Вінницький національний технічний університет
Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра захисту інформації

Бакалаврська дипломна робота на тему:
«Система перевірки контрагентів щодо зв'язку з підсанкційними країнами»

Виконав: студент 4 курсу групи 1БС-19б
спеціальності 125 Кібербезпека
_____ Куйбіда Р.І.

Керівник: к. т. н., доц. каф. ЗІ
_____ Лукічов В.В.
«19» червня 2023р.

Рецензент: к.т.н., доц. каф. ПЗ
_____ Майданюк В.П.
«19» червня 2023р.

Допущено до захисту
Завідувач кафедри ЗІ
д. т. н., проф.
_____ Лужецький В. А.
«19» червня 2023 р.

Вінниця ВНТУ – 2023 року

Вінницький національний технічний університет
Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра захисту інформації
Рівень вищої освіти І (бакалаврський)
Галузь знань – 12 Інформаційні технології
Спеціальність – 125 Кібербезпека
Освітньо-професійна програма – Безпека інформаційних і комунікаційних систем

ЗАТВЕРДЖУЮ
Зав. кафедри ЗІ, д. т. н., проф.
_____ В. А. Лужецький
20 березня 2023 року

ЗАВДАННЯ
НА БАКАЛАВРСЬКУ ДИПЛОМНУ РОБОТУ СТУДЕНТУ
Куйбіді Роману Ігоровичу

1. Тема роботи: «Система перевірки контрагентів щодо зв'язку з підсанкційними країнами», керівник роботи: Лукічов Віталій Володимирович, к.т.н., доцент каф. ЗІ, затверджені наказом ректора ВНТУ №67 від 20 березня 2023 року.
2. Строк подання студентом роботи – 19 червня 2023 року
3. Вихідні дані до роботи:
   – технічне завдання надане ПрАТ СК «ПЗУ Україна»;
   – нормативно правові акти на яких базується санкційна політика України, а саме: Укази Президента України та рішення Ради національної безпеки і оборони України.
4. Зміст текстової частини: Вступ. Теоретичні аспекти системи перевірки контрагентів. Розробка та проектування програмного засобу. Розробка та реалізація перевірки. Висновки. Перелік використаних джерел. Додатки.
5. Перелік ілюстративного матеріалу: Графічна схема роботи системи перевірки контрагентів з підсанкційними країнами. Ілюстрація Технічного завдання. Ілюстрація процесу оновлення бази даних щодо санкційних списків. Графічний опис алгоритму перевірки контрагентів та їх зв'язків з підсанкційними країнами. Опис алгоритму програмного засобу. Оцінка виявленої вразливості. Лист для продавця який намагається реалізувати договір підсанкційному контрагенту. Лист з інформацією для фінансового моніторингу. Результат формування договору з підсанкційною особою. Результат SQL-ін'єкції як доказ правильності концепції (POC).

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
1	Лукічов В. В., к.т.н., доц. кафедри ЗІ	20.03.23	16.06.23
2	Лукічов В. В., к.т.н., доц. кафедри ЗІ	20.03.23	16.06.23
3	Лукічов В. В., к.т.н., доц. кафедри ЗІ	20.03.23	16.06.23

7. Дата видачі завдання – 20 березня 2023 року

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів бакалаврської дипломної роботи	Строк виконання етапів роботи	Приміт
1	Аналіз завдання. Вступ	20.03.23 – 26.03.23	
2	Інформаційний аналіз літературних джерел за напрямком бакалаврської дипломної роботи	27.03.23 – 09.04.23	
3	Технічний аналіз рішень, моделей, алгоритмів	10.04.23 – 23.04.23	
4	Опис та проектування засобу, результати	24.04.23 – 21.05.23	
5	Аналіз виконання ТЗ, висновки	22.05.23 – 24.05.23	
6	Оформлення пояснювальної записки	25.05.23 – 31.05.23	
7	Попередній захист та доопрацювання БДР	01.06.23 – 15.06.23	
8	Представлення БДР до захисту, рецензування	16.06.23 – 19.06.23	
9	Захист БДР	20.06.23 – 23.06.23	

Студент _____ Роман КУЙБІДА
(підпис)

Керівник роботи _____ Віталій ЛУКІЧОВ
(підпис)

АНОТАЦІЯ

Бакалаврська дипломна робота складається зі вступу, трьох розділів та висновків до них, загальних висновків, списку використаних джерел, додатків, загальним обсягом робота складає 66 сторінок, має 12 рисунків, 2 таблиці, 16 сторінок додатків. Список використаних джерел містить 24 найменувань

Бакалаврська дипломна робота присвячена розробці системи перевірки контрагентів щодо зв'язку з підсанкційними країнами. В роботі було проведено аналіз теоретичних аспектів системи перевірки контрагентів, включаючи поняття, значення для бізнесу та держави, а також нормативно-правове забезпечення.

Було розроблено та реалізовано програмний модуль, який включає архітектуру системи та захист від SQL-ін'єкцій. Проведені результати тестування підтвердили ефективність розробленої системи. Робота має важливе значення для бізнесу, оскільки допомагає уникнути правових порушень та фінансових санкцій, пов'язаних з недотриманням санкційного режиму.

Ключові слова: система перевірки контрагентів, підсанкційні країни, безпека, ефективність, кібербезпека.

ABSTRACT

The thesis consists of an introduction, three sections and conclusions to them, general conclusions, a list of used sources, appendices, the total volume of the work is 66 pages, has 12 figures, 2 table, 16 pages of appendices. The list of used sources contains 24 names.

The thesis is devoted to the development of a system for checking counterparties in connection with sanctioned countries. The paper analyzed the theoretical aspects of the counterparty verification system, including concepts, significance for business and the state, as well as regulatory and legal support.

A software tool that includes system architecture and SQL-injection protection was developed and implemented. The test results confirmed the effectiveness of the developed system. The work is important for business, as it helps to avoid legal violations and financial sanctions associated with non-compliance with the sanctions regime.

Key words: contractor verification system, sanctioned countries, security, efficiency, cybersecurity.

ЗМІСТ

ВСТУП

Актуальність. У сучасних умовах глобалізації та зростання міжнародної торгівлі виникає необхідність у забезпеченні безпеки та стійкості економіки держави. Одним із основних напрямів у боротьбі зі злочинністю та фінансуванням тероризму є контроль за здійсненням зовнішньоекономічної діяльності з підсанкційними країнами. Тому розробка та впровадження системи перевірки контрагентів на предмет зв’язку з підсанкційними країнами є актуальною проблемою для бізнесу та держави.

Покращення безпеки підприємства шляхом реалізації системи перевірки контрагентів та за допомогою розробки рекомендацій щодо попередження SQL атак з метою забезпечення безпеки зовнішньоекономічної діяльності та запобігання відмиванню коштів та фінансуванню тероризму. В ході дослідження будуть проаналізовані існуючі підходи до перевірки контрагентів, розглянуті законодавчі акти та регуляторні документи в галузі зовнішньоекономічної діяльності та санкцій, а також запропоновані рекомендації щодо покращення існуючої системи перевірки контрагентів.

Результати дослідження можуть бути корисними для компаній, які займаються зовнішньоекономічною діяльністю, а також для державних органів, які здійснюють контроль за зовнішньоекономічною діяльністю та боротьбу зі злочинністю та фінансуванням тероризму.

З метою забезпечення безпеки зовнішньоекономічної діяльності та запобігання відмиванню коштів та фінансуванню тероризму, в деяких країнах світу було запроваджено санкції проти деяких держав та їх компаній, які мають зв’язок з цими державами. Санкції можуть обмежувати ввезення та вивезення товарів, фінансові транзакції, інвестиції та інші види зовнішньоекономічної діяльності.

У зв'язку з цим, контроль за здійсненням зовнішньоекономічної діяльності з підсанкційними країнами є особливо важливим. Недотримання санкцій може

призвести до значних фінансових втрат, погіршення репутації компанії, а також до порушення законодавства та кримінальної відповідальності.

Однак, забезпечення контролю за зовнішньоекономічною діяльністю з підсанкційними країнами може бути складним завданням. Контрагенти можуть використовувати різні способи для ухилення від перевірки, наприклад, шляхом зміни найменування компанії або місця реєстрації.

Тому відповідальність за забезпечення контролю за зовнішньоекономічною діяльністю з підсанкційними країнами лежить як на бізнес-середовищі, так і на державних органах. Компанії повинні розробляти та впроваджувати ефективні системи перевірки контрагентів на предмет зв'язку з підсанкційними країнами.

Метою є покращення безпеки підприємства шляхом реалізації системи перевірки контрагентів та за допомогою розробки рекомендацій щодо попередження SQL атак.

Для досягнення мети дослідження будуть розглянуті такі завдання:

- Аналіз ТЗ ПрАТ СК «ПЗУ Україна» щодо реалізації системи безпеки.
- Аналіз нормативно-правового забезпечення та наслідків недотримання санкційного режиму.
- Формування робочої моделі перевірки контрагентів.
- Реалізація методу перевірки контрагентів на рівні БД.
- Аналіз вразливості БД до SQL-ін'єкцій.

1 ТЕОРЕТИЧНІ АСПЕКТИ СИСТЕМИ ПЕРЕВІРКИ КОНТРАГЕНТІВ

1.1 Поняття системи перевірки контрагентів

Система перевірки контрагентів є важливим інструментом для бізнесу та держави, який дозволяє забезпечувати дотримання вимог щодо ділової активності та взаємодії з партнерами. Вона передбачає використання певного набору принципів, етапів, методів та засобів, які допомагають перевіряти відповідність потенційних або діючих контрагентів встановленим вимогам та критеріям [1].

Система перевірки контрагентів включає в себе ряд процедур, які дозволяють отримувати та аналізувати інформацію про різні аспекти діяльності контрагентів, такі як юридичний статус, фінансова стійкість, репутація, ділова активність, рівень відповідності законодавству, наявність зв'язків з підсанкційними країнами та інші фактори, що можуть вплинути на ризики взаємодії з контрагентом.

Одним з ключових аспектів системи перевірки контрагентів є встановлення принципів та критеріїв, за якими проводиться оцінка контрагентів. Ці принципи можуть бути внутрішніми для організації або встановлюватися законодавством та регуляторними органами [2]. Важливо також мати чітко визначені етапи перевірки, включаючи збір, аналіз та оцінку інформації про контрагента.

Для реалізації системи перевірки контрагентів використовуються різноманітні методи та засоби. Це можуть бути внутрішні ресурси організації, які включають в себе внутрішні бази даних, аналітичні інструменти, процедури перевірки документів та зв'язків контрагента. Також використовуються зовнішні джерела інформації, такі як реєстри державних органів, бази даних фінансової звітності, відгуки клієнтів, довідкові системи тощо.

При розробці системи перевірки контрагентів враховуються різні фактори, такі як ризики взаємодії з певними контрагентами, наявність регуляторних вимог, специфіка галузі діяльності організації та її стратегія розвитку. Крім того,

в систему можуть бути включені механізми моніторингу контрагентів під час взаємодії з ними на протязі усього терміну співпраці.

Одним із важливих аспектів системи перевірки контрагентів є виявлення зв'язків контрагентів з підсанкційними країнами. Це включає встановлення процедур перевірки наявності бізнес-зв'язків, фінансових транзакцій, власності чи керівництва контрагента в країнах, які перебувають під санкціями міжнародних організацій чи окремих країн [3]. Для цього можуть використовуватися різноманітні джерела інформації, такі як міжнародні реєстри санкцій, бази даних регуляторних органів, засоби моніторингу ринків тощо.

Система перевірки контрагентів є невід'ємною частиною ділової активності та має важливе значення як для бізнесу, так і для держави. Вона допомагає забезпечити дотримання вимог щодо ділової етики, визначених законодавством та стандартами.

Система перевірки контрагентів передбачає використання різних принципів, етапів, методів та засобів, щоб гарантувати відповідність потенційних або діючих контрагентів вимогам та критеріям. Наприклад, це можуть бути принципи екологічної сталості, дотримання прав праці, етичної поведінки, фінансової надійності та інші [4].

Процес перевірки контрагентів включає ретельний збір та аналіз інформації про їхню ділову активність. Це охоплює перевірку юридичного статусу, фінансового здоров'я, історії роботи, репутації та додержання законодавства. Для цього можуть використовуватися інструменти, такі як бази даних, публічно доступна інформація, звіти про фінансовий стан, аналіз ринку та інші джерела.

Оцінка контрагента здійснюється на основі встановлених критеріїв та принципів. Це допомагає визначити, наскільки контрагент відповідає встановленим вимогам та рівню ризику, пов'язаному з його співпрацею. Результати оцінки допомагають прийняти обґрунтовані рішення щодо співпраці з потенційними контрагентами.

Для реалізації системи перевірки контрагентів використовуються різноманітні методи та засоби.

Це можуть бути автоматизовані системи, програмні комплекси, сервіси моніторингу, аналітичні інструменти, а також спеціалістів з відповідною кваліфікацією. Використання сучасних технологій та інноваційних підходів дозволяє підвищити ефективність та точність процесу перевірки контрагентів.

Загальновизнаним фактом є необхідність уваги до виявлення зв'язків контрагентів з підсанкційними країнами. Це сприяє запобіганню порушень санкційних обмежень та мінімізації ризиків, пов'язаних зі співпрацею з такими контрагентами. Для цього використовуються спеціалізовані ресурси та інструменти, які дозволяють виявляти наявність зв'язків контрагентів з підсанкційними суб'єктами.

Організації та держави вкладають значні зусилля у створення ефективних систем перевірки контрагентів, щоб забезпечити безпеку, зменшити ризики та підвищити надійність бізнес-взаємодії [5]. Це допомагає створити сприятливе середовище для розвитку ділових стосунків та зміцнення довіри між сторонами.

Окрема увага приділяється виявленню зв'язків контрагентів з підсанкційними країнами, що є актуальною проблемою в сучасному бізнес-середовищі. Описано процедури та механізми, які можуть бути використані для перевірки наявності бізнес-зв'язків, фінансових транзакцій та власності контрагента в країнах, які перебувають під санкціями. Зазначено важливість використання різноманітних джерел інформації для досягнення максимальної ефективності системи перевірки контрагентів щодо зв'язку з підсанкційними країнами.

Система перевірки контрагентів щодо зв'язку з підсанкційними країнами є важливим елементом в сучасному бізнес-середовищі, оскільки дозволяє забезпечити відповідність вимогам регуляторних органів та міжнародних санкційних режимів [6]. Розробка ефективної системи перевірки контрагентів включає врахування різних аспектів, таких як внутрішні та зовнішні джерела інформації, процедури перевірки документів та зв'язків контрагента.

Використання різноманітних джерел інформації, таких як бази даних, реєстри, відкриті джерела, а також використання технологій аналізу даних, може підвищити ефективність системи перевірки контрагентів щодо зв'язку з підсанкційними країнами.

Розробка процедур та механізмів для виявлення зв'язків контрагентів з підсанкційними країнами є важливим аспектом системи перевірки контрагентів. Це дозволяє уникнути потенційних ризиків взаємодії з контрагентами, які мають зв'язки з країнами, які перебувають під санкціями [7].

Аналіз ризиків, пов'язаних з взаємодією з контрагентами з підсанкційних країн, демонструє важливість ретельного вивчення можливих наслідків такої взаємодії, включаючи фінансові ризики, репутаційні ризики та ризики відповідності законодавству.

1.2 Значення системи перевірки контрагентів для бізнесу та держави

Система перевірки контрагентів має важливе значення як для бізнесу, так і для держав, оскільки вона допомагає в забезпеченні відповідності законодавству, зменшенні ризиків та забезпеченні безпеки бізнес-операцій. Ось кілька прикладів та порівнянь із реальними ситуаціями в різних країнах світу:

Бізнес-аспект: У багатьох країнах світу, бізнес-суб'єкти зобов'язані перевіряти своїх контрагентів з метою виявлення можливих зв'язків з підсанкційними країнами. Наприклад, в Сполучених Штатах Америки, система перевірки контрагентів (наприклад, програма "Office of Foreign Assets Control" – OFAC) використовується для виявлення заборонених торгівельних відносин з країнами, які перебувають під санкціями, такими як Іран, Кримський півострів тощо. Бізнес-суб'єкти мають використовувати цю систему для перевірки своїх контрагентів, щоб уникнути можливих фінансових, репутаційних та правових ризиків [8].

Державний аспект: Для держав також важливо мати ефективну систему перевірки контрагентів для забезпечення національної безпеки та виконання міжнародних зобов'язань. Наприклад, Європейський Союз має систему

перевірки контрагентів (наприклад, "Єдина база даних фінансових санкцій ЄС") для виявлення фінансових та економічних зв'язків контрагентів з країнами, які перебувають під санкціями або терористичними організаціями. Це допомагає державам забезпечувати ефективний контроль над фінансовими операціями та запобігати фінансуванню тероризму та іншої незаконної діяльності [9].

Порівняно з різними країнами світу, системи перевірки контрагентів можуть мати свої особливості та рівень розвиненості. Наприклад, в ряді країн системи перевірки контрагентів є обов'язковими та вимагаються від усіх бізнес-суб'єктів, які здійснюють торговельні операції. У деяких країнах системи перевірки контрагентів можуть бути регульовані законодавством та підконтрольні відповідним відомствам, в той час як у інших країнах це може бути рекомендаційними заходами [10].

Значення системи перевірки контрагентів може бути важливим також для захисту інтересів бізнесу в умовах зростаючої кіберзагрози. Часті випадки кібератак, включаючи фішинг, рейдерство, витік інформації та інші, можуть негативно впливати на бізнес, включаючи фінансові втрати, втрату репутації та відсутність довіри серед контрагентів. Ефективна система перевірки контрагентів, яка враховує різні аспекти безпеки, такі як кібербезпека, може допомогти бізнесу відповідно захищати свої інтереси та забезпечувати безпечну взаємодію з контрагентами.

Правильна та ефективна система перевірки контрагентів є необхідною для захисту бізнесу та держави від потенційних загроз і ризиків. Національні органи регулювання та міжнародні організації активно співпрацюють для розвитку стандартів та спільних підходів до перевірки контрагентів.

Один з глобальних трендів, пов'язаних з системами перевірки контрагентів, полягає в зростанні використання технологій штучного інтелекту та машинного навчання [11]. Це дозволяє автоматизувати процеси перевірки, забезпечити швидку і точну ідентифікацію контрагентів та виявлення потенційних ризиків. Наприклад, розпізнавання обличь, аналіз поведінки та інші

технології можуть допомогти виявити незаконну діяльність або зв'язки з підсанкційними суб'єктами.

Окрім того, важливо зазначити, що системи перевірки контрагентів також мають розширений вплив на фінансовий сектор. Банки, фінансові установи та інші фінансові посередники активно використовують системи перевірки контрагентів для дотримання вимог Анти бланшування грошей та протидії фінансуванню тероризму. Це сприяє забезпеченню фінансової стабільності та зменшенню ризиків фінансових маніпуляцій [12].

Поняття "зелена перевірка контрагентів" стає все більш актуальним у світлі росту інтересу до сталого розвитку та екологічної відповідальності. Деякі країни та організації вимагають включення додаткових критеріїв перевірки контрагентів, які стосуються дотримання екологічних та соціальних стандартів. Це дозволяє бізнесу співпрацювати лише з партнерами, що відповідають вимогам сталого розвитку, та сприяє збереженню навколишнього середовища.

У світі постійно змінюються політичні, економічні та соціальні умови, що ставить перед бізнесом та державами нові виклики у сфері перевірки контрагентів. Адаптація до цих змін та постійне вдосконалення систем перевірки є важливими елементами забезпечення успішної та безпечної бізнес-діяльності в сучасному світі.

На прикладі ряду країн світу, таких як США, Канада, ЄС та інші, можна побачити, що наявність ефективних систем перевірки контрагентів є необхідним елементом ділового клімату та економічного розвитку. Вони допомагають забезпечити відповідність вимогам фінансової діяльності, зменшити ризик фінансових злочинів, підвищити довіру між бізнес-партнерами та державними органами, а також забезпечити безпеку бізнес-операцій.

При налагодженні бізнес-відносин з контрагентами важливо проводити ретельну перевірку їх надійності, репутації, фінансової стійкості, технічних здібностей та досвіду роботи.

Приклади з різних країн світу показують, що недостатня перевірка контрагентів може призвести до серйозних наслідків, таких як втрати фінансових

коштів, втрата репутації, відкликання продукції, штрафи, судові позови та інші негативні наслідки для бізнесу.

Різні види бізнесу можуть постраждати від недобросовісних контрагентів, включаючи виробників, постачальників, експортерів, підрядників та інших. Наприклад, це можуть бути виробники товарів, які можуть стати небезпечними для споживачів через недоліки в комплектуючих, ресторани, які можуть постраждати від постачальників непридатних продуктів, або IT-компанії, які можуть стикнутися з проблемами від ненадійних підрядників.

Важливо вести постійний моніторинг контрагентів під час усього періоду співпраці, оскільки вони можуть змінити свій статус, фінансову стійкість або репутацію в майбутньому [13]. Отже, система перевірки контрагентів має велике значення для бізнесу та держави.

Ефективні системи перевірки контрагентів також відіграють важливу роль у боротьбі зі злочинністю і корупцією. У світі існують численні приклади, коли недобросовісні контрагенти зловживають своїм статусом і завдають шкоди як бізнесу, так і економіці країни в цілому.

США є однією з країн, яка добре розвинула системи перевірки контрагентів. Наприклад, вони мають комплексну програму відому як "Запобігання фінансуванню тероризму" (AML – Anti-Money Laundering), яка вимагає від фінансових установ проводити детальну перевірку клієнтів та контрагентів, щоб уникнути фінансування терористичних організацій [24].

У країнах Європейського Союзу також існують суворі вимоги до перевірки контрагентів. Наприклад, згідно з Директивою ЄС про боротьбу зі шахрайством, підробкою та контрафакцією (Directive on Combating Fraud and Counterfeiting), бізнес-партнери повинні бути перевірені щодо своєї надійності та репутації, а також забезпечувати належну захист інтелектуальної власності [16].

У Канаді, зокрема, існує програма "Забезпечення безпеки постачальників" (Secure Supplier Program), яка забезпечує перевірку постачальників на відповідність стандартам безпеки та якості. Ця програма спрямована на захист внутрішнього ринку від шкідливих та небезпечних продуктів.

Однак, варто зазначити, що система перевірки контрагентів має свої виклики і обмеження. Наприклад, у деяких країнах можуть відсутні деталізовані бази даних або ефективні механізми співпраці між різними органами контролю [9]. Це може ускладнити процес перевірки та зробити його менш надійним.

Усунення таких недоліків і покращення систем перевірки контрагентів є постійним завданням для бізнесу та держав. Розвиток технологій, використання штучного інтелекту та блокчейн-технологій можуть допомогти покращити процес перевірки та забезпечити більш точну та швидку інформацію про контрагентів.

Загалом, наявність ефективних систем перевірки контрагентів є критично важливою для розвитку бізнесу та забезпечення безпеки. Продовження зусиль у цьому напрямку сприятиме покращенню ділового клімату, зменшенню ризиків та створенню сприятливих умов для стабільного економічного росту.

1.3 Основні принципи та етапи системи перевірки контрагентів

В сучасних умовах глобалізації та розвитку бізнесу важливим аспектом є взаємодія з різними контрагентами. Однак, це також може вносити ризики, пов'язані з вибором недобросовісних або ненадійних партнерів. Саме тому система перевірки контрагентів є важливим елементом бізнес-стратегії, що дозволяє забезпечити безпеку та стабільність у відносинах з партнерами.

Мета цього розділу – розглянути основні принципи та етапи системи перевірки контрагентів, які допомагають бізнесу забезпечити вибір надійних та відповідних вимогам партнерів, знизити ризики та захистити свої інтереси.

Основні принципи системи перевірки контрагентів:

1) Об'єктивність: система перевірки контрагентів має базуватися на об'єктивних критеріях та джерелах інформації, таких як офіційні реєстри, фінансові звіти, репутація на ринку, досвід роботи тощо. Об'єктивність дозволяє уникнути суб'єктивного підходу та забезпечити більш точну оцінку потенційного контрагента.

2) Комплексність: система перевірки контрагентів має охоплювати різні аспекти, такі як фінансова стійкість, репутація, досвід роботи, наявність ліцензій та дозволів, кадровий потенціал тощо. Комплексний підхід дозволяє отримати більш повну та об'єктивну картину про контрагента.

3) Систематичність: система перевірки контрагентів має бути систематичною та постійною, забезпечуючи регулярні оновлення інформації про партнерів. Це дозволяє вчасно виявляти зміни в ризиках або стані контрагента, що може впливати на його надійність.

4) Конфіденційність: одним із важливих принципів системи перевірки контрагентів є забезпечення конфіденційності інформації, зокрема персональних даних та комерційних таємниць контрагента. Це дозволяє дотримуватися законодавства про захист даних та уникати можливих правових порушень.

Етапи системи перевірки контрагентів:

1) Збір інформації: перший етап системи перевірки контрагентів – це збір різноманітної інформації про потенційного контрагента з різних джерел, таких як офіційні реєстри, бази даних, довідники, фінансові звіти, репутаційні джерела тощо [26].

2) Аналіз інформації: наступний етап – це аналіз зібраної інформації з використанням об'єктивних критеріїв, враховуючи важливі аспекти, такі як фінансова стійкість, репутація, досвід роботи, наявність ліцензій та дозволів, кадровий потенціал тощо [14].

3) Валідація інформації: після аналізу інформації, наступний етап – це валідація, тобто перевірка достовірності та актуальності інформації, наприклад, через перевірку документів, контактування з постачальником, співпрацею зі спеціалізованими агентствами тощо [15].

4) Оцінка ризиків: оцінка ризиків є важливим етапом системи перевірки контрагентів. На цьому етапі визначаються можливі ризики, пов'язані з партнерством з даним контрагентом, такі як фінансовий ризик, репутаційний ризик, правовий ризик, ризик відповідності законодавству, ризик можливої втрати довіри клієнтів тощо.

5) Прийняття рішення: на основі аналізу і валідації інформації, а також оцінки ризиків, наступний етап – це прийняття рішення щодо встановлення або продовження співпраці з контрагентом. Враховуються всі аспекти, включаючи ризики та можливості, та здійснюється виважене рішення з метою зниження ризиків та забезпечення надійності партнерства.

6) Моніторинг: останній етап системи перевірки контрагентів – це постійний моніторинг діяльності контрагента під час співпраці. Це може включати періодичні оновлення інформації, внутрішні аудити, аналіз змін в стані контрагента, репутаційний моніторинг та інші заходи для виявлення можливих ризиків на ранніх етапах [16].

Ось кілька реальних прикладів того, як етапи системи перевірки контрагентів можуть допомогти бізнесу забезпечити вибір надійних та відповідних вимогам партнерів, знизити ризики та захистити свої інтереси:

Фінансовий ризик: при оцінці фінансового стану потенційного контрагента, бізнес може використовувати етапи системи перевірки контрагентів, такі як збір фінансової звітності, аналіз фінансових показників, порівняння з ринковими стандартами та оцінка ризиків дефолту [19]. Наприклад, компанія може виявити фактичну фінансову нестабільність потенційного контрагента, таку як високий рівень боргів, неплатоспроможність або нездатність розраховуватися з постачальниками, що може свідчити про високий фінансовий ризик. Таким чином, бізнес може прийняти рішення про відмову від співпраці з таким контрагентом, щоб захистити свої фінансові інтереси.

Репутаційний ризик: збір інформації про репутацію потенційного контрагента може бути важливим етапом системи перевірки контрагентів. Бізнес може провести дослідження стосовно репутації контрагента на ринку, включаючи відгуки клієнтів, рейтинги, репутаційні конфлікти тощо. Наприклад, якщо компанія виявляє, що потенційний контрагент має погану репутацію, таку як погане обслуговування клієнтів, неадекватне виконання угод, часті скарги від клієнтів, це може бути ознакою висок репутаційного ризику. Бізнес може

вирішити відмовитися від співпраці з таким контрагентом, щоб уникнути можливих проблем і зберегти свою репутацію.

Правовий ризик: етапи системи перевірки контрагентів також можуть включати перевірку правової діяльності потенційного контрагента, такої як наявність ліцензій, дозволів, стану юридичної реєстрації тощо. Наприклад, бізнес може виявити, що потенційний контрагент має неповний набір необхідних документів, порушення законодавства або наявність судових позовів. Це може свідчити про правовий ризик і може допомогти бізнесу прийняти рішення щодо подальшої співпраці з таким контрагентом, забезпечивши захист своїх інтересів.

Виробничий ризик: бізнес може використовувати етапи системи перевірки контрагентів, пов'язані з виробничим процесом, якщо потенційний контрагент є постачальником сировини, матеріалів або продукції. Наприклад, компанія може перевірити дотримання контрагентом вимог стандартів якості, наявність сертифікатів відповідності, технічних специфікацій та інших виробничих документів. Це може допомогти бізнесу забезпечити вибір надійних партнерів, знизити ризики виробничих невдач та забезпечити високу якість своїх виробів.

Інформаційний ризик: перевірка потенційних контрагентів на наявність витоку чи незаконного використання інформації також може бути важливим етапом системи перевірки контрагентів. Бізнес може перевірити рівень конфіденційності та захисту інформації у контрагента, його історію взаємодії з попередніми партнерами, наявність порушень інтелектуальної власності, а також дотримання правил захисту персональних даних. Наприклад, бізнес може виявити, що потенційний контрагент не має відповідних заходів безпеки, вчасно не оновлює програмне забезпечення або не дотримує правил захисту персональних даних, що може призвести до витоку інформації або інших інформаційних ризиків.

Ці приклади демонструють, як етапи системи перевірки контрагентів можуть допомогти бізнесу забезпечити вибір надійних та відповідних вимогам партнерів, знизити ризики в різних аспектах, таких як фінансовий, репутаційний, правовий, виробничий та інформаційний. Це може допомогти бізнесам

забезпечити стабільну та безпечну співпрацю з контрагентами, захистити свої інтереси, запобігти можливим проблемам та зберегти свою репутацію на ринку.

Для ефективної системи перевірки контрагентів щодо зв’язку з підсанкційними країнами можна використовувати різноманітні методи та засоби. Нижче наведено кілька прикладів таких методів та засобів з використанням реальних прикладів для більшої ясності.

Аналіз списків санкцій. Один з основних методів перевірки контрагентів на зв’язок з підсанкційними країнами – це аналіз списків санкцій, які публікується офіційними органами влади, такими як Уряд США, Європейський Союз, ООН та інші. Ці списки містять інформацію про фізичних та юридичних осіб, які перебувають під санкціями, а також про компанії, організації та країни, з якими заборонено вести бізнес через введені санкції. Прикладом може бути "Список осіб та організацій, з якими заборонено вести бізнес" Міністерства фінансів США, що містить інформацію про фізичних осіб, які перебувають під санкціями, та компанії, які мають зв’язок з підсанкційними країнами.

Перевірка засобами відкритого джерела. Використання засобів відкритого джерела, таких як Інтернет, бази даних, соціальні мережі, друковані видання та інші, може бути ефективним методом перевірки контрагентів.

Аналітичні інструменти та технології. Використання аналітичних інструментів та технологій, таких як штучний інтелект, машинне навчання, аналітика даних та інші, може допомогти в ефективному виявленні зв’язку контрагентів з підсанкційними країнами. Наприклад, за допомогою алгоритмів машинного навчання можна аналізувати великі обсяги даних, такі як фінансові звіти, транзакційні дані, відгуки клієнтів тощо, для виявлення підозрілих взаємозв'язків або шаблонів, що можуть свідчити про зв’язок з підсанкційними країнами.

Додатково, можна використовувати інші методи та засоби, такі як:

- Офіційні запити до контрагентів. Запитувати від контрагентів офіційну інформацію щодо їх бізнес-діяльності та зв'язків з підсанкційними країнами, такі як відомості про власників, ділові партнери, ринки збуту, постачальників тощо.

- Перевірка наявності ліцензій та сертифікатів. Перевірка наявності відповідних ліцензій, сертифікатів та інших документів, які регулюють діяльність контрагента в певній галузі або регіоні. Наприклад, якщо контрагент займається міжнародним експортом, то він повинен мати відповідні дозволи та ліцензії від компетентних органів [17].
- Перевірка репутації. Дослідження репутації контрагента, включаючи відгуки клієнтів, рейтинги та рекомендації від інших бізнес-партнерів, відомості про раніше виявлені випадки порушення законодавства або участі в санкційних справах. Це можна зробити шляхом пошуку в Інтернеті, використання спеціалізованих репутаційних агентств або баз даних, що містять інформацію про компанії та їхніх власників.

Можна зазначити, що важливість перевірки контрагентів на зв'язки з підсанкційними країнами не може бути переоцінена. Дієвий механізм перевірки контрагентів може допомогти компаніям уникнути ризиків порушення санкцій, штрафів та інших негативних наслідків.

У процесі перевірки контрагентів рекомендується використовувати різноманітні джерела інформації, такі як публічні бази даних, списки санкцій, аналіз географічних ризиків та експертну оцінку. Комбінування різних методів може забезпечити більш повну та об'єктивну оцінку зв'язків контрагентів з підсанкційними країнами.

Крім того, важливо дотримуватись відповідних законодавчих вимог та внутрішніх процедур компанії щодо перевірки контрагентів, а також забезпечувати захист конфіденційності та обробки персональних даних під час проведення таких перевірок.

На основі аналізу інформації та використання різних методів перевірки контрагентів, компанії можуть зменшити ризики відносин з підсанкційними країнами та забезпечити дотримання відповідних законодавчих вимог.

Додатково, важливо регулярно оновлювати інформацію про підсанкційні країни та списки санкцій, оскільки вони можуть змінюватись з часом. Компанії

можуть встановити механізми моніторингу змін в списку підсанкційних країн та оновлювати свої процедури перевірки відповідно.

Крім того, важливо мати проактивний підхід до перевірки контрагентів, зокрема при укладанні нових договорів або продовженні існуючих. Перевірка контрагентів перед встановленням ділових відносин може забезпечити зниження ризиків та захист від можливих наслідків порушення санкцій.

Загалом, система перевірки контрагентів на зв'язок з підсанкційними країнами має бути комплексною, з використанням різноманітних методів та засобів, що дозволяють отримати максимально об'єктивну оцінку ризиків. Забезпечення дотримання відповідних законодавчих вимог та внутрішніх процедур, регулярне оновлення інформації та проактивний підхід до перевірки контрагентів можуть допомогти компаніям ефективно управляти ризиками, пов'язаними з підсанкційними країнами, та забезпечити виконання вимог відповідних регуляторних органів.

1.4 Нормативно-правове забезпечення та наслідки недотримання санкційного режиму

24 лютого 2022 року розпочалось повномасштабне вторгнення російської федерації на територію України. Однак, крім збройної агресії, російська федерація використовує інші методи заподіяння шкоди нашій державі, а саме через своїх представників здійснює підривну діяльність проти України, зокрема і в економічній сфері.

Уже неодноразово Президент України за поданням Ради національної безпеки та оборони України на підставі Закону України «Про санкції» з метою захисту національних інтересів, національної безпеки, суверенітету і територіальної цілісності України запроваджував санкції щодо фізичних та юридичних осіб, які провадять вказану підривну діяльність відносно нашої держави [18].

Однак трапляються непоодинокі випадки, коли вищевказані особи ухиляються від накладених на них санкцій самостійно або з допомогою інших осіб.

Враховуючи ці обставини, з метою притягнення до кримінальної відповідальності осіб, які порушують встановлені приписи Закону України «Про санкції» та допомагають особам, на яких накладено, уникати їх наслідків, народними депутатами України було зареєстровано у Верховній Раді України проєкт Закону № 8384 від 25.01.2023 «Про внесення змін до Кримінального та Кримінального процесуального кодексів України та інших законів щодо встановлення кримінальної відповідальності за порушення законодавства про санкції» [19].

Цей законопроєкт передбачає доповнення Особливої частини Кримінального кодексу України (КК України) новою статтею, а саме ст. 111-3 КК України «Порушення вимог законодавства про санкції».

Відповідно до редакції проєкту Закону ст. 111-3 КК України буде передбачати, що невиконання, перешкоджання виконанню або ухилення від виконання спеціальних економічних та/або інших обмежувальних заходів (санкцій) буде каратись штрафом від десяти до п’ятнадцяти тисяч неоподатковуваних мінімумів доходів громадян або позбавленням волі на строк від п’яти до семи років із конфіскацією майна або без неї.

Кваліфікувальними ознаками цього кримінального правопорушення пропонують вказати такі:

- діяння, вчинене повторно, або за попередньою змовою групою осіб, або у значному розмірі;
- діяння, вчинене службовою особою або особою, яка провадить професійну діяльність, пов’язану з наданням публічних послуг (аудиторами, нотаріусами, приватними виконавцями, оцінювачами, а також експертами, арбітражними керуючими, незалежними посередниками, членами трудового арбітражу, третейськими суддями під час виконання ними цих функцій), або у великому розмірі;

– діяння, вчинене службовою особою, яка займає відповідальне становище, або організованою групою;
– діяння, вчинене службовою особою, яка займає особливо відповідальне становище, або злочинною організацією, або в особливо великому розмірі.

Крім того, це кримінальне правопорушення пропонують передати у підслідність органів Служби безпеки України з можливість проведення спеціального досудового розслідування.

Однак важливо зазначити, що об'єктивна сторона кримінального правопорушення за запропонованою редакцією ст. 111-3 КК України, яка зазначена в законопроєкті, має доволі широке і нечітке формулювання. З огляду на це є підстави вважати, що суб'єктами «порушення вимог» законодавства про санкції слід визнавати як осіб, щодо яких застосовуються санкції, так і осіб, уповноважених застосовувати відповідні санкції та/або забезпечувати їх виконання.

Однак для належного застосування зазначеної статті Кримінального кодексу України потрібно враховувати, що ці норми є вторинними (похідними) від норм законодавства, що регулюють порядок запровадження санкцій.

Саме ж регулятивне законодавство України, яке регулює запровадження санкцій та необхідне для належної кваліфікації діяння, за новою статтею КК України містить у собі певну суперечність.

Так, наприклад, згідно з Указом Президента України від 7 січня 2023 року № 4/2023 окремі артисти були позбавлені державних нагород, однак відповідно до ст. 16 Закону України «Про державні нагороди України» позбавлення державних нагород можливе лише в разі засудження нагородженого за тяжкий злочин за поданням суду у випадках, передбачених законом [20].

В будь якому випадку покарання за порушення санкційного режиму може бути доволі суворим, що є безумовним додатковим стимулом убезпечити бізнес від таких наслідків. Так, згідно з редакцією ч. 1 ст. 111-3 КК України за невиконання, перешкоджання виконанню або ухилення від виконання

спеціальних економічних та/або інших обмежувальних заходів (санкцій) пропонується передбачити позбавлення волі на строк від п’яти до семи років.

Важливо зазначити, що подібна міра покарання передбачена за такі кримінальні правопорушення, як вбивство двох або більше осіб, вчинене через необережність (ч. 1 ст. 119 КК України); умисне тяжке тілесне ушкодження (ч. 1 ст. 121 КК України); сексуальне насильство, вчинене групою осіб, або сексуальне насильство щодо неповнолітньої особи (ч. 3 ст. 153 КК України).

Підсумовуючи викладене, зазначимо, що сама можливість притягнення осіб, які порушують запроваджені санкції, є дієвим інструментом захисту національних інтересів, національної безпеки, суверенітету і територіальної цілісності України.

2 РОЗРОБКА ТА ПРОЕКТУВАННЯ ПРОГРАМНОГО ЗАСОБУ

2.1 Розбір та аналіз технічного завдання від ПрАТ СК «ПЗУ Україна»

Перевірка на наявність в списках осіб причетних до Російської Федерації (далі РФ) та Республіки Білорусь (далі РБ) стає все більш важливим елементом систем перевірки контрагентів у різних країнах світу. Недавні події та геополітичні реалії підкреслюють необхідність таких перевірок, які спрямовані на запобігання можливим ризикам та забезпечення безпеки бізнесу [21].

Необхідність проведення перевірки на наявність осіб, причетних до РФ та РБ, стосується не лише страхувальників, але і всіх учасників договору. Це важливо, оскільки особи, причетні до цих країн, можуть мати певну впливовість, політичні зв'язки або займати посади, що можуть впливати на ведення бізнесу або фінансові операції. Такі перевірки допомагають уникнути можливих конфліктів і протидіяти ризикам, пов'язаним зі зловживанням владою або небажаною політичною втручанням.

Різні країни мають різні підходи до проведення перевірок контрагентів на наявність осіб, причетних до РФ та РБ. Деякі країни встановлюють обов'язкові правила і процедури для таких перевірок, вимагаючи від бізнес-партнерів детальної інформації про їх зв'язки та контакти з цими країнами. Інші країни можуть застосовувати ризик-орієнтовані підходи, зосереджуючись на специфічних секторах або типах бізнесу, які мають більшу ймовірність зустрічі з ризиковими контрагентами [22].

Крім того, важливо враховувати, що список осіб, причетних до РФ та РБ, може змінюватися з часом. Політичні, економічні та соціальні зміни в цих країнах можуть призвести до змін у списку осіб, які підлягають перевірці. Тому регулярне оновлення та моніторинг цих списків є важливою складовою ефективної системи перевірки контрагентів.

У світлі зростаючої важливості перевірки контрагентів на наявність осіб, причетних до РФ та РБ, багато компаній та організацій звертаються до спеціалізованих провайдерів послуг, які надають інструменти та експертну

підтримку в цьому процесі. Такі провайдери можуть забезпечити доступ до актуальних списків, здійснювати детальну перевірку контрагентів та надавати звіти та рекомендації з питань безпеки та ризик-управління.

Отже, перевірка на наявність осіб, причетних до РФ та РБ, стає необхідним елементом систем перевірки контрагентів для забезпечення безпеки, ризик-управління та попередження можливих негативних наслідків для бізнесу [26]. Застосування ефективних практик та спеціалізованих інструментів допомагає підвищити рівень довіри, зменшити ризики та створити сприятливі умови для стабільного економічного розвитку.

Нижче наведено список і типи осіб учасників:

- страхувальники;
- власники (в договорах КАСКО Автомікс інформація про власника проходить перевірку, якщо власник має статус фізична особа/ФОП/юридична особа);
- вигодонабувачі (ідентично до власника – фіз. Особа/ФОП/ юр. особа)
- всі застраховані особи.

Також для ідентифікації підсанкційних учасників договору повинні використовуватись такі критерії: для юридичних осіб – співпадіння по ЄДРПОУ або в разі відсутності інформації про ЄДРПОУ – повне співпадіння назви; для фізичних осіб це повне співпадіння імені, прізвища та дати народження.

Перевірка має відбуватись постійно в режимі реального часу. Для нових клієнтів: при внесені даних у QWINS (Quick Insurance), для вже існуючих (діючих клієнтів) – при редагуванні даних у QWINS. А також щомісячно, на початку або в кінці робочого дня. Конкретні вимоги описані в файлі технічного завдання який був доданий до заявки в Service Desk, першу сторінку якого наведено на рис 2.1. Це формалізована збірка вимог для реалізації модулю перевірки, в якій описані всі важливі аспекти і зміни, які мають бути реалізовані в вигляді модулю перевірки контрагентів і які є основою на якій базується загальне покращення системи безпеки ПЗУ Україна при роботі зі всіма контрагентами (як і вже існуючими клієнтами, так і новими)

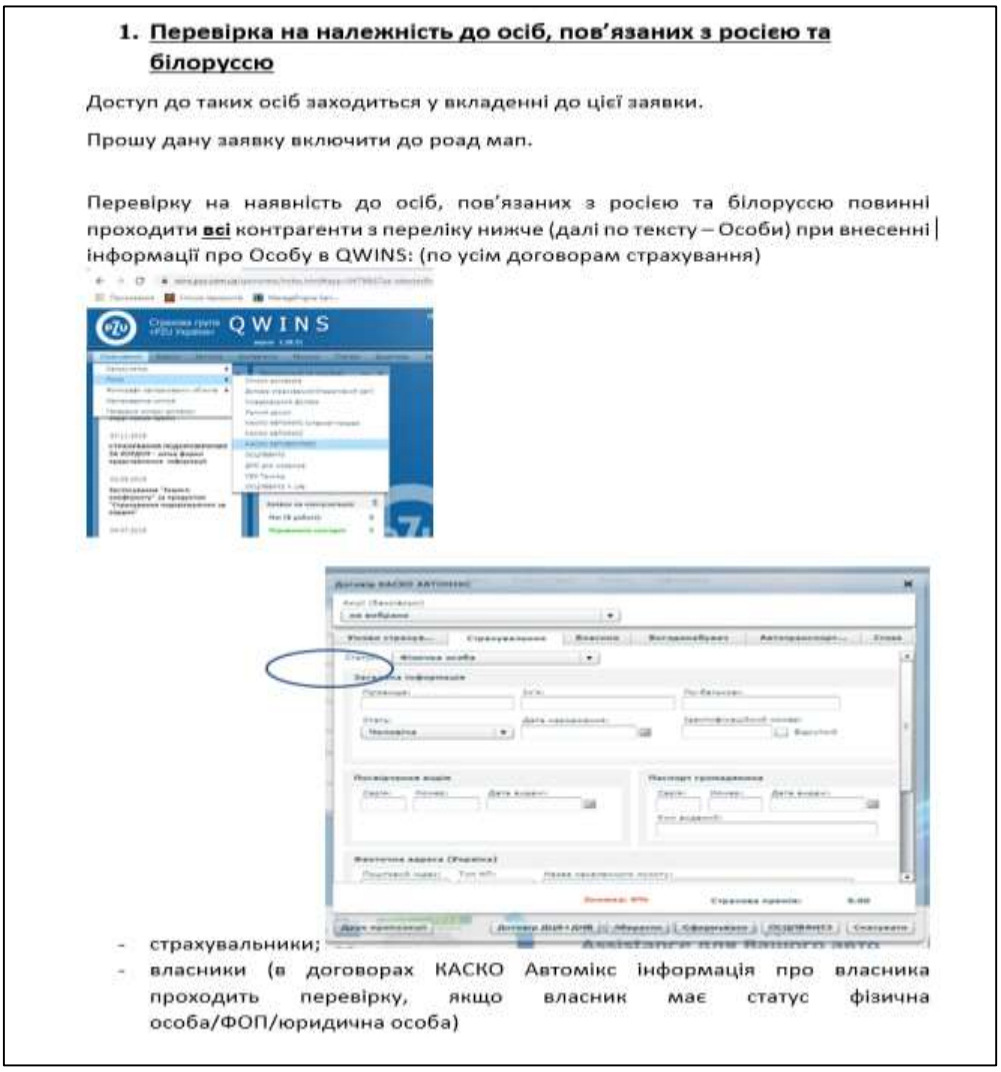
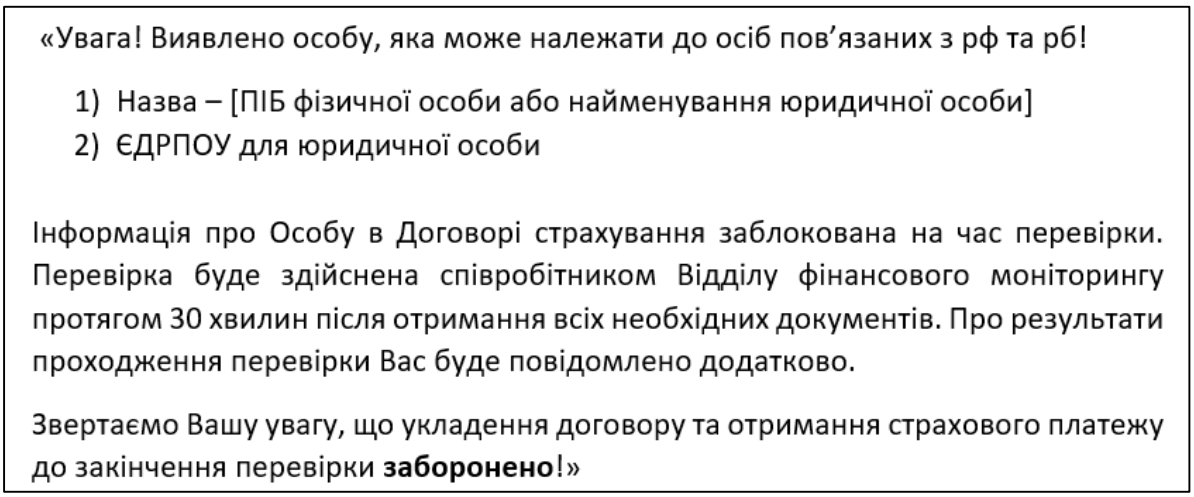


Рисунок 2.1 – Технічне завдання

При переведені договору у статус «проект», в якому було знайдено співпадіння, повинні відбуватись наступні події:

1) Договір має бути заблокований в системі. Це означає, що він повинен перейти із статусу «проект» в статус «заблокований по санкційному списку». Доступ до картки договору, а також право перевести договір в статус «проект», повинні мати лише співробітники Відділу фінансового моніторингу, яким попередньо необхідно надати доступ до системи та присвоїти особливі права доступу. Розблокування картки договору повинно відбуватись лише вручну співробітником відділу фінансового моніторингу;

2) Одночасно з подією №1 для працівника, який вносить інформацію по санкційній особі в договір страхування, на електрону пошту повинен надійти лист який зображений на рисунку 2.2:


«Увага! Виявлено особу, яка може належати до осіб пов'язаних з рф та рб!

1) Назва – [ПІБ фізичної особи або найменування юридичної особи]
2) ЄДРПОУ для юридичної особи

Інформація про Особу в Договорі страхування заблокована на час перевірки. Перевірка буде здійснена співробітником Відділу фінансового моніторингу протягом 30 хвилин після отримання всіх необхідних документів. Про результати проходження перевірки Вас буде повідомлено додатково.

Звертаємо Вашу увагу, що укладення договору та отримання страхового платежу до закінчення перевірки **заборонено**!»

Рисунок 2.2 – Технічне завдання. Приклад листа для продавця

Після виявлення контрагента, який може бути пов'язаний з РФ та РБ, одночасно з подією №2, повинен бути надісланий електронний лист на корпоративну адресу фінансового моніторингу компанії.

Цей лист служить сповіщенням для відповідальних працівників фінансового моніторингу про виявлення контрагента, який може бути пов'язаний з РФ та РБ. У листі наводиться інформація про критерій, за яким було виявлено контрагента (співпадіння ЄДРПОУ, найменування або ПІП), а також вказується назва контрагента, його ідентифікаційний код, номер та дата договору страхування. Крім того, зазначається відповідальний працівник, який створив картку контрагента в системі. Ця інформація дозволяє залучити увагу до потенційно ризикового контрагента та забезпечити подальшу перевірку та вжиття необхідних заходів у відповідності до встановлених процедур фінансового моніторингу.

1) Одночасно з подією №2 повинен відправлятись електронний лист на корпоративну адресу фінмоніторингу компанії, в якому зазначається рис. 2.3.

Тема листа: «УВАГА! Виявлено контрагента, що може бути пов’язаний з рф та рб».
Зміст: «Контрагент присутній в списках осіб, які пов’язані з рф та рб.

1) Критерій – [один з 3-х варіантів в залежності від того, за яким критерієм було виявлено контрагента:
   - співпадіння ЄДРПОУ – 100%;
   - співпадіння найменування – 100%;
   - співпадіння ПІП на 100%;
2) Назва – [ПІБ фізичної особи або назва юридичної особи];
3) Ідентифікаційний код - [ІПН для фіз. особи; ЄДРПОУ для юр. особи];
4) Номер та дата договору страхування;
5) Відповідальний працівник – [ПІБ працівника, який створив картку Особи в системі]»

[Всі дані щодо цієї особи з файлу]

Рисунок 2.3 – Технічне завдання. Приклад листа для фінмоніторингу

Цей лист служить сповіщенням працівникові про виявлення потенційно ризикової особи, яка може бути пов'язана з РФ та РБ. В ньому надається інформація про особу, включаючи її ПІБ або найменування (у випадку юридичної особи) і ЄДРПОУ (для юридичної особи).

Зазначається, що інформація про цю особу в договорі страхування буде заблокована на час перевірки. Відповідальність за перевірку лежить на співробітнику Відділу фінансового моніторингу, який здійснить перевірку протягом 30 хвилин після отримання всіх необхідних документів. Про результати перевірки працівник буде повідомлений окремо.

У листі також наголошується, що укладення договору та отримання страхового платежу заборонено до завершення перевірки. Це зроблено для забезпечення безпеки та дотримання вимог щодо уникнення угод з ризиковими особами, які можуть мати зв'язки з РФ та РБ.

Для забезпечення ефективного контролю і запобігання ризикам, пов'язаним з особами, причетними до санкційних списків, необхідно додатково розширити процедури перевірки договорів. Окрім блокування договорів по

санкційному списку, важливо встановити систему автоматичного перевіряння всіх контрагентів на наявність змін у статусі їхніх санкційних списків.

Це означає, що після блокування договору, система повинна автоматично сповіщати Відділ фінансового моніторингу про будь-які зміни статусу контрагента у санкційному списку. Такий підхід дозволяє оперативно реагувати на будь-які зміни і вживати відповідних заходів, у разі потреби.

Для забезпечення обмеженого доступу та контролю до договорів, важливо встановити ретельну систему управління правами доступу. Лише співробітники Відділу фінансового моніторингу повинні мати доступ до картки договору та право переводити її в статус "проект". Додатково, слід регулярно оновлювати і переглядати список співробітників з доступом до системи, щоб виключити можливість неправомірного доступу чи зловживання.

Розблокування картки договору повинно здійснюватися лише вручну співробітником Відділу фінансового моніторингу. Цей крок забезпечує додатковий рівень перевірки та контролю, оскільки будь-яке розблокування повинно бути обґрунтоване та документоване. Проведення перевірок з боку компетентних фахівців забезпечує відповідність процедур, а також виявлення можливих порушень чи несанкціонованих дій.

Реалізація цих додаткових заходів щодо блокування та розблокування договорів на основі санкційних списків сприятиме забезпеченню дотримання вимог міжнародних санкцій, підвищенню безпеки та ризик-управління в діловому середовищі.

2.2 Реалізація технічного завдання ПЗУ Україна

Отже з чітким технічним завданням потрібно вирішити на якому рівні перевірка контрагентів буде працювати як найкраще. Перше що приходить на думку – це клієнтська сторона в КВІНС. Це очевидний вибір, тому що вона має свої суттєві переваги в тонкості налаштування перевірок і роботи з договором в системі, також можливість інформативно сповіщати користувача про поточний стан перевірки, або про її результати.

Для вирішення питання щодо рівня перевірки контрагентів необхідно детально розглянути технічні вимоги і встановити оптимальну систему, яка забезпечить найкращий результат. Один із потенційних варіантів – використання клієнтської сторони в системі КВІНС.

Вибір цієї сторони є очевидним, оскільки вона має ряд значних переваг. По-перше, вона надає можливість тонко настроїти перевірки та роботу з договорами в системі. Це означає, що можна встановити необхідні параметри для ефективного виявлення потенційних ризиків та контрагентів, пов'язаних з РФ та РБ.

По-друге, використання клієнтської сторони дозволяє надсилати інформативні повідомлення користувачам щодо поточного стану перевірки або її результатів. Це важливо, оскільки такі повідомлення забезпечують прозорість процесу та можуть допомогти вчасно реагувати на виявлені ризики. Користувачі будуть отримувати актуальну інформацію про статус контрагента та перевірку, що сприятиме підвищенню ефективності взаємодії з системою.

Крім того, клієнтська сторона в КВІНС забезпечує можливість роботи з договорами в системі, що спрощує процес обробки і зберігання інформації про контрагентів. Завдяки цьому, компанія може ефективно керувати договорами страхування, виконувати необхідні зміни та забезпечити актуальність даних про контрагентів.

Отже, використання клієнтської сторони в системі КВІНС є раціональним вибором, оскільки вона дозволяє налаштувати перевірки контрагентів з урахуванням конкретних вимог, надсилати інформативні повідомлення користувачам та забезпечувати зручну роботу з договорами страхування. Але навіть реалізація перевірки на стороні БД не може гарантувати високого рівня захисту. Перевірка контрагента в середині процедур бази даних може бути вразливою для всіх загроз які стосуються баз даних, особливо до SQL-ін’єкції. В такому випадку недоброчесний користувач системи знаючи, що при формуванні договору тим чи іншим способом здійснюється перевірка контрагента на наявність в санкційних списках може спробувати обійти перевірку за допомогою

додавання корисного навантаження в до запиту в БД при формуванні договору. Таким чином зловмисник може навіть тільки оформити договір на підсанкційну особу, що в довгостроковій перспективі може принести великі фінансові та репутаційні втрати, а ще й отримати доступ до таблиць бази даних в яких містяться конфіденційні дані всіх клієнтів та користувачів системи, що набагато критичнішим в розрізі вразливостей і наслідків. Тому, для того аби бути певним в високому рівні кібербезпеки бази даних потрібно провести аналіз БД на вразливість до SQL-ін’єкцій в першу чергу і імплеметувати відповідні захисні механізми разом з перевіркою підсанкційних осіб.

Для кращого розуміння проблеми на рис. 2.4 наведено умовне схематичне зображення системи перевірок та безпеки.

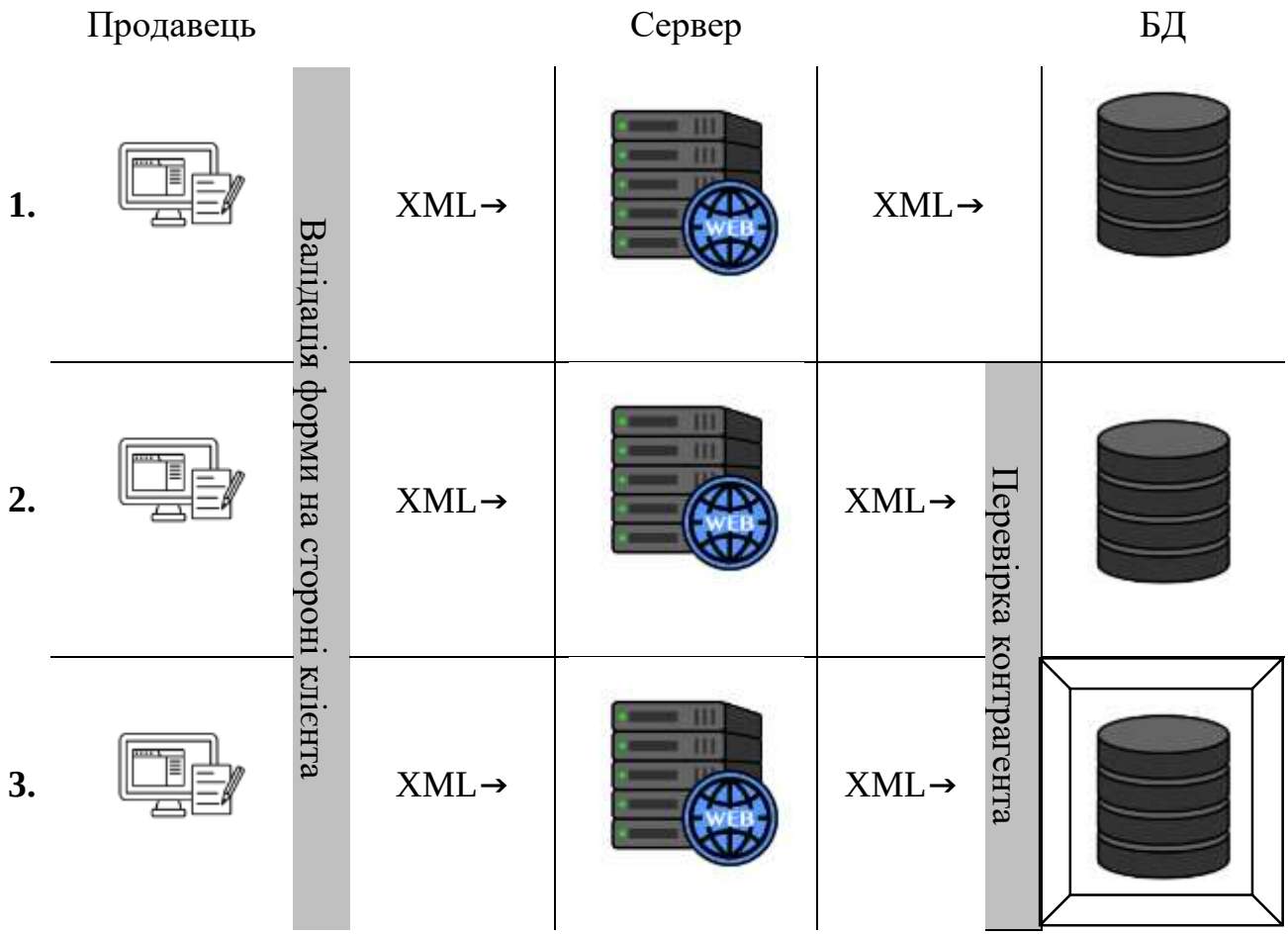


Рисунок 2.4 – Результати порівняння ітерацій систем захисту

В першій ітерації можна побачити, що система в плані кібербезпеки спирається виключно на валіадацію даних на стороні клієнта, що створює низку проблем і шляхів її обходу, тому що ці валідації прописані вручну програмістами і працюють по принципу можна все що не заборонено явно – що очевидно несе з собою ризики в вигляді високої ймовірності впливу людського фактору при реалізації цих перевірок. Відповідальна особа може просто пропустити якийсь момент, або банально допустити помилку в логіці реалізуємих валідацій. Тим не менше, як було описано вище, в випадку перевірки контрагента – спиратись на перевірку на стороні клієнта є небезпечним і трудомістким, тому на ітерації №2 зображено вже реалізацію перевірки контрагента на стороні БД – що збільшує кібербезпеку системи в рази, так як для попередження внесення підсанкційної особи в систему простим продавцем, який не володіє просунутими навичками взлому баз даних, буде достатньо валідації в середині процедури запису договору в базу. В такому випадку користувач буде певен що все зробив правильно і перевірка контрагента буде достатньо точною, адже продавець явно зазначив що всі внесені ним данні були вірні і він підтвердив свій намір сформувати новий договір для його подальшої оплати. Але також завжди існує ймовірність, що до системи QWINS отримає доступ недобросовісний користувач, який може мати на меті завдання шкоди та цілісності даних, чи системі CRM (customer relationship management) в цілому, та в кінцевому результаті отримати доступ до персональних даних обширної бази даних десятки тисяч користувачів. Аби попередити такий значущий витік даних мною було запропоновано провести аналіз БД на вразливість до SQL-ін’єкцій в першу чергу, так як я вважаю цю вразливість найкритичнішою і найактуальнішою для поточної системи «ПЗУ Україна». Схематичний кінцевий результат зображений під номером 3.

Виходячи з даних які наведені на рис. 2.4 для прикладу можна розглянути базові перевірки форми які вже реалізовані на ній. На рис 2.5 наведено приклад інформативного повідомлення інформативного повідомлення про помилку при заповненні поля. В разі якщо поле пусте або внесена інформація не відповідає передбаченому формату в кінці перевірок програма викидає діалогове вікно-

повідомлення, яке містить детальний опис всіх проблемних полів на формі. Також на самій формі, ці поля підсвічуються червоним, що сигналізує користувачу що це поле потребує додаткової уваги. При наведені курсора на це поле, також буде виведена відповідна підказка, яка допоможе користувачу зорієнтуватись.

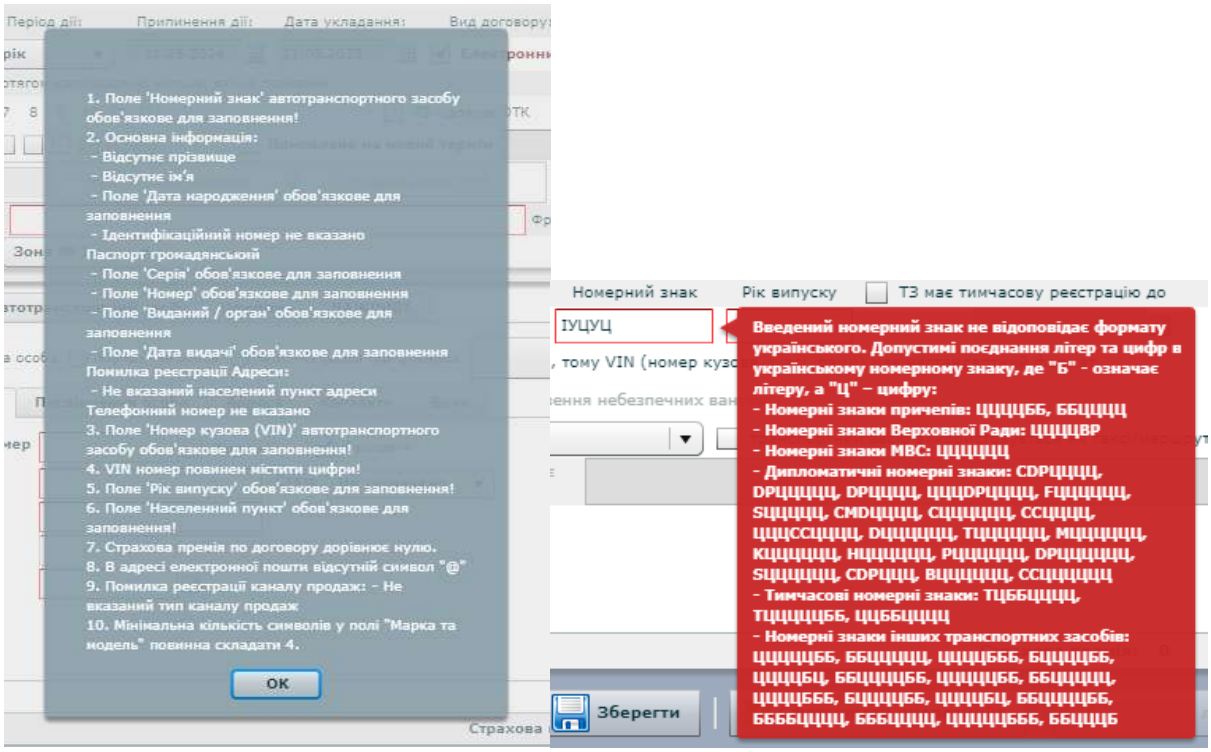


Рисунок 2.5 – Приклад інформативного вікна про помилку в QWINS

Але те що на перший погляд виглядає як очевидне і просте рішення, в випадку з перевіркою на наявність в санкційних списках має деякі суттєві проблеми, або навіть вразливості і ризики обходу системи перевірки.

Для початку рішення реалізації перевірки на формі може бути прийнятним, в випадку уніфікованих форм, які побудовані за базовими принципами ООП, що не є істинним для QWINS. Проблема в тому що QWINS був створений в період, коли метод ООП не був так широко поширений в розробці (2008 рік початку розробки продукту), тому основа цієї системи це процедурний підхід до програмування. При початку розробки не було розуміння якого масштабу програмний застосунок набуде з роками, тому більшість форм мають свої окремі функції валідації, які не уніфіковані і відрізняються одна від одної.

Реалізація перевірки на формі в системі QWINS може бути прийнятним рішенням, проте перед цим потрібно розглянути деякі важливі аспекти. Зокрема, необхідно врахувати, що система QWINS була створена у період, коли методологія об'єктно-орієнтованого програмування (ООП) ще не була настільки поширеною у розробці програмного забезпечення (початок розробки в 2008 році). Тому основним підходом до програмування в QWINS був процедурний стиль.

Виникла проблема тим, що на початку розробки системи не передбачалося масштабування програмного застосунку з плином часу. У результаті більшість форм в системі мають свої власні окремі функції валідації, які не є уніфікованими і відрізняються одна від одної.

Це означає, що при впровадженні нової перевірки на формі потрібно буде уважно аналізувати кожну форму окремо і враховувати її унікальні особливості. Для забезпечення єдиної системи перевірки можуть знадобитися значні зусилля для модифікації і структуризації коду, зокрема для переробки валідаційних функцій в уніфікований і стандартизований спосіб.

Варто врахувати, що впровадження об'єктно-орієнтованого підходу до програмування вже пізніше, після початку розробки QWINS, може створити значні труднощі, оскільки це вимагатиме переписування великої кількості існуючого коду та зміну архітектури системи.

Таким чином, при розгляді варіанту впровадження перевірки на формі в системі QWINS необхідно уважно оцінити переваги та недоліки цього підходу, зосередитися на аналізі впливу на існуючий код і можливих труднощах при внесенні змін.

Тому якщо спробувати реалізувати перевірку на наявність в санкційних списках на рівні клієнтського застосунку, то перед розробником постане задача яка буде потребувати в рази більше людино-годин на розробку, імплементацію і налаштування перевірки на неуніфікованих формах, загальна кількість яких складає близько 53 одиниці.

Але окрім великого часу на розробку такий підхід несе в собі іншу небезпеку – набагато важливішу і суттєвішу, а саме у випадку валідацій на клієнтській стороні, завжди є ризик що, користувач зрозуміючи що визначений контрагент не проходить перевірок на наявність в санкційних списках РФ та РБ, спробує все одно внести договір до системи змінюючи назву юридичної особи (замість скороченого ТОВ можна написати повну назву), або спробувати обійти перевірку змінюючи реєстр букв в імені, тощо. І робити це аж доки не знайдеться умовна вразливість в системі перевірки.

Виходячи з вищеописаного концептуального підходу ми підійшли до розуміння того, що перевірку потрібно здійснювати в самому кінці формування договору, коли запит на створення нового договору вже був відправлений в базу даних, тоді коли користувач впевнений що всі поля заповненні правильно і всі перевірки вже пройдено.

2.3 Архітектура системи перевірки

Виходячи з висновків попереднього розділу, найдоцільніший спосіб реалізації перевірки контрагентів на наявність в санкційних списках має бути побудований на рівні перевірок в самій базі даних, в момент коли користувач вже надав всі необхідні дані для цього і підтвердив чіткий намір сформувати договір в статусі «проект», що означає що договір готовий до оплати і відповідно переведення його на наступний, вже фінальний статус – «діючий».

На цьому етапі вже реалізовані певні перевірки, тож додати ще одну буде логічним кроком. За створення договору в БД відповідає процедура `[Cmd_Add_Contract]`. Вона обслуговує всі договори і через це є доволі масивною (735 рядків коду). Крім того вона запускає і інші окремі процедури які виконують різні функції, а саме: процедура запису в таблицю логування дій користувача в системі; процедура перевірки договору в системі на унікальність номеру і наявність відповідної програми страхування для нього; процедура редагування запису в таблиці пролонгацій; процедура-оператор перевірок учасників договору. В свою чергу процедура `ContractMembers_Check` є лице оболонкою-

оператором ініціалізації перевірок, яка збирає необхідну інформацію про учасників договору і передає її до процедур які відповідальні за фактичні перевірки. Умовну схему перевірки контрагентів наведено на рис. 2.6.

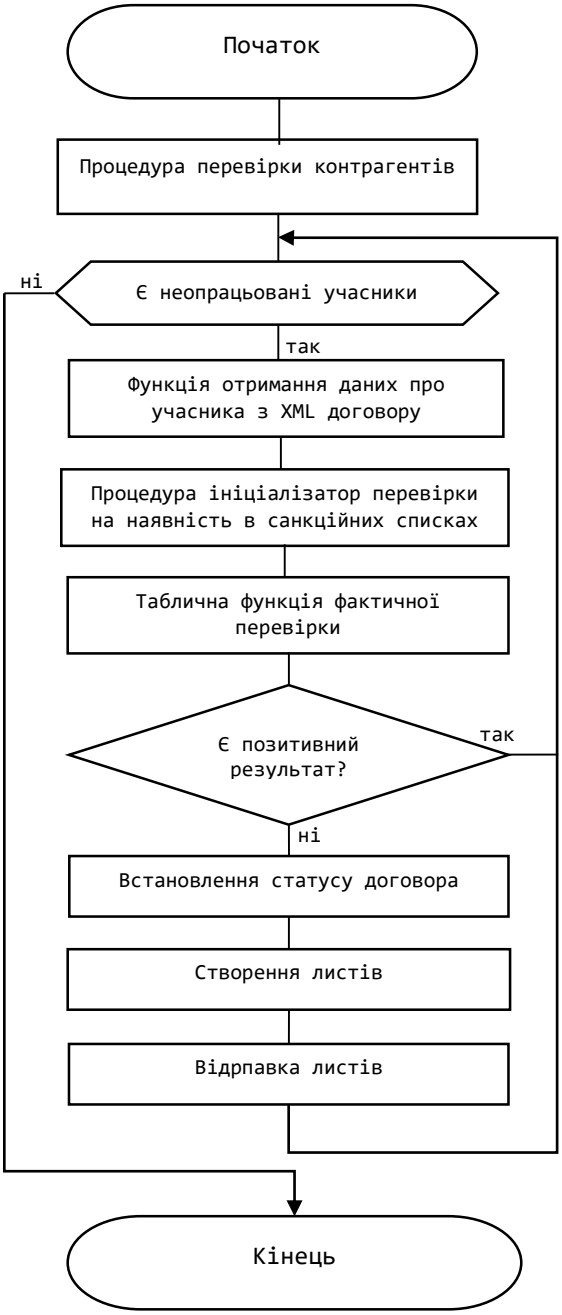


Рисунок 2.6 – Процес перевірки контрагентів

Шляхом виконання табличної функції `fnContractMembers_GetFromXML`, збирається уніфікована інформація про контрагентів з XML коду договору, який може мати різну структуру в різних страхових продуктах. Попередньо для перевірки контрагентів на наявність в санкційних списках було створено окрему

таблицю (`Sanction`) в яку були вивантажені надані в заявці ServiceDesk списки підсанкційних осіб. Після виконання функції по збору інформації вже виконуються процедури фактичної перевірки контрагентів і обробки її результатів. Наступним кроком в буде виконання процедури `ContractMembers_Sanction_Check` яка відповідальна за ініціалізацію вбудованої функції перевірки осіб і обробку результатів цієї перевірки: в разі позитивного результату, а саме – відсутність в списках процедура достроково закривається шляхом виконання команди `return;` , в іншому випадку ініціалізується створення відповідних листів інформування продавця і відділу фінансового моніторингу про наявність в системі договору страхування в якому ідентифіковано підсанкційну особу. Фактична перевірка здійснюється в табличній функції `fnContractMembers_SanctionSelect` .

2.4 Аналіз на вразливість до SQL-ін’єкцій

З попереднього розділу було визначено основний метод реалізації перевірки та наведено причини, чому саме йому було надано перевагу, але з точки зору кібербезпеки і в ньому можуть бути виявлені вразливості критичні для системи і бази даних в цілому. Тому в даному розділі пропоную розглянути результату тесту на вразливість бази даних до зовнішнього втручання шляхом додавання SQL-ін’єкцій в запит (get) на отримання даних про словники продукту КАСКО. Але перед тим як буде описано результат тесту, мушу зауважити, що тест був проведений на реальній робочій базі даних, в якій міститься персональна інформація про десятки тисяч клієнтів яка захищена Законом України «Про захист персональних даних» [23]. Тому з очевидних міркувань безпеки в бакалаврській роботі не може бути описаний весь процес зламу і тестування вразливості, так як і деякі критичні дані.

З метою валідації потенційної вразливості була проведена атака на вразливий параметр запиту в базу даних, в результаті якої був отриманий доступ до конфіденційних даних бази даних Компанії (домене ім’я БД приховане).

Далі у табл. 2.1 наведено інформацію про об’єкт тестування.

Таблиця 2.1 – Інформація щодо об'єкту тестування

Об’єкт	Тип
Веб-сервер	Nginx
Веб-фреймворк	Bootstrap 3.3.5
Бібліотеки JavaScript	Modernizr2.8.3; jQuery1.11.3

Вразливість легко експлуатується, дозволяє отримати повний доступ до критичних даними системи, відповідно є критичною і вимагає прийняття негайних заходів щодо усунення

Корисне навантаження (`) було додано до значення параметру d[city], та у відповідь було повернуто повідомлення про помилку бази даних, що свідчить про можливу вразливість.

Крім того, корисні навантаження 96992236 or 8985 = 08985 та 23323 or 555 = 555 були додані до значення параметру d[city]. Ці два запити призвели до різних відповідей, що вказує на те, що вхідні дані вводяться до SQL запиту небезпечним способом (табл. 2.2).

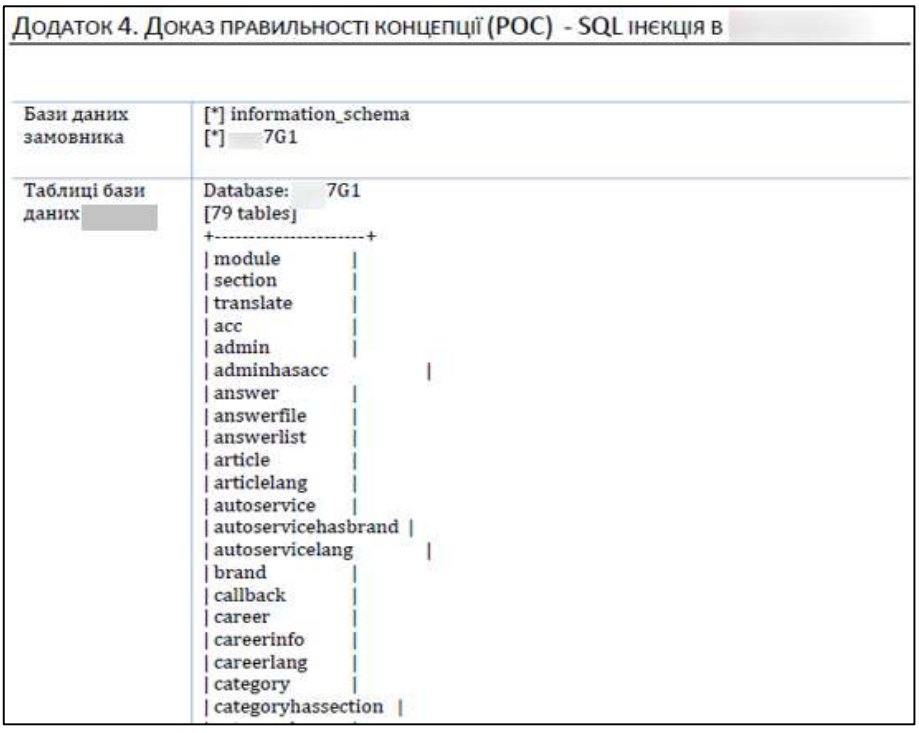
Таблиця 2.2 – Результати тестування SQL-ін’єкції в запиті до бази даних

Вразливий параметр	d[city]
Інформація про вразливість	Параметр d[city] є вразливим до SQL-ін'єкцій. Тип ін'єкції: error-based – WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
CVE #	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
Рівень ризику (CVSS v3)	10.0 CRITICAL
Запит	POST /ajax.php?JsHttpRequest=15590382705008-xml HTTP/1.1 Host: Помилка! Недопустимий об’єкт гіперпосилання. User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:60.0) Gecko/20100101 Firefox/60.0 Accept: */* Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Referer: https://[redacted]kasko.html Content-Type: application/octet-stream Content-Length: 85

	Cookie: _ga=GA1.3.235900388.1558515921; _ym_uid=1558515921110330897; _ym_d=1558515921; _gid=GA1.3.488430760.1558950892; _ym_isad=1 DNT: 1 Connection: close 52' c=default&a=getfilials&d[lang]=1&d[city]= &d[form_name]=form_kasko&d[this_is_l ife]=0
Відповідь сервера	HTTP/1.1 200 OK Server: nginx Date: Fri, 07 Jun 2019 08:04:14 GMT Content-Type: text/plain; charset=UTF-8 Content-Length: 1592 Connection: close Vary: Accept-Encoding Front-End-Https: on Strict-Transport-Security: max-age=300; [redacted] {"id":"15590382705008","js":null,"text":"<br \/>\n<b>Fatal error<\/b>: Uncaught exception 'Exception' with message 'Database query failed: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '' AND filialhaskind.kind_id IN (1,2,3,8) AND filiallang_active=1 AND filial_noco' at line 1; Query: SELECT * FROM `filial` NATURAL JOIN `filiallang` NATURAL JOIN `filialhaskind` WHERE 1 AND city_id=52' AND filialhaskind.kind_id IN (1,2,3,8) AND filiallang_active=1 AND filial_noconsult=0 AND lang_id=1 GROUP BY filial.filial_id ORDER BY filiallang_street' in \/var\/www\/[redacted]class\/DB.php:74\nStack trace:\n#0 \/var\/www\/[redacted]class\/DB.php(243): DB->query('SELECT * FROM `...')\n#1 \/var\/www\/[redacted]class\/Collection.php(271): RowIterator>__construct('SELECT * FROM `...', Object(RowFetchEntity), NULL)\n#2 \/var\/www\/[redacted]model\/Filial.php(270): Collection->getCustomIterator('', 'filiallang_stre...')\n#3 \/var\/www\/[redacted]controller\/DefaultController.php(4423): FilialCollection->getByParams(Array, 'filiallang_stre...')\n#4 \/var\/www\/[redacted]class\/Controller.php(67): DefaultAjaxController>GetfilialsAction()\n#5 \/var\/www\/[redacted]class\/Controller.php(169): AbstractFrontController->Process()\n#6 \/var\/www\/[redacted]ajax.php(6): AjaxFrontController>Process()\n#7 {main}\n thrown in

	<b>\/var\/www\/[redacted]class\/DB.php<\/b> on line <b>74<\/b> \/>\n"}
Наслідки експлуатації	- втрата конфіденційних даних - втрата цілісності даних (внесення змін до конфіденційних даних) - пошкодження веб-сайту (defacement) - доступ до системи і системних файлів - підвищення привілеїв - віддалене виконання коду
Рекомендації щодо усунення	первинний захист: - використання підготовлених запитів (з параметризованими запитами) - використання збережених процедур - перевірка введених даних згідно білого списку (white list) - перевірка і валідація усіх даних введених користувачем додаткові засоби захисту: - забезпечення найменших привілеїв користувачів - виконання перевірки введених даних по білому списку як вторинна лінія оборони

На рис. 2.7 наведено доказ правильності концепції в вигляді списку таблиць який можна було отримати в результаті SQL-ін’єкції описаної в табл. 2.2. Доменне ім’я бази даних на яку здійснювалась атака закрите в цілях безпеки.


Додаток 4. Доказ правильності концепції (POC) - SQL інєкція в

Бази даних замовника	[*] information_schema [*] 7G1
Таблиці бази даних	Database: 7G1 [79 tables] +----------+ | module | | section | | translate | | acc | | admin | | adminhasacc | | answer | | answerfile | | answerlist | | article | | articlelang | | autoservice | | autoservicehasbrand | | autoservicelang | | brand | | callback | | career | | careerinfo | | careerlang | | category | | categoryhassection |

Рисунок 2.7 – Результат SQL-ін’єкції як доказ правильності концепції (POC)

Також на рис. 2.8 наведено дамп таблиці admin, з якої зловмисник може отримати такі критичні дані як домене ім’я пошти, логін та паролі

admin_id	admin_key	admin_pass	admin_name	admin_login	admin_email	admin_act
1	a488a2987bc237b42e1319047e913d95	d2aaef75d8adc76332041bba6a42741b	\\041b\\0438\\043a\\043d\\0438\\043a	oly	ma	0
2	244ab5466 3eeb38dc6a49b24db727065	59c36b1eeae1d9ec112654 3b6c6888ec	\\0424\\041e\\0421 \\0412\\043e\\0438\\043e\\0448\\0438\\043d\\043e\\0432\\0441\\043a\\0438\\0439	uri	vo	1
3	fd2be77cf6802dc8f52add8cadd8d0e9	d822896469e9315fb5bbfe62a2dc552a	\\0424\\041e\\0421 \\0421\\0439\\0438\\0441\\0439\\0448\\0435\\043d\\043a\\043e	cor	sl	1
4	b1cf81f6e58171d3fc1f7364b7225fe0	f126826c78c6d197d9457ab84aa405448	\\041c\\0435\\043b\\044c\\043d\\0438\\0447\\0443\\043a	ana	ch	1
7	313de19e627ff21d4cc52972c819a8aa	c2d80d2873d3a1928f7c782a7049f34d	\\041e\\043b\\044c\\0433\\0438 \\0413\\0435\\0442\\044c\\043c\\0430\\043d	opa	op	1
8	f87a28747380866477774299dcdfe4ad	edebc8d4d69a1c690f9d96e9a75c3587	\\0410\\043b\\0438\\0438 \\0412\\045e\\043b\\0446\\0435\\0435\\0446	ave	av	1
11	29e4e2b1d5109b915652586816e5ac22	941817957c22e8d3ab4d344d42f87646	\\041b\\0435\\0431\\0435\\0434\\0438\\043d\\0441\\043a\\0439\\044f \\0418\\0440\\0438\\043d\\0430	ile	il	1
12	5ca41834883cf5381f4c3d9623a5d56d	4936ff5225cf649417cfbeaf02d3a070	\\041d\\0430\\0439\\0447\\0443\\043a \\041a\\0440\\0438\\0441\\0442\\0438\\043f\\0430	kn	kn	1

Рисунок 2.8 – Дамп таблиці admin

Отже, в результаті тестування бази даних на вразливості було можна прийти до висновку, що навіть побудова перевірки на рівні бази даних не убезпечує систему від несанкціонованих дій і завжди зберігається ризик експлуатації цих вразливостей, що може понести за собою матеріальні та репутаційні збитки.

2.5 Інші види атак на базу даних

У цифровому віці бази даних стали ключовим компонентом сучасних організацій, що зберігають та обробляють величезний обсяг конфіденційної інформації. Проте, разом зі зростанням значення даних для бізнесу зросла й загроза їхньої безпеки. Атаки на бази даних стали однією з найпоширеніших та найнебезпечніших форм кіберзлочинності, здатних завдати серйозної шкоди як фінансовій, так і репутаційній стійкості компаній та організацій.

Варіанти атак на бази даних різноманітні, і кожна з них може мати серйозні наслідки. Крім ін'єкцій, існує кілька інших видів атак на бази даних (БД). Ось декілька з них [31]:

1) Cross-Site Scripting (XSS) – ця атака відбувається, коли зловмисник вставляє зловісний скрипт у веб-сторінку, яку переглядають користувачі. Цей скрипт виконується в браузері користувача і може бути використаний для збору чутливої інформації або зловживання діями користувача.

2) Cross-Site Request Forgery (CSRF) – ця атака полягає в тому, що зловмисник змушує автентифікованого користувача виконати небезпечну дію на

веб-додатку без його належного дозволу. Зловмисник використовує довіру до веб-додатку і підставляє зловісний запит, щоб зловживати повноваженнями користувача.

3) Denial of Service (DoS) і Distributed Denial of Service (DDoS) – ці атаки мають на меті перевантажити ресурси сервера або мережі, змушуючи їх перестати обробляти законні запити. DoS-атака виконується з одного джерела, тоді як DDoS-атака використовує багато комп'ютерів (часто заражених ботнетом) для одночасного навантаження на цільовий сервер або мережу.

4) Атаки на перебір паролів – це атаки, де зловмисник намагається зламати паролі, спробуючи багато різних комбінацій або використовуючи словники з популярними паролями. За допомогою автоматизованих програм, зловмисники можуть швидко перебирати паролі і здобути несанкціонований доступ до БД.

5) Фізичний доступ до сервера – ця атака відбувається, коли зловмисник отримує фізичний доступ до сервера або носіїв даних, що містять БД. Вони можуть використовувати цей доступ для крадіжки, зміни або видалення даних.

6) Атаки на переповнення буфера – ці атаки спрямовані на вразливості програмного забезпечення, коли зловмисники вводять більшу кількість даних у буфер, ніж він може обробити. Це може призвести до перезапису важливих даних або виконання зловісного коду.

7) Атаки на слабкі місця автентифікації та авторизації – ці атаки спрямовані на вразливості в механізмах автентифікації та авторизації. Зловмисники можуть намагатись обійти механізми перевірки прав доступу, зламати або підробити облікові записи користувачів для отримання несанкціонованого доступу до БД.

Враховуючи розмаїття атак, важливо приділити належну увагу заходам безпеки, таким як належне шифрування, строга автентифікація та авторизація, моніторинг активності та регулярні оновлення програмного забезпечення, щоб запобігти атакам на бази даних.

Детально розглянемо декілька з них.

Cross-Site Scripting (XSS) – це тип атаки на веб-додатки, при якому зловмисник вставляє зловісний скрипт у веб-сторінку, яку переглядають

користувачі [31]. Цей скрипт потім виконується в браузері жертви, що може призвести до крадіжки даних, зміни вмісту сторінки або виконання дій в імені користувача без його згоди.

Існують три основні типи XSS-атак: stored (збережений), reflected (відображений) і DOM-based (DOM-заснований).

1) Stored XSS (збережений XSS): Цей тип атаки відбувається, коли зловмисник вставляє зловісний скрипт безпосередньо в базу даних або веб-додаток. При завантаженні сторінки з вразливою точкою введення, зловісний скрипт витягується з бази даних і виконується в браузері кожного користувача, який переглядає цю сторінку [31]. Це може призвести до викрадення кукі-файлів автентифікації, виконання дій в імені користувача або показу зловісного контенту.

2) Reflected XSS (відображений XSS): У цьому випадку зловмисник вбудовує зловісний скрипт у параметр URL або форму запиту, який передається на сервер. Сервер обробляє цей запит і повертає сторінку, додавши введений скрипт безпосередньо в HTML-відповідь. При отриманні відповіді браузер виконує зловісний скрипт, що призводить до потенційних атак на користувачів.

3) DOM-based XSS (DOM-заснований XSS): Цей тип XSS-атаки використовує вразливості у маніпулюванні DOM-об'єктами веб-сторінки. Зловмисник вставляє зловісний скрипт, який використовується для зміни структури DOM-дерева, що впливає на відображення сторінки. Коли користувачі переглядають таку змінену сторінку, скрипт виконується в їх браузерах, що може мати негативні наслідки [24].

Щоб запобігти XSS-атакам, необхідно вживати наступні заходи захисту:

- Перевіряти та екранувати всі дані, які введені користувачами, перед тим, як вони використовуються в HTML-відповіді.

- Використовувати механізми екранування, які вбезпечують вставлення коду, наприклад, HTML-екрани або функції екранування.

- Не довіряти неперевіреним джерелам введення, таким як параметри URL або дані з форм.

- Встановлювати правильні заголовки безпеки, такі як Content Security Policy (CSP), щоб обмежити виконання скриптів з ненадійних джерел.

- Регулярно оновлювати програмне забезпечення, включаючи веб-сервери, фреймворки та бібліотеки, для усунення відомих вразливостей XSS.

- Навчати розробників та аудиторів безпеки про вразливості XSS та найкращі практики захисту від них.

Запобігання XSS-атакам – важлива складова забезпечення безпеки веб-додатків, оскільки вони можуть призвести до викрадення особистої інформації користувачів, порушення конфіденційності та навіть контролю над веб-сторінкою користувача.

Cross-Site Request Forgery (CSRF) – це тип атаки на веб-додатки, при якому зловмисник змушує автентифікованого користувача виконати небезпечну дію на веб-додатку без його належного дозволу [24]. Атака полягає в експлуатації довіри, яку веб-додаток має до запитів, що надходять з браузера користувача.

Основний сценарій атаки CSRF наступний:

1) Користувач, який вже автентифікований на веб-додатку, відвідує зловмисну веб-сторінку або веб-сторінку, що містить зловісний код.

2) Зловмисник вставляє в HTML-код сторінки або використовує інші методи, які автоматично виконують запити до цільового веб-додатку без знання користувача.

3) Запити включають в себе дії, такі як зміна пароля, виконання фінансових операцій, видалення або зміна вмісту користувача та інші дії, які можуть мати негативний вплив.

4) Браузер користувача автоматично відправляє ці запити до цільового веб-додатку з використанням наявних кукі або інших механізмів автентифікації, що робить їх вигляд справжніми запитами від автентифікованого користувача.

5) Якщо веб-додаток не вживає відповідних заходів безпеки, запити будуть виконані без перевірки джерела або відповідних механізмів перевірки дозволів, що може призвести до несанкціонованих дій.

Щоб запобігти атакам CSRF, необхідно вживати наступні заходи захисту:

1) Використовуйте механізми захисту CSRF-токенів: Веб-додаток повинен генерувати та включати у форми або запити унікальні CSRF-токени. Ці токени потрібно перевіряти на сервері перед виконанням будь-яких дій, що змінюють стан додатку.

2) Встановлюйте правильні заголовки HTTP: Заголовок "SameSite" може бути використаний для обмеження відправки кукі-файлів зовнішнім джерелам. Заголовок "Referer" може вказувати на посилання, з якого прийшов запит, що дозволяє перевірити його джерело.

3) Вимагайте авторизацію для критичних дій: Веб-додаток повинен запитувати підтвердження автентифікації користувача перед виконанням критичних дій, таких як зміна пароля або виконання фінансових операцій.

4) Регулярно оновлюйте програмне забезпечення: Важливо мати оновлені версії веб-серверів, фреймворків та бібліотек, оскільки вони часто містять виправлення вразливостей CSRF.

5) Проводьте аудит безпеки: Регулярно проводьте аудит веб-додатків з метою виявлення вразливостей CSRF та інших потенційних проблем безпеки.

Прийняття цих заходів безпеки може допомогти запобігти успішним атакам CSRF та зберегти безпеку інформації користувачів веб-додатків.

Атаки на переповнення буфера є одними з найпоширеніших і небезпечних видів атак у сфері кібербезпеки. Ці атаки використовують вразливості в програмах або операційних системах, де зловмисники намагаються передати більше даних у буфер пам'яті, ніж він може вмістити, що призводить до переповнення і може дозволити зловмиснику виконувати небажані дії або навіть набути контролю над системою [24].

Основний механізм атаки на переповнення буфера включає наступні кроки:

1) Зловмисник вивчає цільову систему або програму, щоб знайти вразливості, пов'язані з буфером. Вразливості можуть бути спричинені неправильною обробкою введення або недостатньою перевіркою розміру буфера.

2) Зловмисник створює спеціально сформований ввід, який перевищує максимальний розмір буфера або не враховується при обробці програмою. Це може бути рядок символів, мережевий пакет або інший тип даних.

3) Зловмисник передає цей шкідливий ввід у вразливу програму або систему, яка приймає дані у буфер пам'яті.

4) Унаслідок переповнення буфера додаток може втратити контроль над пам'яттю і дозволити зловмиснику виконувати небажані дії. Це може включати запис шкідливого коду у пам'ять, зміну контрольного потоку програми або виконання власного коду зловмисника.

Наслідки атак на переповнення буфера можуть бути серйозними, включаючи:

- Зловмисник може виконувати свій власний код на компрометованій системі, отримуючи контроль над нею.

- Атака може призвести до переповнення буфера і зупинки роботи системи, що призводить до відмови в обслуговуванні легітимних користувачів.

- Зловмисник може використовувати атаку для обходу механізмів безпеки і отримання несанкціонованого доступу до системи або даних.

Щоб захистити системи від атак на переповнення буфера, рекомендується вживати наступні заходи захисту:

- Використання безпечних функцій та бібліотек: Розробники повинні використовувати безпечні функції та бібліотеки, які автоматично керують розміром буферів і перевіряють вхідні дані.

- Перевіряйте розмір буфера перед записом в нього даних, щоб уникнути переповнення.

- Забезпечуйте належну перевірку та обробку вхідних даних, щоб запобігти передачі шкідливих даних.

- Використовуйте механізми захисту, такі як Address Space Layout Randomization (ASLR) та Data Execution Prevention (DEP), які допомагають ускладнити атаки на переповнення буфера.

- Регулярно оновлюйте програмне забезпечення, операційні системи та бібліотеки, оскільки вони можуть містити виправлення вразливостей.

- Проводьте регулярні аудити безпеки системи для виявлення вразливостей і вчасного їх виправлення.

Прийняття цих заходів безпеки може допомогти уникнути атак на переповнення буфера та забезпечити безпеку системи.

Перелічені вище атаки, є серйозною загрозою для безпеки веб-додатків. Вони можуть призвести до виконання шкідливого коду, втрати конфіденційності даних та навіть контролю над системою. Щоб захиститися від цих атак, важливо використовувати валідацію та екранизацію даних, фільтрування введення, встановлення безпечних заголовків HTTP, використання CSRF-токенів та регулярне оновлення програмного забезпечення. Аудит безпеки і постійне підтримання високих стандартів безпеки є необхідними. Запобігання цим атакам забезпечить надійний рівень захисту для веб-додатків і захистить конфіденційні дані користувачів.

3 РОЗРОБКА ТА РЕАЛІЗАЦІЯ ПЕРЕВІРКИ

3.1 Обґрунтування вибору засобів розробки

Виходячи з аналізу який був проведений в розділі 2.2 очевидним вибором середовища для розробки буде Microsoft SQL Server Managment Studio 17, який вже встановлений і широко використовується в відділах Dev Ops та IT Aplication для написання скріптів Transact SQL, підготовки вибірок на замовлення, написання процедур та функцій та інших взаємодій з базою данних. Також на рівні БД реалізований сервіс розсилки службових листів, що повністю забезпечує можливість виконання завдання в частині оперативного сповіщенні продавців та відділу фінансового моніторингу.

Microsoft SQL Server Management Studio (SSMS) 17 є інтегрованою середовищем розробки та керування базами даних Microsoft SQL Server. Це потужний інструмент, який надає розширені можливості для адміністрування, розробки, оптимізації та моніторингу баз даних.

SSMS 17 пропонує багато корисних функцій і інструментів для роботи з SQL Server. Основні можливості включають створення, редагування та виконання запитів SQL, розробку та управління базами даних, а також моніторинг та налагодження їх продуктивності. Давайте детальніше розглянемо деякі ключові компоненти та функціональність SSMS 17.

1) З'єднання з сервером: SSMS дозволяє підключатися до різних серверів баз даних SQL Server. Ви можете вказати параметри підключення, такі як ім'я сервера, тип автентифікації та обліковий запис користувача, для отримання доступу до бази даних.

2) Редагування запитів SQL: SSMS надає зручний редактор запитів, в якому можна створювати, редагувати та виконувати SQL-запити. Є можливість автодоповнення коду, перегляд схеми бази даних, відстеження помилок та відображення результатів запитів.

3) Розробка баз даних: SSMS дозволяє створювати нові бази даних, таблиці, збережені процедури, функції та інші об'єкти бази даних. Ви можете

використовувати вбудовані інструменти для моделювання даних, роботи зі схемами та відносинами між таблицями.

4) Керування базами даних: SSMS дозволяє виконувати різні адміністративні завдання, такі як резервне копіювання та відновлення баз даних, керування користувачами та ролями доступу, налаштування безпеки, моніторинг та оптимізація продуктивності.

5) Моніторинг та налагодження: SSMS надає інструменти для моніторингу та налагодження продуктивності баз даних. Ви можете переглядати статистику виконання запитів, використання ресурсів сервера, виконувати профілювання запитів та аналізувати їх ефективність.

6) Інтеграція з іншими інструментами Microsoft: SSMS взаємодіє з іншими інструментами Microsoft, такими як Visual Studio, Azure Data Studio та Power BI. Це дає можливість зручно обмінюватися даними та використовувати розширені можливості розробки та аналізу даних.

7) Розширення та настроювання: SSMS підтримує розширення, які дозволяють розширити його функціональність. Ви можете встановлювати додаткові компоненти, плагіни та засоби розширення, що відповідають вашим потребам.

8) Візуалізація даних: SSMS надає можливість візуалізувати дані шляхом створення діаграм, графіків та звітів. Це допомагає аналізувати дані бази даних за допомогою інтерактивних візуальних засобів.

9) Робота з версіями: SSMS підтримує роботу з різними версіями Microsoft SQL Server. Ви можете підключатися та керувати базами даних, які працюють на SQL Server 2008, 2012, 2014, 2016, 2017 та більш пізніх версіях.

10) Інтеграція з інструментами розробки: SSMS інтегрується з різними інструментами розробки, такими як Visual Studio. Це дозволяє зручно працювати з базами даних під час розробки програмного забезпечення, забезпечуючи безперервну робочу обстановку.

11) Скриптування та автоматизація: SSMS надає можливість скриптування та автоматизації завдань. Ви можете створювати скрипти для автоматичного

виконання певних дій, таких як створення бази даних, таблиць або запуск запитів на регулярній основі.

12) Збереження з'єднань: SSMS дозволяє зберігати налаштування з'єднань до баз даних, що дозволяє швидко підключатися до раніше використаних серверів і зменшує час на конфігурацію підключень.

13) Підтримка мов програмування: SSMS підтримує різні мови програмування, такі як T-SQL, C#, VB.NET тощо. Це дозволяє розробникам створювати та виконувати складні скрипти та програми безпосередньо з інтерфейсу SSMS.

14) Співпраця в команді: SSMS надає можливість співпрацювати в команді розробників та адміністраторів баз даних. Ви можете керувати доступом до бази даних, обмінюватися скриптами та об'єктами бази даних, а також спілкуватися з іншими членами команди через інтегрований функціонал коментування та спільної роботи.

SSMS 17 є незамінним інструментом для розробників, адміністраторів та аналітиків баз даних SQL Server. Його потужні можливості дозволяють ефективно керувати та оптимізувати роботу з базами даних, спрощуючи завдання розробки та адміністрування. Завдяки інтуїтивно зрозумілому інтерфейсу та широкому набору функцій, SSMS допомагає забезпечувати високу продуктивність і надійність вашої бази даних SQL Server.

Але крім цього Microsoft SQL Server Managment Studio 17 також має наступні переваги:

- Широкі можливості: Microsoft SQL Server надає широкі можливості для управління базами даних різних розмірів і складності. Він підтримує реляційну модель даних, а також здатний обробляти складні структури даних, такі як XML, JSON.
- Висока продуктивність: MS SQL Server пропонує високу швидкодію та продуктивність завдяки оптимізованим запитам, покращеним індексам та плануванню запитів. Він також має вбудовані засоби кешування, реплікації та кластеризації для підвищення продуктивності та доступності даних.

- Розширена безпека: це різноманітні засоби для забезпечення безпеки даних, включаючи рівні автентифікації та авторизації, шифрування даних, аудит доступу та розширені засоби для управління правами доступу.
- Інтеграція з іншими продуктами: Microsoft SQL Server 2017 має глибоку інтеграцію з іншими продуктами Microsoft, такими як Microsoft Azure, Power BI, Excel, SharePoint та інші. Це дозволяє легко обмінюватися даними та інтегрувати SQL Server з іншими рішеннями Microsoft.
- Підтримка розподілених систем: SQL Server 2017 має вбудовану підтримку розподілених систем, дозволяючи створювати розподілені бази даних та кластери. Це дозволяє масштабувати систему та забезпечувати високу доступність даних.

Крім всього вище перерахованого ця інтегроване середовище управління інфраструктурою SQL використається всередині організації і надається розробника вже передустановленою на робочій віртуальній машині.

3.2 Програмна реалізація

Для початку потрібно створити відповідну таблицю в якій буде міститись основна інформація по перевіряємих контрагентах. Основуючись на даних які були додані до технічного завдання, поки що списки є лише по юридичних особах, або фізичних особах але без ІПН або необхідної дати народження, що унеможливлює точну ідентифікацію особи, тому для перевірки працездатності системи потрібно буде створити підсанкційну фізичну особу окремо, але це згодом. Спочатку таблиця для перевірки, код якої наведено нижче

```
create table dbo.Sanction
(
          Id int identity,
          FullName nvarchar(1000),
          CompanyName nvarchar(1000),
          DateBorn datetime,
          INN nvarchar(20),
          DateCreate datetime not null constraint
DF_Sanction_DateCreate default (getdate()),
          Comment nvarchar(256)
          constraint PK_Sanction primary key clustered (Id)
```

```
)
```

Таблиця створюється з кластерним стовпцем Id, який визначається як первинний ключ, що у майбутньому при необхідності дозволить підв’язати додаткові таблиці під таблицю Sanction. Імена визначені типом nvarchar в розмірі 1000 знаків що повинно повністю покрити навіть найдовші назви юридичних, або імена фізичних осіб. Також поле INN визначено текстовим, аби уникнути колізій коли для полів ІПН використовується тип int, який не покриває значення які починаються з цифри 3 і більше. Поле DateCreate визначене значенням по замовчуванню – поточною датою, що дозволяє відстежити дату додавання конкретного контр агента у внутрішні списки ПЗУ.

Після створення таблиці можна приступати до створення основної процедури яка буде обслуговувати санкційну перевірку. Код наведено нижче

```
create or alter procedure [dbo].[ContractMembers_Sanction_Check]
(
     @ContractID int,
     @CompanyName nvarchar(1000),
     @Surname nvarchar(128),
     @Name nvarchar(128),
     @FatherName nvarchar(128),
     @DateOfBorn nvarchar(16),
     @Inn nvarchar(20),
     @MemberType nvarchar(128)
)
as
begin
```

Ця процедура створена для роботи вже з заздалегідь вибраними даними з XML договора, тому в ній ми описуємо тільки необхідні для перевірки змінні. Дата народження визначена як текстове поле розміром в 16 знаків, тому що з XML воно вибирається в текстовому вигляді розміром від 10 знаків до 16.

Після вибірки основної інформації яка може знадобитись для розсилки листів:

```
select
     @ContractNumber = c.ContractNumber
     ,@SellerName = u.UserName
     ,@SellerMail = u.UserEMAIL
from Contract c
inner join [User] u on u.MemberID = c.ContractSellerID
where c.ContractID = @ContractID
```

```
Здійснюється вже сама перевірка на наявність в санційних списках.
select @SanctionId = SanctionId,
@SanctionName = SanctionName,
@SearchComment = SearchComment
from fnContractMembers_SanctionSelect(@CompanyName, @Surname,
@Name, @FatherName, @DateOfBorn, @Inn)
```

За санкційну перевірку відповідальна таблична функція `fnContractMembers_SanctionSelect` яка повертає таблицю-список результат пошуку по санкційних особах, тобто всіх осіб дані яких співпадають з наявними даними в таблиці `Sanction`. В разі якщо у відповідь функція не повернула нічого, процес перевірки, як і робота процедури `ContractMembers_Sanction_Check` закінчується:

```
if @SanctionId is null
     return;
```

Але у випадку співпадіння – договір блокується шляхом додавання нового (попередньо створеного) статусу, який унеможливлює подальшу роботу з договором або його оплату в системі ПЗУ. Після блокування договору в процедурі створюються два листи: один для відділу фінансового моніторингу компанії, інший для самого продавця, аби він розумів що відбувається:

```
declare @SellerLetterBody nvarchar(max) =
     replace(replace(cast((select
          '<p><b>Увага!</b><br/>Виявлено особу, яка може належати
до осіб пов''язаних з РФ та РБ!<br/>'
          ,concat('<br/>Результат пошуку: <b>', @SearchComment,
'</b>')
          ,concat('<br/>Номер договору: <b>', @ContractNumber,
'</b>')
          ,concat('<br/>Ід договору: <b>', cast(@ContractID as
nvarchar(50)), '</b>')
          ,concat('<br/>Статус особи в договорі: <b>', @MemberType,
'</b></p>')
          ,concat('<p><ol><li> Назва в договорі: ',
iif(len(@Surname) = 0 and len(@CompanyName) > 0, @CompanyName,
concat(@Surname, ' ', @Name, ' ', @FatherName)), '</li>')
          ,iif(len(@DateOfBorn) > 0, concat('<li>Дата народження в
договорі: ', @DateOfBorn, '</li>'), null)
          ,iif(len(@Inn) > 0, concat('<li>Код в договорі: ', @Inn,
'</li>'), null)
          ,'</ol></p>'
          ,'Інформація про Особу в Договорі страхування заблокована
на час перевірки.<br/>'
```

```
          ,'Перевірка буде здійснена співробітником Відділу
фінансового моніторингу протягом 30 хвилин після отримання всіх
необхідних документів. Про результати проходження перевірки Вас
буде повідомлено додатково.<br/>'
          ,'Звертаємо Вашу увагу, що укладення договору та
отримання страхового платежу до закінчення перевірки
<b>заборонено</b>!'
     for xml path(''), elements, type) as nvarchar(max)), '&lt;',
'<'), '&gt;', '>')
```

Далі виконується збережена процедура (`sp_send_dbmail`) яка відправляє відпвідні листи.

Вище був описаний базовий алгоритм дій та реакція на результати перевірки, але не була описана робота функції яка відповідальна за саму перевірку на наявність в санкційних списках. Отже таблична функція оперує ідентичними даними з процедур вище, далі навенедо частина коду, який описує ствоерння процедури і допустимий результат

```
create function dbo.fnContractMembers_SanctionSelect
(
     @CompanyName nvarchar(1000),
     @Surname nvarchar(128),
     @Name nvarchar(128),
     @FatherName nvarchar(128),
     @DateOfBorn nvarchar(16),
     @Inn nvarchar(20)
)
returns @SanctionsInfo table
(
    SanctionId int null,
    SanctionName nvarchar(1000) null,
    SearchComment nvarchar(256) null
)
```

В даному випадку передбачено повернення пустих полів, для випадків коли перевірка нічого не виявила. В частині коду нижче описано перевірку для юридичних осіб по коду ЄДРПОУ:

```
if len(@Surname) = 0 and len(@CompanyName) > 0 -- Ur
     begin
          -- search by code
          select top 1 @SanctionId = s.Id, @SanctionName =
s.CompanyName, @SearchComment = 'Співпадіння ЄДРПОУ' from Sanction
s where s.INN = @Inn
```

Відповідні перевірки передбачені і по іншим параметрам для фізичних осіб:

```
else if len(@Surname) > 0 -- fiz
     begin
          declare @FullName1 nvarchar(256) =
ltrim(rtrim(concat(@Surname, ' ', @Name, ' ', @FatherName)))
          declare @FullName2 nvarchar(256) =
ltrim(rtrim(concat(@Name, ' ', @Surname, ' ', @FatherName)))
          -- search by code
          select top 1 @SanctionId = s.Id, @SanctionName =
s.FullName, @SearchComment = 'Співпадіння ІНН' from Sanction s
where s.INN = @Inn
          -- search by name if code search failed
          if @SanctionId is null
               select top 1 @SanctionId = s.Id, @SanctionName =
s.FullName, @SearchComment = 'Співпадіння Фамілії, Імені та дати
народження(якщо присутня)' from Sanction s
               where ((s.FullName = @FullName1) or (s.FullName =
@FullName2))
               and (s.DateBorn is not null and Cast(s.DateBorn as
date) = Cast(@DateOfBorn as date))
     end
```

При перевірці імені передбачено варіант коли продавець внесе ім’я у відповідні поля невірно, тому перевіряються обидва варіанти повного імені контрагента. Також перевірка зупиняється, якщо є результат пошуку по коду особи ІПН, або ЄДРПОУ – це дозволяє не витрачати зайвий час на вже непотрібні додаткові пошуки в таблиці.

В кінці перевірок в таблицю яка повертається вносяться результати перевірок:

```
insert into @SanctionsInfo select @SanctionId, @SanctionName,
@SearchComment
     return
```

В цьому розділі було описано реалізований процес перевірок контрагентів на наявність в санційних списках на рівні БД. В наступному будуть наведені результати тестування.

3.3 Результати тестування

Після реалізації алгоритму перевірок контрагентів його можна протестувати вже в самому клієнтському застосунку.

Для прикладу візьмемо договір автострахування КАСКО, так як в ньому можна розглянути такі типи учасників договору як страхувальник, власник та вигодонабувач. При заповненні всіх даних по договору і збережені його в системі в статусі «чорновик», на клієнтській стороні він проходить всі перевірки і з ним не виникає жодних проблем, навіть якщо в ньому фігурує підсанкційна особа. На рис. 3.1 наведено результат збереження договору як чорновика.

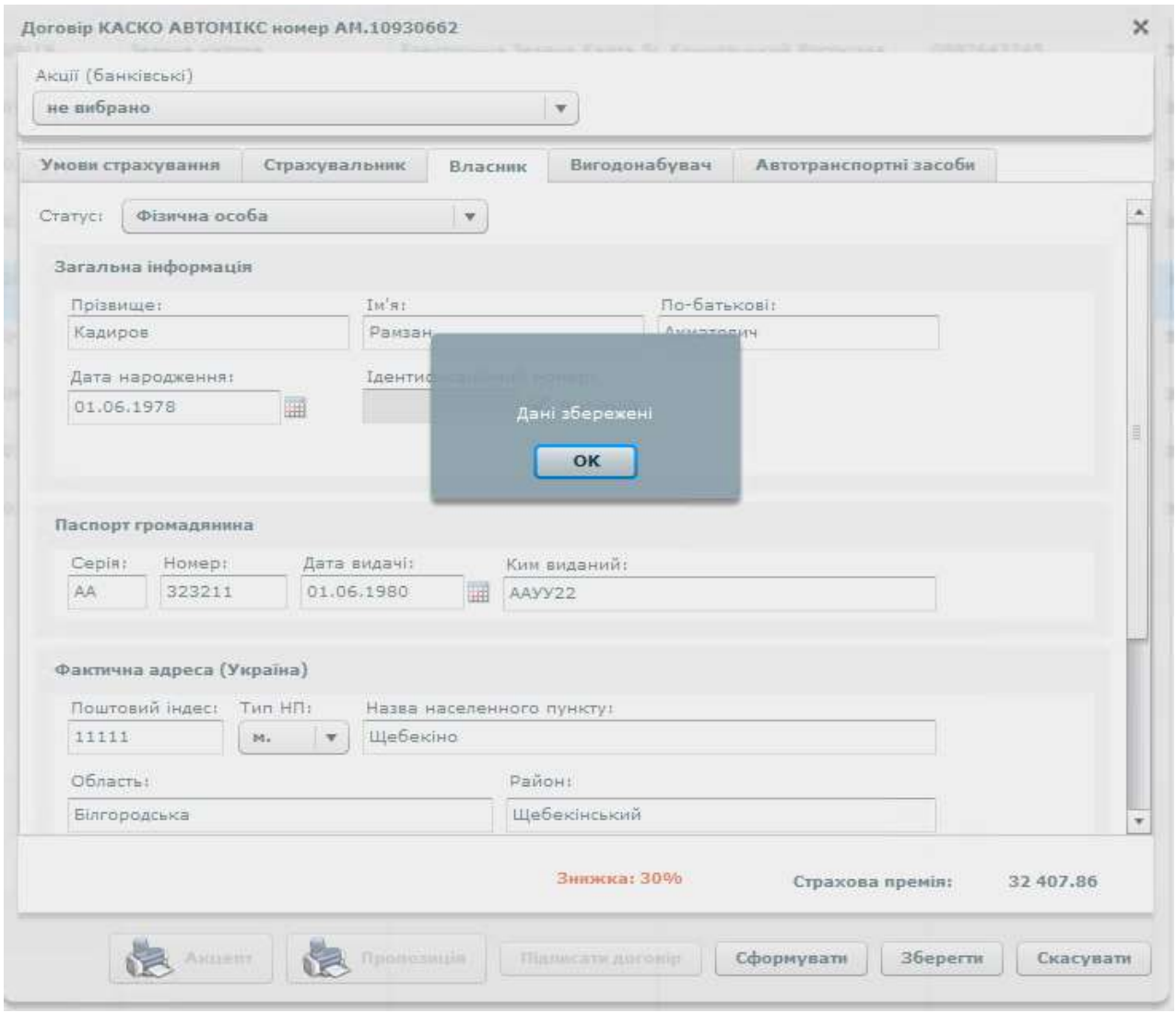


Рисунок 3.1 – Результат спроби зберегти договір з підсанкційною особою

Але вже при спробі сформувати договір в статусі проект, після всіх визначених перевірок користувач отримує відповідь на пошту, що в щойно оформленому договорі наявні підсанкційні особи. Як це виглядає для нього наведено на рисунку 3.2:

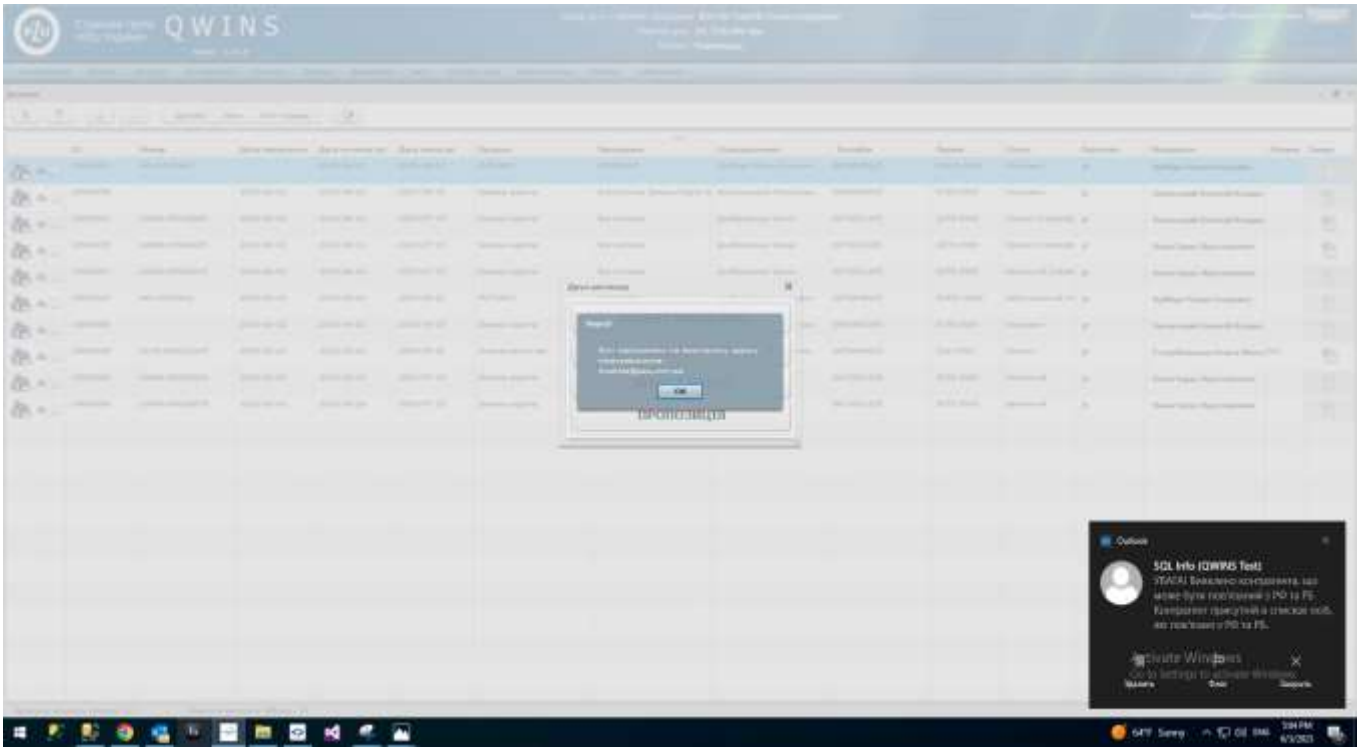


Рисунок 3.2 – Результат формування договору з підсанкційною особою

Далі на рис. 3.3 і 3.4 наведено прилади листів, які отримує продавець і відповідальна особа в відділу фінансового моніторингу:

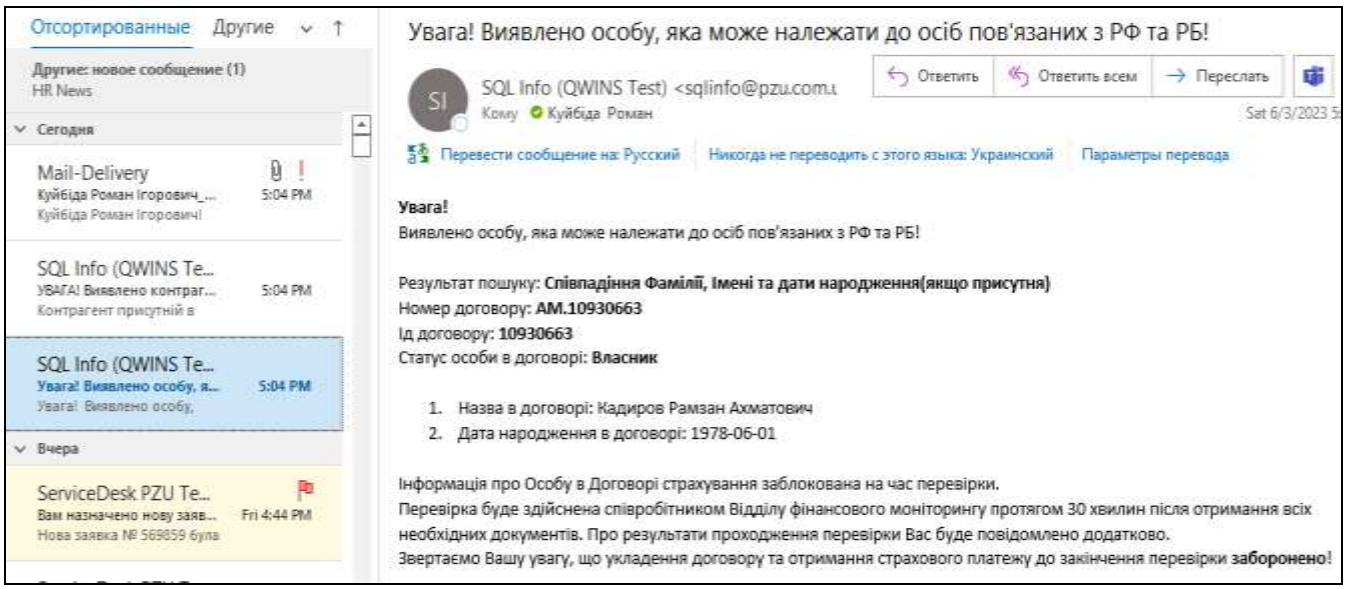


Рисунок 3.3 – Лист для продавця який намагається реалізувати договір підсанкційному контрагенту

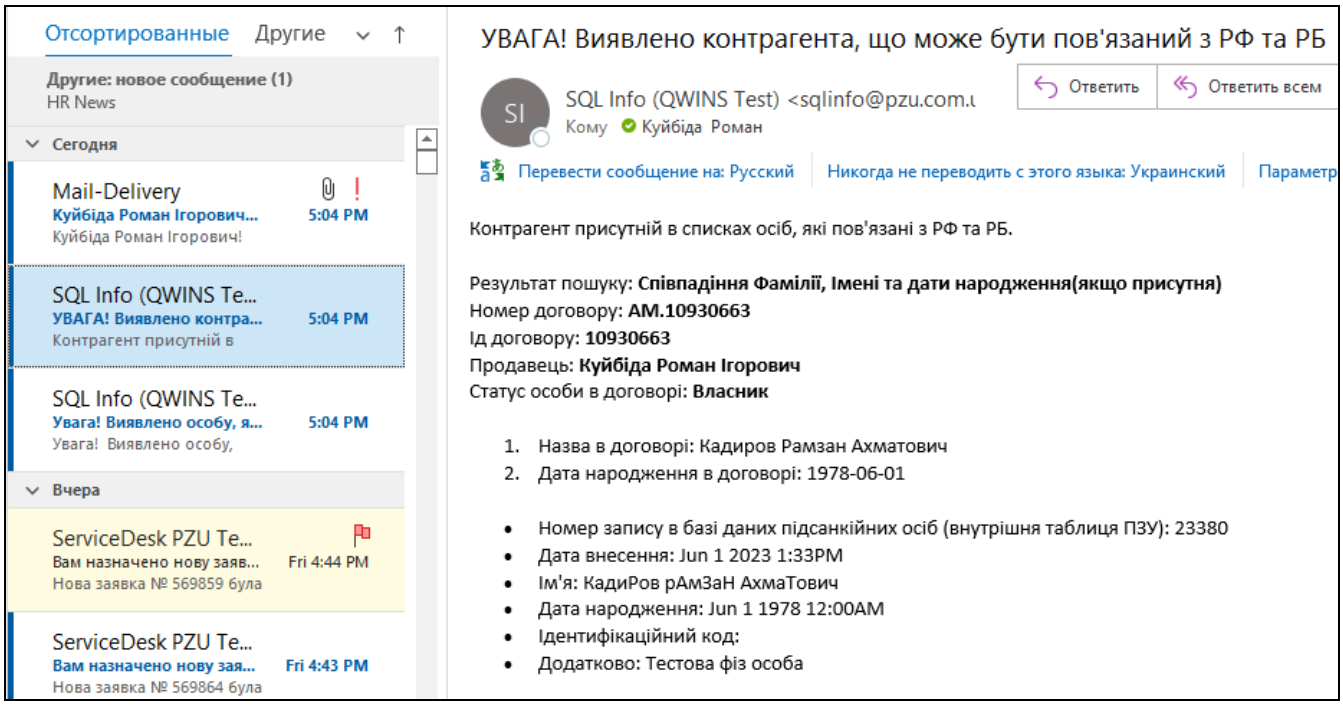


Рисунок 3.4 – Лист з інформацією для фінансового моніторингу

Таким чином виконано всі вимоги ПЗУ Україна щодо моделі перевірки контрагентів на наявність в санкційних списках. Але чи є такий метод на всі 100%? Розглянемо результати тестування на вразливість до SQL-ін’єкцій в наступному розділі.

3.4 Вразливість до SQL-ін’єкцій і рекомендації щодо покращення кібербезпеки

З розділу 2.3 було встановлено що в система є вразливою для SQL-ін’єкцій, що може складати пряму втрати або порушення цілісності даних в БД, що в свою чергу може вплинути на точність перевірок контрагентів. Також якщо покладатись на дані тестування які були в таблиці 2.2 можна оцінити рівень критичності вразливості системи за допомогою калькулятора Common Vulnerability Scoring System Version 3.0 Calculator (Системи Оцінки Загальної Вразливості). Результат оцінки калькулятора вразливостей нараховує вразливості найбільший бал (10.0) – що визначає її як критичну. На рисунку 3.5 наведено інтерфейс калькулятора з результатом оцінки.

Рисунок 3.5 – Оцінка виявленої вразливості

Виходячи з даних наведених вище можна навести наступні рекомендації щодо усунення критичної вразливості:

1) Використання підготовлених запитів (з параметризованими запитами).

Параметризовані запити, також відомі як підготовлені запити, є ефективним методом захисту від SQL-ін'єкцій і використовуються для забезпечення безпеки взаємодії з базою даних. Цей підхід полягає в тому, що замість безпосереднього включення вхідних даних до SQL-запиту, використовуються плейсхолдери або параметри. Значення для цих параметрів підставляються в запит після того, як він був інтерпретований базою даних, що дозволяє уникнути проблем, пов'язаних з інтерпретацією вхідних даних як частини SQL коду.

Одним із ключових переваг параметризованих запитів є те, що вони дозволяють використовувати попередньо скомпільовані та оптимізовані плани виконання запитів. При виконанні параметризованого запиту, база даних вже має план виконання для нього, що знижує накладні витрати на оптимізацію та виконання запиту. Це призводить до покращення продуктивності та швидкодії бази даних.

Крім того, використання параметризованих запитів забезпечує важливий рівень безпеки. Оскільки значення підставляються в запит після його інтерпретації базою даних, ін’єкції SQL-коду через вхідні дані стають

неможливими. Це допомагає запобігти атакам, які спрямовані на зловживання довіри до вхідних даних і спробам виконання шкідливого SQL-коду.

Додатковою перевагою використання параметризованих запитів є покращена читабельність та підтримка коду. Код, що використовує параметризовані запити, зазвичай більш зрозумілий і легко змінюється. Це полегшує розробку, підтримку та налагодження програм, що використовують базу даних.

Узагалі, використання параметризованих запитів є рекомендованим підходом для розробки програм, що взаємодіють з базою даних. Вони не лише забезпечують безпеку від SQL-ін'єкцій, але й покращують продуктивність, читабельність та підтримку коду. Розробники повинні активно використовувати параметризовані запити у своїх проектах, щоб забезпечити надійність та ефективність роботи з базою даних.

2) Використання збережених процедур.

Збережені процедури є ще одним засобом, який може допомогти в захисті від SQL-ін'єкцій. Вони є набором SQL-запитів та логіки, які зберігаються безпосередньо в базі даних і можуть бути викликані за допомогою відповідного імені.

Однією з переваг збережених процедур є їх здатність використовувати параметризовані запити, що дозволяє попередити SQL-ін'єкції. Замість конкатенації строк для створення SQL-запитів, збережені процедури можуть використовувати параметри, які передаються у запиті. Це значно знижує ризик вразливості до SQL-ін'єкцій, оскільки вхідні дані не інтерпретуються як частини SQL-коду, а вважаються значеннями параметрів.

Проте, важливо пам'ятати, що збережені процедури не є універсальним захистом від SQL-ін'єкцій. Якщо вони використовуються неправильно і дозволяють конкатенацію строк для створення SQL-запитів всередині процедури, вони все ж можуть стати вразливими до SQL-ін'єкцій. Тому, правильна розробка та використання збережених процедур є важливим аспектом безпеки бази даних.

Крім того, використання збережених процедур може сприяти забезпеченню безпеки шляхом скриття внутрішньої структури бази даних від зовнішнього світу. Замість прямого доступу до таблиць та схем бази даних, зовнішні користувачі можуть викликати відповідні збережені процедури, що дозволяє контролювати доступ до даних та захищати їх від несанкціонованого змінення або витоку.

Загалом, використання збережених процедур разом з параметризованими запитами може позитивно вплинути на безпеку бази даних, знижуючи ризик SQL-ін'єкцій і обмежуючи доступ до внутрішньої структури. Проте, слід бути уважними при розробці збережених процедур та впевнитися в їх правильному використанні для досягнення найвищого рівня безпеки.

3) Перевірка введених даних згідно білого списку (white list).

Використання білого списку для перевірки даних є надзвичайно ефективним підходом до забезпечення безпеки та запобігання вразливості до небезпечних вхідних даних. Білий список, відомий також як список допустимих значень, визначає, які значення або формати даних є прийнятними і дозволеними для використання в програмному коді або операціях з базою даних.

У цьому методі перевірки даних виключається будь-яке значення або формат, яке не знаходиться у білому списку. За допомогою цього підходу можна точно визначити, які дані допускаються, і відкинути будь-які інші дані, незалежно від того, як вони були надані. Це значно знижує ризик небезпечних або некоректних даних, які можуть спричинити уразливості, помилки або порушення безпеки системи.

Використання білого списку для перевірки даних може забезпечити надійний контроль над вхідними даними, забезпечуючи, що лише валідні, очікувані та допустимі значення можуть бути оброблені або використані в програмі. Цей підхід дозволяє позбутися від залежності від зовнішніх даних та небажаних вхідних параметрів, що забезпечує більшу безпеку та надійність програмного забезпечення.

Важливо враховувати, що використання білого списку може мати певні обмеження. Наприклад, цей підхід може вимагати регулярного оновлення списку допустимих значень, щоб відображати зміни в додатку або базі даних. Крім того, цей метод може бути менш гнучким, оскільки не дозволяє обробляти непередбачувані або невідомі значення. Тому важливо ретельно розглядати весь діапазон можливих даних та упевнитися, що білий список відповідає потребам програми та безпековим вимогам.

Незважаючи на обмеження, використання білого списку для перевірки даних є потужним інструментом безпеки, який може значно знизити ризик небезпечних вхідних даних та ін'єкцій SQL. Цей метод сприяє створенню надійного та стійкого програмного забезпечення, яке захищене від вразливостей і небажаних впливів.

4) Перевірка і валідація усіх даних введених користувачем.

Після того, як дані отримані від користувачів, їх необхідно піддати ретельній перевірці та валідації, щоб гарантувати їхню безпеку та правильне використання у SQL запитах. Це важливий крок для запобігання SQL-ін’єкціям та некоректній обробці даних.

Одним з методів перевірки даних є використання регулярних виразів, які дозволяють визначити правила та шаблони для прийнятних значень. Регулярні вирази використовуються для порівняння вхідних даних з заданими шаблонами, що дозволяє виявляти невідповідності або некоректні значення. Наприклад, за допомогою регулярного виразу можна перевірити, чи відповідає введений електронний адрес формату електронної пошти.

Крім регулярних виразів, більшість мов програмування надають спеціальні функції та класи для перевірки даних. Ці функції дозволяють валідувати різні аспекти даних, такі як довжина рядка, тип даних (наприклад, число або рядок), формат дати та інші. Використовуючи ці функції, можна забезпечити, що дані відповідають визначеним критеріям перед їх використанням у SQL запитах.

Окрім перевірки самого вмісту даних, валідація може також включати перевірку на відповідність конкретному набору допустимих значень. Наприклад,

можна використовувати білий список, де передбачено список припустимих значень або критеріїв, що допустимі для конкретного поля або операції. Цей підхід дозволяє відкинути будь-які неприпустимі дані та забезпечити, що використовуються лише коректні значення.

Важливо зауважити, що перевірка та валідація даних повинна здійснюватися як на стороні клієнта, так і на стороні сервера. Перевірка на стороні клієнта може забезпечити більш оперативну зворотну зв'язок з користувачем та попередити надіслання некоректних даних до сервера. Однак, необхідно також здійснювати перевірку на стороні сервера, оскільки дані, які передаються з клієнта, можуть бути підробленими або обходити перевірки на стороні клієнта.

Загальною метою перевірки та валідації даних є забезпечення відповідності вхідних даних визначеним правилам та критеріям. Цей підхід допомагає запобігти SQL-ін’єкціям, виконанню небажаних запитів до бази даних та некоректному використанню даних, що може призвести до вразливостей та проблем з безпекою системи.

5) Забезпечення найменших привілеїв користувачів.

Принцип найменших привілеїв (Principle of Least Privilege – PoLP) є важливим аспектом забезпечення безпеки системи. Він передбачає, що кожному користувачеві або процесу надаються тільки ті привілеї, які є необхідними для виконання їхніх конкретних функцій або завдань. Це означає, що кожен обліковий запис отримує доступ лише до обмеженого набору ресурсів і операцій, необхідних для його роботи, і не має зайвих або непотрібних привілеїв.

Використання принципу найменших привілеїв має декілька важливих переваг. По-перше, це обмежує можливість пошкодження або компрометації системи у разі зловмисного використання облікового запису або вразливості. Якщо користувач або процес має лише обмежений доступ, то потенційний збиток, який може бути завданий, обмежений його привілеями.

По-друге, принцип найменших привілеїв сприяє зменшенню ризику людських помилок. Зменшення кількості доступних привілеїв для користувачів

або процесів зменшує ймовірність неправильної або несанкціонованої дії, оскільки доступ до критичних або небезпечних операцій обмежений.

Крім того, використання принципу найменших привілеїв допомагає зменшити потенційний вплив атаки, якщо обліковий запис користувача стає компрометованим. Навіть якщо зловмисник здобуде доступ до такого облікового запису, обмежені привілеї дозволять обмежити його можливості виконання шкідливих дій і поширення збитків по системі.

Принцип найменших привілеїв також сприяє легкості адміністрування системи. Зменшення привілеїв для кожного облікового запису дозволяє краще контролювати доступ та зменшує необхідність управління складними наборами привілеїв для кожного користувача окремо.

У випадку баз даних, застосування принципу найменших привілеїв означає, що кожен користувач має доступ лише до тих таблиць, стовпців і операцій, які безпосередньо потрібні для його роботи. Наприклад, якщо користувач має лише читаючі права на певні таблиці і не має можливості виконувати записи або змінювати структуру бази даних, то ризик небажаних дій або нанесення шкоди обмежується.

Отже, використання принципу найменших привілеїв є важливою складовою безпеки системи та баз даних, оскільки він допомагає зменшити ризик зловмисного використання, помилок та поширення збитків. Цей принцип слід застосовувати при розробці систем та при визначенні привілеїв для користувачів та процесів.

6) Виконання перевірки введених даних по білому списку як вторинна лінія оборони.

Крім того, використання білого списку дозволяє вам виключити або обмежити використання певних типів даних, значень або параметрів у SQL запитах. Ви можете створити список допустимих значень, які вважаються безпечними для використання в запитах, і відхиляти будь-які дані, які не входять до цього списку.

Наприклад, якщо ви маєте форму для введення даних користувачем і потрібно обмежити використання певних символів або типів даних, ви можете створити білий список, що містить дозволені значення. Під час виконання SQL запиту ви перевіряєте, чи належить введене значення до білого списку. Якщо воно не збігається з жодним значенням у списку, ви можете відхилити запит або вжити інших заходів безпеки.

Використання білого списку є ефективним доповненням до параметризованих запитів та збережених процедур, оскільки воно забезпечує додатковий шар контролю над даними, що використовуються у запитах. Це може допомогти уникнути вразливостей, пов'язаних з SQL-ін’єкціями, навіть у випадках, коли використовуються захисні механізми, такі як підготовлені запити.

Однак слід пам'ятати, що білий список сам по собі не є бездоганним заходом безпеки. Він вимагає добре побудованого та підтримуваного списку дозволених значень, а також правильної реалізації перевірки відповідності значень списку. Потрібно ретельно враховувати можливі зміни або оновлення списку при зміні вимог до системи або додаванні нових функцій.

Таким чином, використання білого списку, як додаткового заходу безпеки разом з параметризованими запитами та збереженими процедурами, може підвищити рівень захисту системи від SQL-ін’єкцій та зменшити ризик вразливостей, пов'язаних з обробкою вхідних даних.

ВИСНОВКИ

У даній дипломній роботі було проведено детальний аналіз та розробка системи перевірки контрагентів щодо зв'язку з підсанкційними країнами з метою покращення безпеки підприємства. Результати дослідження свідчать про важливість і актуальність такої системи як інструмента для забезпечення безпеки та легальності бізнес-процесів.

У першому розділі дипломної роботи були розглянуті теоретичні аспекти системи перевірки контрагентів, її значення для бізнесу та держави, а також нормативно-правове забезпечення та наслідки недотримання санкційного режиму.

У другому розділі було проведено розбір технічного завдання та аналіз реалізації системи перевірки контрагентів. Була розроблена концептуальна модель та описана архітектура системи. Також було проведено аналіз на вразливість до SQL-ін'єкцій для забезпечення безпеки системи.

У третьому розділі було розроблено та реалізовано засоби перевірки контрагентів з урахуванням виявлених вразливостей до SQL-ін'єкцій. Після реалізації були проведені тестування, які підтвердили працездатність та ефективність розробленої системи.

Отже, на основі проведеного дослідження можна зробити висновок, що розроблена система перевірки контрагентів щодо зв'язку з підсанкційними країнами відповідає поставленим вимогам і може бути успішно використана для забезпечення безпеки та легальності бізнес-процесів підприємства. Результати роботи є корисними для компаній та організацій, які мають потребу у перевірці своїх контрагентів щодо зв'язку з підсанкційними країнами та бажають підвищити рівень безпеки своїх операцій.

Крім того, розроблена система перевірки контрагентів може сприяти виконанню вимог міжнародних санкційних режимів, що покликані обмежити торгівлю та фінансові відносини з підсанкційними країнами. Вона допоможе

підприємствам уникнути можливих правових порушень, втрати репутації та фінансових санкцій, пов'язаних з незаконними торговими операціями.

Отже, на основі проведеного дослідження можна зробити висновок, що реалізація системи перевірки контрагентів та впровадження рекомендацій щодо попередження SQL атак є ефективними заходами для покращення безпеки підприємства. Розроблена система перевірки контрагентів відповідає вимогам та може успішно використовуватися для забезпечення безпеки та легальності бізнес-процесів.

Результати дослідження мають велике значення для підприємств, які мають потребу у перевірці своїх контрагентів щодо зв'язку з підсанкційними країнами та бажають запобігти можливим SQL атакам. Впровадження рекомендацій з попередження SQL атак допоможе зменшити ризик порушення безпеки даних та захистити підприємство від потенційних кібератак.

Однак, важливо пам'ятати, що система перевірки контрагентів та рекомендації щодо попередження SQL атак є лише частиною комплексної стратегії забезпечення безпеки. Для досягнення максимальної ефективності, їх слід поєднувати з іншими заходами, такими як навчання персоналу, використання захищених систем і мереж, резервне копіювання даних та постійне вдосконалення заходів безпеки.

Можливі напрямки подальших досліджень включають розширення функціональних можливостей системи перевірки контрагентів, а також вдосконалення рекомендацій щодо попередження SQL атак шляхом врахування нових видів загроз і вразливостей. Крім того, можна розглянути можливість автоматизації процесів перевірки контрагентів та виявлення SQL атак за допомогою машинного навчання та штучного інтелекту.

В цілому, дане дослідження сприяє підвищенню рівня безпеки підприємств шляхом реалізації системи перевірки контрагентів та розробки рекомендацій щодо попередження SQL атак. Використання цих заходів допоможе забезпечити захист від потенційних загроз і зберегти надійність та інтегритет бізнес-процесів підприємства.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бухгалтерський канал №1. Як перевірити через е-кабінет чи ризиковий контрагент | 11.05.2023, 2023. YouTube. URL: https://www.youtube.com/watch?v=oQOMvgFSlHI (дата звернення: 17.06.2023).
2. Крьока С. Попит на сервіси перевірки контрагентів зростає у всьому світі. Як уникнути токсичних клієнтів та бізнес-партнерів і не потрапити під санкції – Delo.ua. Останні новини України та світу онлайн – Головний діловий портал Delo.ua. URL: https://delo.ua/telecom/popit-na-servisi-perevirki-kontragentiv-zrostaje-u-vsyomu-svitu-yak-uniknuti-toksicnix-klijentiv-ta-biznes-partneriv-i-ne-potrapiti-pid-sankciyi-414950/ (дата звернення: 17.06.2023).
3. Методи забезпечення комплаєнсу третіх сторін – Юридична Газета. Юридична газета – онлайн версія. URL: https://yur-gazeta.com/publications/practice/korporativne-pravo-ma/-metodi-zabezpechennya-komplaensu-tretih-storin.html (дата звернення: 17.06.2023).
4. Міжнародні санкції проти росії через вторгнення в Україну. Юридична фірма GOLAW – комплексні юридичні послуги та консультації. URL: https://golaw.ua/ua/insights/publication/mizhnarodni-sankcziyi-proti-rosiyi-cherez-vtorgnennya-v-ukrayinu/ (дата звернення: 17.06.2023).
5. Віктор Шульга. Підозрілий контрагент: на що слід звернути увагу під час перевірки | Think brave. Think brave | Останні новини бізнесу України. URL: https://biz.ligazakon.net/analitycs/206894_pdozrliy-kontragent-na-shcho-sld-zvernuti-uvagu-pd-chas-perevrki (дата звернення: 17.06.2023).
6. Механізм державного регулювання банківської діяльності. URL: http://socrates.vsau.org/b04213/html/cards/getfile.php/17522.pdf (дата звернення: 17.06.2023).
7. Олександра Кознова. Законопроєкт про стимулювання розвитку зеленої генерації пройшов перше читання | Think brave. Think brave | Останні новини бізнесу України.

URL: https://biz.ligazakon.net/news/219284_zakonoprokt-pro-stimulyuvannya-rozvitku-zeleno-generats-proyshov-pershe-chitannya (дата звернення: 17.06.2023).

8. Боротьба з переведенням у готівку: які методи використовують податківці? "Вісник МСФЗ" №10, 2020р. URL: https://msfz.ligazakon.ua/ua/magazine_article/FZ002300 (дата звернення: 17.06.2023).
9. Підтримка україни з боку ЄС | європейський союз. European Union. URL: https://european-union.europa.eu/priorities-and-actions/eu-support-ukraine_uk (дата звернення: 17.06.2023).
10. Положення про ліцензування та реєстрацію. Національний банк України. URL: https://bank.gov.ua/admin_uploads/article/proekt_2021-06-30-1.pdf (дата звернення: 17.06.2023).
11. Довіряй, але перевіряй: навіщо бізнесу потрібен integrity due diligence. Mind.ua. URL: https://mind.ua/openmind/20203282-doviryaj-ale-pereviryaj-navishcho-biznesu-potriben-integrity-due-diligence (дата звернення: 17.06.2023).
12. Про затвердження Положення про здійснення банками фінансового моніторингу. Офіційний вебпортал парламенту України. URL: https://zakon.rada.gov.ua/go/v0065500-20 (дата звернення: 17.06.2023).
13. Хто такий контрагент і що це означає в бізнесі – Юридична компанія ENTIRE. URL: https://entire.com.ua/uk/news/761-khto-takyi-kontrahent-i-shcho-tse-oznachaie-v-biznesi.html (дата звернення: 17.06.2023).
14. Вибір та перевірка контрагента під час укладання зовнішньоекономічного договору. URL: https://pravdop.com/ua/publications/praktiki-kompanii/vibor-i-proverka-kontragenta-pri-zaklyuchenii-vneshneekonomicheskogo-dogovora-06-2022-138/ (дата звернення: 17.06.2023).
15. What is Anti-Money Laundering?. Sanction Scanner: Anti-Money Laundering Solutions – Sanction Scanner. URL: https://sanctionscanner.com/knowledge-base/anti-money-laundering-aml-

49#:~:text=In%20the%20most%20general%20sense,from%20entering%20the%20financial%20system. (date of access: 17.06.2023).

16. Міжнародні санкції: що потрібно знати бізнесу? – European Business Association. European Business Association. URL: https://eba.com.ua/mizhnarodni-sanktsiyi-shho-potribno-znaty-biznesu/ (дата звернення: 17.06.2023).
17. Про внесення змін до Закону України. URL: https://ips.ligazakon.net/document/view/ji08700a (дата звернення: 17.06.2023).
18. Закон України «Про санкції» URL: https://zakon.rada.gov.ua/laws/show/1644-18#Text
19. Проєкт Закону № 8384 від 25.01.2023 URL: https://itd.rada.gov.ua/billInfo/Bills/Card/41227
20. Указ Президента України від 7 січня 2023 року URL: https://www.president.gov.ua/documents/42023-45517
21. Як перевірити бізнес партнера у воєнний час. KPMG. URL: https://kpmg.com/ua/uk/home/media/press-releases/2022/05/yak-pereviryty-biznes-partnera-u-voyennyy-chas.html (дата звернення: 17.06.2023).
22. СВІТОВЕ ГОСПОДАРСТВО ТА НАЦІОНАЛЬНА ЕКОНОМІКА. Освітній проект для вчителів. URL: https://naurok.com.ua /test/svitove-gospodarstvo-ta-nacionalna-ekonomika-381199.html (дата звернення: 17.06.2023).
23. Закон України «Про захист персональних даних» URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text
24. Types of Database Attacks URL: https://www.salvationdata.com/crime-cases/6-types-of-database-attacks-hackers-use-to-obtain-unauthorized-access/ (дата звернення: 17.06.2023).

70

Додаток А

ПРОТОКОЛ ПЕРЕВІРКИ КВАЛІФІКАЦІЙНОЇ РОБОТИ НА НАЯВНІСТЬ ТЕКСТОВИХ ЗАПОЗИЧЕНЬ

Назва роботи: Система перевірки контрагентів щодо зв'язку з підсанкційними країнами.

Автор роботи: Куйбіда Роман Ігорович

Тип роботи: бакалаврська дипломна робота .
(БДР, МКР)

Підрозділ кафедра захисту інформації ФІТКІ .
(кафедра, факультет)

Показники звіту подібності Unicheck

Оригінальність – 96,5%. Схожість – 3,5%.

Аналіз звіту подібності (відмітити потрібне):

√ 1. Запозичення, виявлені у роботі, оформлені коректно і не містять ознак плагіату.

□ 2. Виявлені у роботі запозичення не мають ознак плагіату, але їх надмірна кількість викликає сумніви щодо цінності роботи і відсутності самостійності її виконання автором. Роботу направити на розгляд експертної комісії кафедри.

□ 3. Виявлені у роботі запозичення є недобросовісними і мають ознаки плагіату та/або в ній містяться навмисні спотворення тексту, що вказують на спроби приховування недобросовісних запозичень.

Особа, відповідальна за перевірку _____ Каплун В. А.
(підпис) (прізвище, ініціали)

Ознайомлені з повним звітом подібності, який був згенерований системою Unicheck щодо роботи.

Автор роботи _____ Куйбіда Р. І.

Керівник роботи _____ Лукічов І. В.

Додаток Б

Код програми

```
if (OBJECT_ID('dbo.ContractMembers_Check', 'P') is NULL)
     exec('create procedure [dbo].[ContractMembers_Check] as')
go

alter procedure [dbo].[ContractMembers_Check]
(
     @xml xml
     ,@ContractID int
)
as
begin
/*
Date: 20.10.2020
Creator: ipaseka
Description: Перевірка учасників договору
*/
set nocount on

     declare
     @CompanyName nvarchar(1000),
     @Surname nvarchar(128),
     @Name nvarchar(128),
     @FatherName nvarchar(128),
     @DateOfBorn nvarchar(16),
     @Inn nvarchar(16),
     @MemberType nvarchar(128),
     @TypeName nvarchar(256),
     @BankMFO int

     declare MembersCursor cursor for
     select
          Companyname
          ,Surname
          ,Name
          ,Fathername
          ,Dateofborn
          ,Inn
          ,MemberType
          ,TypeName
          ,BankMFO
     from fnContractMembers_GetFromXML(@xml)
     open MembersCursor
     fetch next from MembersCursor into @CompanyName, @Surname, @Name,
@FatherName, @DateOfBorn, @Inn, @MemberType, @TypeName, @BankMFO
     while @@FETCH_STATUS = 0
          begin
               exec ContractMembers_Terrorism_Check @ContractID,
@CompanyName, @Surname, @Name, @FatherName, @DateOfBorn, @Inn,
@MemberType
```

```
                exec ContractMembers_Sanction_Check @ContractID,
@CompanyName, @Surname, @Name, @FatherName, @DateOfBorn, @Inn,
@MemberType

                fetch next from MembersCursor into @CompanyName,
@Surname, @Name, @FatherName, @DateOfBorn, @Inn, @MemberType, @TypeName,
@BankMFO
           end
      close MembersCursor
      deallocate MembersCursor

end
go

create or alter procedure [dbo].[ContractMembers_Sanction_Check]
(
      @ContractID int,
      @CompanyName nvarchar(1000),
      @Surname nvarchar(128),
      @Name nvarchar(128),
      @FatherName nvarchar(128),
      @DateOfBorn nvarchar(16),
      @Inn nvarchar(20),
      @MemberType nvarchar(128)
)
as
begin
/*
Date: 03.05.2023
Creator: rkuibida
Description: Перевірка учасників договору на наявність в санкійних
списках
*/
set nocount on

      declare @ContractNumber nvarchar(256), @SellerName nvarchar(256),
@SellerMail nvarchar(128)
                ,@SanctionId int, @SanctionName nvarchar(1000),
@SearchComment nvarchar(256)

      select
            @ContractNumber = c.ContractNumber
            ,@SellerName = u.UserName
            ,@SellerMail = u.UserEMAIL
      from Contract c
      inner join [User] u on u.MemberID = c.ContractSellerID
      where c.ContractID = @ContractID

      select @SanctionId = SanctionId, @SanctionName = SanctionName,
@SearchComment = SearchComment
      from fnContractMembers_SanctionSelect(@CompanyName, @Surname,
@Name, @FatherName, @DateOfBorn, @Inn)

      if @SanctionId is null
            return;

      --locking contract
```

```
     insert into ContractStatus select 39, @ContractID,
'ContractMembers_Sanction_Check', getdate() -- Заблокований по
санкційному списку

     declare @SellerLetterBody nvarchar(max) =
     replace(replace(cast((select
          '<p><b>Увага!</b><br/>Виявлено особу, яка може належати до
осіб пов''язаних з РФ та РБ!<br/>'
          ,concat('<br/>Результат пошуку: <b>', @SearchComment, '</b>')
          ,concat('<br/>Номер договору: <b>', @ContractNumber, '</b>')
          ,concat('<br/>Ід договору: <b>', cast(@ContractID as
nvarchar(50)), '</b>')
          ,concat('<br/>Статус особи в договорі: <b>', @MemberType,
'</b></p>')
          ,concat('<p><ol><li> Назва в договорі: ', iif(len(@Surname) =
0 and len(@CompanyName) > 0, @CompanyName, concat(@Surname, ' ', @Name, '
', @FatherName)), '</li>')
          ,iif(len(@DateOfBorn) > 0, concat('<li>Дата народження в
договорі: ', @DateOfBorn, '</li>'), null)
          ,iif(len(@Inn) > 0, concat('<li>Код в договорі: ', @Inn,
'</li>'), null)
          ,'</ol></p>'
          ,'Інформація про Особу в Договорі страхування заблокована на
час перевірки.<br/>'
          ,'Перевірка буде здійснена співробітником Відділу фінансового
моніторингу протягом 30 хвилин після отримання всіх необхідних
документів. Про результати проходження перевірки Вас буде повідомлено
додатково.<br/>'
          ,'Звертаємо Вашу увагу, що укладення договору та отримання
страхового платежу до закінчення перевірки <b>заборонено</b>!'
     for xml path(''), elements, type) as nvarchar(max)), '&lt;', '<'),
'&gt;', '>')

     declare @LetterBody nvarchar(max) =
     replace(replace(cast((select
          '<p>Контрагент присутній в списках осіб, які пов''язані з РФ
та РБ.<br/>'
          ,concat('<br/>Результат пошуку: <b>', @SearchComment, '</b>')
          ,concat('<br/>Номер договору: <b>', @ContractNumber, '</b>')
          ,concat('<br/>Ід договору: <b>', cast(@ContractID as
nvarchar(50)), '</b>')
          ,concat('<br/>Продавець: <b>', @SellerName, '</b>')
          ,concat('<br/>Статус особи в договорі: <b>', @MemberType,
'</b></p>')
          ,concat('<p><ol><li> Назва в договорі: ', iif(len(@Surname) =
0 and len(@CompanyName) > 0, @CompanyName, concat(@Surname, ' ', @Name, '
', @FatherName)), '</li>')
          ,iif(len(@DateOfBorn) > 0, concat('<li>Дата народження в
договорі: ', @DateOfBorn, '</li>'), null)
          ,iif(len(@Inn) > 0, concat('<li>Код в договорі: ', @Inn,
'</li>'), null)
          ,'</ol></p><p><ul>'
          ,concat('<li>Номер запису в базі даних підсанкійних осіб
(внутрішня таблиця ПЗУ): ', cast(@SanctionId as nvarchar(16)), '</li>')
          ,concat('<li>Дата внесення: ', s.DateCreate, '</li>')
          ,concat('<li>Ім''я: ', s.FullName, '</li>')
          ,concat('<li>Дата народження: ', s.DateBorn, '</li>')
          ,concat('<li>Ідентифікаційний код: ', s.INN, '</li>')
```

```
            ,concat('<li>Додатково: ', s.Comment, '</li>')
            ,'</ul></p>'
      from Sanction s
      where s.Id = @SanctionId
      --and s.FullName = @SanctionName
      for xml path(''), elements, type) as nvarchar(max)), '&lt;', '<'),
'&gt;', '>')

      exec msdb.dbo.sp_send_dbmail
            @recipients     = @SellerMail
            ,@subject = 'Увага! Виявлено особу, яка може належати до осіб
пов''язаних з РФ та РБ!'
            ,@body = @SellerLetterBody
            ,@body_format = 'HTML';

      exec msdb.dbo.sp_send_dbmail
            @recipients     =
'finmonPZU@pzu.com.ua;yharbovskyi@pzu.com.ua'
            --@recipients   = 'rkuibida@pzu.com.ua'
            ,@subject = 'УВАГА! Виявлено контрагента, що може бути
пов''язаний з РФ та РБ'
            ,@body = @LetterBody
            ,@body_format = 'HTML';
end
go
if object_id (N'dbo.fnContractMembers_SanctionSelect', N'TF') is not null
    drop function dbo.fnContractMembers_SanctionSelect;
go
create function dbo.fnContractMembers_SanctionSelect
(
      @CompanyName nvarchar(1000),
      @Surname nvarchar(128),
      @Name nvarchar(128),
      @FatherName nvarchar(128),
      @DateOfBorn nvarchar(16),
      @Inn nvarchar(20)
)
returns @SanctionsInfo table
(
    SanctionId int null,
    SanctionName nvarchar(1000) null,
      SearchComment nvarchar(256) null
)
as
begin
      declare @SanctionId int, @SanctionName nvarchar(1000),
@SearchComment nvarchar(256)

      if len(@Surname) = 0 and len(@CompanyName) > 0 -- Ur
      begin
            -- search by code
            select top 1 @SanctionId = s.Id, @SanctionName =
s.CompanyName, @SearchComment = 'Співпадіння ЄДРПОУ' from Sanction s
where s.INN = @Inn

            -- search by name if code search failed
            if @SanctionId is null
```

```
                select top 1 @SanctionId = s.Id, @SanctionName =
s.CompanyName, @SearchComment = 'Співпадіння Назви' from Sanction s where
s.CompanyName = @CompanyName and s.INN is null

     end
     else if len(@Surname) > 0 -- fiz
     begin
          declare @FullName1 nvarchar(256) =
ltrim(rtrim(concat(@Surname, ' ', @Name, ' ', @FatherName)))
          declare @FullName2 nvarchar(256) = ltrim(rtrim(concat(@Name, '
', @Surname, ' ', @FatherName)))

          -- search by code
          select top 1 @SanctionId = s.Id, @SanctionName = s.FullName,
@SearchComment = 'Співпадіння ІНН' from Sanction s where s.INN = @Inn

          -- search by name if code search failed
          if @SanctionId is null
               select top 1 @SanctionId = s.Id, @SanctionName =
s.FullName, @SearchComment = 'Співпадіння Фамілії, Імені та дати
народження(якщо присутня)' from Sanction s
               where ((s.FullName = @FullName1) or (s.FullName =
@FullName2))
               and (s.DateBorn is not null and Cast(s.DateBorn as date)
= Cast(@DateOfBorn as date))
     end

     insert into @SanctionsInfo select @SanctionId, @SanctionName,
@SearchComment

     return
end;
```

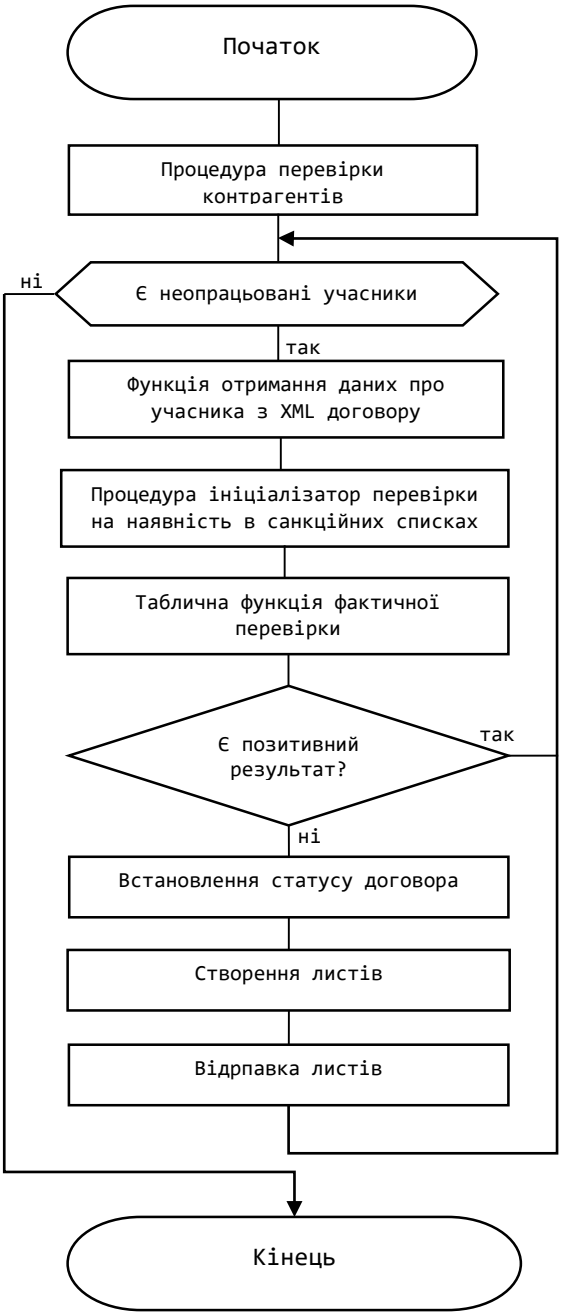
ІЛЮСТРАТИВНА ЧАСТИНА

Система перевірки контрагентів щодо зв’язку з підсанкційними країнами

Виконав: студент 4 курсу групи 1БС-19б
спеціальності 125 Кібербезпека
_____ Роман КУЙБІДА
_____ 2023 р.

Керівник: к. т. н., доцент каф. ЗІ
_____Віталій ЛУКІЧОВ
_____ 2023 р.

АЛГОРИТМ РОБОТИ СИСТЕМИ ПЕРЕВІРКИ КОНТРАГЕНТІВ З ПІДСАНКЦІЙНИМИ КРАЇНАМИ



Процес перевірки контрагентів

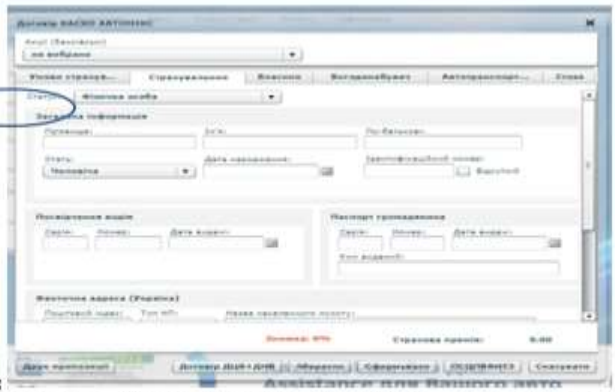
ІЛЮСТРАЦІЯ ТЕХНІЧНОГО ЗАВДАННЯ

1. **Перевірка на належність до осіб, пов'язаних з росією та білоруссю**

Доступ до таких осіб заходиться у вкладенні до цієї заявки.

Прошу дану заявку включити до роад мап.

Перевірку на наявність до осіб, пов'язаних з росією та білоруссю повинні проходити **всі** контрагенти з переліку нижче (далі по тексту – Особи) при внесенні інформації про Особу в QWINS: (по усім договорам страхування)



- страхувальники;
- власники (в договорах КАСКО Автомікс інформація про власника проходить перевірку, якщо власник має статус фізична особа/ФОП/юридична особа)

Технічне завдання

«Увага! Виявлено особу, яка може належати до осіб пов'язаних з рф та рб!

1) Назва – [ПІБ фізичної особи або найменування юридичної особи]
2) ЄДРПОУ для юридичної особи

Інформація про Особу в Договорі страхування заблокована на час перевірки. Перевірка буде здійснена співробітником Відділу фінансового моніторингу протягом 30 хвилин після отримання всіх необхідних документів. Про результати проходження перевірки Вас буде повідомлено додатково.

Звертаємо Вашу увагу, що укладення договору та отримання страхового платежу до закінчення перевірки **заборонено**!»

Технічне завдання. Приклад листа для продавця

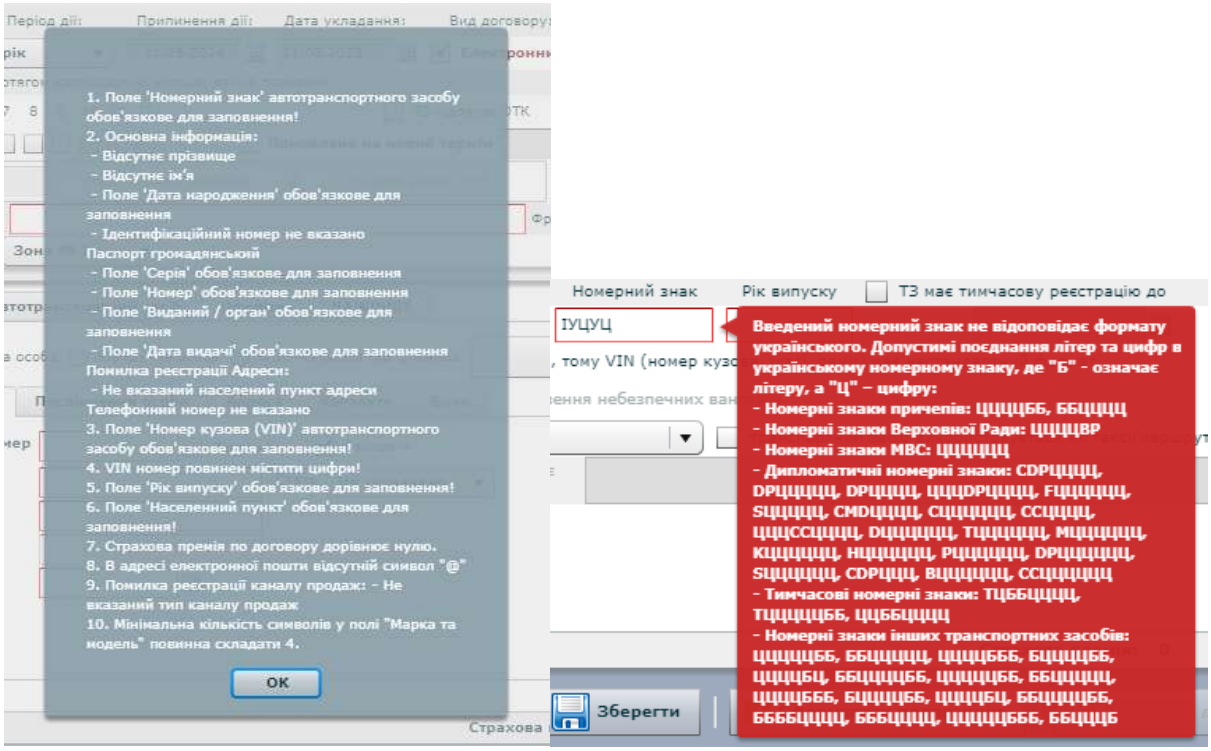
Тема листа: «УВАГА! Виявлено контрагента, що може бути пов’язаний з рф та рб».
Зміст: «Контрагент присутній в списках осіб, які пов’язані з рф та рб.

1) Критерій – [один з 3-х варіантів в залежності від того, за яким критерієм було виявлено контрагента:
   - співпадіння ЄДРПОУ – 100%;
   - співпадіння найменування – 100%;
   - співпадіння ПІП на 100%;
2) Назва – [ПІБ фізичної особи або назва юридичної особи];
3) Ідентифікаційний код - [ІПН для фіз. особи; ЄДРПОУ для юр. особи];
4) Номер та дата договору страхування;
5) Відповідальний працівник – [ПІБ працівника, який створив картку Особи в системі]»

[Всі дані щодо цієї особи з файлу]

Технічне завдання. Приклад листа для фінмоніторингу

ІЛЮСТРАЦІЯ ПРОЦЕСУ ОНОВЛЕННЯ БАЗИ ДАНИХ ЩОДО САНКЦІЙНИХ СПИСКІВ



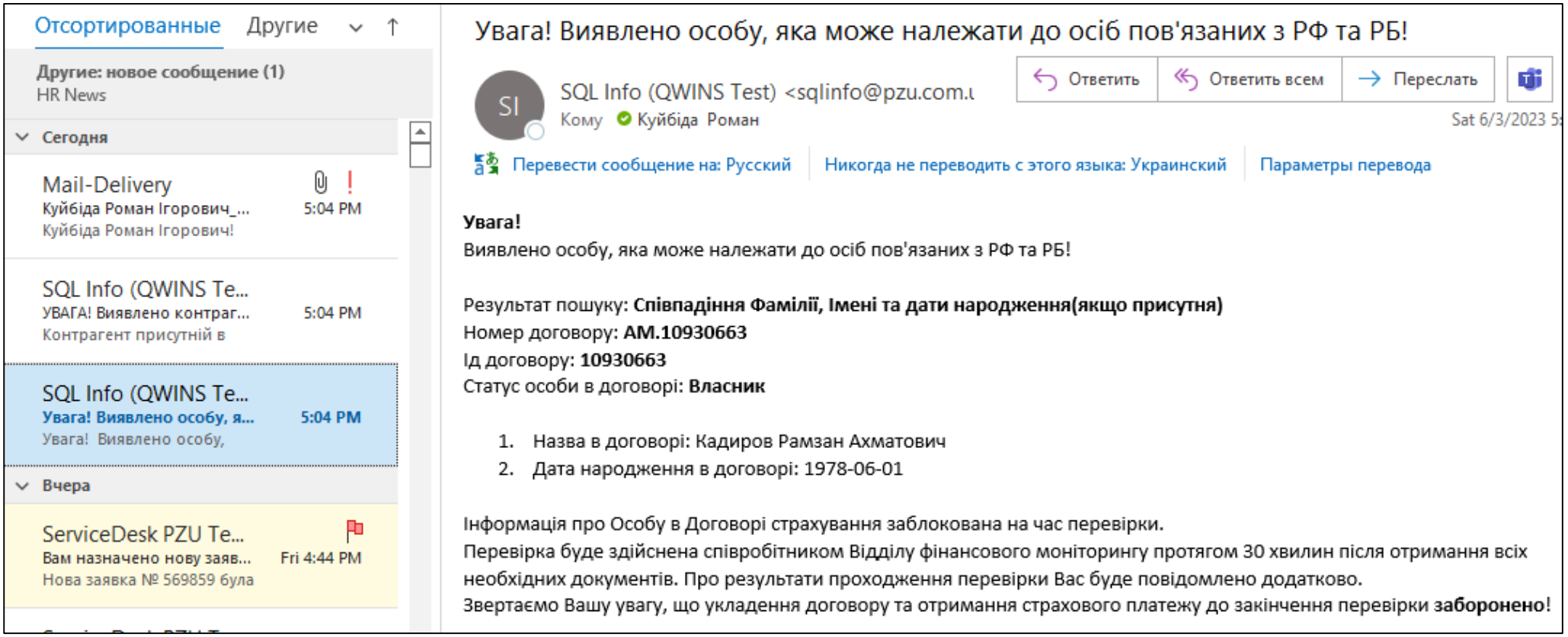
Приклад інформативного вікна про помилку в QWINS

ОЦІНКА ВИЯВЛЕНОЇ ВРАЗЛИВОСТІ

Оцінка виявленої вразливості

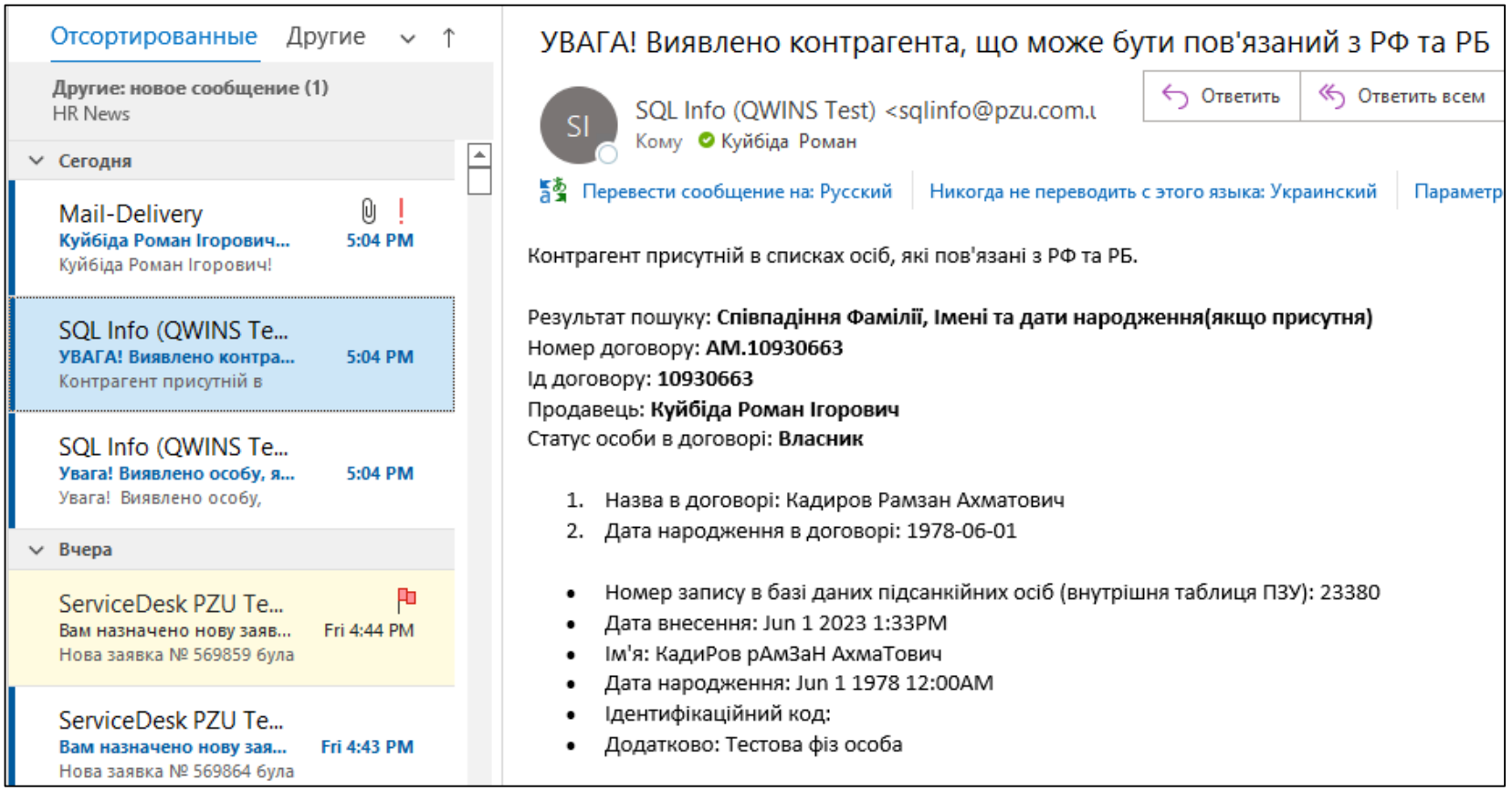
ЛИСТ ДЛЯ ПРОДАВЦЯ ЯКИЙ НАМАГАЄТЬСЯ РЕАЛІЗУВАТИ

ДОГОВІР ПІДСАНКЦІЙНОМУ КОНТРАГЕНТУ



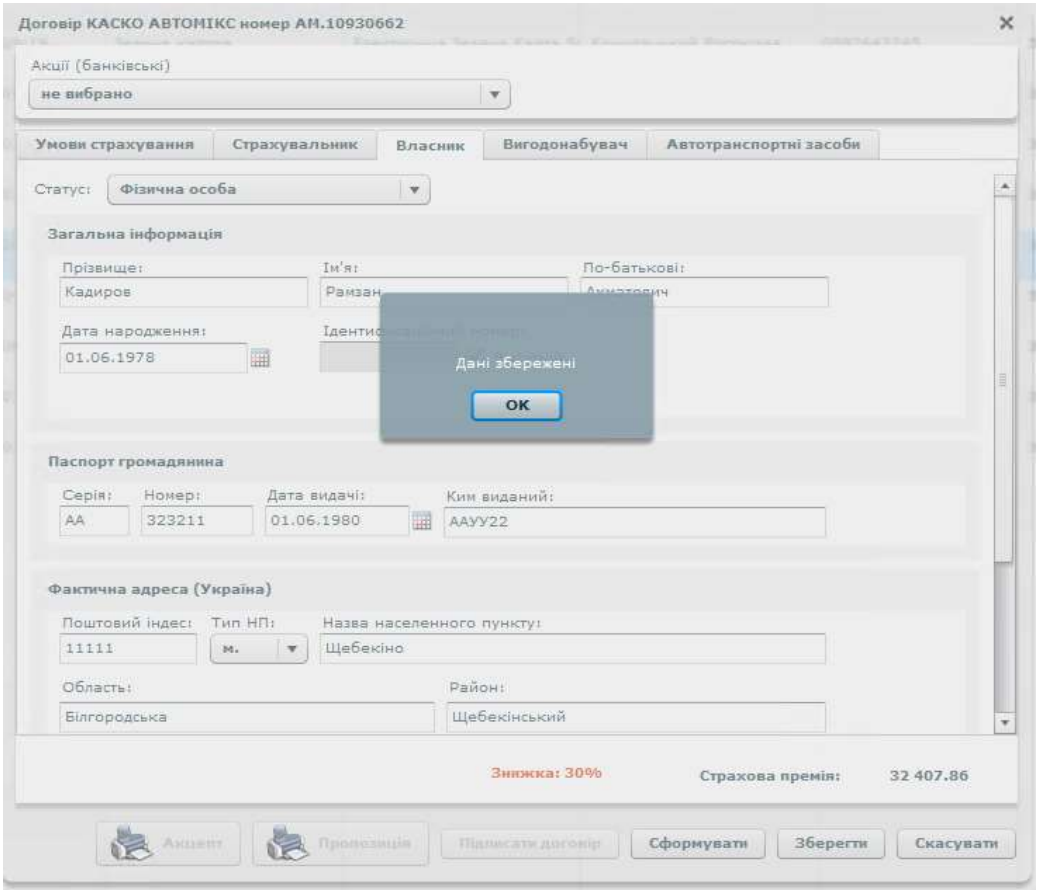
Лист для продавця який намагається реалізувати договір підсанкційному контрагенту

ЛИСТ З ІНФОРМАЦІЄЮ ДЛЯ ФІНАНСОВОГО МОНІТОРИНГУ

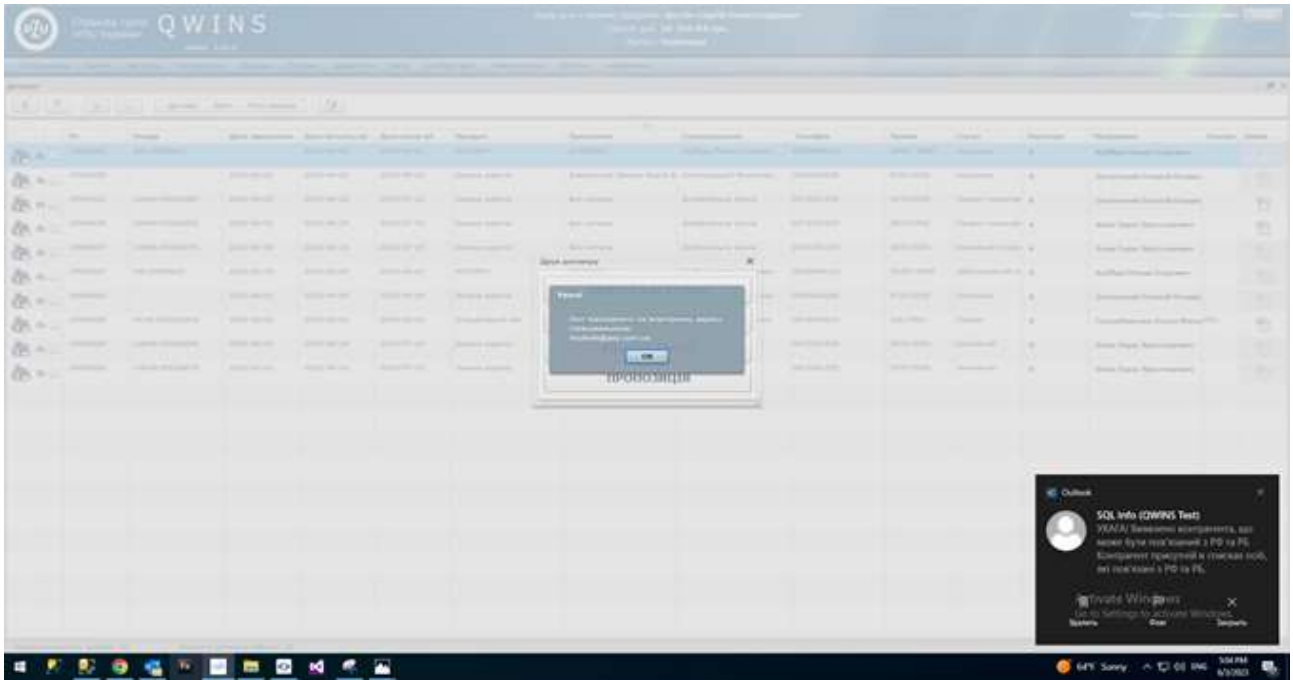


Лист з інформацією для фінансового моніторингу

РЕЗУЛЬТАТ ФОРМУВАННЯ ДОГОВОРУ З ПІДСАНКЦІЙНОЮ ОСОБОЮ



Результат спроби зберегти договір з підсанкційною особою



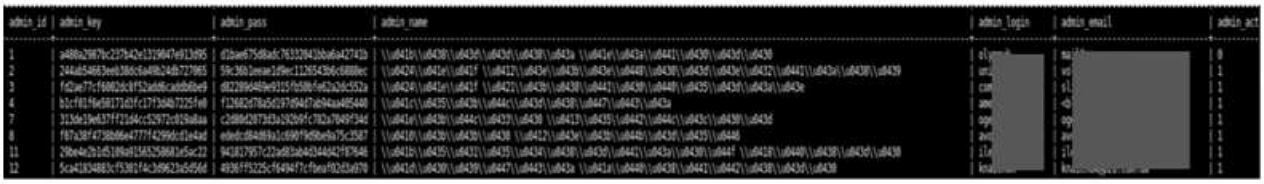
Результат формування договору з підсанкційною особою

РЕЗУЛЬТАТ SQL-ІН’ЄКЦІЇ ЯК ДОКАЗ ПРАВИЛЬНОСТІ КОНЦЕПЦІЇ (POC)

Додаток 4. Доказ правильності концепції (POC) - SQL інєкція в

Бази даних замовника	[*] information_schema [*] 7G1
Таблиці бази даних	Database: 7G1 [79 tables] +----------+ | module | | section | | translate | | acc | | admin | | adminhasacc | | answer | | answerfile | | answerlist | | article | | articlelang | | autoservice | | autoservicehasbrand | | autoservicelang | | brand | | callback | | career | | careerinfo | | careerlang | | category | | categoryhassection |

Результат SQL-ін’єкції як доказ правильності концепції (POC)



Дамп таблиці admin

ЗАТВЕРДЖУЮ
Член Правління ПрАТ СК «ПЗУ Україна»
_____ Василь ЗУБАЧ
«___» _____ 2023 р.

АКТ
про впровадження результатів бакалаврської дипломної роботи
Куйбіда Романа Ігоровича

Комісія у складі: голова комісії – директор департаменту інформаційних технологій Усенко О. О., провідний фахівець відділу розробки Куйбіда А. І, розглянувши матеріали бакалаврської роботи Куйбіди Р. І. на тему "Система перевірки контрагентів щодо зв'язку з підсанкційними країнами", склала цей акт про те, що у ПрАТ СК «ПЗУ Україна» впроваджено результати цієї роботи, а саме:

– Покращення безпеки підприємства шляхом реалізації системи перевірки контрагентів та за допомогою розробки рекомендацій щодо попередження SQL атак.

Впроваджені результати дозволяють здійснювати перевірку контрагентів при оформленні договорів страхування, що дало змогу підвищити безпеку компанії на новий рівень.

Голова комісії:
Директор департаменту ІТ _____ Олег УСЕНКО

Члени комісії:
Провідний фахівець відділу розробки _____ Андрій КУЙБІДА