МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

КАФЕДРА КОМП'ЮТЕРНИХ НАУК

ВИПУСКНА РОБОТА

на тему:

«Експертна система ідентифікації користувачів мережі Інтернет»

Завідувач випускаючої кафедри — **Довбиш А.С.**

Керівник роботи — **Лаврик Т.В.**

Студента групи КБ – 61 — **Підгорного П.В.**

СУМИ 2020

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

Кафедра комп'ютерних наук

Затверджую_____

Зав. кафедрою Довбиш А.С.

"_____" _____2020 р.

ЗАВДАННЯ
до випускної роботи

Студента четвертого курсу, групи КБ-61 спеціальності "Кібербезпека" денної форми навчання Підгорного Павла Володимировича.

Тема: " Експертна система ідентифікації користувачів мережі Інтернет "

Затверджена наказом СумДУ

№_____ від _____2020 р.

Зміст пояснювальної записки: 1) аналітичний огляд особливостей кіберзагроз; 2) постановка завдання й формування завдань дослідження; 3) опис основних компонентів та алгоритмів функціонування експертних систем та їх використання для задач кібербезпеки; 5) розробка інформаційного й програмного забезпечення експертної системи; 6) тестування працездатності експертної системи.

Дата видачі завдання "_____" _____ 2020 р.

Керівник випускної роботи _____ Лаврик Т.В.

Завдання приняв до виконання _____ Підгорний П.В.

РЕФЕРАТ

Записка: 77 стор., 16 рис., 1 табл., 1 додаток, 34 джерела.

Об'єкт дослідження — слабоформалізований процес ідентифікації користувачів мережі Інтернет.

Мета роботи — розробка експертної системи ідентифікації користувачів мережі Інтернет.

Методи дослідження — теорія систем штучного інтелекту, моделі та методи представлення знань в експертних системах.

Результати — сформовано вхідний математичний опис експертної системи; створена база знань, яка включає опис основних властивостей поведінки користувачів, які ведуть нелегальну діяльність в мережі у вигляді продукційних правил; розроблені та програмно реалізовані алгоритми зберігання та обробки таких правил; працездатність експертної системи перевірена на прикладі ідентифікації конкретного користувача.

КЛАСИФІКАЦІЯ КІБЕРЗАГРОЗ, АНОНІМІЗАЦІЯ КОРИСТУВАЧІВ, ІДЕНТИФІКАЦІЯ КОРИСТУВАЧІВ, ВІРТУАЛЬНІ ВАЛЮТИ, НЕЛЕГАЛЬНА ДІЯЛЬНІСТЬ, ЕКСПЕРТНА СИСТЕМА, МОДЕЛЬ ЗНАНЬ, БАЗА ЗНАНЬ

ЗМІСТ

ВСТУП

З розвитком мережевих технологій користувачі отримали можливість зручно приховуватись і залишатися анонімними в мережі. Хоча користування Інтернетом без відстеження наших дій з боку корпорацій та провайдера є, по суті, гарною ідеєю, деякі користувачі почали використовувати надані можливості для отримання прибутку та просування заборонених товарів, речовин, програм, послуг тощо. Інша група користувачів незгорнула свої сервіси з надання постуг з обміну з моменту блокування доступу до деяких гаманців та ресурсів або немає відповідної ліцензії.

Робота присвячена пошуку та ідентифікації особи зловмисників в мережі Інтернет за допомогою рекомендацій, наданих розробленою експертною системою з використанням відкритих джерел інформації.

В роботі розглядається класифікація кіберзагроз, які поширюються, в тому числі, через мережу Інтернет, а також основні принципи та технології анонімізації користувачів з фактичними наслідками.

В роботі експертної системи розглядаються нелегальні обмінні пункти в мережі, а також продаж нелегального програмного забезпечення (ПЗ) та іншого контенту. В обох випадках діяльність заборонена Законом України, так як у випадку з обмінними пунктами існує факт маємо нелегальної діяльності з обміну валют через електронні гаманці, заборонені на території України, та без ліцензії Нацбанку з метою отримання прибутку; у випадку з ПЗ порушення можуть бути обумовлені нелегальним його використанням, якщо, наприклад, ПЗ розроблено з метою зламу легального ПЗ, з метою отримання доступу до конфіденційної, комерційної таємниці або ухилення від оплати за користування тощо. Також, якщо мова йде про так зване «піратське» ПЗ (яке також може поширюватися на платній основі), то його використання нетільки є незаконним, але й несе загрозу даним, які містяться не тільки безпосередньо на машині, на яку виконана інсталяція, але й, можливо, в усій мережі.

РОЗДІЛ 1. ОСОБЛИВОСТІ КІБЕРЗАГРОЗ ДЛЯ КОРИСТУВАЧІВ В МЕРЕЖІ ІНТЕРНЕТ

1.1 Аналіз кіберзагроз для користувачів мережі Інтернет

З розвитком комп'ютерної техніки з'явилась необхідність з'єднання машин між собою у мережі. З плином часу увесь світ поглинула глобальна мережа Інтернет. Очевидно, шахраї нестали нехтувати цими можливостями і перейшли у кіберпростір. За виключенням критичних помилок у програмному забезпеченні кіберзагрози створюються людьми навмисно задля завдання шкоди іншим особам або організаціям з метою викрадення даних, отримання прибутку або створення загроз на державному та світовому рівні. Витяг із Закону України (№ № 2163-VIII від 05.10.2017 р.):

Кіберзагроза – наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об'єктів.

На даний час існує багато видів кіберзагроз. Сьогодні своєчасна та об'єктивна інформація є важливим фактором виробництва, який розглядають, як один з основних ресурсів розвитку суспільства. Сучасні інформаційні системи та технології є засобом підвищення продуктивності та ефективності роботи працівників.

Проте глобальна комп'ютеризація у багатьох сферах управління та виробництва супроводжується появою принципово нових загроз інтересам особистості, підприємства, суспільства, держави [1].

Паралельно з розвитком і ускладненням засобів, методів, форм автоматизації процесів обробки інформації підвищується залежність суб'єктів підприємництва від ступеню безпеки інформаційних технологій, що використовуються ними [2].

Можна виділити цілу низку джерел загроз інформаційній безпеці сучасного підприємства:

- протизаконна діяльність деяких економічних структур у сфері формування, поширення і використання інформації;
- порушення встановлених регламентів збору, обробки та передачі інформації;
- навмисні дії та ненавмисні помилки персоналу інформаційних систем;
- помилки в проектуванні інформаційних систем;
- відмова технічних засобів і збої програмного забезпечення в інформаційних і телекомунікаційних системах тощо [3].

На сьогоднішній день фахівцями досліджується досить широкий перелік загроз безпеці інформаційних систем, які класифікують за рядом ознак.

Захист інформації – галузь науки і техніки, яка динамічно розвивається, пропонує ринку широкий спектр засобів для захисту даних. Проте жоден з них окремо взятий неможе гарантувати адекватну безпеку інформаційної системи. Необхідною умовою ефективного захисту є проведення комплексу взаємодоповнюючих заходів.

Комплексне забезпечення інформаційної безпеки автоматизованих систем – це сукупність криптографічних, програмно-апаратних, технічних, правових, організаційних методів і засобів забезпечення захисту інформації при її обробці, зберіганні та передачі з використанням сучасних комп'ютерних технологій.

З липня 2003 р. в Україні введена кримінальна відповідальність за незаконне втручання у роботу комп'ютерів і комп'ютерних мереж, а також за поширення комп'ютерних вірусів, що призвело до спотворення, зникнення, блокування інформації чи її носіїв [4].

Досвід показує, що практично кожне підприємство має антивірусні засоби захисту, системи ідентифікації користувачів, системи управління доступом до інформаційної системи тощо. Тобто потенціал засобів захисту є,

але він нереалізується фірмами повністю. Більше того, володіючи складними апаратними засобами захисту інформації, більшість підприємств навіть наполовину невикористовують їх потенціал. Переважна більшість вимог стандартів інформаційної безпеки можуть бути реалізовані наявними у фірм засобами захисту.

Сучасне підприємство повинно вміти належним чином будувати політику інформаційної безпеки, тобто розробляти і ефективно впроваджувати комплекс превентивних заходів по захисту конфіденційних даних та інформаційних процесів. Така політика передбачає відповідні вимоги на адресу персоналу, менеджерів і технічних служб.

Головними етапами побудови політики інформаційної безпеки є:

1. реєстрація всіх ресурсів, які мають бути захищені;
2. аналіз та створення переліку можливих загроз для кожного ресурсу;
3. оцінка ймовірності появи кожної загрози;
4. вжиття заходів, які дозволяють економічно ефективно захистити інформаційну систему [5].

Більшість фахівців у галузі захисту інформації вважають, що інформаційна безпека підтримується на належному рівні, якщо для всіх інформаційних ресурсів системи підтримується відповідний рівень конфіденційності (неможливості несанкціонованого отримання будь-якої інформації), цілісності (неможливості навмисної або випадкової її модифікації) і доступності (можливості оперативно отримати запитувану інформацію).

Можна виділити такі підсистеми ефективного захисту інформації на підприємстві:

1. Підсистема антивірусного захисту шлюзів входу в мережу Інтернет, файлових серверів, робочих місць користувачів, централізованого управління, періодичного оновлення антивірусних баз даних.

2. Підсистема управління контролем доступу та ідентифікацією в інформаційній системі.

3. Підсистема міжмережного екранування, яка дозволяє реалізувати безпеку міжмережної взаємодії через використання програмних і програмно-апаратних міжмережних екранів.

4. Підсистема криптографічного захисту, яка гарантує безпеку передачі інформації завдяки шифруванню даних.

5. Підсистема забезпечення цілісності інформації та програмного середовища шляхом застосування відповідних засобів для фіксації та контролю стану програмного комплексу, управління зберіганням даних для резервного копіювання та архівування.

6. Підсистема захисту від інсайдерів, яка контролює дії порушників, реалізує інформаційну безпеку при управлінні доступом і реєстрації.

7. Підсистема захисту систем управління базами даних.

8. Підсистема виявлення вторгнень і спроб несанкціонованого доступу до інформаційних ресурсів підприємства. Підсистема забезпечує реалізацію захисних заходів з протидії атакам хакерів і поширенню спаму.

9. Підсистема захисту мобільних пристроїв.

10. Підсистема моніторингу подій інформаційної безпеки, яка дозволяє своєчасно виявляти загрози інформаційній системі та оперативно реагувати на них [6].

Сьогодні спеціалізовані фірми пропонують широкий спектр засобів захисту інформаційних систем з урахуванням їх вартості та функціональних можливостей. Найбільш прийнятним підходом при виборі того чи іншого варіанту є дотримання принципу «розумної достатності», суть якого полягає в тому, що визначальними при проектуванні політики інформаційної безпеки повинні бути: розмір підприємства, його ресурсні та фінансові можливості, поточний рівень інформаційної безпеки, стадія функціонування фірми.

Постійна робота в сфері підтримки інформаційної безпеки на належному рівні є необхідною умовою ефективності підприємницької діяльності [7].

Водночас безпека інформаційної системи має розглядатися як важлива складова загальної безпеки підприємства. Причому необхідна розробка концепції інформаційної безпеки, в якій слід передбачити не тільки заходи, пов'язані з інформаційними технологіями (криптозахист, програмні засоби адміністрування прав користувачів, їх ідентифікації та автентифікації, брандмауери для захисту входів-виходів мережі тощо), але і відповідні заходи адміністративного та технічного характеру.

Метою захисту інформації має бути збереження цінності інформаційних ресурсів для їх власника. Виходячи з цього, безпосередні заходи захисту спрямовують нетак на самі інформаційні ресурси, як на збереження певних технологій їх створення, обробки, зберігання, пошуку та надання користувачам. Ці технології мають враховувати особливості інформації, які роблять її цінною, а також давати змогу користувачам різних категорій ефективно працювати з інформаційними ресурсами. Кіберзагрози класифікуються за наступними критеріями:

За ступенем навмисності прояву:

- навмисні дії;
- випадкові дії;

За природою виникнення:

- природні;
- штучні;

За безпосереднім джерелом:

- природне середовище;
- людина;
- санкціоновані програмні засоби;
- несанкціоновані програмні засоби;

За ступенем залежності від активності інформаційних систем (ІС):

- проявляються незалежно від активності ІС;
- проявляються тільки в процесі активності ІС;

За ступенем впливу на ІС:

- активні;
- пасивні;

За місцем розташування інформації:

- на зовнішньому запам’ятовуючому пристрої;
- в оперативній пам’яті;
- в лініях зв’язку;
- на терміналі або друкованому принтері;

За розташуванням загроз:

- джерело - поза контрольованою зоною;
- джерело - в межах контрольованої зони;
- джерело має доступ до периферійних пристроїв;
- джерело - в інформаційній системі.

90% кібератак та вірусів націлені на отримання прибутку. Такі атаки не націлюються на якихось конкретних користувачів. Зловмисники намагаються заразити якомога більше користувачів. Дуже популярним прикладом є рекламні додатки, які встановлюються разом із легальним ПЗ. Таким чином, зараженому користувачеві буде демонструватись додаткова реклама на вебсторінках або навіть на робочому столі. Автор додатку буде отримувати від рекламодавця грошову винагороду. А якщо жертв декілька, то і винагорода помножується на їх кількість. Також цей відсоток атак включає створення так званих ботнетів. Ботнет — це комп'ютерна мережа, що складається з деякої кількості хостів, із запущеними ботами — автономним програмним забезпеченням. Найчастіше бот у складі ботнета є програмою, яка приховано встановлюється на комп'ютері жертви і дозволяє зловмисникові виконувати певні дії з використанням ресурсів інфікованого комп'ютера. Зазвичай використовуються для протиправної діяльності — розсилки спаму, перебору паролів на віддаленій системі, атак на відмову в обслуговуванні, отримання персональної інформації про користувачів, крадіжка номерів кредитних карток та паролів доступу. Кожен комп’ютер в мережі діє як «бот» і управляється шахраєм для передачі шкідливих програм або шкідливого контенту для за-

пуску атаки. Ботнет деколи називають «армією зомбі», так як комп'ютери контролюються кимось іншим, крім їх власника.

Приблизно 10% від атак являють собою таргетовані атаки, які направлені на компрометацію пристроїв конкретних користувачів або організацій. На них витрачається найбільша кількість часу, а кількість заражень дуже мала. Наприклад, ви директор крупної компанії, перебуваєте в отелі в іншому місті. Для доступу до місцевої мережі WiFi вам необхідно ввести номер кімнати та своє ім'я. Потім на пристрої з'являється повідомлення, ніби то необхідно оновити Flash. Разом з оновленням завантажується Backdoor (алгоритм, який дає можливість віддалено керувати пристроєм жертви). Теперь вся інформація з пристрою доступна нетільки його власнику. Але руйнівна дія вірусу може проявитися лише коли користувач під'єднається до корпоративної мережі своєї організації вже після повернення додому. Таким чином зловмисник може отримати доступ до секретної інформації, правильне використання якої може принести величезні збитки.

Лише 0,1% це кіберзброя. Шкідливі програми які перетворилися на смертоносну і небезпечну зброю. Сьогодні ця загроза проявляється як на персональному, так і на глобальному рівні. Об'єктами атак і цільових заражень є промислові підприємства, політичні інститути і навіть силові структури. У 2010 році було виявлено шкідливе програмне забезпечення Stuxnet, яке продемонструвало реальність загроз, які до того вважали лише уявними. Програма була призначена для атаки на промислове обладнання ядерного об'єкта в Ірані. Програма була здатна атакувати локальну мережу цього об'єкта, яка небула підключена до Інтернету. Вірус потрапив до 5 компаній, які поставляли обладнання для цільового об'єкта і очікував, пока хтось із співробітників непідключить заражений запам'ятовуючий пристрій до машини на об'єкті. Це шкідливе ПО перевіряло операційну систему пристроїв, на які потрапляло для визначення, як далекознаходиться від цілі. Програма була розроблена великою і добре скоординованою групою розробників. Пізніше виявили зразки програмного забезпечення, яке мало розвідувальні фун-

кції, і було розроблене такими ж великими і професійними групами. Приклади таких програмних засобів – DuQu, Flamer, Red October.

Як з'ясувалось, деякі з масштабних розвідувальних операцій у кіберпросторі проводились протягом майже десяти років.

Повернемось до загроз, які можуть завдати шкоди звичайним користувачам з метою отримання прибутку. Ось ще приклади деяких з них.

1. Фішинг – вид шахрайства, метою якого є отримання конфіденційної інформації довірливих чи неуважних користувачів (паролів, логінів, даних кредитних карток тощо). Згідно із дослідженням Wombat 2017 State of the Fish, 44% організацій стали жертвами фішингу через SMS-повідомлення (smishing) і телефонні дзвінки (vishing). Хакери також можуть відправляти шахрайські листи електронною поштою від імені співробітників чи з акаунтів, котрим довіряють.

61% компаній відчули на собі наслідки так званого цілеспрямованого фішингу. У таких випадках збирається інформація про важливих осіб серед співробітників компанії з метою створення більш персоналізованих, індивідуальних, а отже, і більш переконливих повідомлень, щоб спонукати жертв добровільно надати конфіденційну інформацію.

2. Малвертайзинг (або шкідлива реклама) є способом поширення шкідливих програм через онлайн-рекламу. Сучасні методи дозволяють обійти блокування реклами без дозволу користувача, щоб запустити код вірусу. RiskIQ 2016 Malvertising Report показав, що випадки малвертайзингу зросли на 132,6% в 2016 у порівнянні з 2015 роком.

3. Програми-вимагачі здатні заблокувати доступ жертви до своїх даних. Зловмисники їх використовують для вимагання викупу, погрожуючи оприлюднити отриману секретну інформацію або її знищити. Доповідь, підготовлена SonicWall у 2017 на основі їхніх щорічних досліджень показала, що кількість випадків шкідливому ПЗ із метою отримання викупу останнім часом різко зросла від 3,2 млн. у 2014 та 3,8 млн. у 2015 до 638 млн. у 2016 році. «Locky» — один з видів вищезгаданого шкідливого програмного забез-

печення. Це програма-шифрувальник, яка виглядає, як Word-документ, який просить користувача активувати макроси. Locky шифрує всі файли жертви, включаючи зображення, відеозаписи і т. п.

4. Кардинґ – рід шахрайства, при якому проводиться операція з використанням платіжних карток або їх реквізитів, яка неініційована або непідтверджена її власником.

Реквізити платіжних карток, як правило, беруть зі зламаних серверів інтернет-магазинів, платіжних і розрахункових систем, а також з персональних комп'ютерів (або безпосередньо, або через програми віддаленого доступу, так звані «трояни» або «черв'яки»).

Крім того, найпоширенішим методом крадіжки номерів платіжних карток на сьогодні є фішинг — створення шахраями сайту, який буде користуватися довірою у користувача, наприклад — сайт, схожий на сайт банку користувача, через який і крадуться реквізити платіжних карток.

Одним з наймасштабніших злочинів в області кардингу вважається зламування глобального процесингу кредитних карток Worldpay та крадіжка за допомогою його даних більше ніж 9 мільйонів доларів США. У листопаді 2009 р. у цій справі були пред'явлені звинувачення злочинній групі, що складається з громадян СНД.

Окремим випадком кардинґу є **скімінґ**, при якому використовується скимер — інструмент зловмисника для зчитування, наприклад, магнітної доріжки платіжної картки. Такі пристрої зазвичай встановлюють на банкомати, тому важливо оглядати їх перед початком користування.

5. Соціальна інженерія – окремий вид загроз, який може бути навіть непов’язаним із створенням шкідливого коду або пристроїв. Так чи інакше цей метод може використовуватися вкупі з вищенаведеними видами загроз (наприклад для привернення уваги жертви). За таким методом можуть працювати шахраї, переконуючи жертв надати персональні дані, які можуть бути використані для підтвердження особи в банку тощо, або напряму надіслати грошові кошти. Також до цього пункту можна віднести нелегальну торгі-

влю, відмивання грошових коштів шляхом продажу легальних товарів по аномально низьким цінам, ненадання сплачених послуг.

Як можна побачити, кожна з загроз є способом кражі грошових коштів, шантажу або прибуткового використання персональних даних.

1.2 Анонімізація користувачів мережі Інтернет та її наслідки

Для анонімізації користувачів використовуються так звані анонімні мережі. Це комп'ютерні мережі, створені для досягнення анонімності в Інтернеті і працюють поверх глобальної мережі. Специфіка таких мереж полягає в тому, що розробники змушені йти на компроміс між ступенем захисту та легкістю використання системи, її «прозорістю» для кінцевого користувача. Також важливий аспект збереження анонімності та конфіденційності за умови впливу методів соціальної інженерії або будь-якого тиску на оператора сервера. Багаторівневе шифрування і розподілений характер анонімних мереж, усуваючи єдину точку відмови і єдиний вектор атак, дозволяють зробити перехоплення трафіку або навіть злом частини вузлів мережі нефатальною подією. За анонімність користувач розплачується збільшенням часу відгуку, зниженням швидкості, а також великими обсягами мережевого трафіку. Першою відносно успішною анонімною мережею був комерційний сервіс Freedom, який функціонував з 1998 до 2001 року. Компанією ZKS були встановлені виділені сервери, з якими клієнти з'єднувалися за допомогою криптографічного протоколу. Вузол, на який приходили пакети від користувача Freedom, неміг ідентифікувати цього відправника. Сама мережа функціонувала на рівні протоколу IP. У цей же час почали активно розвиватися інші проекти.

Найбільш відомою і розвиненою серед анонімних мереж є мережа The Onion Router (TOR).

Tor (скор. від англ. ***The Onion Router***) — це система, створена для забезпечення анонімності в мережі Інтернет. Клієнтське програмне забезпе-

чення Tor маршрутизує Інтернет-трафік через всесвітню мережу добровільно встановлених серверів з метою приховування розташування користувача. Окрім того, використання Tor робить складнішим відслідковування Інтернет-активності як на рівні веб-сайту, так і на рівні Інтернет-провайдера, включаючи «відвідування веб-сайтів, залишені повідомлення та коментарі на відповідних ресурсах, миттєві повідомлення та інші форми зв'язку», до користувача і призначений для захисту приватності користувача та можливості проведення конфіденційних операцій, приховуючи користувацьку активність в мережі від стороннього моніторингу.

«Цибулева маршрутизація» (англ. *Onion Routing*) показує шаровий принцип передачі даних цього сервісу: від відправника дані шифруються та розшифровуються декілька разів, потім передаються далі через ішні маршрутизатори Tor, кожен з яких розшифровує «шар» шифру перед передачею даних наступному вузлу і, за таким принципом, трафік доходить до отримувача. Це майже унеможливлює можливість розшифрування початкових даних під час передачі. Інакше кажучи, принцип заснований на створенні криптографічного маршруту через кілька маршрутизаторів між двома комп’ютерами [8].

Клієнтське програмне забезпечення Tor — вільне ПЗ і використання мережі Tor безкоштовне. Додатковою опцією є обхід блокувань.

Для з’єднання з мережею використовується TOR браузер.

Переваги використання:

– захист від стеження, яке може становити загрозу конфіденційності;

– відсутність вбудованих систем стеження за користувачем;

– простота системи, навіть недосвідчений користувач легко впорається з програмою;

– технологія немає вигоди з даних користувача;

– браузер рекомендується багатьма експертами безпеки;

– динамічність програми - запускати її можна з будь-якого типу носія, включаючи портативний;

– браузер блокує всі функції мережі, які можуть загрожувати безпеці; опціонально налаштовуються такі, на перший погляд, малозначущі параметри, як заборона відкривати вікно на повний екран для попередження отримання сайтами інформації про справжню роздільну здатність монітору користувача.

Використання TOR непозбавлене недоліків. При цьому, користувач є обмеженим у можливостях використання всіх функцій деяких з ресурсів. Також стилізація і функціонал сайтів нагадує початок нульових років, а релевантність пошуку часто залишає бажати кращого.

Нелегальна діяльність в анонімних мережах

Мережа TOR використовується також для нелегальної діяльності по продажу заборонених речовин, зброї, людей, товарів, придбаних на кошти, здобуті шляхом кардингу. Одним з найменш серйозних правопорушень в мережі є піратське ПЗ та інший контент. В наш час все більше торрент-трекерів закриваються через звернення до правоохоронних органів власників авторських прав, тож багато ресурсів з піратським змістом переїжджають на простір TOR. Тут можна знайти все від музики до підручників.

Також нерідко можна зустріти продаж техніки та інших товарів за привабливими цінами. В такий спосіб кардери мають можливість відмивати грошові кошти. Існують також так звані “дропи” - особи, які приймають на себе партії цілком легальних товарів, придбаних за крадені кошти або отримують банківські зарахування, беруть відсоток і відправляють гроші далі, або отримують готівкові і передають іншим особам в угрупуванні різноманітними способами. Потрібно бути обережним, адже іноді можна навіть непідозрювати цього, але стати співучасником злочину, просто допомагаючи комусь в роботі з банкоматом.

Віртуальні валюти

У зв'язку з тим, що децентралізовані, засновані на математичних принципах, віртуальні валюти, зокрема, біткоін, привертають підвищену увагу, сформувалися дві поширені точки зору: по-перше, віртуальні валюти є трам-

пліном для майбутнього розвитку платіжних систем; і, по-друге, віртуальні валюти в руках злочинних осіб, які займаються фінансуванням тероризму, та інших злочинних елементів, які намагаються обійти санкції, стають новим потужним інструментом для переміщення та зберігання грошових коштів таким чином, що вони опиняються поза досяжності правоохоронних та інших компетентних органів [9].

Віртуальна валюта являє собою засіб вираження вартості. Віртуальною валютою можна торгувати в цифровій формі, вона функціонує в якості засобу обміну обміну або розрахункової грошової одиниці або засобом зберігання вартості, але неволодіє статусом законного платіжного засобу (тобто неє офіційно чинним і законним засобом платежу при розрахунках з кредиторами) в жодній юрисдикції. Віртуальна валюта неемітується і незабезпечується жодної юрисдикцією (офіційно не може бути виконаний обмін на державну валюту) і виконує вищевказані функції тільки за згодою в рамках спільноти користувачів віртуальної валюти. Віртуальна валюта відрізняється від фіатної валюти («реальні гроші» або «Національна валюта»), що представляє собою монети і паперові гроші країни, які є її законним засобом платежу, який повсюдно використовується і приймається як засіб обміну в країні-емітенті [10].

Віртуальна валюта також відрізняється від електронних грошей, які є цифровим засобом вираження фіатної валюти і використовуються для електронного переказу вартості (вираженій) в фіатній валюті.

Електронні гроші є механізмом цифрового переказу фіатної валюти, тобто вони використовуються для електронного переказу валюти і мають статус законного платіжного засобу.

Цифрова валюта може виступати як засіб цифрового виразу або віртуальної валюти (нефіатной валюти), або електронних грошей (фіатной валюти), і тому часто вживається як синонім «віртуальної валюти» [11].

Децентралізовані віртуальні валюти (криптовалюти) являють собою розподілені (в широкому сенсі дані зберігаються одночасно в усіх учас-

ників системи), основані на математичних принципах пірінгові віртуальні валюти з відкритим вихідним кодом, у яких відсутній централізований контроль або нагляд. Прикладами є: Bitcoin, LiteCoin, Ripple і т.д. Такі валюти використовують для свого захисту криптографічні методи для забезпечення фактору децентралізації та неможливості відстежування, такі як блокчейн [12]. Блокчейн – безперервний послідовний ланцюжок блоків, які містять інформацію. Їх взаємозв'язок забезпечується нетільки нумерацією, але й тим, що кожен блок містить власну хеш суму і суму попереднього блока. Для зміни інформації в блоці доведеться редагувати і всі наступні блоки. Найчастіше копії ланцюжків блоків зберігаються на безлічі різних комп'ютерів незалежно один від одного. Це робить вкрай скрутним внесення змін до інформації, вже включену в блоки.

Вартість одиниці такої валюти залежить від її популярності, обговорюваності серед суспільства та зазвичай непідкріплюється матеріально, тобто визначається за згодою сторін. У криптовалютах використовуються відкриті і закриті ключі для переказу валюти від однієї (фізичної чи юридичної) особи іншій, і для переказу криптовалюти кожен раз потрібен криптографічний підпис. Безпека, цілісність і актуальність реєстрів операцій з криптовалютами забезпечується мережею пов'язаних одна з однією осіб (у випадку біткоіна званих майнерів), які захищають мережу в обмін на можливість отримання довільно розподілених комісійних зборів. (У випадку біткоіна – невелика кількість нових створених біткоінів, званих «винагородою за блок» (block reward), а в деяких випадках також комісійні за операції, які виплачуються користувачами в якості матеріального стимулу майнерам для включення їх операцій в наступний блок). Були виявлені сотні варіацій криптовалют, більшість з яких пов'язані з біткоін, в яких використовується принцип «proof-of-work» («докази виконання роботи» - система, заснована на тому, що будь-яка операція вимагає певної кількості обчислень) для перевірки і підтвердження правильності операцій і ведення ланцюжка блоків. Хоча біткоіни є першим працюючим криптографічним протоколом для криптовалют,

росте інтерес до розробки альтернативних, більш ефективних методів перевірки і підтвердження правильності операцій, таких, як системи «proof-of-stake» («доказ володіння» - система, в якої нові монети генеруються неза рахунок використання обчислювальних ресурсів, а за рахунок тривалості зберігання старіших монет»).

Біткоін (Bitcoin) був запущений в 2009 році і став першою децентралізованою конвертованою валютою і першою криптовалютою. Біткоіни представляють собою розрахункові одиниці в формі унікальною ланцюжка цифрових і буквених знаків, мають цінність тільки внаслідок того, що користувачі готові платити за них. Торгівля біткоінами здійснюється користувачами в цифровій формі з високим рівнем анонімності, і біткоіни можуть обмінюватися (купуватися або продаватися) на долари США, євро та інші фіатні або віртуальні валюти. Будь-хто може завантажити безкоштовне відкрите програмне забезпечення з веб-сайту для відправки, отримання та зберігання біткоінів, а також для контролю операцій в системі. Користувачі також можуть отримати біткоін-адреси, які функціонують як рахунки на сайтах провайдерів послуг з обміну або на сайтах служб онлайнових гаманців. Інформація про операції (грошові потоки) є загальнодоступною і розміщується в загальному реєстрі операцій, де самі операції ідентифікуються за біткоін-адресою, який представляє собою ланцюжок цифрових і буквених знаків без систематичної прив'язки до фізичній особі. У зв'язку з цим систему біткоіни називають «псевдонімною». Отже, якщо всі дані про грошові потоки з валютою наявні у відкритому доступі, можемо переглянути, яка кількість валюти була перерахована на той чи інший гаманець. Наприклад, стало відомо, що творці віруса Petya (2017) приблизно через 7 годин після початку атаки отримали на свій Біткоін гаманець приблизно $8000 (вірус-вимагач потребував приблизно $300 з кожної зараженої машини), що є невеликим показником з огляду на масштаби розповсюдження віруса. Максимальне число біткоінів, яке буде згенеровано, становить 21 мільйон (проте кожна одиниця може бути розділена на більш дрібні частини), і цей рівень буде досягнутий до 2140 року.

Станом на 2 квітня 2014 року був емітовано понад 12 з половиною мільйонів біткоінів, загальна вартість яких трохи перевищувала 5,5 мільярдів доларів США, виходячи з середнього обмінного курсу на цю дату [13].

Альткоін (Altcoin) означає засновану на математичних принципах децентралізовану конвертовану віртуальну валюту, відмінну від Біткоін. На даний момент відомо більш ніж 1100 видів таких валют [14].

Анонімайзер (Anonymiser) означає інструменти і сервіси, такі, як «Темні мережі» (darknets) і «міксери» (mixers), призначені для приховування джерела біткоін-операцій і сприяння забезпеченню анонімності. Прикладами є: мережа Tor (анонімна мережа), Dark Wallet (сервіс анонімної мережі), Bitcoin Laundry («міксер») [15].

«Міксер» (Mixer) (сервіс по відмиванню, «змішувач») є одним з видів Анонімайзера, який забезпечує приховування ланцюжка операцій в ланцюжку блоків шляхом прив'язування всіх операцій до однієї і тієї ж біткоін-адреси, і, посилаючи їх усі разом таким чином, що створюється враження, що вони спрямовані з іншої адреси. Суть полягає в тому, щоб об'єднати кошти одного користувача з біткойнами інших людей, тим самим опускаючи шлях назад до вихідного джерела коштів. У традиційних фінансових системах це еквівалентно передачі коштів через ряд банківських рахунків [16]. Сервіси «міксерів» працюють, отримуючи розпорядження від користувача на відправку грошових коштів на конкретну біткоін-адресу. Після цього «міксер» «змішує» цю операцію з операціями інших користувачів таким чином, що стає неясно, кому користувач має намір направити кошти. Прикладами сервісів «міксерів» є: Bitmixer.io; SharedCoin; Blockchain.info; Bitcoin Laundery; Bitlaunder; Easycoin. Існують додатки, які автоматично забезпечують анонімність за допомогою «міксерів» та є компонентами браузерів. Таке програмне забезпечення може також розроблятися в незаконних цілях, наприклад, розробник / оператор «Міксера» може працювати в інтересах незаконних користувачів, використовувати продукти, спеціально розроблені для ухилення від перевірки регулюючими і правоохоронними органами.

1.2.1. Учасники системи віртуальної валюти (централізованої і децентралізованої)

Провайдер послуг з обміну або обмінний пункт (Exchanger) (також іноді званий біржею віртуальних валют) – фізична або юридична особа, що займається за комісійну винагороду комерційною діяльністю з обміну віртуальної валюти на реальну валюту, безготівкові грошові кошти або на іншу віртуальну валюту, а також на дорогоцінні метали, і навпаки. В цілому, провайдери послуг з обміну приймають різні види платежів, включаючи платежі готівкою, електронні перекази, кредитні карти та інші віртуальні валюти. Провайдери послуг з обміну можуть виступати в якості біржі або в якості обмінного пункту. Фізичні особи зазвичай використовують послуги провайдерів для депонування (зберігання) і зняття грошей з рахунків в віртуальній валюті.

Адміністратор (Administrator) – фізична або юридична особа, що займається комерційною діяльністю по емісії (введення в обіг) централізованої віртуальної валюти, визначення та запровадження правил її використання, ведення централізованого реєстру платежів і має правовикуповувати (виводити з обігу) віртуальну валюту.

Користувач (User) – фізична або юридична особа, яка може придбати віртуальну валюту і використати її для покупки реальних або віртуальних товарів / послуг або відправляє переклади в приватному порядку іншій особі (для особистого використання), або яка тримає віртуальну валюту в якості (особистих) інвестицій. Користувачі можуть отримувати віртуальну валюту декількома шляхами. Наприклад, вони можуть: 1) придбати віртуальну валюту за реальні гроші (у провайдера послуг з обміну, або в обмін на певну централізовану віртуальну валюту безпосередньо у адміністратора / емітента); 2) брати участь у певній діяльності, оплата за яку здійснюється у віртуальній валюті (наприклад, беручи участь в промо-акціях, опитуваннях / анкетуванні, надаючи реальні або віртуальні товари або послуги); 3) в разі деяких

децентралізованих віртуальних валют (наприклад, біткоін) самостійно генерувати одиниці валюти шляхом майнінгу і отримувати її в подарунок, винагороду або в рамках безкоштовного розподілу.

Майнер (Miner) – фізична або юридична особа, яка бере участь в функціонуванні мережі децентралізованої віртуальної валюти за допомогою використання спеціального програмного забезпечення для вирішення складних алгоритмів в розподіленій системі «proof-of-work» («докази виконання роботи») або інший розподіленій підтверджуючій системі, що використовується для перевірки і підтвердження правильності операцій в системі віртуальної валюти. Майнери можуть бути користувачами, якщо вони самостійно генерують конвертовану віртуальну валюту виключно в своїх особистих цілях, наприклад, в якості інвестицій або для оплати за поточними зобов'язаннями, або для придбання товарів і послуг. Майнери також можуть брати участь в роботі системи віртуальної валюти в якості провайдерів послуг з обміну шляхом створення віртуальної валюти в рамках комерційної діяльності для її продажу в обмін на фіатну валюту або інші віртуальні валюти [17].

Гаманець віртуальної валюти (Virtual currency wallet) – засіб (програмний додаток або інший механізм / носій) для депонування, зберігання і переказу біткоінів або іншої віртуальної валюти. Зберігання валюти може бути «гарячим» (гаманець існує в онлайн режимі, тому більше схильний до зламу і хакерських атак) і «холодним» (зберігання без доступу в Інтернет у вигляді пристроїв та автономного програмного забезпечення).

Провайдер гаманця (Wallet provider) – це особа, яка надає гаманець віртуальних валют. Гаманець містить особисті (закриті) ключі користувача, що дозволяють йому витрачати віртуальну валюту, закріплену за адресою віртуальної валюти в ланцюжку блоків. Провайдер гаманця сприяє участі в системі віртуальної валюти, надаючи користувачам, провайдерам послуг з обміну і торговцям більш просту і зручну можливість для проведення операцій з віртуальною валютою. Провайдер гаманця веде баланс віртуальної валюти клієнта, а також в цілому забезпечує безпеку зберігання і операцій з

віртуальною валютою. Наприклад, крім надання біткоін-адреси, послуги гаманця можуть включати кодування, захист підписом з використанням декількох ключів, резервне / «холодне» зберігання і «міксери». Всі біткоіни-гаманці можуть бути пов'язані між собою. Гаманці можуть зберігатися як в режимі онлайн («Гаряче зберігання»), так і в режимі оффлайн («холодне зберігання»). Приклади: Coinbase, Multibit, Bitcoin Wallet.

Необхідно підкреслити, що наведений список учасників не є вичерпним. Більш того, з урахуванням стрімкого розвитку технологій віртуальної валюти і бізнес-моделей, в подібних системах можуть з'являтися додаткові учасники, які представляють потенційні ризики в області відмивання коштів [13].

Потенційні ризики при використанні віртуальних валют

Конвертовані віртуальні валюти, які можна обміняти на реальні гроші або інші віртуальні валюти, є потенційно вразливими з точки зору їх незаконного використання з метою відмивання грошей та фінансування тероризму. По-перше, вони можуть забезпечити більш високу ступінь анонімності в порівнянні з традиційними способами безготівкових платежів. Системи віртуальних валют, якими можна торгувати через Інтернет, в цілому характеризуються відсутністю прямої взаємодії з клієнтами і можуть дозволити здійснювати анонімне фінансування (фінансування готівкою або фінансування третіми особами через віртуальні обмінні пункти, в яких неідентифікується належним чином джерело фінансування). Також вони можуть забезпечити можливість здійснення анонімних переказів, якщо особи відправника і одержувача невстановлені належним чином.

Децентралізовані системи особливо вразливі з точки зору ризику анонімності. Наприклад, біткоіни-адреси, що функціонують в якості рахунків, за своєю суттю немістять імен чи іншої ідентифікаційної інформації про клієнтів, а в самій системі відсутній центральний сервер або провайдер послуг. Біткоін-протокол невимагає і незабезпечує встановлення і перевірку особистостей учасників або формування і ведення даних про операції за минулий

період, які неодмінно пов'язані з особистостями учасників в реальному світі. Крім того, відсутній центральний контролюючий орган, і в даний час немає програмного забезпечення для цілей протидії відмивання коштів, за допомогою якого можна було б відслідковувати і виявляти схеми підозрілих операцій. Правоохоронні органи не в змозі визначити одне центральне місце або особу (адміністратора) для проведення розслідувань або арешту активів (хоча відповідні органи можуть виявити окремих провайдерів послуг з обміну для отримання від них інформації про клієнтів, яку вони можуть збирати). Таким чином, все це забезпечує такий рівень потенційної анонімності, який просто неможливий у випадку кредитних і дебетових карт або старіших традиційних систем онлайнових платежів, таких як PayPal [13].

Широке поширення віртуальної валюти також підвищує потенційні ризики в області протидії відмивання коштів і фінансування тероризму. Системи віртуальних валют доступні через Інтернет (в тому числі, з мобільних пристроїв) і можуть використовуватися для здійснення транскордонних платежів і переказів грошових коштів. Крім того, віртуальні валюти, як правило, функціонують в рамках складної інфраструктури, що включає ряд осіб, котрі перебувають в декількох різних країнах, що забезпечують перекази грошових коштів і здійснення платежів. Така сегментація послуг ускладнює пошук злочинців. Більш того, дані і записи про операції і клієнтів можуть вестися і зберігатися у різних осіб, часто знаходяться в різних юрисдикціях, що додатково ускладнює їх доступність для правоохоронних і регулюючих органів. Ця проблема посилюється стрімко мінливим і розвиваючимся характером технологій і бізнес-моделей децентралізованих віртуальних валют, в тому числі зміною кількості і видів / функцій учасників, які надають послуги в рамках платіжних систем з використанням віртуальної валюти. Також важливо враховувати той факт, що різні елементи системи віртуальної валюти можуть перебувати в юрисдикціях, в яких відсутні належні заходи контролю в сфері протидії відмивання коштів / фінансування тероризму (ПВД / ФТ). Учасники систем централізованих віртуальних валют можуть бути замішані

у відмиванні грошей і навмисно вишукувати юрисдикції зі слабким режимом ПВД / ФТ. Децентралізовані конвертовані віртуальні валюти, що дозволяють здійснювати анонімні операції між особами, можуть існувати в цифровому просторі, який є повністю недоступним для будь-якої окремої держави.

1.2.2. Діяльність правоохоронних органів, пов'язана з віртуальною валютою

В поле зору правоохоронних органів потрапляють випадки протиправного використання віртуальної валюти з метою відмивання грошей. Нижче наведені деякі відомі приклади.

«Ліберті Резерв» (Liberty Reserve)

На сьогоднішній день це є найбільшим в історії випадком відмивання грошей в онлайн-режимі. У травні 2013 року Міністерство юстиції США пред'явило звинувачення компанії «Liberty Reserve» (представляла собою систему електронних переказів, яка базувалася в Коста-Ріці) і семи її керівникам і співробітникам. Вони були звинувачені в здійсненні незареєстрованої комерційної діяльності з надання послуг грошових переказів і відмиванні грошей шляхом сприяння переміщенню незаконних доходів на суму понад 6 мільярдів доларів США. В результаті вжитих скоординованих дій Міністерство фінансів США визначило «Liberty Reserve» як фінансову установу, що викликає найбільшу заклопотаність в плані відмивання грошей відповідно до Розділу 311 Закону США про боротьбу з тероризмом, і повністю позбавила її доступу до фінансової системи Сполучених Штатів Америки. Система «Liberty Reserve» була створена в 2006 році спеціально для того, щоб уникнути перевірок з боку регулюючих і правоохоронних органів і сприяти злочинцям в розподілі, зберіганні і відмиванні доходів одержаних злочинним шляхом, пов'язаної з шахрайством з кредитними картами, шахрайством у сфері інвестицій, комп'ютерним хакерством, незаконним обігом наркотиків і дитячою порнографією. Вона дозволяла злочинним елементам

здійснювати анонімні операції, які неможливо було відстежити. Ця система, що функціонувала в колосальних масштабах, налічувала мільйон користувачів у всьому світі, в тому числі більше 200 000 користувачів із США. В її рамках було проведено приблизно 55 мільйонів операцій, майже всі з яких були незаконними. В системі використовувалася власна віртуальна валюта «Liberty Dollars» («Ліберті Долари» або «ЛД»), але при цьому в початковій і кінцевій точці операцій грошові кошти конвертувалися і зберігалися в фіатной валюті (в доларах США). Після того, як стало відомо, що правоохоронні органи США проводять розслідування щодо «Liberty Reserve», ця компанія зробила вигляд, що повністю припинила свій бізнес в Коста-Ріці. Однак система продовжувала працювати через ряд фіктивних компаній, забезпечуючи переміщення мільйонів через їх рахунки в Австралії, Кіпрі, Китаї, Гонконгу, Марокко, Росії, Іспанії та інших країнах [13].

«Шовковий Шлях» (SILK ROAD)

У вересні 2013 року Міністерство юстиції США заявило про порушення кримінальної справи щодо, як передбачалося, власника і оператора «Шовкового шляху» - прихованого веб-сайту, через який його користувачі могли анонімно купувати і продавати наркотики, зброю, крадені персональні ідентифікаційні дані та інші незаконні товари і послуги, поза досяжності правоохоронних органів. Крім того, Міністерство юстиції заарештувало веб-сайт і приблизно 173 991 біткоіни, які перебували на арештованому комп'ютерному обладнанні, вартість яких на момент арешту становила понад 33,6 мільйонів доларів США. Зазначена особа була заарештована в жовтні в Сан-Франциско, і в лютому 2014 йому було пред'явлено офіційне звинувачення. В даний час розслідування триває. «Шовковий шлях» був запущений в січні 2011 року і функціонував як глобальний віртуальний чорний ринок. Через нього здійснювалися анонімні злочинні операції, він використовувався кількома тисячами наркоторговців і іншими незаконними продавцями для збуту заборонених товарів і послуг сотням тисяч покупців, третина з яких, як вважається, перебувала в США. Передбачається, що загальний прибуток від

продажів через цей сайт складав приблизно $1,2 млрд. За допомогою цих незаконних операцій були відмиті сотні мільйонів доларів. «Шовковий шлях» забезпечував анонімність за рахунок того, що функціонував в межаї анонімної мережі Tor, і як засіб оплати приймав тільки біткоіни. Використання біткоінів в якості єдиної валюти на сайті «Шовковий шлях »дозволяло продавцям і покупцям додатково приховувати свої особистості, оскільки ідентифікаційна інформація про відправників і одержувачів пірінгових (P2P) біткоін-операцій обмежувалася тільки анонімними біткоін-адресами / рахунками. Крім цього, користувачі могли отримати необмежену кількість біткоіни-адрес і використовувати різні рахунки при проведенні кожної операції, тим самим ще більше приховуючи «сліди» незаконних доходів. Користувачі також могли використовувати додаткові «анонімайзери», крім послуги «змішування» (mixer), вбудованої в операції, здійснювані через сайт «Шовковий шлях». Платіжна система на веб-сайті «Шовковий шлях» функціонувала в якості внутрішнього біткоін-банку, в якому кожен користувач повинен був мати рахунок для здійснення операцій на сайті. Кожен користувач «Шовкового шляху» мав неменше однієї біткоін-адреси, прив'язаної до рахунку користувача сайту. Для здійснення покупки користувач здобував біткоіни (як правило, через провайдера послуг по обміну біткоінів) і посилав їх на біткоін-адреси, прив'язані до його рахунку на сайті «Шовковий шлях» для поповнення рахунку. Після здійснення покупки біткоіни користувача переводилися в рамках системи «Шовковий шлях» на цільовий депозитний рахунок до повного завершення операції, після чого біткоіни користувача / покупця переводилися з цільового депозитного рахунку на біткоін-адресу продавця «Шовкового шляху». Крім цього, при здійсненні кожної покупки на сайті «Шовковий шлях» використовувався «змішувач», який, як пояснювалося на сайті, «направляє всі платежі за допомогою складної серії квазі-довільних фіктивних операцій практично виключаючи можливість прив’язки вашого платежу до будь-яких біткоінів, які були відправлені з сайту» [13].

«Вестерн Експресс Інтернешнл» (Western Express International)

Результатом восьмирічного розслідування діяльності кіберзлочинного угруповання, що діяло в Інтернеті, - «Western Express Cybercrime Group» - стали обвинувальні вироки або визнання провини 16 учасниками цього угруповання за участь в глобальній схемі розкрадання персональних даних / кібершахрайстві. Члени угруповання взаємодіяли і спілкувалися в основному через так звані сайти «Кардерів» в Інтернеті, на яких здійснювалася незаконна торгівля краденими кредитними картами і персональними ідентифікаційними даними, і використовували неправдиві ідентифікаційні дані, системи анонімних миттєвих повідомлень, анонімні системи електронної пошти і анонімні рахунки віртуальної валюти. Це робилося для приховання факту існування і цілей злочинного співтовариства, а також з тим, щоб уникнути уваги з боку правоохоронних і регулюючих органів та зберегти свою анонімність. Продавці угрупування реалізували майже 100 000 номерів крадених кредитних карт і інші персональні ідентифікаційні дані через Інтернет, приймаючи в якості платіжного засобу головним чином одиниці e-Gold і WebMoney. Покупці використовували викрадені ідентифікаційні дані для підробки кредитних карт і придбання дорогих товарів, які вони скуповували (в тому числі з використанням схем перевідправки), здійснюючи, таким чином, додаткові злочини, такі як розкрадання майна, незаконне володіння краденим майном і шахрайство. В результаті цієї шахрайської діяльності з кредитними картами були отримані злочинні доходи на суму близько 5 мільйонів доларів США. Провайдери кіберзлочинних послуг в мережі допомагали купувати, продавати і використовувати шахрайським чином номера крадених кредитних карт і інші персональні ідентифікаційні дані шляхом надання комп'ютерних послуг продавцям і покупцям. Через різні злочинцями було переведено понад 35 мільйонів доларів США. Центром всієї злочинної діяльності була «Western Express International Inc.», компанія, зареєстрована в Нью-Йорку з офісом в Манхеттені, яка функціонувала в якості провайдера послуг з обміну віртуальної валюти і незареєстрованого провайдера послуг

грошових переказів з метою координації та сприяння здійсненню онлайн-платежів, здійснюваних в рамках злочинної діяльності, і відмивання доходів угруповання. Будучи одним з найбільших провайдерів послуг з обміну віртуальної валюти в Сполучених Штатах Америки, компанія «Western Express International» обміняла в цілому 15 мільйонів одиниць Вебмані (WebMoney) і 20 мільйонів одиниць електронного золота (e-Gold (наразі сервіс нефункціонує)) для членів угрупування. Компанія також використовувала банки і провайдерів традиційних послуг грошових переказів для переміщення великих сум грошей. У лютому 2013 року в штаті Нью-Йорк компанія «Western Express International» і її власник / оператор, громадянин України, визнали себе винними в відмиванні грошей, шахрайстві і змові. Дві людини, яким було пред'явлено звинувачення, знаходяться в бігах до нашого часу [13].

Методи зберігання віртуальної валюти

Окрім наведених вище існують також загрози, що стосуються безпечного зберігання криптовалют. У випадку шахрайства є всі шанси залишитися безкарним: в разі несанкціонованого доступу до гаманця і крадіжки коштів можливість скасування транзакції і повернення коштів власнику відсутня. Це основна причина, чому питання зберігання криптовалюти не втрачає своєї актуальності. На сьогоднішній день існує багато способів зберігання криптовалюти: від традиційних гаманців при біржах до інноваційних розробок, які можна носити в кишені. Всі ці способи мають свої недоліки і переваги. Отже, зберігання можно поділити на «гаряче» та «холодне».

«Гаряче зберігання»

Оскільки криптобіржі залишаються найпоширенішим способом заробітку, обміну та конвертації криптовалют - ідея зберігання в цих же місцях здається цілком доцільною: немає необхідності робити зайві транзакції і витрачатися на комісійні збори. Біржові гаманці криптовалют, власне як і веб-гаманці, є програмним засобом зберігання віртуальних грошей. Їх основна робота – безперервний зв’язок з безліччю блокчейнів в майнінговому процесі, для забезпечення якого ці програми зберігають ключі. В такому ви-

падку, ресурс (біржа, обмінник і т.д.) - це посередник між користувачем і його грошима, який зберігає публічний (для зарахування) і приватний (для переказів) ключі. Якщо взяти для порівняння будь-апаратний біткоін гаманець, де користувач повністю контролює всі його функції і фінанси, біржа або веб-гаманець нічого крім доступу до операцій забезпечити неможуть. Постійно зберігати криптовалюти на біржових ресурсах або на веб-гаманцях потрібно з обережністю. Вибирати краще ті ресурси, які приділяють особливу увагу питанням безпеки.

«Холодне зберігання»

В цьому випадку приватний ключ зберігається в офлайновому режимі. Цей спосіб є лідером по частині безпеки, тому до нього вдаються навіть для зберігання великих сум. Холодний гаманець для зберігання біткоінів (і не тільки) передбачає використання публічної адреси для отримання коштів, вивід же здійснюється за допомогою приватного ключа. Коли з приватного сховища виводяться кошти - це означає що приватний ключ вже з'являється онлайн і з цього моменту переходить в розряд гарячого. Приклади: паперові купюри з надрукованими QR-кодами, в яких зашифровані публічний і приватний ключі; апаратний метод – використання пристроїв, які нагадують USB накопичувачі. Сам пристрій доступу до Інтернету немає, однак може бути підключений до ПК та іншої техніки з виходом до мережі. Якщо бути створений запит на транзакцію, пристрій підписує його без передачі приватного ключа. Також такі ключі можуть зберігатися фрагментовано на пристроях різних осіб, які можуть знаходяться в різних кутах світу, що ускладнює їх пошук та затримання.

Нелегальна діяльність без ліцензії

Процвітає також діяльність без ліцензії, робота із забороненими ресурсами. Це питання буде розглянуте детальніше на прикладі обмінних пунктів електронних валют. Наразі в мережі Інтернет існує безліч ресурсів, що пропонують послуги з обміну електронних грошей та криптовалют. Судячи з опису, власники ресурсів пропонують вельми широкий спектр гаманців та

банківських карток для виводу коштів та деколи навіть пропонують більш вигідний курс, ніж можна побачити в банках, що є підозрілим фактором. По-перше, діяльність має негативний вплив на економіку держави в цілому, так як такі обмінні пункти, як правило, неє легальними та неє платниками податків. По-друге, занадто вигідний курс може вказувати на відмивання коштів, до того ж при багатьох ітераціях обміну заплутується грошовий потік, отже, стає дуже важко визначити, звідки кошти поступили на рахунок обмінного пункту, куди вони були переведені далі та яким засобом виведені (переведені в готівку тощо). По-третє, більша частина таких пунктів має обмеження на мінімальну обмінну суму, отже, маємо високий ризик шахрайства та інколи навіть неможливість перевірити пункт на доброчесність через ці обмеження.

1.3 Постановка задачі

Аналіз діяльності нелегальних обмінних пунктів дозволяє констатувати, що власники ресурсів намагаються приховати свою особистість і також працюють із забороненими ресурсами (Webmoney, ЯндексДеньги тощо).

Для вирішення проблеми ідентифікації власників подібних ресурсів було вирішено розробити алгоритм дій, спираючись на інформацію з відкритих джерел, який повинен відповідати таким критеріям:

1. висока вірогідність ідентифікації;
2. пошук за допомогою соціальних мереж;
3. пошук за даними в платіжних системах (електронних гаманцях);
4. пошук номера телефону на сайтах обмінного пункту;
5. пошук за номером телефону імені власника через Telegram-бота;
6. пошук якомога більшої кількості номерів банківських карт на сайті;
7. встановлення імені власника картки за номером.

Метою даної роботи є розробка експертної системи ідентифікації користувачів, які ведуть нелегальну діяльність в мережі Інтернет.

РОЗДІЛ 2. ХАРАКТЕРИСТИКА ЕКСПЕРТНИХ СИСТЕМ ДЛЯ ЗАДАЧ КІБЕРБЕЗПЕКИ

2.1 Основні компоненти експертної системи

Створення і використання експертних систем є одним з концептуальних етапів розвитку інформаційних технологій. В основі інтелектуального вирішення проблем в деякій предметній області лежить принцип відтворення знань досвідчених фахівців-експертів.

Виходячи з власного досвіду, експерт аналізує ситуацію і розпізнає найбільш корисну інформацію, оптимізує прийняття рішень, відсікаючи тупикові шляхи [18].

Під експертною системою (ЕС) розуміється система, що об'єднує можливості комп'ютера зі знаннями і досвідом експерта в такій формі, що система може запропонувати розумну пораду або здійснити розумне рішення поставленого завдання. Додатково бажаною характеристикою такої системи, яка багатьма розглядається як основна, є здатність системи пояснювати, на вимогу, хід своїх міркувань у зрозумілій для користувача формі.

Експертна система (ЕС) – це сукупність методів і засобів організації, накопичення і застосування знань для вирішення складних завдань в деякій предметній області. Експертна система досягає більш високої ефективності за рахунок перебору великого числа альтернатив при виборі рішення, спираючись на високоякісний досвід групи фахівців, аналізує вплив великого обсягу нових факторів, оцінюючи їх при побудові стратегій, додаючи можливості прогнозу [19].

Основою експертної системи є сукупність знань (бази знань), структурованих в цілях формалізації процесу прийняття рішень.

ЕС покликані надавати допомогу фахівцям, коли їм невистачає для самостійного вирішення виникаючих проблем власних знань і досвіду.

Головна ідея використання експертних систем полягає в тому, щоб отримати від експерта його знання і, завантаживши їх у пам'ять комп'ютера,

використовувати кожного разу, коли в цьому виникне необхідність. Особливості експертних систем полягають в наступному:

- технологія ЕС найчастіше пропонує користувачеві прийняти рішення, що перевершує його можливості;

- ЕС використовують новий компонент інформаційної технології - знання.

Експертні системи розробляються з розрахунком на допомогу експертам і здатні надати логічні та впорядковані кроки для досягнення поставленої цілі. Дуже важливим є визначення області застосування експертної системи, меж її використання і дії.

Переваги експертних систем в порівнянні з використанням досвідчених фахівців полягають у наступному:

• досягнута компетентність невтрачається, може документуватися, передаватися, відтворюватися і нарощуватися;

• мають місцебільш стійкі результати, відсутні емоційні та інші чинники людської ненадійності;

• висока вартість розробки врівноважується низькою вартістю експлуатації, можливістю копіювання, а в сукупності вони дешевше висококваліфікованих фахівців.

Недоліком експертних систем, характерним для їх сучасного стану, є менша пристосованість до навчання новим правилам і концепціям, до творчості та винахідництва. Використання експертних систем дозволяє в багатьох випадках відмовитися від висококваліфікованих фахівців, але припускає залишити в системі місце експерту з більш низькою кваліфікацією. Існує необхідність залучення людини-експерта з проблемної області, що є носієм знань для заповнення бази знань; неможливість повного відмовлення від експерта-людини [20]. Експертні системи служать засобом для розширення і посилення професійних можливостей кінцевого користувача.

Експертна система повинна демонструвати компетентність, тобто досягати в конкретній предметній області того ж рівня, що і фахівці-експерти.

Недостатньо знаходити хороші рішення, це треба робити швидко. Системи повинні мати нетільки глибоке, а й досить широке розуміння предмета. Методи знаходження рішень проблем досягаються на основі міркувань, що виходять з фундаментальних принципів у випадку некоректних даних або неповних наборів правил. Такі властивості найменш розроблені в комп'ютерних експертних системах, але саме вони притаманні фахівцям високого рівня.

Відмінностями експертних систем від звичайних комп'ютерних є:

• експертні системи маніпулюють знаннями, тоді як будь-які інші системи - даними;

• експертні системи, як правило, дають ефективні оптимальні рішення і здатні іноді помилятися, але на відміну від традиційних комп'ютерних систем вони мають потенційну здатність вчитися на своїх помилках.

Розробка ЕС починається з:

- визначення проблемної області та завдання;

- знаходження експерта, який бажає співпрацювати при вирішенні проблеми;

- визначення попереднього підходу до вирішення проблеми;

- аналізу витрат і прибутку від розробки;

- підготовки докладного плану розробки.

Правильний вибір проблеми представляє найкритичнішу частину розробки в цілому. Якщо вибрати неправильну проблему, можна почати проектувати завдання, які ніхто не знає, як вирішувати. Невідповідна проблема може привести до створення системи, яка коштує набагато більше, ніж економить, або яка працює, але неприйнятна для користувачів.

Наведемо деякі факти, що свідчать про необхідність розробки і впровадження ЕС:

- нестача фахівців;

- потреба в численному колективі фахівців, оскільки жоден з них не володіє знаннями в достатній кількості;

- знижена продуктивність, оскільки завдання вимагає повного аналізу складного набору умов, а звичайний фахівець нев змозі переглянути (за відведений час) всі ці умови;

- велика розбіжність між рішеннями найкращих і найгірших виконавців;

- наявність конкурентів, що мають перевагу в тому, що вони краще справляються з поставленим завданням.

Зазвичай ЕС розробляються шляхом отримання специфічних знань від експерта та введення їх в систему.

У колектив розробників ЕС входять як мінімум чотири фахівця:
- експерт – провідний фахівець в певній галузі діяльності, який володіє унікальними знаннями;

- інженер зі знань – фахівець зі штучного інтелекту, який виступає в ролі проміжного буфера між експертом і базою знань;

- програміст – фахівець в області розробки програмного забезпечення;

- користувач – фахівець предметної області, для якого призначена система. Зазвичай його кваліфікація недостатньо висока, і тому він потребує допомоги і підтримки своєї діяльності з боку ЕС [21]. Очолює колектив інженер по знанням, це ключова фігура при розробці систем, заснованих на знаннях.

В процесі розробки системи інженер зі знань та експерт зазвичай працюють разом. Інженер зі знань допомагає експерту структурувати знання, визначати і формалізувати поняття і правила необхідні для вирішення проблеми. Програмну реалізацію завдання здійснює програміст.

Прибуток від розробки ЕС можливий за рахунок зниження ціни продукції, підвищення продуктивності праці, розширення номенклатури продукції і послуг або навіть розробки нових видів продукції і послуг в цій галузі.

Компоненти експертних систем

Експертна система містить наступні основні компоненти:

- база знань;

- механізм виведення (засіб комп'ютерного мислення).

Основний процес полягає в застосуванні механізму виведення до вихідних знань з метою отримання результуючих знань, що представляють інтерес для користувача експертної системи. Методи вирішення завдань, засновані на зведенні їх до пошуку, залежать від особливостей предметної області, в якій вирішується завдання, і від вимог, що пред'являються користувачем до рішення [22].

Крім основних компонентів експертна система може включати додаткові підсистеми, що забезпечують спілкування з користувачем, перенесення знань від експерта в комп'ютерну програму, пояснення і обгрунтування результатів виведення і т.д.

Класифікація експертних систем

Можна виділити сім основних класів задач, для вирішення яких створюються ЕС.

1. Інтерпретація даних, тобто аналіз даних, що надходять в систему з метою ідентифікації ситуації в предметній області. Наприклад:

- виявлення та ідентифікація різних типів кіберзагроз;

- визначення можливих підозрюваних кіберзлочинців на основі скоєних правопорушень та інших несанкціонованих втручань в роботу систем.

2. Діагностика, тобто ідентифікація критичних ситуацій в предметної області на основі інтерпретації даних. Під діагностикою зазвичай розуміється виявлення несправності в деякій системі. наприклад:

- діагностика і виявлення причин некоректного функціонування комп’ютерних систем;

- діагностика помилок в апаратурі і математичному забезпеченні ЕОМ;

3. Моніторинг, тобто стеження за ходом подій в предметної області з метою визначення моменту виникнення критичних ситуацій на основі безперервної інтерпретації даних. Наприклад:

- контроль та захист роботи електростанцій, допомога диспетчерам атомного реактора;

- контроль датчиків на заводах.

4. Проектування, тобто розробка об'єктів, які відповідають певним вимогам. Наприклад:

- проектування системи захисту на підприємстві;

- проектування системи реагування на інциденти інформаційної безпеки.

5. Прогнозування, тобто передбачення виникнення в предметної області тих чи інших ситуацій в майбутньому на основі моделей минулого і сьогодення з ймовірними. наприклад:

- передбачення можливих збитків за умови успішного проведення атаки на інформаційну систему;

- розрахунок витрат на захист у відповідності з цілями та розмірами підприємства;

- розрахунок вірогідності пошкодження системи, що захищається, за умови дотримання рекомендованих заходів безпеки.

6. Планування, тобто створення програм дій, виконання яких дозволить досягти поставленої мети.

наприклад:

- планування дій при виявленні загрози (у випадку антивірусного ПЗ);

- планування дій при спробі несанкціонованого втручання в інформаційну систему;

- планування експерименту в захищеній області пам’яті ЕВМ (на віртуальній машині) та ін.

7. Навчання, тобто діагностика помилок при вивченні будь-якої дисципліни і підказка правильних рішень. Наприклад:

- вивчення мови програмування;

- система для допомоги в навчанні працівникам та ін [23].

За своїм призначенням ЕС можна умовно розділити на консультаційні або інформаційні, дослідницькі та керуючі.

Консультаційні ЕС призначені для отримання користувачем кваліфікованих порад; дослідні ЕС покликані допомагати користувачеві кваліфіковано вирішувати наукові завдання; керуючі ЕС служать для автоматизації управління процесами в реальному масштабі часу.

Експертні системи створюються для вирішення різного роду проблем (таблиця 2.1), типи яких можна згрупувати в категорії.

Таблиця 2.1 – Класифікація експертних систем

Категорія	**Розв'язувана проблема**
Інтерпретація	Опис ситуації за інформацією, що надходить від датчиків
Прогноз	Визначення ймовірних наслідків заданих ситуацій
Діагностика	Виявлення причин неправильного функціонування системи за результатами спостережень
Проектування	Побудова конфігурації об'єктів при заданих обмеженнях
Планування	Визначення послідовності дій
Спостереження	Порівняння результатів спостережень з очікуваними результатами
Налагодження	Складання рецептів виправлення неправильного функціонування системи
Ремонт	Виконання послідовності запропонованих виправлень
Навчання	Діагностика, налагодження та виправлення поведінки учня
Управління	Управління поведінкою системи в цілому

Експертні системи як інструмент в роботі користувачів вдосконалюють свої можливості вирішувати важкі, неординарні завдання в ході практичної роботи.

Найбільш уразливі експертні системи в розпізнаванні меж своїх можливостей і демонструють ненадійне функціонування поблизу меж їх застосування. Подальший прогрес в області штучного інтелекту з часом запропонує способи виявлення меж своїх можливостей. Іншим недоліком експертних систем є значні трудовитрати, необхідні для поповнення бази знань. Отримання знань від експертів і внесення їх в базу знань являє собою складний процес, пов'язаний зі значними витратами часу і коштів. Проектування експерт-

них систем також має певні труднощі та обмеження, які впливають на їх розробку.

Іноземний досвід показує, що експертні системи розробляються в основному в університетах, науково-дослідних центрах і комерційних організаціях, в тому числі і для фінансової індустрії. У сфері фінансового обслуговування ці системи допомагають страховим компаніям аналізувати і оцінювати комерційний ризик, встановлювати розміри позик при кредитуванні організацій, складати кошториси проектів і т.д.

Область застосування експертних систем розширюється. Крім охоплення різних областей діяльності, одним з найбільш важливих наслідків розробки експертних систем є модифікація знань. У міру того як розробники будуватимуть великі, складні бази знань, з'являється ринок знань, незалежних від комп'ютерних систем. З'являться засоби навчання для тих, хто вивчає певну прикладну область. Комерційним продуктом стануть метазнання, тобто знання про оптимальні стратегії та процедури використання предметних знань. Розвиток експертних систем в інтелектуальні складається в злитті концепцій обладнання, засобів їх створення (мов) і самих експертних систем. Об'єднання інтелектуальних систем особливо ефективно в складних інфраструктурах. Інтелектуальні системи вже розробляються і впроваджуються за кордоном для комерційного використання та головним чином ставлять своєю задачею змінити традиційні підходи до взаємодії людини та комп’ютера [24].

Приклад експертної системи, що використовується для задач кібербезпеки

Розглянемо експертні системи на основі евристичних правил.

В даному підході використовується один з популярних методів представлення знань - правила в формі IF <умова> THEN <дія>. Одним із застосувань такого підходу є створення антивірусного програмного забезпечення і систем виявлення вторгнень. Можливі такі варіанти евристичного аналізу:

- Аналізується програмний код файлу і порівнюється з сигнатурами,

що зберігаються в базі антивірусного ПЗ. Ці сигнатури характеризують не який-небудь конкретний вид шкідливого ПЗ, а деяку сукупність вірусів, виходячи з припущення про те, що нові віруси мають схожість з вже існуючим шкідливим ПЗ.

- Аналізуються дії, що здійснюються поточним процесом під час роботи, і порівнюються з правилами, збереженими в базі антивірусного ПЗ. У цьому випадку з'являється можливість виявити шкідливе ПЗ, сигнатури для якого ще небули додані в базу, якщо воно спрямоване на виконання тих же дій, що і віруси, які зустрічалися раніше.

Прикладами антивірусного ПЗ, що використовує евристичний аналіз, можуть послужити ESET, Kaspersky, Dr.Web.

Крім того, евристичні механізми можуть також використовуватися з метою автоматизації аудиту інформаційної безпеки. Наприклад, система контролю захищеності та відповідності стандартам MaxPatrol, розроблена компанією Positive Technologies, використовує евристичний аналіз для виявлення вразливостей в мережевих службах і додатках, даючи оцінку захищеності мережі з боку зловмисника [25].

Даний підхід до створення експертних систем забезпечує простоту програмування та подання даних, так як знання, що використовуються в розроблюваних системах, можуть бути представлені в порівняно простій формі евристичного правила. Крім того, системи на основі евристичних правил можуть бути розроблені без використання спеціальних засобів (таких, як середовище програмування CLIPS, мова логічного програмування PROLOG). До недоліків подібних систем можна віднести необхідність постійного оновлення баз знань і поліноміальне зростання числа помилкових спрацьовувань систем, що створюються при надмірній чутливості евристичного аналізатора [26].

Штучна компетентність експертних систем незамінює повністю людину. Експерт-людина здатна реорганізувати інформацію і знання та використовувати їх для синтезу нових знань. В області творчої діяльності люди во-

лодіють великими здібностями і можливостями в порівнянні з найрозумнішими системами. Експерти справляються з несподіваними поворотами подій і, використовуючи нові підходи, здатні проводити аналогії з інших предметних областей. Експерти адаптуються до мінливих умов, і пристосовують свої стратегії до нових обставин в більш широкому діапазоні проблем і завдань. Експертні системи менш пристосовані до навчання на рівні нових концепцій і нових правил. Вони виявляються ненастільки ефективні і мало придатні в тих випадках, коли треба враховувати всю складність реальних завдань.

Експерти можуть безпосередньо сприймати весь комплекс вхідної інформації: символьної, візуальної, графічної, текстової, звукової, тактильної тп ін. У експертної системи є тільки символи, за допомогою яких представлені бази знань, що втілюють ті чи інші концепції. Перетворення сенсорної інформації в символьну супроводжується втратою частини інформації.

Але головне, що величезний обсяг знань, яким володіють експерти-фахівці (професійні знання і знання про світ і діючих в ньому законах), не вдається поки вбудувати в інтелектуальну систему, тим більше настільки спеціалізовану, якою є будь-яка експертна система.

2.2 Алгоритми функціонування експертної системи

Експертна система працює в двох основних режимах:

1) в режимі отримання знань;

2) в режимі вирішення задачі (так званий режим консультації, або режим використання експертної системи).

Це логічно і зрозуміло, адже спочатку необхідно як би завантажити експертну систему інформацією з тієї предметної області, в якій їй належить працювати, це і є режим «навчання» експертної системи, режим, коли вона отримує знання. А вже після завантаження всієї необхідної для роботи інформації слідує сама робота. Експертна система стає готовою для експлуатації, і її тепер можна використовувати для консультацій або для вирішення поставленої задачі.

Розглянемо більш докладніше режим отримання знань.

У режимі отримання знань роботу з експертною системою здійснює експерт за посередництва інженера по знаннях [27]. В цьому режимі експерт, використовуючи компонент придбання знань, наповнює систему знаннями (даними), які, в свою чергу, дозволяють системі в режимі рішення вже без участі експерта вирішувати завдання з даної предметної області, тим самим допомагаючи користувачу.

Слід зазначити, що режиму набуття знань в традиційному підході до розробки програм відповідають етапи алгоритмізації, програмування і налагодження. В процесі розробки і подальшого розширення системи інженер по знанням та експерт звичайно працюють разом [23].

Тепер розглянемо другий режим функціонування експертної системи, тобто режим вирішення задач (консультації).

У режимі вирішення задачі (консультації) спілкування з експертними системами здійснює безпосередньо кінцевий користувач, якого цікавить кінцевий підсумок роботи і іноді спосіб його отримання. Необхідно відзначити, що в залежності від призначення експертної системи користувач необов'язково повинен бути фахівцем у цій проблемної області [28].

Продукційна модель знань

У розробленій експертній системі використовується продукційний підхід. Продукційні моделі знань можна вважати найбільш поширеними моделями подання знань. Продукційна модель - це модель, заснована на правилах, що дозволяє уявити знання у вигляді пропозицій типу: «ЯКЩО умова, ТО дія».

Продукційна модель має недолік, що при накопиченні досить великого числа (порядку декількох сотень) продукцій вони починають суперечити один одному.

У загальному випадку продукційну модель можна представити в наступному вигляді: N = <A, U, C, I, R>, де N - ім'я продукції; A - сфера застосування продукції; U - умова застосовності продукції; C - ядро продукції; I -

постумови продукції, що актуалізуються при позитивній реалізації продукції; R - коментар, неформальне пояснення (обґрунтування) продукції;

Системи обробки знань, що використовують продукціонну модель отримали назву «продукційних систем». До складу експертних систем продукційного типу належать база правил (знань), робоча пам'ять і інтерпретатор правил (вирішувач), який реалізує певний механізм логічного висновку. Будь-яке продукційне право, яке міститься в базі знань, складається з двох частин: антецедент і консеквент. Антецедент представляє собою умовну частину і складається з елементарних пропозицій, з'єднаних логічними зв'язками «і», «або». Консеквент (висновок) включає одне або кілька пропозицій, які висловлюють або деякий факт, або вказівку на певну дію, яка підлягає виконанню. Продукційні правила прийнято записувати у вигляді антецедент-консеквент [29]. Наприклад: ЯКЩО «резервне копіювання виповнялося» І «дані було втрачено» ТО «виконати відновлення з резервної копії».

Будь-яке правило складається з однієї або декількох пар «атрибут-значення». У робочій пам'яті систем, заснованих на продукційних моделях, зберігаються пари атрибут-значення, істинність яких встановлена в процесі вирішення конкретного завдання до деякого поточного моменту часу. Вміст робочої пам'яті змінюється в процесі виконання завдання. Це відбувається в міру спрацювання правил. Правило спрацьовує, якщо при зіставленні фактів, що містяться в робочій пам'яті, з антецедентом аналізованого правила має місцезбіг, при цьому висновок спрацювавшого правила заноситься в робочу пам'ять. Тому в процесі логічного висновку обсяг фактів в робочій пам'яті, як правило, збільшується (зменшуватися він може в тому випадку, якщо дія якого-небудь правила полягає у видаленні фактів з робочої пам'яті). В процесі логічного висновку кожне правило з бази правил може спрацювати тільки один раз.

Існують два типи продукційних систем - з «прямими» і «зворотними» висновками. Розроблена експертна система відноситься до типу з «прямими»

висновками. Прямі висновки реалізують стратегію «від фактів до висновків». При зворотних висновках висуваються гіпотези імовірнісних висновків, які можуть бути підтверджені або спростовані на підставі фактів, що надходять в робочу пам'ять. Існують також системи з двонаправленими висновками.

Основні переваги систем, заснованих на продукційних моделях, пов'язані з простотою подання знань і організації логічного висновку, а саме:

- модифікованість (якщо додається або модифікується будь-яке правило, то все, що було зроблено раніше, залишається в силі і до нового правила невідноситься);

- доступність читання (переважна частина людських знань може бути записана у вигляді продукцій. Людські знання є модульними і тому продукційні системи ближчі для їх подання і легкі для читання);

- наглядність (система відображає послідовність правил, яку вона використовувала для отримання висновку).

До недоліків таких систем можна віднести наступне:

- відміну від структур знань, властивих людині;

- неясність взаємних відносин правил;

- складність оцінки цілісного образу знань;

- низька ефективність обробки знань.

При розробці невеликих систем (десятки правил) проявляються в основному позитивні сторони продукційних моделей знань, проте при збільшенні обсягу знань більш помітними стають слабкі сторони [30].

РОЗДІЛ 3 ПРОГРАМНА РЕАЛІЗАЦІЯ ЕКСПЕРТНОЇ СИСТЕМИ ІДЕНТИФІКАЦІЇ КОРИСТУВАЧІВ МЕРЕЖІ ІНТЕРНЕТ

3.1 Програмні засоби для проектування експертних систем

Важливу роль при створенні ЕС відіграють інструментальні засоби. Серед інструментальних засобів для створення ЕС найбільш популярними є такі мови програмування, як LISP і PROLOG, а також експертні системи-оболонки (ЕСО): KEE, CENTAUR, G2 і GDA, AT_ТЕХНОЛОГІЯ, що надають в розпорядження розробника-інженера зі знань широкий набір для комбінування систем уявлення знань, мов програмування, об'єктів і процедур.

Коротко зупинимося на деяких вищенаведених мовах програмування. LISP, як випливає з його назви, призначений для обробки списків, що складаються з атомів – абстрактних елементів, що представляють собою формально необмежені по довжині ланцюжки символів. Вони можуть трактуватися як рядки в більш звичному розумінні, числа або становити якісь логічні структури з вкладеними на необмежену глибину підсписками у вигляді ієрархічних дерев. Для обробки списків використовується функціональна модель, що базується на теорії Lambda-обчислень Черча. Фактично програма на LISP представляє собою набір lambda-функцій, при цьому робота зі списками здійснюється за допомогою базового набору примітивів типу CAR / CDR (взяти перший елемент списку, який сам може бути списком / отримати список без першого елемента). Таких примітивів в мінімальному наборі налічується 13 штук. З їхньою допомогою і, головне, завдяки рекурсивній системі обробки інформації LISP дозволяє дуже компактно описувати функції, для реалізації яких на інших мовах програмування потрібні були б сотні і тисячі рядків коду. Такі завдання, як автоматичне доведення теорем, розуміння природної мови і навколишнього світу, логічні числення, написання компіляторів, всюди, де потрібна обробка абстрактної структурної інформації, як ви-

явилося, дуже вдало описуються і програмуються на LISP. З недоліків даної мови можна виділити складність освоєння і високу вартість засобів розробки [28].

Програма на мові PROLOG складається з набору фактів, визначених відношень між об'єктами даних (фактами) і набором правил (зразками відносин між об'єктами бази данних). Ці факти і правила вводяться в базу даних. Для роботи програми користувач повинен ввести запит - набір термінів, серед яких всі повинні бути істинні. Факти і правила з бази даних використовуються для визначення того, які підстановки для змінних в запиті (звані уніфікацією) узгоджуються з інформацією в базі даних. Мова PROLOG, як інтерпретатор, запрошує користувача вводити інформацію. Користувач набирає запит або ім'я функції. Виводиться значення (істина – yes, або хибність – no) цього запиту, а також можливі значення змінних запиту, привласнення яких робить запит істинним, тобто уніфікує запит. Хоча виконання програми на мові PROLOG ґрунтується на специфікації предикатів, воно нагадує виконання програм на мовах LISP або ML. До недоліків даної мови можна віднести відсутність механізму прямого виведення [31].

Незважаючи на всі переваги вище перелічених мов створення експертних систем, на сьогоднішній день на перше місцевиходить нова розробка – середовище CLIPS. Назва мови CLIPS - абревіатура від C Language Integrated Production System. Мова була розроблена в Центрі космічних досліджень NASA (NASA's Johnson Space Center) в середині 1980-х рр. і багато в чому схожа з мовами, створеними на базі LISP, зокрема OPS5 і ART. Для створення експертних систем, як і в будь-який іншому середовищі, в CLIPS використовуються дві основні конструкції: правила і факти.

Мова CLIPS немістить недоліків, виявлених у попередніх інструментальних засобів для створення ЕС, заснованих на мові LISP. Мова CLIPS отримала велике поширення в державних організаціях і навчальних закладах завдяки низькій вартості, потужності, ефективності та кросплатформності. Наприклад, навіть Web-орієнтований інструментарій JESS (Java Expert

System Shell), який використовує мову подання знань CLIPS, набув популярності в даний час.

Отже, основними конкурентними перевагами інструментального засобу CLIPS є:

1. Мова є вільно поширюваним програмним продуктом, його без труднощів можна знайти в Інтернеті.

2. Має відносно низьку вартість.

3. Реалізація CLIPS на мові C ++ дозволяє переносити конкретні ЕС на різні типи операційних систем.

4. За допомогою CLIPS може бути забезпечена можливість роботи в реальному масштабі часу, коли реакція системи на зміни повинна неперевищувати декількох мілісекунд.

5. Його виконавча система має цілком прийнятну продуктивність.

6. Має чітко сформульований синтаксис.

7. У мову включено безліч випробуваних на практиці конструкцій з інших інструментальних засобів.

8. Мова допускає виклик зовнішніх функцій, написаних на інших мовах програмування; в свою чергу модулі, написані на CLIPS, можуть бути викликані програмами, написаними іншими мовами.

9. Мова включає засоби, що дозволяють комбінувати породжуючі правила і об'єктно-орієнтований підхід.

Слід зазначити, що, незважаючи на численні переваги функціонального програмування, деякі завдання краще вирішувати з використанням засобів об'єктно-орієнтованого програмування (ООП), для якого характерні три основні можливості: інкапсуляція, поліморфізм, успадкування. ООП підтримує багато мов, в тому числі Smalltalk, C ++, Java, Common LISP Object System (CLOS). Мова CLIPS, в свою чергу, увібрала в себе основні переваги C ++ і CLOS.

Таким чином, веб-орієнтовані засоби на базі JAVA (системи Exsys Corvid, JESS) є більш повільними, ніж, наприклад, CLIPS 6.0 або OPS-2000.

Тому CLIPS це кращий на сьогодні вибір для роботи в реальному часі серед поширюваних вільно оболонок ЕС, розроблених на C ++. Отже, зважаючи на наведені переваги й особливості, CLIPS було вибрано як середовище для розробленої експертної системи.

Розроблена експертна система включає наступні основні компоненти: база знань; механізм виводу. Основний процес полягає в застосуванні механізму звернення до вихідних знань з метою отримання результуючих знань, що представляють інтерес для користувача ЕС [32].

Крім основних компонентів ЕС включає додаткові підсистеми, що забезпечують: спілкування з користувачем, перенесення знань від експерта в комп'ютерну програму, надання інформації про кожний наступний крок і т.д.

Для вирішення завдання розробки ЕС ідентифікації користувачів необхідно виконати наступні дії:

1. сформувати вхідний опис ЕС в якості блок-схеми;

2. сформувати базу знань, яка містить опис основних кроків та варіантів ідентифікації користувачів на основі вхідних даних у вигляді правил (блоків-блок-схеми);

3. розробити та програмно реалізувати алгоритм ідентифікації у вигляді придатної для використання ЕС;

4. виконати тестування ЕС на прикладі ресурсу або користувача.

3.2 Формування бази знань

База знань – сукупність знань, що відносяться до деякої предметної області і формально представлені таким чином, щоб на їх основі можна було здійснити міркування. При формуванні бази знань враховувалось, що при проході від запуску експертної системи до останньої відповіді, наданої від системи, вся інформація, зібрана в процесі роботи враховується як необхідна для ідентифікації користувача, тому що, якщо брати до уваги лише останню відповідь від системи, ідентифікація може бути ускладнена через нестачу інформації.

База знань містить такі запити:

- Користувач може вести діяльність на власному сайті (ідентифікація проходить через дані, представлені на сайті та виконати пошук за доменним ім’ям, використовуючи, наприклад, https://viewdns.info/ або аналоги), а може використовувати інший сайт як дошку оголошень (ідентифікація проходить за пошуком нікнейму та інших даних).
- Користувач може проводити операції з віртуальною валютою (вилучаємо інформацію з платіжних систем), а може пропонувати для покупки нелегальне ПЗ або інший контент (вступаємо в переписку, робимо вигляд, наче намагаємось щось купити або просто цікавимося товаром; вилучаємо інформацію).
- Якщо користувач непропонує нелегальних товарів або послуг – ідентифікація непотребується.
- Якщо користувач пропонує нелегальні товари та послуги (не має відношення до обміну віртуальних валют), все одно є можливість ідентифікувати його за реквізитами для оплати.
- Якщо користувач використовує анонімні месенджери, приймає оплату на криптовалютний гаманець та передає товар нечерез пошту та без особистої зустрічі – ідентифікація неможливе.
- Якщо користувач пропонує товари та відправляє їх поштою – можемо визначити його ім’я та населений пункт через поштовий клієнт (або в переписці запитати з якого населеного пункту буде прямувати замовлення нібито з метою дізнатися як довго замовлення буде прямувати до нас).
- Якщо користувач приймає оплату або приймає кошти на обмін на електронний гаманець, основним ідентифікатором якого є український телефонний номер (qiwi) – можемо виконати спробу дізнатись ім’я та прізвище користувача через telegram бот. Якщо номер російський – скористатися іншим telegram ботом (таким чином зможемо отримати доступ до регіону проживання користувача).

- Якщо ім’я було знайдене – виконати спробу знайти профіль користувача в соцмережах (профіль можно зіставити із іншими знайденими даними, окрім ім’я, наприклад, місто проживання тощо).
- Якщо користувач приймає оплату або кошти на обмін на банківську картку – можливо визначити ім’я та прізвище користувача через інтернет-банкінг, спробувавши виконати переказ коштів (без підтвердження переводу).
- Якщо користувач має власний сайт, можемо в деяких таких сайтах внизу сторінки побачити напис “атестовано webmoney”. При переході за цим посиланням побачимо так званий атестат системи електронних грошей, в якому деякі дані можуть бути доступні для публічного перегляду (наприклад, місто проживання).

Блок-схема ЕС створена у відповідності до бази знань та представлена на рис. 3.1. Блок-схема слугує для наочної демонстрації запитів (блоків) та зроблених виборів (стрілок). Лістинг коду представлений в додатку А.

3.3 Короткий опис програмної реалізації

Програмна реалізація ЕС ідентифікації користувачів виконана в середовищі CLIPS, яке представляє собою сучасний інструмент, призначений для створення ЕС. CLIPS складається з інтерактивного середовища - експертної оболонки зі своїм способом представлення знань, гнучкої та потужної мови і декількох допоміжних інструментів. CLIPS є абсолютно вільно поширюваним програмним продуктом. Завдяки цьому останнім часом було випущено безліч програм і бібліотек, які вдосконалюють і доповнюють можливості CLIPS [33]. Деякі з цих продуктів є власністю компаній, що їх випустили і призначені для внутрішнього використання або комерційного розповсюдження, інші, як і сам CLIPS, поширюються вільно. У даній роботі використовувалося середовище CLIPS версії 6.3.

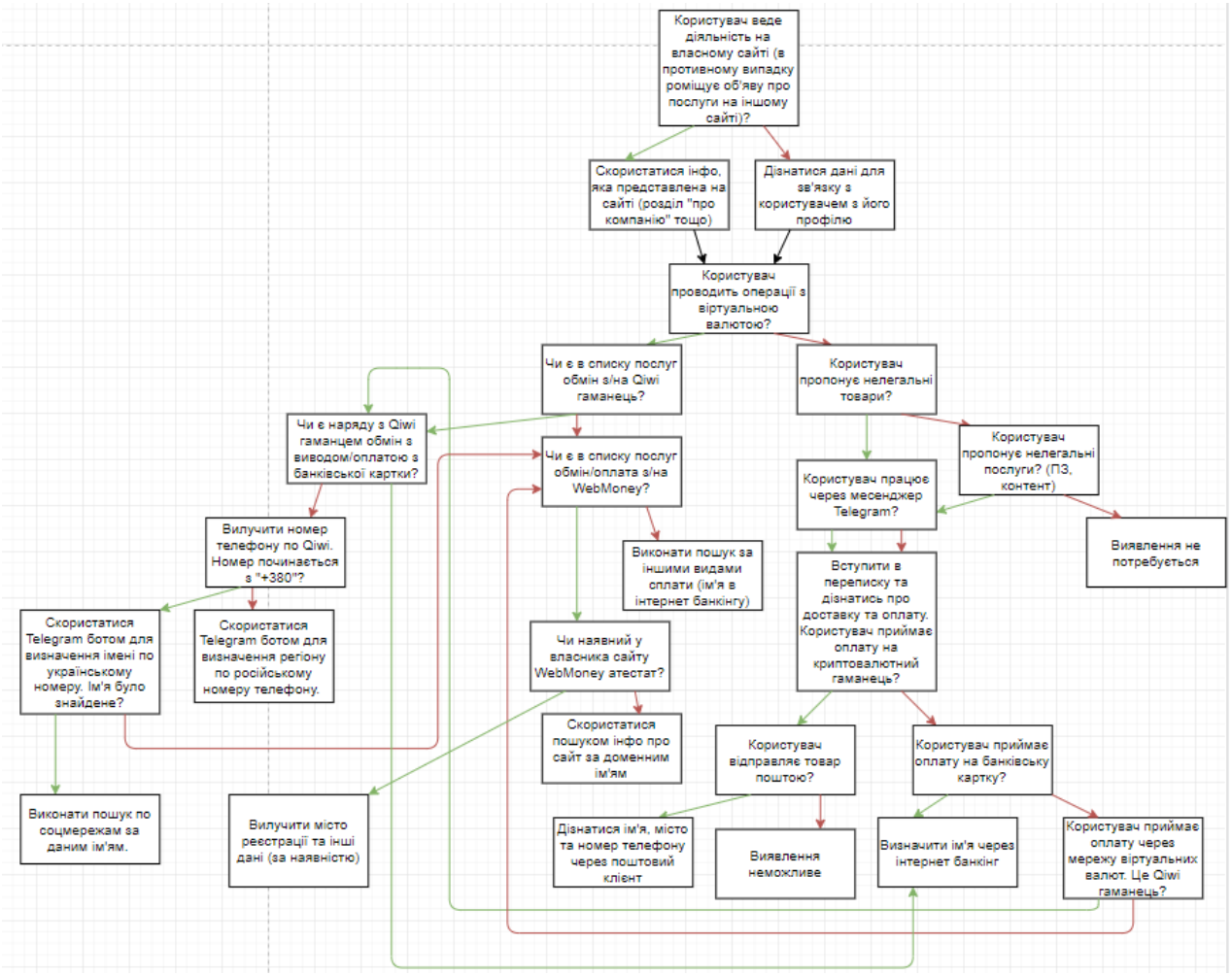

Рисунок 3.1 – Блок-схема ЕС

Дана ЕС працює за принципом yes-or-no і запитує експерта на кожному кроці, після чого надає наступний крок, який експерт повинен виконати, таким чином приводячи експерта до рішення. З кожним кроком експерт отримує більше інформації про користувача, якого ідентифікують.

Нижче наведені деякі основні фрагменти коду (з коментарями), що наочно показують відповідність до блок-схеми та пояснюють основні принципи синтаксису мови, яка була використана для розробки ЕС.

(deffunction ask-question (?question $?allowed-values) //об’явлення функції. На даному етапі передається питання (question) і варіанти відповідей (allowed values)

(printout t ?question) // вивід питання

(bind ?answer (read)) // зчитування відповіді у змінну answer

(if (lexemep ?answer) // перевірка чи є відповідь символом або строкою

then (bind ?answer (lowcase ?answer))) // відповідь переводиться до нижнього регістру

(while (not (member ?answer ?allowed-values)) do // початок циклу, перебор, поки answer небуде являтися елементом масиву allowed-values (в нашому випадку “y” або “n”)

(printout t ?question) // якщо такої відповіді немає в списку, то задати питання знову

(bind ?answer (read)) // знову зчитати відповідь

(if (lexemep ?answer) // перевірка чи є відповідь символом або строкою

then (bind ?answer (lowcase ?answer)))) // кінець циклу

?answer)

(deffunction yes-or-no-p (?question) // об’явлення функції, в яку передається запитання

(bind ?response (ask-question ?question yes no y n)) // в змінну response присвоюється результат визову функції ask-question з варіантами відповідей (yes, no (y, n))

(if (or (eq ?response yes) (eq ?response y)) // якщо response дорівнює yes або y то повернути True, інакше False

then TRUE

else FALSE))

// Правило виводу початкової информації на екран

(defrule system-banner "" // об’явлення правила, воно буде виконуватися, якщо в базі фактів є правила

// для наступних строк ніякі факти непотрібні, вони будуть виконуватися завжди при запуску

(declare (salience 10)) // задається пріоритет 10, найвищий

=> // після => описується, що саме робить правило

(printout t crlf crlf) // перенос два рази на нову строку

```
(printout t "Експертна система") // вивід на екран тексту
(printout t crlf crlf))

// Правила виводу результату (в програмі результат – це факт типу (repair ?))
(defrule print-repair ""
(declare (salience 10)) // пріоритет
(repair ?item) // відбувається запис в змінну item для виводу результату роботи ЕС
=>
(printout t crlf crlf)
(printout t "Рекомендований метод рішення:") // вивід тексту і значення змінної item
(printout t crlf crlf)
(format t "Рішення: %s %n" ?item ))
```

Рекомендований метод рішення виводиться на екран в кінці роботи програми і, як правило, відображає останній крок збору даних. Скріншот виводу рекомендованого методу рішення представлено на рис. 3.2.

```
Рекомендований метод рішення:

Рішення: Визначити ім'я через інтернет банкінг
```

Рисунок 3.2 – Вивід рекомендованого методу рішення

```
// Правила, що стосуються структури блок-схеми
(defrule where_seller_posted ""
 (not (seller use site ?s))// якщо немає факту (seller use site) і фактів (repair ?), то виконувати те, що після =>
 (not (repair ?)) // факт (repair ?)
 =>
```

(if (yes-or-no-p "Користувач веде діяльність на власному сайті? (yes no)? ") // перевірка, що поверне функція yes-or-no-p на запитання

then // якщо відповідь yes

(assert (seller use site ownsite)) // в базу фактів вставити факт (seller use site ownsite)

(printout t crlf) // перенос на нову строку

(printout t " Спробуйте скористатися інформацією яка представлена на сайті (розділ про компанію тощо) ") // вивід на екран

Якщо на перше питання від ЕС “Користувач веде діяльність на власному сайті?” користувач надає відповідь “yes”, то цьому фрагменту коду буде відповідати фрагмент блок-схеми, представлений на рис. 3.3.

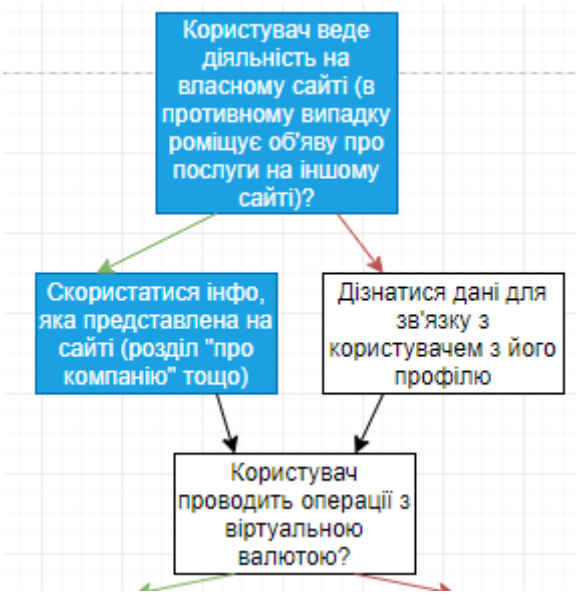

Рисунок 3.3 – Фрагмент блок-схеми, що відповідає коду при даній відповіді “yes” на перше запитання

(printout t crlf)

(printout t crlf)

else // якщо відповідь no, то виводиться наступне

(printout t crlf)

(printout t "Спробуйте дізнатися дані для зв'язку із його профілю")

На рис. 3.4 представлено фрагмент блок-схеми, що відповідає коду при даній відповіді “no” на перше запитання

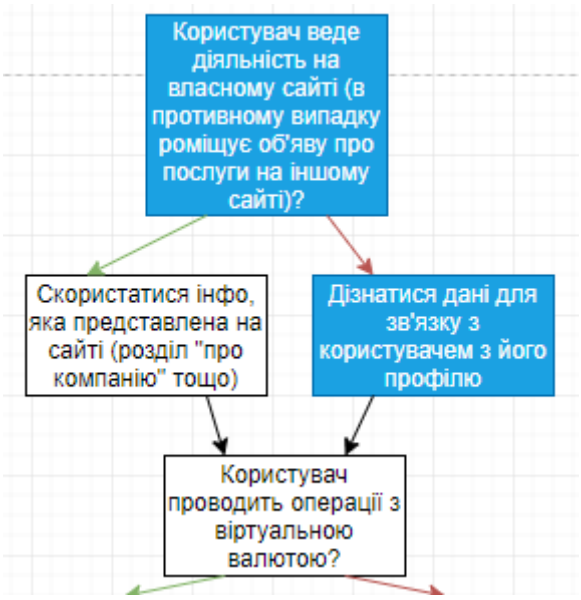

Рисунок 3.4 – Фрагмент блок-схеми, що відповідає коду при даній відповіді “no” на перше запитання

(printout t crlf)

(printout t crlf)

(assert (seller use site marketplace)))) // якщо відповідь no, також вставляється факт (seller use site marketplace)

(defrule virual_card ""

(seller use site ?) // якщо є факт (seller use site) и немає факта (repair ?), то виконується те, що після =>

(not (repair ?))

=>

(if (yes-or-no-p "Користувач проводить операції з віртуальною валютою? (yes no)? ") // користувачу задається запитання

then

(assert (seller use card virtual)) // якщо так, то вставляється факт (seller use card virtual)

На рис. 3.5 представлено фрагмент блок-схеми, що відповідає відповіді “yes” на питання “Користувач проводить операції з віртуальною валютою?”

Рисунок 3.5 – Фрагмент блок-схеми. Відповідь “yes” на питання “Користувач проводить операції з віртуальною валютою?”

else

(assert (seller use card nonvirtual)))) // якщо ні, то вставити факт (seller use card nonvirtual)

На рис. 3.6 представлено фрагмент блок-схеми, що відповідає відповіді “no” на питання “Користувач проводить операції з віртуальною валютою?”

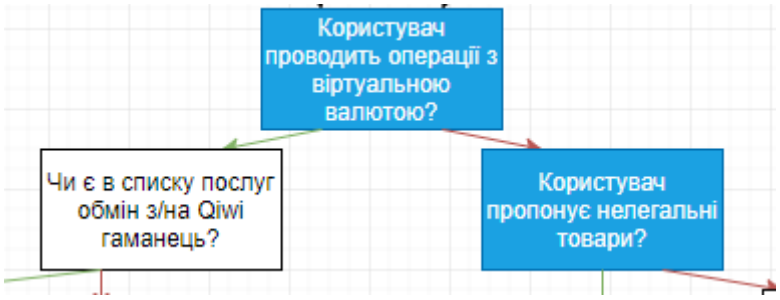

Рисунок 3.6 – Фрагмент блок-схеми. Відповідь “no” на питання “Користувач проводить операції з віртуальною валютою?”

3.4 Тестування експертної системи

Працездатність розробленої ЕС перевірялась методом вирішення задачі ідентифікації користувача. На рис. 3.7. представлений інтерфейс програми CLIPS та повний прохід в експертній системі від запуску до отримання рішення з випадковими відповідями “y”, “n”.

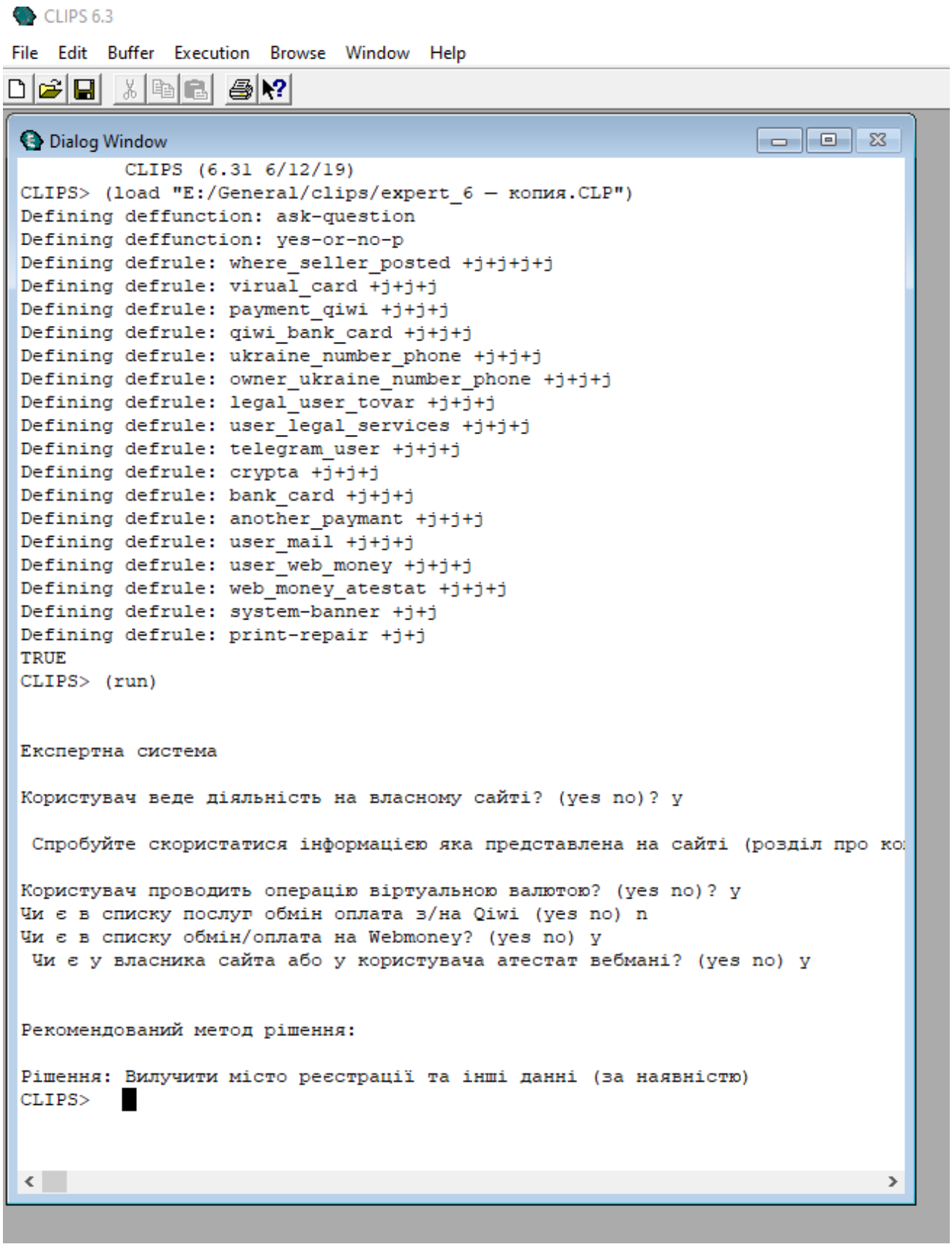

Рисунок 3.7 – Тестування ЕС

У якості прикладу було обрано сайт eexchanger.co, так як він має широкий функціонал з обміну віртуальних валют.

Виконуємо пошук інформації про власника сайту:

1. Користувач веде діяльність на власному сайті, отже спробуємо дізнатись дані, представлені на поточному ресурсі. Вилучені дані представлені на рис. 3.8.

Рисунок 3.8 – Інформація з розділу “Контакты”

2. Користувач проводить операції з віртуальною валютою.

3. В списку послуг є обмін з/на qiwi гаманець. Інформація про представлені віртуальні валюти (напрями обміну) на рис. 3.9.

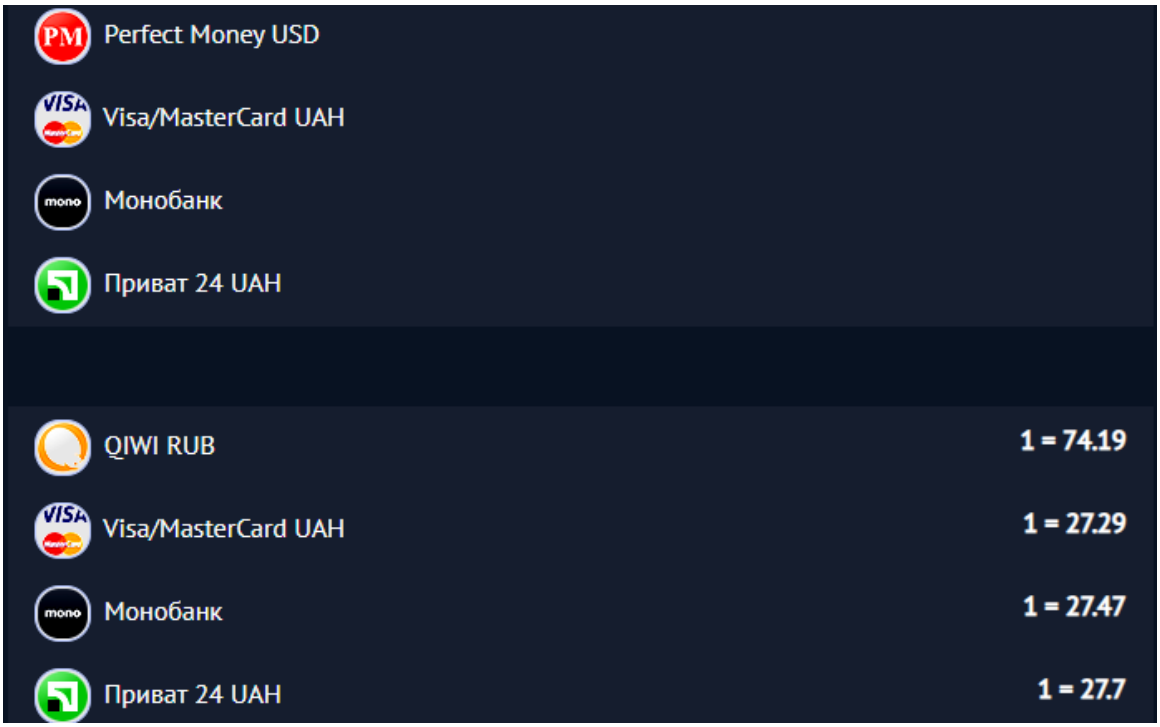

Рисунок 3.9 – Напрями обміну

4. Поряд з qiwi-гаманцем на сайті представлені напрями обміну з використанням банківської картки. Отже, для подальшої деанонімізації кращим рішенням буде використовувати саме цей варіант. Після створення заявки на обмін, сайт пропонує перевести кошти на банківську картку, номер якої представлений на рис. 3.10.

Рисунок 3.10 – Номер картки для поповнення

5. Вилучаємо ім’я через інтернет-банкінг “Приват24” шляхом введення номеру картки (рис. 3.10), на яку збираємося перевести кошти. Побачимо ім’я отримувача. Інформація представлена на рис. 3.11.

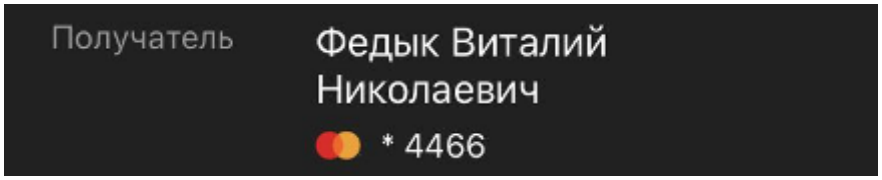

Рисунок 3.11 – Ім’я отримувача

Скріншот з CLIPS, який відповідає даному випадку ідентифікації, представлено на рис.3.12; відповідний скріншот блок-схеми представлено на рис. 3.13.

```
Користувач веде діяльність на власному сайті? (yes no)? y

 Спробуйте скористатися інформацією яка представлена на сайті (розділ про компанію тощо)

Користувач проводить операції з віртуальною валютою? (yes no)? y
Чи є в списку послуг обмін/оплата з/на Qiwi гаманець? (yes no) y
Чи є наряду з Qiwi гаманцем обмін з виводом/оплатою з банківскої карти?  (yes no) y


Рекомендований метод рішення:

Рішення: Визначити ім'я через інтернет банкінг
CLIPS>
```

Рисунок 3.12 – Випадок ідентифікації, останнім кроком якого є визначення імені по номеру банківської картки (скріншот CLIPS)

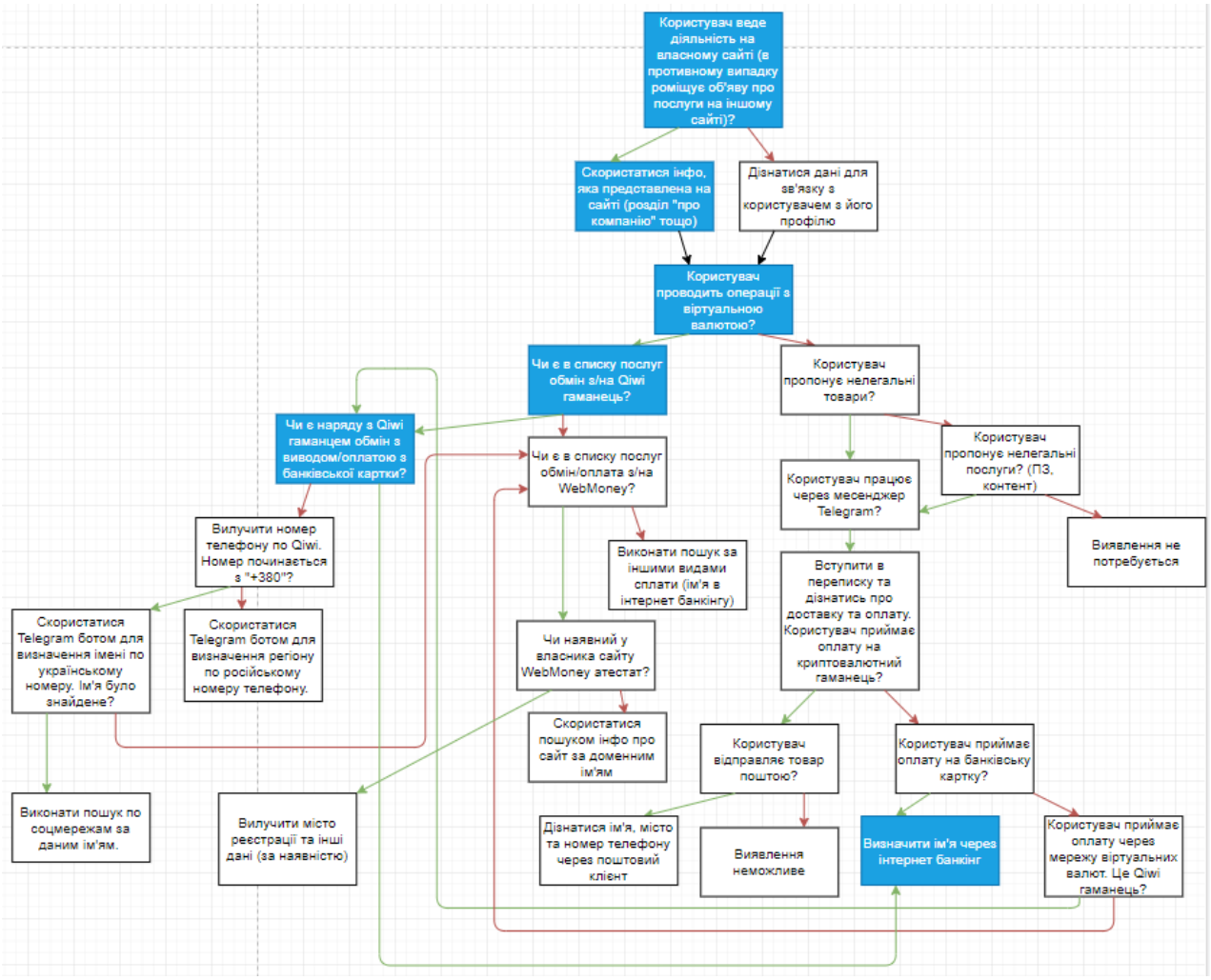

Рисунок 3.13 – Випадок ідентифікації, результатом якого є визначення імені за номером банківської картки (скріншот блок-схеми)

Варіант пошуку користувачів за номером банківської картки є більш точним, але для демонстрації інших можливостей експертної системи спробуємо провести ідентифікацію через номер телефону, прив’язаний до qiwi-гаманця. Цей шлях буде корисним, якщо на сайті немає напрямів обміну з використанням банківської картки. Повернемось до пункту експертної системи, в якому представлене запитання “Чи є наряду з qiwi-гаманцем обмін з виводом/оплатою з банківської картки?” Відповідь “ні”.

1. Аналогічно попередньому методу створимо заявку на обмін для отримання реквізитів qiwi для поповнення (варіант зарахування коштів можна вибрати будь-який, адже заявка небуде сплачена і дана операція проводиться лише задля того, щоб отримати реквізити qiwi гаманця). Отримаємо

номер телефону, до якого прив’язаний гаманець в якості реквізитів. Номер представлено на рис. 3.14.

Рисунок 3.14 – Номер телефону для подальшого пошуку

2. Скористаємось безкоштовним telegram ботом для пошуку імені за номером телефону (@info_baza_bot). Цей бот дуже простий у використанні. Достатньо лише запустити його відповідною кнопкою і можна одразу ввести номер для пошуку. Як видно на рис. 3.15 знайдене ім’я за номером телефону співпадає з ім’ям, отриманим через інтернет-банкінг за номером банківської картки.

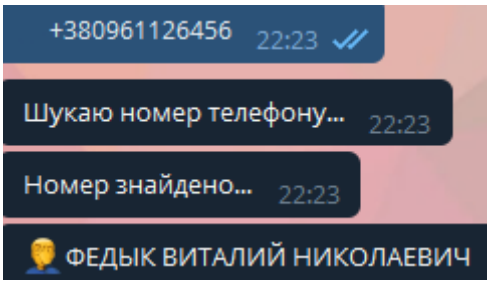

Рисунок 3.15 – Результат пошуку через telegram-бота за номером телефону

3. Далі, згідно алгоритму експертної системи, якщо номер телефону було знайдено, наступним кроком виконаємо пошук в мережі Інтернет за даним ім’ям. У даному випадку було знайдено сторінки користувача в декількох соціальних мережах.

Скріншот з CLIPS, який відповідає даному випадку ідентифікації, представлено на рис.3.16; відповідний скріншот блок-схеми представлено на рис. 3.17

```
Експертна система

Користувач веде діяльність на власному сайті? (yes no)? y

 Спробуйте скористатися інформацією яка представлена на сайті (розділ про компанію тощо)

Користувач проводить операції з віртуальною валютою? (yes no)? y
Чи є в списку послуг обмін/оплата з/на Qiwi гаманець? (yes no) y
Чи є наряду з Qiwi гаманцем обмін з виводом/оплатою з банківскої карти?  (yes no) n
Вилучити номер телефону по Qiwi. Номер починається з +380? (yes no) y
Скористатися Telegram ботом для визначення імені по українському номеру телефону. Ім'я знайдене? (yes no) y


Рекомендований метод рішення:

Рішення: Виконати пошук по соцмережам за даним ім'ям
CLIPS>
```

Рисунок 3.16 – Випадок ідентифікації, результатом якого є пошук у соцмережах за іменем, здобутим з telegram-боту (скріншот CLIPS)

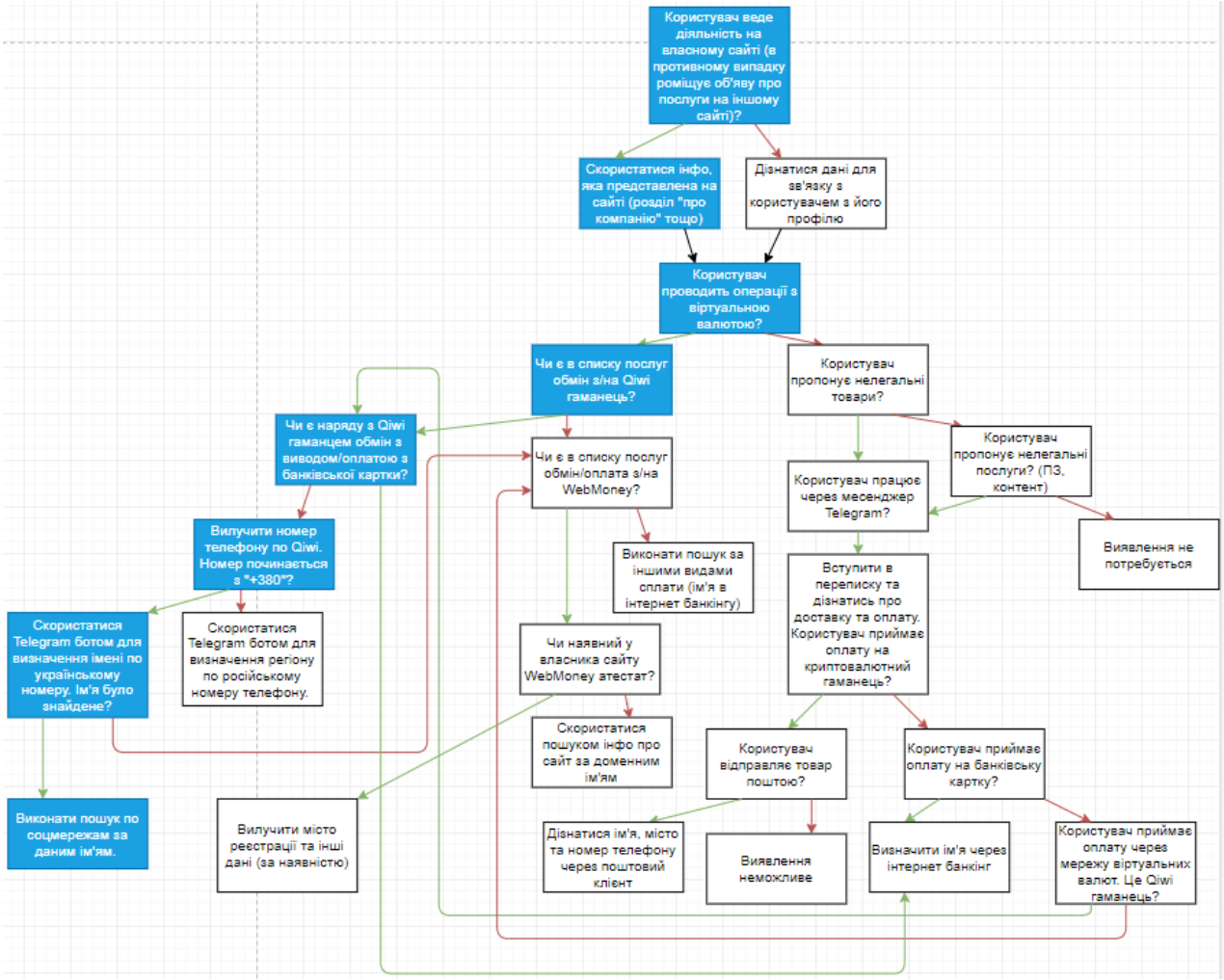

Рисунок 3.17 – Випадок ідентифікації, результатом якого є пошук у соцмережах за іменем, здобутим з telegram-боту (скріншот блок-схеми)

Отримана інформація може бути передана в підрозділи кіберполіції з метою полегшення пошуку порушників або цілеспрямовано використовуватися співробітниками кіберполіції.

ВИСНОВКИ

Аналізуючи значну кількість кіберзагроз та їх наслідків, можна впевнено наголосити на важливості використовувати легальне ПЗ та, що неменш важливо, стежити за каналами його надходження, адже можливі витоки, втрата інформації та відмова в обслуговуванні можуть завдати чималі збиткі, які значно перевищать вигоду від економії на придбанні легальних програмних продуктів.

Дана робота присвячена проблемі ідентифікації користувачів в мережі, які ведуть нелегальну діяльність з метою подальшого використання здобутих даних у правоохоронних органах. В ході дослідження встановлено, що вирішення даної проблеми можливо із аналізом і застосуванням інформації, добутої з відкритих джерел за алгоритмом дій експертної системи. Запропоноване рішення має недолік. Це пов’язано з тим, що відкритої для перегляду особистої інформації може бути недостатньо або вона не є загальнодоступною.

У даній роботі було досліджено варіанти, коли продавці нелегальних цифрових та фізичних товарів максимально приховують інформацію про себе, а також ситуації, коли користувачі, які надають послуги з обміну валют із забороненим доступом, намагаються підвищити довіру до своїх ресурсів (обмінних пунктів), тим самим, розкриваючи персональну інформацію. Отже, досить часто для ідентифікації користувача може бути достатньо лише інформації, що отримана з відкритих джерел, та інформації, яку користувач сам публікує або нехтує її належним приховванням.

Досліджена продукційна модель представлення знань в практичному завданні є дуже зручною, зрозумілою та за структурою нагадує структуру людських знань. Отже, дану модель було використано в ході розробки експертної системи. У ході розробки було використано середовище CLIPS – потужний інструмент із власною мовою програмування. Розроблена експертна система може надати порядок дій для ідентифікації необхідного користувача

та може бути використана як помічник в підрозділах кіберполіції для полегшення пошуку порушників.

СПИСОК ЛІТЕРАТУРИ

1. Решение № 5/16. Усилия ОБСЕ по сокращению рисков возникновения конфликтов в результате использования информационных и коммуникационных технологий [Електронний ресурс] // Organization for Security and Co-operation in Europe. Матеріали 23-ї зустрічі, м. Гамбург, Німеччина, 2016. – 3 с. Режим доступу: https://www.osce.org/ru/cyber-ict-security .

2. Власова Л. А. Защита информации / Л.А. Власова. – Хабаровск: РИЦ ХГАЭП. – 2007. – 84 с. – С. 14.

3. Литвинюк, А. А. Основи інформаційної безпеки. Комплексна система захисту інформації: структура, встановлення та підтримка функціонування / А.А. Литвинюк // Вісник ЦВК. – 2008. – № 4. – С. 18-21.

4. Про внесення змін до Кримінального кодексу України щодо відповідальності за незаконне втручання в роботу мереж електрозв'язку: Закон України, 5 червня 2003. // Відомості Верховної Ради України. – 2003. – № 38. – С. 320.

5. Батюк А. Є. Інформаційні системи в менеджменті / А.Є. Батюк, З.П. Двуліт, К.М. Обельовська, І.М. Огороднік, Л.П. Фабрі. – Львів: «Інтелект-Захід», 2004. – 520 с. – С. 343–384.

6. Легомінова С. В. Теоретичні засади інформаційної безпеки підприємства / С. В. Легомінова // Економіка. Менеджмент. Бізнес. – 2015. – № 3. – С. 87-92. Режим доступу: http://nbuv.gov.ua/UJRN/ecmebi_2015_3_18

7. Матиев Д. Средства защиты информации: проблема выбора и соответствия / Д. Матиев. [Електронний ресурс]. // Известия Тульского государственного университета. Технические науки – 2018. – №11 – С.4. Режим доступу: http://bankir.ru/publikacii/s/sredstva-zaschiti-informacii-problema-vibora-i-sootvetstviya-5386161/.

8. Tor: The Second-Generation Onion Router [Електронний ресурс] / R. Dingledine, N. Mathewson, P. Syverson. – 2004. – Режим доступу: https://svn.torproject.org/svn/projects/design-paper/tor-design.pdf.

9. Волосович С. В. Віртуальна валюта: глобалізацій ні виклики і перспективи розвитку / С.В. Волосович // Економіка України. – 2016. – № 4 (653). Режим доступу: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/EkUk_2016_4_8.pdf .

10. Розпорядження національної комісії, що здійснює державне регулювання у сфері ринків фінансових послуг № 4180 м. Київ – 2017. С. 2.

11. Pflaum I. A bit of a problem: national and extraterritorial regulation of virtual currency in the age of financial disintermediation / I. Pflaum, E. Hateley // Georgetown Journal of International Law. – Vol. 45. – P. 1169-1215. Режим доступу: http://www.law.georgetown.edu/academics/law-journals/gjil/recent/upload/zsx00414001169.PDF.

12. Проект Закону про стимулювання ринку крипто валют та їх похідних в Україні від 10.10.2017. Офіційний веб-портал Верховної Ради України. Режим доступу: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=62710.

13. Звіт ФАТФ. Віртуальні валюти. Ключові визначення і потенційні ризики в сфері ПВК/ФТ. – 2014. – С. 13-31.

14. Онищенко Ю. І. Криптовалюта як фінансовий актив для інвестування банками / Ю. І. Онищенко, С. Ю. Капсамун // Науковий вісник Ужгородського національного університету. Серія: Міжнародні економічні відносини та світове господарство. – 2019. – Вип. 25, Ч. 2. – С. 25-30.

15. Вепрев С. Б. Перов В. А. Вопросі информационной безопасности при использовании крипто валют / С. Б. Вепрев В. А. Перов // Вестник РосНоу. Серия «Сложные системыЖ модели, анализ и управление», 2018. – Вып. 2. – С. 67.

16. Шевченко Д.І. Аналіз способів забезпечення анонімності при криптовалютних транзакціях. Дипломна магістерська робота. / Д.І. Шевченко. – ДВНЗ «Національний гірничий університет»: Інститут електроенергетики. – 2018. – 64 с. – С. 30. Режим доступу:

http://ir.nmu.org.ua/handle/
123456789/151389 .

17. Баранов Р.О. Протидія легалізації злочинних доходів та фінансуванню тероризму з використанням віртуальних валют / Р.О. Баранов // Державне управління: удосконалення та розвиток. – 2016. – № 6. – С. 31-32.

18. Чернов В.А. Теория экономического анализа / В.А. Чернов. – М.: Проспект, 2017. – 384 с. – С. 167.

19. Семеріков С. О. Оболонка CLIPS як засіб вивчення експертних систем / С. О. Семеріков, І. О. Теплицький // Науковий часопис Національного педагогічного університету імені М. П. Драгоманова. – Серія №2. Комп'ютерно-орієнтовані системи навчання, 2007. – №5 (12). – С. 31–36.

20. Субботін С. О. Подання й обробка знань у системах штучного інтелекту та підтримки прийняття рішень / С.О. Субботін. – Запоріжжя: ЗНТУ, 2008. – 341 с. – С. 27.

21. Гаврилова Т. А. Подготовка коллектива разработчиков экспертной системы / Т.А. Гаврилова // Доклад на школе-семинаре «Проблемы применения ЭС в народном хозяйстве». Кишинев. – 1989. – С. 59-62.

22. Молокова О. С. Методология анализа предметных знаний / О.С. Молокова // Российская ассоциация искусственного интеллекта. Новости искусственного интеллекта, 1992. – № 3. – С. 11-60.

23. Джарратано Д. Экспертные системы: принципы разработки и программирование / Д. Джарратано. – М.: Вильямс, 4- е изд. – 2007. – 1152 с. – С.652.

24. Гущина Ю. И. Применение искусственного интеллекта при разработке маркетинговых информационных систем / Ю.И. Гущина, В.В. Рекеда // Известия Волг. ГТУ, 2014. – Т. 20. – Вып.№ 17 (144). – С. 54.

25. Цветков В.Я. Эвристический анализ как инструмент информационной безопасности / В.Я. Цветков, С.В. Булкагов // Современные наукоемкие технологии. – 2010. – № 1. – С. 53-54.

26. Новиков Е.А. Сравнительный анализ методов обнаружения вторжений / Е.А. Новиков, А.А. Краснопевцев // Безопасность информационных технологий. – 2012. – Том 19. № 1. – С. 47-50.

27. Хох В.Д. Дослідження методів побудови експертних систем / В. Д. Хох, Є. В. Мелешко, М. С. Якименко // Системи управління, навігації та зв'язку. – 2016. – Вип. 4. – С. 48-52. – Режим доступу: http://nbuv.gov.ua/UJRN/suntz_2016_4_14

28. Джексон П. Введение в экспертные системы / П. Джексон. – М.: СПб.; К.: Вильямс, 2001. – 624 с. – С. 11-12.

29. Ясницкий Л. Н. Введение в искусственный интеллект / Л. Н. Ясницкий. – М.: Академия. 2005. 420 с. – С. 122.

30. Тарков М.С. Нейрокомпьютерные системы / М.С. Тарков. – М.: Интернет-Университет Информационных Технологий; БИНОМ. Лаборатория знаний, 2006. – 140с. – С. 142.

31. Братко И.М. Алгоритмы искусственного интеллекта на языке PROLOG / И.М. Братко. – М.: Вильямс, 2001. 640 с. – С. 27.

32. Brown C. Introduction to artificial intelligence and expert systems / C. Brown, D. O'Leary // Artificial Intelligence. Expert Systems Section of the American Accounting Association. – 1995. – С. 10.

33. Семеріков С.О. CLIPS: локалізована оболонка експертної системи для вітчизняної системи освіти / Семеріков С.О., Теплицький І.О. – Кривий Ріг. Видавничий відділ КДПУ – 2006. – 34с. – С. 14.

ДОДАТОК А

```
(deffunction ask-question (?question $?allowed-values)
 (printout t ?question)
 (bind ?answer (read))
 (if (lexemep ?answer)
  then (bind ?answer (lowcase ?answer)))
  (while (not (member ?answer ?allowed-values)) do
  (printout t ?question)
  (bind ?answer (read))
 (if (lexemep ?answer)
  then (bind ?answer (lowcase ?answer))))
?answer)

(deffunction yes-or-no-p (?question)
 (bind ?response (ask-question ?question yes no y n))
 (if (or (eq ?response yes) (eq ?response y))
  then TRUE
 else FALSE))

(defrule where_seller_posted ""
 (not (seller use site ?s))
 (not (repair_f ?))
 (not (repair ?))
 =>
 (if (yes-or-no-p "Користувач веде діяльність на власному сайті? (yes no)? ")
  then
  (assert (seller use site ownsite))
  (printout t crlf)
```

```
(printout t " Спробуйте скористатися інформацією яка представлена на сайті (розділ про компанію тощо) ")
(printout t crlf)
(printout t crlf)
else
(printout t crlf)
(printout t "Спробуйте дізнатися дані для зв'язку із його профілю")
(printout t crlf)
(printout t crlf)

(assert (seller use site marketplace))))

(defrule virual_card  ""
(seller use site ?)
(not (repair ?))
=>
(if (yes-or-no-p "Користувач проводить операції з віртуальною валютою? (yes no)? ")
then
(assert (seller use card virtual))
else
(assert (seller use card nonvirtual))))

;; QIWI node

(defrule payment_qiwi ""
(seller use card virtual)
(not (repair ?))
=>
```

```
(if (yes-or-no-p "Чи є в списку послуг обмін/оплата з/на Qiwi гаманець? (yes no) ")
 then
  (assert (payment qiwi yes))
 else
  (assert (payment qiwi no))))


(defrule qiwi_bank_card ""
 (payment qiwi yes)
 (not (repair ?))
=>
 (if (yes-or-no-p "Чи є наряду з Qiwi гаманцем обмін з виводом/оплатою з банківскої карти? (yes no) ")
 then
  (assert (bank_card in qiwi yes))
  (assert (repair "Визначити ім'я через інтернет банкінг"))
 else
  (assert (bank_card in qiwi no))))


(defrule ukraine_number_phone ""
 (bank_card in qiwi no)
 (not (repair ?))
=>
 (if (yes-or-no-p "Вилучити номер телефону по Qiwi. Номер починається з +380? (yes no) ")
 then
  (assert (seller number phone ukraine))
 else
```

```
 (assert (repair "Скористатися Telegram ботом для визначення регіону по російському номеру телефону (yes no) "))
 (assert (seller number phone another country))))

(defrule owner_ukraine_number_phone ""
 (seller number phone ukraine)
 (not (repair ?))
=>
 (if (yes-or-no-p "Скористатися Telegram ботом для визначення імені по українському номеру телефону. Ім'я знайдене? (yes no) ")
 then
 (assert (repair "Виконати пошук по соцмережам за даним ім'ям"))
 (assert (seller name_number_phone yes))
 else
  (assert (payment qiwi no))
  (assert (seller name_number_phone no))))

;; no virtual card node

(defrule legal_user_tovar ""
 (seller use card nonvirtual)
 (not (repair ?))
=>
 (if (yes-or-no-p "Користувач пропонує нелегальні товари? (yes no) ")
 then
 (assert (user_legal illegal))
 else
 (assert (user_legal legal))))
```

```
(defrule user_legal_services ""
 (user_legal legal)
 (not (repair ?))
=>
 (if (yes-or-no-p "Користувач пропонує нелегальні послуги (ПЗ, контент)? (yes no) ")
 then
 (retract 3)
 (assert (user_legal illegal))
 else
  (assert (repair "Виявлення непотребується"))
  (assert (tovar legal legal))))


(defrule telegram_user ""
 (user_legal illegal)
 (not (repair ?))
=>
 (if (yes-or-no-p "Користувач працює через месенджер Telegram? (yes no) ")
 then
 (assert (user_use messanger telegram))
 else
 (assert (user_use messanger another))))

(defrule crypta ""
 (user_use messanger ?)
 (not (repair ?))
=>
```

```
(if (yes-or-no-p "Вступити в переписку та дізнатись про доставку та оплату. Користувач приймає оплату на криптовалютний гаманець? (yes no) ")
 then
 (assert (user_crypta yes))
 else
 (assert (user_crypta no))))

(defrule bank_card ""
 (user_crypta no)
 (not (repair ?))
=>
 (if (yes-or-no-p "Користувач приймає оплату на банківську карту? (yes no) ")
 then
 (assert (user_bank_card yes))
 (assert (repair "Визначити ім'я через інтернет банкінг"))
 else
 (assert (user_bank_card no))))

(defrule another_paymant ""
 (user_bank_card no)
 (not (repair ?))
=>
 (if (yes-or-no-p "Користувач приймає оплату через мережу віртуальних валют. Це Qiwi гаманець? (yes no) ")
 then
 (assert (payment qiwi yes))
 else
 (assert (payment qiwi no))))
```

```
(defrule user_mail ""
 (user_crypta yes)
 (not (repair ?))
=>
 (if (yes-or-no-p "Користувач відправляє товар поштою? (yes no) ")
 then
 (assert (user_use_post no))
 (assert (repair "Дізнатися ім'я, місто та номер телефону через поштовий клієнт"))
 else
 (assert (user_use_post yes))
 (assert (repair "Виявлення неможливе"))))


;; webmoney node

(defrule user_web_money ""
 (payment qiwi no)
 (not (repair ?))
=>
 (if (yes-or-no-p "Чи є в списку обмін/оплата з/на Webmoney? (yes no) ")
 then
 (assert (paymant webmoney yes))
 else
 (assert (repair "Виконати пошук за іншими видами оплати (ім'я в інтернет банкінгу)"))
 (assert (paymant webmoney no))))

(defrule web_money_atestat ""
```

```
(paymant webmoney yes)
(not (repair ?))
=>
(if (yes-or-no-p "Чи є у власника сайта або у користувача атестат веб-мані? (yes no) ")
then
(assert (atestat_webmoney yes))
(assert (repair "Вилучити місто реєстрації та інші данні (за наявністю)"))
else
(assert (repair "Скористатися пошуком інфо про сайт за доменним ім'ям"))
(assert (atestat_webmoney no))))


(defrule system-banner ""
(declare (salience 10))
=>
(printout t crlf crlf)
(printout t "Експертна система")
(printout t crlf crlf))

(defrule print-repair ""
(declare (salience 10))
(repair ?item)
=>
(printout t crlf crlf)
(printout t "Рекомендований метод рішення:")
(printout t crlf crlf)
(format t "Рішення: %s %n" ?item ))
```