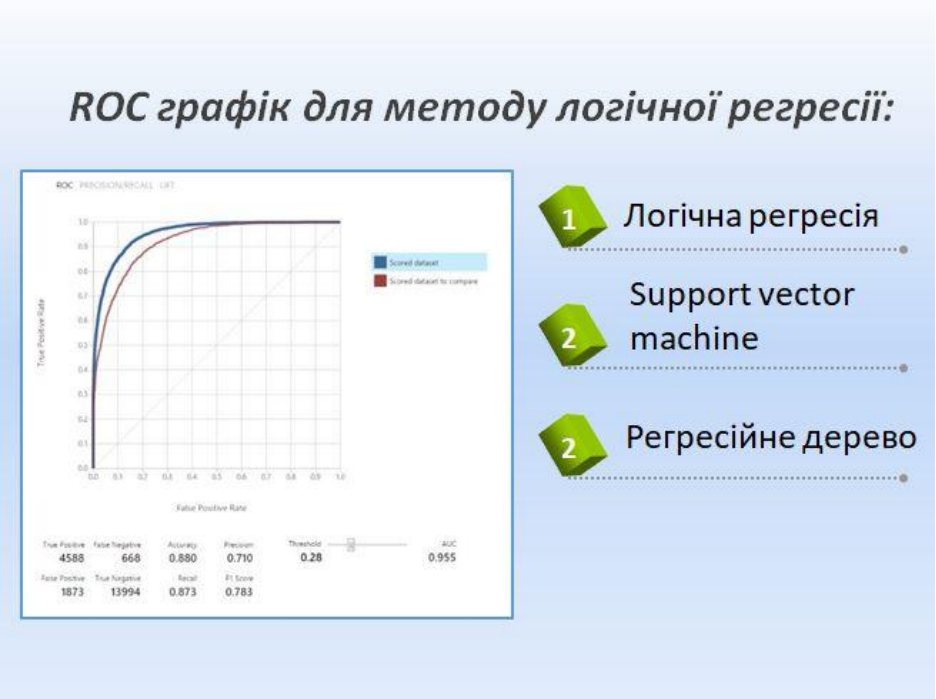


Рисунок А.11 – Презентація. Результат роботи моделі

Рисунок А.12 – Презентація. Остання сторінка