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

До захисту допущено
В.о. завідувача кафедри
_____ **Микола ГРАЙВОРОНСЬКИЙ**
(підпис)
«_____»_____2021 р.

Дипломна робота

на здобуття ступеня бакалавра

за освітньо-професійною программою «Системи, технології та математичні методи кібербезпеки»
спеціальності: 125 «Кібербезпека»

на тему: Моделювання залишкового ризику для банківської інформаційної системи.

Виконав (-ла): здобувач вищої освіти **IV** курсу, групи ФБ-71
(шифр групи)
Семичастний В’ячеслав Сергійович
(прізвище, ім’я, по батькові) (підпис)

Керівник_____ _____
(посада, науковий ступінь, вчене звання, прізвище, ім’я, по батькові) (підпис)

Рецензент_____ _____
(посада, науковий ступінь, вчене звання, науковий ступінь, прізвище, ім’я, по батькові) (підпис)

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

Київ - 2021 року

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

Рівень вищої освіти - перший (бакалаврський)
Спеціальність - 125 «Кібербезпека»
Освітньо-професійна програма «Системи, технології та математичні методи кібербезпеки»

ЗАТВЕРДЖУЮ
В.о. завідувача кафедри
_____ Микола ГРАЙВОРОНСЬКИЙ
(підпис)
«___»_____2021 р.

ЗАВДАННЯ
на дипломну роботу здобувачу вищої освіти

Семичастний В’ячеслав Сергійович
(прізвище, ім’я, по батькові)

1. Тема роботи: «Моделювання залишкового ризику для банківської інформаційної системи.», керівник роботи к.т.н., доцент Гальчинський Леонід Юрійович,

затверджені наказом по університету від « »_____2021 р. №

2. Термін подання здобувачем вищої освіти роботи 07 червня 2021 р.

3. Вихідні дані до роботи: попередні дослідження методів залишкового ризику.

4. Зміст роботи: аналіз існуючих моделей залишкових ризиків, адаптація моделі залишкового ризику для банківської інформаційної системи.

5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо) Моделювання залишкового ризику для банківської інформаційної системи – презентація.

6. Дата видачі завдання 27.08.2020

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів дипломної роботи	Примітка
1	Отримання завдання	27.08.2020	виконано
2	Вивчення та аналіз літератури	27.08.2020 – 23.11.2020	виконано
3	Аналіз існуючих моделей залишкового ризику	23.11.2020 – 15.01.2021	виконано
4	Адаптація моделі	15.01.2021 – 21.03.2021	виконано
5	Дослідження роботи моделі	21.03.2021 – 01.05.2021	виконано
6	Проходження преддипломної практики	12.04.2021 – 16.05.2021	виконано
7	Написання дипломної роботи	01.04.2021 – 02.06.2021	виконано
8	Отримання допуску до захисту	03.06.2021	виконано
9	Захист дипломної роботи	16.06.2021	

Здобувач вищої освіти _____ В’ячеслав СЕМИЧАСТНИЙ
(підпис) (Власне ім’я, ПРІЗВИЩЕ)

Керівник роботи _____ Леонід ГАЛЬЧИНСЬКИЙ
(підпис) (Власне ім’я, ПРІЗВИЩЕ

РЕФЕРАТ

Робота складається з 3 розділів, містить 2 ілюстрації, 14 таблиць, 51 літературних посилань, обсяг роботи - 57 сторінок.

Завданням роботи є адаптація моделі залишкових ризиків для банківської інформаційної системи.

Мета цієї дипломної роботи полягає у дослідженні моделі залишкових ризиків з використанням її для банківської інформаційної системи.

Об’єктом дослідження є модель залишкових ризиків.

Предметом дослідження є робота моделі залишкових ризиків в умовах банківської системи.

Актуальність роботи зумовлюється тим, що на сьогодні банківські продукти та послуги стають все більш популярними. Інноваційне використання інтернету та мобільних технологій. З цієї причини банківська інформаційна система повинна бути захищена від ризиків, пов'язаних з фізичними або логічними атаками, які можуть викликати серйозні фінансові втрати.

Методами дослідження є аналіз інформаційних джерел, новітніх публікацій за темою дослідження, нечітке моделювання.

Наукова новизна полягає в тому, що на основі аналізу існуючого стану інформаційних систем банків був зроблений вибір моделі для оцінки залишкового ризику.

Практичне застосування полягає в отримані моделі яку зможуть використовувати для підвищення безпеки банківської інформаційної системи, та зниження рівня витрат.

Ключові слова: залишкові ризики, банківська інформаційна система, модель.

ABSTRACT

The work consists of 3 sections, contains 2 illustrations, 14 tables, 51 references, volume of work - 57 pages.

The task of the work is to adapt the model of residual risks for the banking information system.

The purpose of this thesis is to study the model of residual risks using it for the banking information system.

The object of the study is a residual risk model.

The subject of the study is the work of the model of residual risks in the banking system.

The urgency of the work is due to the fact that today banking products and services are becoming increasingly popular. Innovative use of the Internet and mobile technologies. For this reason, the banking information system must be protected from the risks associated with physical or logical attacks that could cause serious financial losses.

Research methods are the analysis of information sources, the latest publications on the research topic, fuzzy modeling.

The scientific novelty is that based on the analysis of the current state of information systems of banks, a choice of model was made to assess the residual risk .

Practical application is the obtained model which can be used to increase the security of the banking information system and reduce costs.

Key words: residual risks, banking information system, model.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

Ризик – це потенційна шкода, яка може виникнути в результаті поточною діяльністю або будь-якого майбутнього події. Ризик інформаційної системи є функцією ймовірності виникнення заданих джерел загроз і результуючого впливу цього несприятливого події на організацію. [1]

Загроза – це потенційна можливість для джерела загрози проявити певну вразливість, а джерело загрози - це ситуація, яка може випадково викликати вразливість. [2]

Залишковий ризик – це ймовірність настання події, яка може залишати вплив на досягнення визначених цілей і завдань, виконання суб’єктами внутрішнього контролю функцій, процесів і операцій або мати негативні фінансово-господарські, юридичні та/або інші наслідки після впровадження заходу впливу на попередньо ідентифікований ризик.[36]

Властивий (невід’ємний) ризик – відображає вразливість тверджень щодо класу операцій, залишку рахунку або розкриття інформації до викривлення, яке може бути суттєвим окремо або в сукупності з іншими викривленнями, перед тим, як брати до уваги будь-які відповідні заходи контролю. Тобто це всі можливі ризики, пов’язані з діяльністю клієнта, всі помилки та некоректності, які властиві певній галузі.[37]

Невід'ємний ризик - це сприйнятливість інформації або даних до суттєвого спотворення за умови відсутності пом'якшує контролю.[25]

Оцінка ризиків – це структурована та систематизована процедура, яка залежить від правильної ідентифікації небезпек та відповідної оцінки ризиків, що випливають, з метою порівняння ризиків для їх контролю та уникнення.

RPN – Risk Priority Number (число пріоритету ризику)

FMECA – Failure Mode Effects and Criticality Analysis (Аналіз ефектів режиму відмови та аналіз критичності)

FMEA – Failure Mode and Effects Analysis (Режим відмови та аналіз ефектів)

FTA – Fault tree analysis (Аналіз дерева несправностей)

NASA – National Aeronautics and Space Administration

CA – Critical Analysis (Критичний аналіз)

RCM – Reliability Centered Maintenance (Обслуговування, орієнтоване на надійність)

ISM – Information Security Management (Управління інформаційною безпекою)

IT – Інформаційні Технології

РІС – Розподілена Інформаційна Система

ОС – Операційна Система

СКБД – Система Управління Базами Даних

БД – База Даних

ВСТУП

Актуальність роботи. Банківські продукти та послуги стають все більш популярними. Інноваційне використання Інтернету та мобільних технологій. З цієї причини банківська інформаційна система повинна бути захищена від ризиків, пов'язаних з фізичними або логічними атаками, які можуть викликати серйозні фінансові втрати.

Мета. Мета роботи полягає в дослідженні моделі залишкових ризиків з використанням її для банківської інформаційної системи.

Завдання. Завданням роботи є аналіз існуючих моделей залишкового ризику та адаптація їх для банківської інформаційної системи.

Об’єкт дослідження. Об’єктом дослідження в даній роботі є моделі залишкового ризику, банківська інформаційна система.

Наукова новизна. Наукова новизна полягає в тому, що на основі аналізу існуючого стану інформаційних систем банків був зроблений вибір моделі для оцінки залишкового ризику.

Предмет дослідження. Предметом дослідження в даній роботі є моделі залишкового ризику.

Методи дослідження. Методами дослідження в даній роботі є аналіз інформаційних джерел, публікацій за темою дослідження, аналіз моделей залишкового ризику, банківської інформаційної системи.

Практичне значення. Практичне значення полягає в отримані моделі яку зможуть використовувати для підвищення безпеки банківської інформаційної системи, та зниження рівня витрат.

1 ОГЛЯД ТЕОРЕТИЧНИХ МАТЕРІАЛІВ ЗА ЗАДАНОЮ ТЕМОЮ

1.1 Огляд сучасних банківських систем та їх інформаційних систем

Інформаційні технології, як технологія з найшвидшими темпами розвитку та застосування у всіх галузях бізнесу, вимагають належного захисту для забезпечення високої безпеки. Метою аналізу безпеки, що застосовується в інформаційній системі, є виявлення та оцінка загроз, вразливостей та характеристик безпеки. IT-активи піддаються ризику пошкодження або збитків. IT-безпека передбачає захист інформації, що зберігається в електронному вигляді. Цей захист передбачає цілісність, доступність та конфіденційність даних. На сьогоднішній день існує багато видів комп'ютерних злочинів: крадіжка грошей 44%, пошкодження програмного забезпечення 16%, крадіжка інформації 16%, зміна даних 12%, крадіжка послуг 10%, зловживання 2%.[38]

Інформаційна система - або IT-компонент банківської установи - має визначальну роль на рівні внутрішнього середовища, а також на рівні відносин із зовнішнім середовищем. Взагалі кажучи, інформаційна система включає апаратний компонент та програмний компонент - системи та додатки, які забезпечують введення, обробку та зберігання даних та експлуатуються спеціалізованим персоналом. На рівні фінансово-банківського сектору роль IT-компонента є більш складною, враховуючи, що це інформаційно інтенсивний сектор, з точки зору інформаційного змісту продуктів та послуг.

Підкреслюється, особливо для фінансово-банківського сектору, необхідність вдосконалених інформаційних систем, які дозволяють експлуатувати великий обсяг інформації на різних стадіях обробки. Крім того, для банківських установ та їх клієнтів аспекти, що стосуються безперервності, точності, безпеки та доступності

даних, - які збільшують внесок у автоматизацію, досягнутий у всіх інформаційних системах у фінансово-банківському секторі, є важливими.

Тому в банківських установах характер і складність виконуваної діяльності накладає засвоєння інформаційних систем, призначених для автоматизації великої кількості видів діяльності та забезпечення необхідної інформації для процесу прийняття рішень. В основному банківські установи здійснюють комерційну, інвестиційну та депозитну діяльність, серед яких: залучення фінансових ресурсів від населення та економічних операторів у вигляді строкових або на депозитах на вигляд; грантові позики; розрахунково-розрахункові операції в леях та іноземній валюті; операції в іноземній валюті: обмін валюти, торгівля іноземною валютою. Інформаційна система банківських установ повинна забезпечувати виконання цих конкретних видів діяльності, але в той же час задовольняти деякі основні запити, на які посилаються: [50]

- забезпечення сумісності всіх компонентів системи - належним обладнанням та програмними елементами повинен керувати уповноважений персонал для забезпечення зв’язку, програм, послуг з управління даними та стандартів тощо;
- інтеграція із системами, для яких вони надають підтримку - головним чином з точки зору доступності - ансамбль точок, які можуть бути взаємопов’язаними, та діапазон - ансамбль заходів, які можна виконувати та спільно використовувати на різних рівнях доступу;
- пропозиція підтримки організаційної стратегії - важливий аспект, але досить важкий для реалізації, що можна пояснити відсутністю спільної мови між сферами управління та інформацією. Ефективним методом у цьому відношенні є "Збалансована система показників" - передбачає визначення ключових аспектів, які необхідно розглядати з різних точок зору, дозволяючи інтегративний підхід до організаційного розвитку.

Збалансована система показників - як система планування та управління стратегією, що широко застосовується в різних організаціях, з метою узгодження діяльності з баченням та стратегією організації, підвищення внутрішньої та зовнішньої комунікації та моніторингу результатів у досягненні цілей стратегії (Інститут збалансованих показників) , 2010) - часто використовується в банківській системі для різних процесів та проектів.

У функціональному підході, що характеризується орієнтацією на клієнта, як переважна риса на рівні банківського сектору - але також і на рівні послуг загалом - інформаційна система забезпечує підтримку всіх компонентів структурної та процедурної організації.[51]

Для мінімізації збитків необхідно залучати управління ризиками та оцінку ризиків у сферах інформаційних технологій та операційних ризиків. Управління ризиками та оцінка ризиків є найважливішими частинами Управління інформаційною безпекою (ISM). Існують різні визначення управління ризиками та оцінки ризиків [ISO 13335-2], [NIST], [Положення ENISA], але більшість експертів визнають, що управління ризиками передбачає аналіз, планування, впровадження, контроль та моніторинг впроваджених вимірювань та оцінку ризиків , як частина Управління ризиками.

Він складається з декількох процесів:

- Ідентифікація ризику,
- Аналіз відповідного ризику,
- Оцінка ризику

Управління ризиками розпізнає ризик, отримує доступ до ризику та вживає заходів для зменшення ризику, а також заходів щодо підтримання ризиків на прийнятному рівні. Основною метою Оцінки Ризику є прийняття рішення про те, чи є система прийнятною та які заходи забезпечують її прийнятність. Для кожної організації, яка використовує IT у своєму бізнес-процесі, важливо провести оцінку

ризику. Представлені численні загрози та вразливості, їх ідентифікація, аналіз та оцінка дозволяють оцінити вплив ризику та запропонувати відповідні заходи та засоби контролю для його пом'якшення на прийнятному рівні. Політика безпеки змінилася за останні роки. З контрольних списків для виявлення конкретних подій інформаційна безпека піднялася на більш високий рівень, тобто політика та стратегія безпеки враховують загрози та слабкі сторони ділового середовища та IT-інфраструктури.[39]

1.2 Аналіз залишкового ризику для банків

Банківські продукти та послуги стають все більш популярними. інноваційне використання Інтернету та мобільних технологій. З цієї причини банківська інформаційна система повинна бути захищена від ризиків, пов'язаних з фізичними або логічними атаками, які можуть викликати серйозні фінансові втрати.

Пропонується модель кількісної оцінки залишкових ризиків інформаційної системи, яка являє собою ризики, що залишаються після реакції керівництва.

Модель забезпечує автоматичний розрахунок впливу заходів безпеки на ризики інформаційної системи і заснована на FMECA (Failure Modes and Effect Criticality Analysis Method) (типи відмов і метод аналізу їх критичності) який є індуктивним методом міркувань, що вивчає причини, наслідки відмов системи та їх критичність.

Банківська інформаційна система має кілька ризиків з урахуванням нових продуктів і послуг, пов'язаних з мобільним і онлайн-банкінгом. Можливі шахрайства мають фінансові, комерційні та юридичні наслідки. Це тягне за собою зниження прибутку банку і довіри клієнтів. Щоб управляти своїми ризиками, які можуть мати серйозні наслідки для бізнесу банку, необхідно запобігати загрозі, зменшувати і усувати уразливість, захищати і переміщати активи. [3]

Процес управління ризиками складається з різних етапів, включаючи оцінку, час виконання, послідовність в підході і реалізації. [4] Він також включає аналіз витрат і вигод, а також вибір, тестування і оцінку захисних заходів. У цьому контексті впровадження передової практики повинно узгоджуватися зі структурою управління ризиками і контролю підприємства, що підходить для підприємства і інтегрованої з іншими використовуваними методами і практиками. [5]

Пропонуються різні стандарти безпеки, які стосуються різних галузей інформаційної системи:

- MEHARI: метод аналізу ризиків та набір інструментів спеціально розроблений для управління безпекою. [6]
- COBIT: управління IT та передовий досвід в управлінні ресурсами, інфраструктурою, процесами, обов'язками і контролем. [7]
- ITIL: Бібліотека передових практик, пов'язаних з інформацією технологічні послуги. [8]
- ISO 27001: Методи і практика впровадження інформаційна безпека в організації. [9]
- ISO 22301: Процес управління підтримується менеджментом по впровадженню і підтримці бізнесу, управління безперервністю. [10]

Банки застосовують безліч заходів безпеки для захисту інформації і транзакцій. В даний час шахрайство в банківському секторі найбільше пов'язано з шахрайством з використанням банкоматів або торгових точок, шахрайства з використанням Інтернет-банкінгу та шахрайських перекладів або зняття коштів. З цих причин банки повинні запобігати шахрайству, покращувати захист від проникнення в продукти, залучити значну кількість клієнтів з невеликим досвідом або без досвіду роботи в банківській сфері і залучати більше вкладників. [11]

Крім того, постачальник повинен бути поінформований про такі стандарти, як PCI DSS (Стандарт безпеки даних індустрії платіжних карт). [12] Для онлайн-

транзакцій 3D-Secure - це протокол адаптивної аутентифікації, який дозволяє продавцям і емітентам використовувати інші додаткові засоби захисту власників карток. Аутентифікація - це спроба підтвердити, що особа, яка ініціює транзакцію, є законним і справжнім власником картки. [13]

Також, необхідно враховувати рівні безпеки в міру завершення циклу впровадження чіпових карт EMV (Europay Mastercard Visa). В ідеалі кожна зацікавлена сторона повинна боротися з шахрайством за допомогою своєї стратегії міграції чіпа EMV. [14] Торговці повинні стримувати зростаючі збитки від шахрайства, в той час як емітенти повинні стримувати шахрайство, а також підтримувати впевненість споживачів у безпеці онлайн-транзакцій. [15]

Періодично банки оцінюють вплив реалізованих засобів контролю на ризики інформаційних систем, використовуючи реальний метод, який має деякі обмеження. Цей метод є ручним, вимагає часу і особистих вкладень і має деяку похибка в оцінці. Тому пропонується автоматизувати оцінку остаточних ризиків банківської інформаційної системи.

Ризик інформаційної системи є функцією ймовірності того, що дане джерело загроз проявляє конкретну потенційну вразливість, і результуючого впливу цього несприятливого події на організацію. Як правило, оцінка ризиків включає процес виявлення ризиків, визначення ймовірності виникнення і результуючого впливу, а також додаткових запобіжних заходів, які могли б пом'якшити цей вплив. Управління ризиками інформаційної системи дозволяє реалізувати відповідні засоби контролю для зниження або усунення ризиків. [16]

Існують різні етапи: визначення рівня невід'ємного ризику, моніторинг ефективності методів управління ризиками, визначення того, чи покращується залишковий ризик, стає стабільним або зменшується з плином часу. [17] Беручи до уваги фактичні банківські продукти і послуги, постачальники фінансових, платіжних і мережевих послуг повинні застосовувати відповідні заходи безпеки.

Кожен банк повинен впровадити жорсткі заходи контролю для захисту таких даних під час їх зберігання, ідентифікувати особисті та конфіденційні дані і забезпечити наявність відповідних механізмів. [18] З мобільними платежами пов'язані різні ризики, такі як боротьба з відмиванням грошей, кредит, ліквідність, шахрайство і комплаенс. [19]

Стратегічний ризик мобільних платежів пов'язаний з атакою, яка настільки спрощує шахрайство, що платформа або канал стають уразливими [20]. Ризик інформаційної безпеки - це шкоди процесу або пов'язаної з ним інформації в результаті цілеспрямованого або випадкового події, яке негативно впливає на процес або пов'язану інформацію.

Африканські банки вважають регіональну експансію ключовий віссю своїх стратегій зниження ризиків. [21] Однак відсутність даних, на жаль, не дозволило оцінити всі ризики, і схильність банків явно зростає. [22] Фінансові злочини зазвичай пов'язані з шахрайством, але воно може приймати різні форми з метою експлуатації споживачів, банків і державних установ. Найбільш небезпечні з них прагнуть проникнути в банківські мережі, при цьому кіберзлочинці отримують доступ до рахунків і викачують гроші. [23] З цієї причини інформаційні ризики повинні управлятися шляхом розуміння факторів, які можуть призвести до порушення конфіденційності, цілісності або доступності інформаційної системи, і реагування на них. Процес оцінки ризиків включає оцінку невід'ємних ризиків і оцінку остаточних ризиків. [24]

Невід'ємний ризик - це сприйнятливість інформації або даних до суттєвого спотворення за умови відсутності пом'якшує контролю. Це фактор, який слід враховувати при визначенні залишкового ризику. [25] Залишковий ризик визначається як ризик, що залишається після того, як керівництво зробить дії щодо зниження серйозності і / або ймовірності несприятливого події, включаючи заходи контролю у відповідь на ризик. Зокрема, залишковий ризик інформаційної системи

- це ймовірність того, що ця загроза скористається вразливістю активу і тим самим завдасть шкоди при наявності засобів контролю. Ризик залишається навіть після того, як будуть реалізовані всі основні заходи безпеки і заходи щодо запобігання ризику. [26] У цьому контексті запобіжних заходів і обробка ризику дозволяють знизити ризик до певного залишкового значення. [27] Залишкова критичність ризику представляє рівень фактичного впливу і дає оцінку впливу засобів контролю на невід'ємні ризики. [28]

На практиці залишкові ризики отримують шляхом оцінки впливу засобів контролю на невід'ємні ризики. Однак в 2015 році ми пропонуємо математичну модель, яка дозволяє кількісно оцінити залишкові банківські ризики. [29] Після цього ми також визначили дві математичні моделі, які забезпечують автоматичний розрахунок зрілості засобів управління інтернет-банкінгом. [30] Але рейтинг залишкового ризику часто виходить шляхом оцінки впливу, яке поточні засоби контролю надають на невід'ємний ризик, з використанням певних шкал ймовірності ризику і строгість. Щоб визначити рейтинг залишкового ризику, необхідно оцінити вплив, яке контроль надає на загальні джерела ризику. [31]

Висновок до розділу 1

Проведено огляд джерел по окресленню проблеми залишкових ризиків для інформаційних систем організацій, зокрема для банківських інформаційних систем. Виявлені підходи до побудови оцінок ризиків.

Вся сутність банків полягає в тому, що вони завжди працюють з грошима і саме це спокушає злочинців, тому банкам необхідно завжди вдосконалювати свою безпеку, бо і злочинці також вдосконалюють свої методи. Таким чином треба використовувати запобіжні заходи, а які в першу чергу допоможе визначити залишковий ризик.

Залишкові ризики інформаційної системи оцінюються оцінювачами протягом декількох робочих сеансів ручним методом, що має деякі обмеження: вимагає багато робочих сесій з компромісами, в разі розбіжностей це вимагає значного рівня знань, часу і особистих вкладень. Оцінювачі по-різному оцінюють вплив впроваджених засобів контролю – це є деякою помилкою оцінки при оцінці залишкового ризику.

2 ОПИС МОДЕЛІ ЗАЛИШКОВОГО РИЗИКУ ДЛЯ БАНКІВСЬКОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ

2.1 Загальний підхід до оцінки залишкового ризику для організації

2.1.1 Передумови

Клієнти висувають підвищені вимоги до компаній щодо високоякісних, надійних продуктів. Зростаючі можливості та функціональність багатьох продуктів створюють додатковий комплекс для виробника, щоб підтримувати якість та надійність. Звичайно надійність досягається шляхом широкомасштабних випробувань і застосовується такий метод, як імовірнісне моделювання надійності. Це методи, зроблені на пізній фазі вдосконалення. Завдання полягає у розробці якості та надійності на початку фази розширення.

Аналіз режимів відмов та ефектів (FMEA) є тактикою для оцінки можливих проблем із надійністю в перші години циклу прогресу, де простіше зайнятися діями для подолання цих питань, тим самим покращуючи узгодженість за допомогою проектування. FMEA може застосовуватися для розпізнавання ймовірних режимів відмов, висновку про їх вплив на процес виготовлення продукту та категоризації дій для зменшення відмов. Життєво важливим кроком є передбачення того, що може піти неправильно з продуктом.

Тоді як передбачити кожен режим відмов неможливо, команда вдосконалення повинна зробити якомога більше записів можливих режимів відмов, наскільки це можливо.

Майже на початку постійне використання FMEA у процесі проектування дозволило інженерам виявляти несправності та виготовляти надійні, захищені та задовольняючі споживача товари. FMEA також містять хронологічну інформацію для використання у майбутній розробці продукту. [40]

2.1.2 Визначення FMEA та FMECA

Аналіз режимів відмов та ефектів (FMEA) та Режими відмов, Аналіз ефектів та критичності (FMECA) - це методології, призначені для виявлення потенційних режимів відмов для виробу чи процесу до виникнення проблем, для оцінки ризику. В ідеалі, FMEA проводиться на стадіях розробки продукту або процесу, хоча проведення FMEA на існуючих продуктах або процесах також може принести користь.

Команда FMEA визначає, аналізуючи режим відмов, ефект кожного збою та визначає окремі точки відмови, які є вирішальними. Він також може класифікувати кожну несправність відповідно до критичності ефекту несправності та ймовірності її виникнення. FMECA є результатом двох кроків:

- Режим відмов та аналіз ефектів (FMEA)
- Аналіз критичності (CA). [41]

2.1.3 Опис методу FMEA

Для розрахунку ризику методом FMEA ризик має три складові, які множаться, щоб отримати число пріоритету ризику (RPN):

1) Серйозність (S): Серйозність описується за 10-бальною шкалою, де 10 - найвища.

2) Поява (O): Поява описується за 10-бальною шкалою, де 10 є найвищим.

3) Виявлення (D): Визначення описується за 10-бальною шкалою, де 10 є найвищим.

$$\mathrm{RPN} = \mathrm{S} * \mathrm{O} * \mathrm{D} \tag{2.1}$$

RPNmin = 1, тоді як RPNmax = 1000.

Пояснення методики прийняття рішення щодо встановлення пріоритетності процесу на основі RPN.

Таблиця 2.1 - Приклад розрахунку ризику FMEA.

	Серйозність (S)	Поява (O)	Виявлення (D)	RPN $= S * O * D$
Потенційний збій 1	2	10	5	100
Потенційний збій 2	10	2	5	100
Потенційний збій 3	2	5	10	100
Потенційний збій 4	10	5	2	100

Нашим першочерговим завданням буде потенційний збій 2 і 4, оскільки ми маємо найвищий рейтинг серйозності там. Потенційні збої 1 та 3 мають однаковий рейтинг серйозності «2». Але 1 трапляється частіше, ніж 3. Тож слід надавати пріоритет наступним. Тож результати є.

Перший пріоритет - Потенційний збій 4

Другий пріоритет - Потенційний збій 2

Третій пріоритет - Потенційний збій 1

Четвертий пріоритет - Потенційний збій 3. [41]

Немає порогового значення для RPN. Іншими словами, немає жодного значення, вище якого обов’язковим є використання рекомендованої дії, або нижче якого команда автоматично звільняється від дії. Важливі примітки: Нульові (0) рейтинги за ступенем тяжкості, виникнення або виявлення не дозволяються. [42]

Існує кілька типів FMEA, такі як:

- Система FMEA
- Дизайн FMEA
- Процес FMEA
- Надання послуг FMEA.

2.1.4 Описи аналізу критичності (FMECA)

Документ MIL-STD-1629A описує два типи аналізу критичності: кількісний та якісний. Для використання методу кількісного аналізу критичності група аналітиків повинна: Визначити надійність / ненадійність для кожного елемента в певний час роботи; визначити частину ненадійності елементів, яку можна віднести до кожного потенційного режиму відмови, оцінити ймовірність втрати (або тяжкості), яка буде наслідком кожного режиму відмови, що може виникнути. Обчисліть критичність для кожного потенційного режиму відмови, отримавши добуток трьох факторів: Критичність режиму = Ненадійність елемента x Коефіцієнт режиму ненадійності x Імовірність втрати Розрахуйте критичність для кожного елемента, отримавши суму критичних показників для кожного режиму відмови, який має бути визначений для товару. Критичність елемента = Сума критичності режимів. Для використання методу якісного аналізу критичності для оцінки ризику та визначення пріоритетів коригувальних дій, група аналітиків повинна: Оцінити ступінь серйозності потенційних наслідків відмови; оцінити імовірність виникнення для кожного потенційного режиму відмови.

Порівняти режими відмов за допомогою матриці критичності, яка визначає появу на горизонтальній осі та важкість на вертикальній осі.

Деякі переваги аналізу критичності:

- Допомога в аналізі процесу виготовлення або складання.

- Документування змін з поясненнями. [43]

2.1.5 Застосування FMEA / FMECA

Методи FMEA / FMECA використовуються в усіх галузях промисловості для свого роду застосувань, і цей гнучкий метод може бути виконаний на різних етапах життєвого циклу товару. Метод FMEA / FMECA може бути використаний для здійснення проектування, розробки, виробництва, обслуговування та інших видів діяльності для підвищення надійності та підвищення ефективності. Як приклад, в автомобільній промисловості широко використовується як проектний, так і технологічний FMEA, і документація цього розслідування є загальним реквізитом для постачальників автомобілів. Цей метод також зазвичай використовується в аерокосмічній, медичній, ядерній та інших галузях промисловості. [44, 45]

2.1.6 Переваги FMEA / FMECA

Аналіз режимів відмов та ефектів (FMEA) - це методологія, призначена для:

- Визначення потенційних режимів відмов для продукту або процесу.
- Оцінки ризик, пов’язаного із цими режимами відмов, та визначення пріоритетів для коригувальних дій.
- Визначення та виконання коригувальних дій для вирішення найсерйозніших проблем.

Деякі переваги проведення аналізу FMEA / FMECA включають:

1. Сприяння вдосконаленню конструкцій продуктів та процесів.
    a) Вища надійність.
    b) Краща якість.
    c) Збільшена безпека.

2. Підвищення рівня задоволеності споживачів.
    a) Сприяє економії коштів.
    b) Скорочує час розробки та прогнозує витрати.
    c) Зменшує гарантійні витрати.
    d) Зменшує кількість відходів та операцій без доданої вартості.
3. Сприяє розробці планів контролю, випробувальних вимог, оптимальних планів технічного обслуговування, аналізу зростання надійності та пов'язаних з ними заходів.

Вигідні витрати, пов'язані з FMEA, як правило, можуть виникати завдяки здатності розпізнавати режими відмов заздалегідь під час процесу, коли їх вирішення є менш дорогим. Фінансові вигоди також є результатом прогресу проектування, який, ймовірно, сприятиме FMEA, а також мінімізувати гарантійні витрат, збільшуватиме продажі за рахунок кращого задоволення споживачів, тощо. [46, 47]

2.1.7 Недоліки FMEA / FMECA

Якщо він використовується як інструмент зверху-вниз, FMEA може виявляти лише основні режими відмов у системі. FTA більше підходить для аналізу "зверху-вниз". Коли FMEA використовується як інструмент "знизу-вгору", він може доповнювати FTA та виявляти багато інших причин та режимів збою, що призводять до симптомів верхнього рівня. Він не може виявити складні режими відмов, що включають кілька відмов у підсистемі, або повідомити про очікувані інтервали відмов окремих режимів відмов аж до підсистеми або системи верхнього рівня. Крім того, множення ранжувань за ступенем тяжкості, виникнення та виявлення може призвести до скасування рангу, коли менш серйозний режим відмови отримує вищу RPN, ніж більш серйозний режим відмови. Причиною цього

є те, що рейтинги є порядковими номерами шкали, і множення не є допустимою операцією над ними. Порядкові рейтинги говорять лише про те, що один рейтинг кращий чи гірший за інший, але не на скільки. Наприклад, рейтинг "2" може бути не вдвічі гіршим, ніж рейтинг "1", або "8" може бути не вдвічі гіршим, ніж "4", але множення розглядає їх так, ніби вони є. FMEA вимагає глибоких знань цього питання, яке слід вивчити. Загалом, необхідний мозковий штурм із кількома людьми, які беруть участь від зачаття до пологів. Це означає, що команда може домовитись про вивчені режими відмов. Таким чином, цей метод є громіздким для реалізації. [44]

2.1.8 Подібності та відмінності між FMEA та FMECA

Режим відмов та аналіз ефектів (FMEA) та режими відмов, аналіз ефектів та критичності (FMECA) - це методи, що використовуються для виявлення способів виходу з ладу продукту або процесу. Основна методологія однакова в обох випадках, але між процесами існують важливі відмінності.

Якісна порівняно з кількісною: FMEA надає лише якісну інформацію, тоді як FMECA також надає обмежену кількісну інформацію або інформацію, яку можна виміряти. FMEA широко використовується в промисловості як процес "що якщо". Він використовується в NASA як частина його програми забезпечення польоту для космічних кораблів. FMECA надає рівень критичності режимам відмов; він використовується армією США для оцінки критично важливого обладнання та систем.

Розширення: FMECA є фактично продовженням FMEA. Для того, щоб виконати FMECA, аналітики повинні виконати FMEA з подальшим критичним аналізом (CA). FMEA визначає режими відмов продукту або процесу та їх наслідки,

тоді як CA класифікує ці режими відмов у порядку важливості відповідно до рівня відмов та тяжкості відмов.

Критичний аналіз: CA не додає інформацію до FMEA. Насправді він обмежує сферу застосування FMECA режимами відмов, визначених FMEA як такі, що вимагають технічного обслуговування, орієнтованого на надійність (RCM). [48]

2.2 Альтернативний підхід для оцінки залишкового ризику

Сучасна розподілена інформаційна система (РІС) підприємства перед ставлять собою складну систему, що складається з великого числа компонентів різного ступеня автономності, які пов'язані між собою і обмінюються даними. Практично кожен компонент РІС піддається впливу атак зловмисника.

Найбільш уразливими до атак є програмні засоби і засоби захисту інформації РІС. Це можуть бути атаки на операційну систему (ОС), на системи управління базами даних (СКБД), на міжмережевий екран, на web-сервер (мережеві атаки), на комунікаційне обладнання і т. д.

Кожна атака може залишити після себе сліди. Сліди - це інформація, на підставі якої можна прийти до висновку про вплив атаки на будь-який компонент РІС.

Результатом роботи системи моніторингу та аудиту є дані про атаки, що дозволяють оцінити рівень безпеки РІС - інформаційний ризик. Найбільшого поширення серед методів оцінки ризиків отримав метод «матриці ризиків».

Загальний ризик - це ризик, перед обличчям якого стоїть підприємство, не впровадило ніяких захисних заходів. Якщо його рівень неприпустимий для компанії, вона впроваджує захисні заходи, щоб знизити ризик до прийнятного рівня. Однак систем або середовищ, що мають нульовий ризик, не існує - завжди є

певний залишковий ризик. Рівень залишкового ризику повинен бути прийнятним для компанії .

На підготовчому етапі оцінки ризику експертами визначаються ймовірності виникнення кожного ризику P, розміри пов'язаних з ним втрат Y (вартість збитку), а також допустимий залишковий ризик $R_{зал\ доп}$ і заносяться в БД.

Всі оцінки ризиків представляються у вигляді матриці, яка представлена в таблиці. У розглянутій матриці ризиків вартісна міра шкоди визначається у відсотках від цінності інформаційного ресурсу на і-м компоненті. Залишковий ризик обчислюється за формулою:

$$R_{зал} = P * Y \tag{2.2}$$

де P - ймовірність впливу атак, Y - вартість збитку. Оцінка $R_{зал}$ буде достовірною тільки за умови врахування одночасної дії всіх атак на всі компоненти PIC від всіх категорій зловмисників.

Нехай на і-й компонент (і $=\overline{1,I}$, де I - кількість вразливих до атак компонентів розглянутої PIC) впливає j-я атака (j $=\overline{1,J}$, де J - кількість можливих атак зловмисника на об'єкт) в l-й зоні компонента з боку порушника k-ї категорії (k = K, K - число категорій порушників).

Таблиця 2.2 – Матриця ризиків (Згідно з рекомендаціями NIST «Посібник з управління ризиками для систем інформаційних технологій»)

Імовірність атаки (P)	Збиток		
	Низький 0 < Y < = 10 (%)	Середній 10 < Y < = 50 (%)	Високий 50 <Y < = 100 (%)
Висока (0,5 < P < = 1)	Низький 5 < R < = 10 (%)	Середній 10 < R < = 50 (%)	Високий 50 < R < = 100 (%)
Середня (0,1 < P < = 0,5)	Низький 1 < R < = 5 (%)	Середній 5 < R < = 25(%)	Середній 10 < R < = 50 (%)
Низька (0 < P < = 0,1)	Низький 0 < R < = 1 (%)	Низький 0 < R < = 5 (%)	Низький 0 < R < = 10 (%)

Ймовірності P_{ijkl} впливу j-й атаки на і-й компонент через l-ю зону уразливості. При цьому вірогідність несанкціонованого доступу до інформації на і-м компоненті PIC шляхом проведення j-й атаки через l-ю зону буде дорівнює добутку впливають на нього атак від k-го зловмисника:

$$P_{ikj} = Y_l \, P_{ikjl} \tag{2.3}$$

де l = $\overline{1,\ L_k}$, L_k - кількість захисних зон компонента для k-го зловмисника. Імовірність впливу атак з боку k-го зловмисника буде дорівнює:

$$P_{ik} = \mathcal{E}_{j=1}^{J} P_{ikj} \tag{2.4}$$

Тоді ймовірність несанкціонованого отримання інформації на і-м компоненті з боку всіх потенційних зловмисників:

$$P_i = \mathcal{E}_{k=1}^{K} P_{ik}$$

(2.5)

Вірогідність несанкціонованого доступу до інформації РІС в цілому дорівнюватиме:

$$P = \mathcal{E}_{i=1}^{I} P_i$$

(2.6)

При цьому вартість збитку для всієї РІС підприємства буде дорівнює:

$$Y = \mathcal{E}_{i=1}^{I} Y_i$$

(2.7)

Таким чином, при підстановці формул (2.6) і (2.7) в формулу (2.2) отримана формула загального залишкового ризику для всієї РІС підприємства:

$$R_{\text{зал}} = \mathcal{E}_{i=1}^{I} P_i * \mathcal{E}_{i=1}^{I} Y_i$$

(2.8)

Невиконувані умови:

$$R_{\text{зал}} \text{ ὺ } R_{\text{зал доп}}$$

(2.9)

Для реалізації формальної моделі розроблена система моніторингу та аудиту (на першому етапі для операційної системи РІС), архітектура якої представлена на рисунку 2.1.

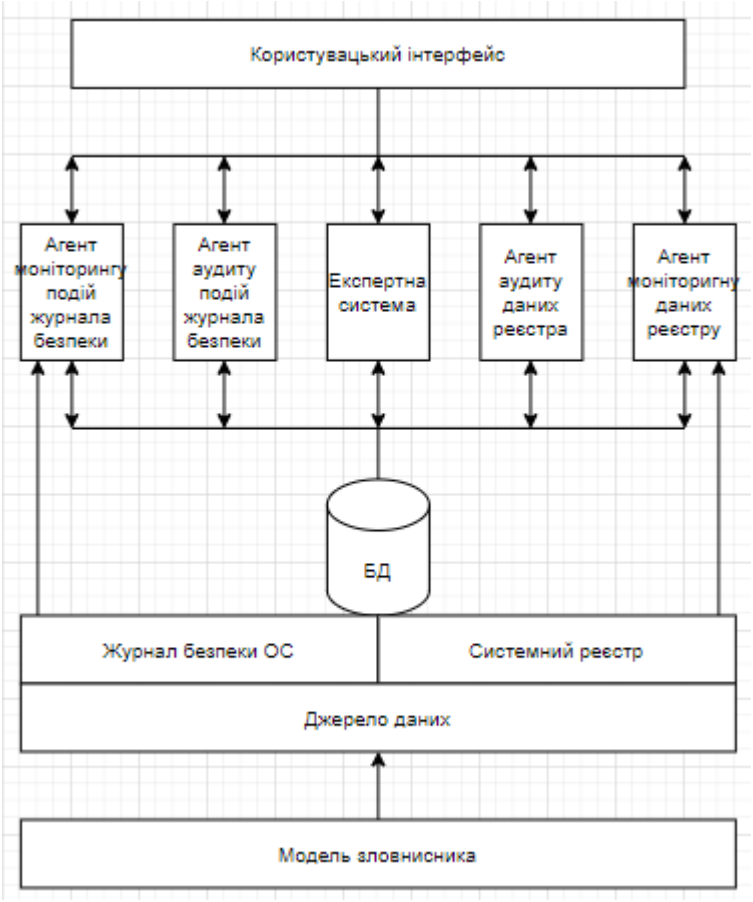

Рисунок 2.1 – Система моніторингу та аудиту

Джерелами інформації про атаки на даному компоненті PIC є журнал безпеки Windows і системний реєстр.

Розроблений програмний комплекс моделі моніторингу та аудиту складається з наступних компонентів: програмного комплексу, що включає програмні агенти, експертну систему, базу даних і призначений для користувача інтерфейс, що здійснює управління програмним комплексом і взаємодія з фахівцем із захисту інформації; моделі зловмисника, необхідної для реалізації програмного комплексу; моделі операційної системи.

База даних. Для кожного об'єкта PIC в БД є 3 таблиці: таблиця відомостей про події, в яку внесено інформацію, зібрана в результаті моніторингу; таблиця контрольних значень, з якими в процесі аудиту порівнюються значення з таблиць

першої групи; таблиця подій, ідентифікованих як атаки на PIC, в якій міститься інформація, отримана в результаті аудиту подій з першої таблиці.

Приклад. Оцінюваний компонент PIC - хост 1, підключений до сервера 1. На даний хост впливають інсайдер і зовнішній зловмисник (2 категорії зловмисників). Нехай з боку зловмисника першої категорії можуть впливати такі атаки: атака 1 «несанкціонований вхід в систему» за допомогою підбору пароля входу в систему, атака 2 «несанкціонований доступ до об'єктів», атака 3 «несанкціонована завантаження системи». При цьому інсайдер здійснює злочинні дії тільки за допомогою атаки 1, тобто $A_{11} = 1$, $A_{12} = 0$, $A_{13} = 0$.

Дана атака залишає слід в журналі безпеки - подія 4625 - «не вдалося здійснити вхід в аккаунт»: $G_{111} = 1$.

На підставі цих даних, а також даних експертної системи, обчислений за формулою (2.2.7) залишковий ризик для компонента PIC становить 23% від цінності захищається ресурсу в 100 тис. рублів. Допустимий залишковий ризик становить 10%. Так, умова (2.2.8) для даного компонента не виконується. Згідно матриці ризиків (див. Таблицю),допустимий залишковий ризик є низьким, а обчислений залишковий ризик - середнім. Отже, система не захищена і необхідно вжити заходів щодо зниження залишкового ризику до прийнятного рівня і щодо посилення захисту PIC. [49]

2.3 Вибір моделі оцінки залишкового ризику

Ми автоматизуємо рівень оцінки залишкового ризику FMECA, визначаючи модель кількісної оцінки. FMECA заснований на індуктивних розширеннях та вивченні причин, останніх відказів та критичності. [32] Щоб запропонувати модель, ми розглянемо наступні 10 принципів:

- Принцип 1. Ризик може мати один або кілька засобів контролю, які представляють собою набір мір за його зменшенням.
- Принцип 2: Контроль визначає зниження критичності ризику, який є сукупною величиною ризику.
- Принцип 3: Міри контролю мають одну ступінь зрілості та чотири типи: стримувальний, превентивний, детективний і коригуючий.
- Принцип 4: Стримувальні засоби контролю призвані знеохотити потенційного зловмисника.
- Принцип 5: Попереджувальні заходи контролю призвані мінімізувати ймовірність повернення інциденту.
- Принцип 6: Детективний контроль призначений для визначення того, коли стався інцидент.
- Принцип 7: Коригуючі заходи контролю призначені для виправлення компонентів інформаційної системи після того, як інцидент стався.
- Принцип 8: Коригуються лише виявлені ризики, коли ризики не виявляються, коригуючі заходи не можуть застосовуватися.
- Принцип 9: Лише зрілий стримуючий або попереджувальний контроль може знизити ймовірність ризику.
- Принцип 10: Лише зрілий детективний або коригуючий контроль може знизити серйозність ризику.

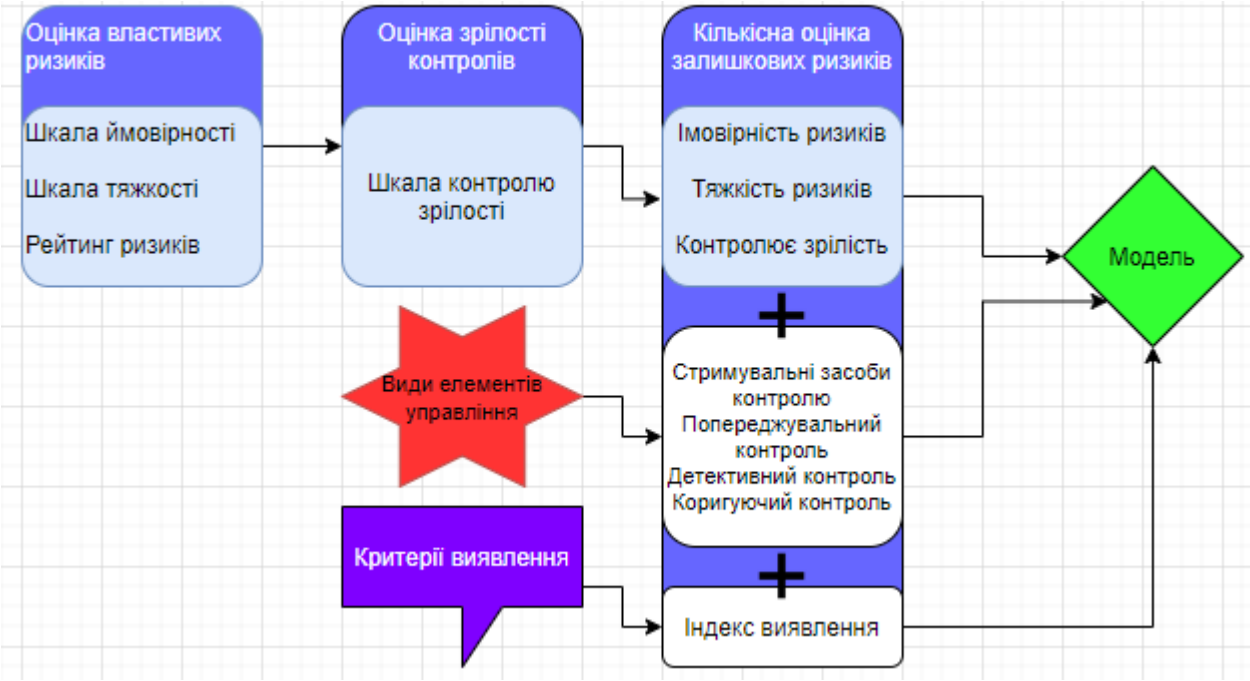

Рисунок 2.2 - Модельний підхід

Як показано вище, пропонується кількісна оцінка впливу заходів безпеки на ризики банківської інформаційної системи з використанням FMECA. Пропонований підхід складається з трьох етапів і враховує зрілість засобів контролю, типи засобів контролю і критерії виявлення. Перший крок стосується оцінки невід'ємних ризиків з використанням шкал, пов'язаних з ймовірністю виникнення і серйозністю впливу, щоб привласнити невід'ємну цінність кожному ризику. Другий крок стосується оцінки зрілості засобів контролю з використанням шкали зрілості засобів контролю, щоб привласнити значення зрілості кожному контролю. Третій крок пов'язаний з кількісною оцінкою залишкової вартості. Цей крок враховує параметри двох попередніх кроків і додаткові параметри, які пов'язані з типом контролю і критеріями виявлення.

2.3.1 Визначимо різні масштаби, які будуть параметрами моделі.

Використовувані шкали ймовірності і серйозності мають не більше шести значень;

Під час внутрішньої оцінки одне значення присвоюється ймовірності ризику і одне значення - серйозності ризику. Наступна шкала визначена для оцінки ймовірності виникнення ризику при відсутності контролю. Це дасть інформацію для оцінки невід'ємного ризику і дозволить оцінити ефективність будь-яких поточних засобів контролю, які знижують ймовірність виникнення ризикової події.

Таблиця 2.3 – Значення імовірності ризику.

Рейтинг	Опис	Значення
1	Майже ніколи	Загрозам важко використовувати вразливості
2	Малоймовірно	Загрози потребують значних навичок для використання вразливості
3	Можливо	Загрози потребують помірних навичок для використання вразливості
4	Велика ймовірність	Загрози потребують мінімальних навичок для використання вразливості
5	Майже напевно	Загрозам легко використовувати вразливості
6	Абсолютно впевнено	Загрозам дуже легко використовувати вразливості

Наступні шкали визначені для оцінки серйозності ризику, що виникає при відсутності засобів контролю. Це дасть інформацію для оцінки невід'ємного ризику і дозволить оцінити ефективність будь-яких поточних засобів контролю, які знижують вплив виникає ризикової події.

Таблиця 2.4 – Значення ступеня ризику.

Рейтинг	Опис	Значення
1	Мінімальний	Будь-який вплив на стратегічні цілі
2	Незначний	Впливом можна керувати за допомогою поточних ресурсів
3	Помірний	Впливом можна керувати за допомогою скромних додаткових ресурсів
4	Значний	Впливом неможливо управляти без зайвих ресурсів
5	Серйозний	Впливом неможливо управляти без значних додаткових ресурсів
6	Дуже серйозний	Це може серйозно скомпрометувати стратегічні цілі

Використовувана шкала для оцінки зрілості контролів показана у наступній таблиці. Як зазначено, шкала має не більше п’яти значень. Кожному оціненому контролю буде присвоєно одне значення зрілості.

Таблиця 2.5 – Значення контрольної зрілості.

Рейтинг	Опис	Значення
1	Не існує	Банк навіть не визначив проблеми які необхідно вирішити
2	Початкова	Проблеми існують, але підхід до управління дезорганізований.
3	Систематичний	Процедури не є складними, але вони формалізовані
4	Керований	Керівництво контролює та вимірює дотримання процедур
5	Оптимізований	Процеси вдосконалено до рівня належної практики

2.3.2 Визначення індексів

Також визначаємо п'ять індексів, пов'язаних зі зрілістю засобів контролю, і чотири типи засобів контролю, які будуть використовуватися в рівняннях моделі. Для кожної контрольної зрілості ми визначили відповідний індекс. Як зазначено нижче, індекс зрілості має деревовидні значення 0, 1 і 2.

Таблиця 2.6 – Значення індексу зрілості.

Рейтинг	Індекс	Опис
1	0	Не існує
2	0	Початковий
3	1	Систематичний
4	2	Керований
5	2	Оптимізований

Наступний покажчик відноситься до чотирьох типів елементів управління. У них є не більше двох значень: 0 або 1. Ми також будемо враховувати ці індекси при обчисленні впливу елементів управління, тому що кожен елемент управління має значення індексу зрілості і значення індексу типу.

Таблиця 2.7 – Значення стримуючого індексу.

Тип контроля	Індекс
Стримуючий засіб	1
Не стримуючий	0

Таблиця 2.8 – Значення індексу профілактики.

Тип контроля	Індекс
Профілактичний	1
Не профілактичний	0

Таблиця 2.9 – Значення індексу виявлення.

Тип контроля	Індекс
Виявлено	1
Не виявлено	0

Таблиця 2.10 – Значення коригуючого індексу.

Тип контроля	Індекс
Коригуючий	1
Не коригуючий	0

2.3.3 Визначення моделі

Щоб визначити модель, враховуємо попередні принципи, шкали і показники. Також беремо до уваги банківські правила, стандарти безпеки інформаційних систем і електронних платежів, співпрацю і партнерство. А ще використовуємо такі визначення:

• Невід'ємні ризики: ризик без урахування коштів контролю

• Термін дії засобів контролю: зрілість коштів стримуючого, превентивного, виявленого і коригуючого контролю.

• Залишкові ризики: ризик після обліку всіх видів контролю

Розглядаючи рівняння, яке забезпечує критичність ризику [33] шляхом обчислення добутку ймовірності і серйозності, модель, яка автоматизує оцінку впливу заходів безпеки на ризики банківської інформаційної системи, відхиляється наступним чином:

$$C_{res} = \left[P - \left(\sum_{e=0}^{r} \frac{a * i}{r} + \sum_{e=0}^{s} \frac{b * j}{s}\right)\right] * [G - \left(\sum_{e=0}^{t} \frac{c * k}{t}\right) + \sum_{e=0}^{u} \frac{\left(\frac{d}{2}\right) * l}{u}] \quad (2.10)$$

Параметри нашої моделі пояснюються нижче:

- Залишкові ризики: C_{res}
- Власна ймовірність: P

- Власна серйозність: G

Рівняння (2.11) дозволяє кількісно оцінити вплив стримуючих засобів контролю з використанням зрілості стримуючих засобів контролю (a), індексу стримуючих засобів контролю (i) і кількості стримуючих засобів контролю (r). Він заснований на принципах 4 і 9, в яких йдеться про те, що стримуючі заходи покликані відлякати потенційного зловмисника і, коли вони стануть зрілими, можуть знизити ймовірність ризику.

$$\sum_{e=0}^{r} \frac{a * i}{r}$$

(2.11)

Рівняння (2.12) дозволяє кількісно оцінити вплив превентивних засобів контролю, використовуючи зрілість превентивних засобів контролю (b), індекс превентивних засобів контролю (j) і кількість превентивних засобів контролю (s). Він заснований на принципах 5 і 9, які свідчать, що превентивні заходи призначені для мінімізації ймовірності виникнення інциденту, а коли вони стануть зрілими, вони можуть знизити ймовірність ризику.

$$\sum_{e=0}^{s} \frac{b * j}{s}$$

(2.12)

Рівняння (2.13) дозволяє кількісно оцінити вплив детективних засобів контролю, використовуючи зрілість виявлених засобів контролю (c), індекс виявлених засобів контролю (k) і кількість виявлених засобів контролю (t). Він заснований на принципах 6 і 10, в яких йдеться про те, що кошти виявленого контролю призначені для визначення того, коли стався інцидент, а коли вони стануть зрілими, вони можуть знизити серйозність ризику.

$$\sum_{e=0}^{t} \frac{c * k}{t}$$

(2.13)

Рівняння (2.14) дозволяє кількісно оцінити вплив коригувальних засобів контролю, використовуючи зрілість коригувальних засобів контролю (d), індекс коригувальних засобів контролю (l) і кількість коригувальних засобів контролю (u). Він заснований на принципах 7 і 10, які свідчать, що коригувальні заходи контролю призначені для виправлення компонентів інформаційної системи після того, як стався інцидент, і коли вони стануть зрілими, вони можуть знизити серйозність ризику. Принцип 8 також використовується, тому що коригуються тільки виявлені ризики, а це означає, що, коли ризики не виявлені, коригувальні заходи не можуть застосовуватися. Як було сказано раніше, ми знаємо, що максимальний термін погашення індексу дорівнює 2; потім ми пропонуємо, щоб ступінь зрілості заходів стримуючого, превентивного і детективного контролю не потребувала зміні, оскільки вони незалежні. Але зрілість коригувальних заходів контролю необхідно розділити на 2, тому що вони залежать від виявлення засобів контролю.

$$\sum_{e=0}^{u} \frac{\left(\frac{d}{2}\right) * l}{u}$$

(2.14)

Висновок до розділу 2

Проведений аналіз методик обчислення залишкових ризиків для інформаційних систем організацій. Визначено найбільш релевантний підхід до побудови моделі оцінки залишкових ризиків для банківських інформаційних систем.

Було вибрано модель на основі FMECA, бо вона є більш досконалою, також в краще сформульовані принципи і бажано її використовувати для банківської інформаційної системи.

В результаті аналізу буде розроблена модель, яка на мою думку зможе використовуватися для банківської діяльності та мати в собі концепт залишкових ризиків.

3 ПРАКТИЧНЕ ЗАСТОСУВАННЯ МОДЕЛІ ЗАЛИШКОВОГО РИЗИКУ ДЛЯ БАНКІВСЬКОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ

3.1 Принцип тестування

Для тестування підходять банки, які пропонують традиційні банківські послуги і продукти електронного банкінгу, такі як зняття, оплата або переказ з використанням кредитних, дебетових або передплачених карт. Ця вибірка є репрезентативною, оскільки у інших банків приблизно такі ж ризики, з огляду на їх аналогічну діяльність, інфраструктуру і їх залежність від законів і нормативних актів.

3.1.1 Виявлення ризиків

Щоб ідентифікувати ризики інформаційної системи, необхідно брати до уваги загрози і вразливості, тому що відповідний ризик визначається як здійснення загрози щодо вразливості. Ідентифікація загроз включає джерела загроз для забезпечення точної оцінки і виявлення вразливостей різними способами. Збираємо ризики і засоби контролю, пов'язаних з банківською інформаційною системою.

3.1.2 Оцінка невід'ємних ризиків

Оцінка невід'ємних ризиків - це процес визначення ймовірності загрози, спрямованої проти уразливості, і результуючого впливу успішного компромісу. При оцінці невід'ємною ймовірності і серйозності ми не беремо до уваги реалізовані засоби контролю. Під час оцінки присвоїмо кожному ризику значення ймовірності і серйозності з використанням раніше визначеної шкали.

3.1.3 Оцінка залишкових ризиків

Оцінка залишкового ризику оцінює ймовірність загроз, яких не можна уникнути за допомогою заходів безпеки, таких як залишкові загрози. Ці загрози можна усунути за допомогою додаткових заходів безпеки. Таким чином, ризик буде знижений до прийнятного рівня. [34] Невід'ємні ризики в поєднанні з оцінкою засобів контролю забезпечують залишкові ризики, які називаються довідковими значеннями.

3.1.4 Застосування моделі до всіх ризиків інформаційної системи

Для тестування застосовуємо модель до всіх ризиків банківської інформаційної системи і порівнюємо отримані значення зі значеннями, зазначеними оцінювачами, які називаються еталонними значеннями. Перед затвердженням моделі необхідно протестувати її на компонентах інформаційної системи, критерії інформаційної безпеки і етапах SDLC (Software Development Life Cycle) (життєвого циклу розробки програмного забезпечення).

1) Застосування моделі до компонентів інформаційної системи:

   Класифікуємо всі ризики по компонентах інформаційної системи, які включають обладнання, програмне забезпечення, мережу, базу даних, сайт, інформацію і користувачів, перш ніж застосовувати модель. Для цього розраховуємо для кожного компонента середній термін погашення контролю за типом засобів контролю, визначаємо кількість засобів контролю і застосовуємо запропоновану модель. Ступінь кореляції між модельним і еталонним залишковими ризиками показана в наступній таблиці. Відзначаємо, що коефіцієнт кореляції по

компонентах становить від 95,8% до 97,8%. Це означає, що для кожного компонента інформаційної системи значення моделі приблизно рівні довідковим значенням. Середнє значення коефіцієнта кореляції становить 97%, що означає, що залишкові ризики по компонентах інформаційної системи в цілому рівні довідковим значенням, наданим оцінювачами.

Таблиця 3.1 – Швидкість кореляції моделі і опорних залишкових ризиків по компонентам інформаційної системи.

Компоненти інформаційної системи	Коефіцієнт кореляції
Обладнання	96,6%
Програмне забезпечення	97,5%
Мережа	97,8%
База даних	96,7%
Сайт	97,3%
Інформація	95,8%
Користувачі	96,8%
В середньому	97%

2) Застосування моделі за критеріями інформаційної безпеки:

Також класифікуємо всі ризики за критеріями інформаційної безпеки, які включають ефективність, дієвість, цілісність, конфіденційність, відповідність, доступність, надійність, перед застосуванням моделі. Для цього розраховуємо для кожного критерію середнє значення зрілості контролю за типом засобів контролю, визначаємо кількість

засобів контролю і застосовуємо запропоновану модель. Ступінь кореляції між модельним і еталонним залишковими ризиками показана в наступній таблиці:

Таблиця 3.2 – Швидкість кореляції моделі і опорних залишкових ризиків по критеріям інформаційної безпеки.

Критерії інформаційної безпеки	Коефіцієнт кореляції
Ефективність	97%
ККД	97,3%
Цілісність	96,8%
Конфіденційність	97%
Відповідність	96,9%
Доступність	97,3%
Надійність	96,1%
В середньому	97%

Відзначимо, що коефіцієнт кореляції щодо запропонованих критеріїв різний і становить від 96,1% до 97,3%. Це означає, що для кожного критерію значення моделі приблизно рівні довідковим значенням. Середнє значення коефіцієнта кореляції однаковий, тому що тести проводяться для всієї інформаційної системи, і його значення 97% показує, що значення моделі в цілому рівні довідковим значенням.

3) Застосування моделі на етапах SDLC:

Нарешті класифікуємо всі ризики по етапах SDLC (життєвого циклу розробки програмного забезпечення). Ці етапи включають сім різних етапів: вимога, аналіз, проектування, розробка, тестування і технічне обслуговування. [35] Для тестування розраховуємо для кожної фази

середнє значення зрілості контролю за типом засобів контролю, визначаємо кількість засобів контролю і застосовуємо запропоновану модель. Ступінь кореляції між модельними і еталонними залишковими ризиками показана в наступній таблиці:

Таблиця 3.3 – Швидкість кореляції між моделлю та опорно залишковими ризиками по фазах SDLC.

Фази SDLC	Коефіцієнт кореляції
Вимога	96,8%
Аналіз	96,7%
Проектування	97,6%
Розробка	96,7%
Тестування	97,5%
Технічне обслуговування	96,8%
В середньому	97%

Відзначили, що значення коефіцієнта кореляції за фазами SDLC різниться і становить від 96,7% до 97,6%. Це означає, що для кожної фази SDLC значення моделі приблизно рівні контрольних значень. Середнє значення коефіцієнта кореляції завжди одне і те ж, тому що тести проводяться для всіх ідентифікованих ризиків, і його значення, рівне 97% і показує, що залишкові ризики моделі в цілому рівні, і дорівнює еталонним залишковим ризикам.

3.2 Економія часу

Нарешті, вимірюємо виграш у часі, який забезпечувався б моделлю, як показано в таблиці нижче:

Таблиця 3.4 – Економія часу моделі.

Критерії	Економія часу для 1 експерта	Економія часу для 10 експертів
За ризик	30 хвилин	5 годин
За 20 ризиків	1,25 робочих днів	12,5 робочих днів
За 40 ризиків	2,5 робочих днів	25 робочих днів
За 60 ризиків	3,75 робочих днів	37,5 робочих днів
За 80 ризиків	5 робочих днів	50 робочих днів
За 100 ризиків	6,25 робочих днів	62,5 робочих днів

Як видно з таблиці (3.4), модель забезпечує виграш в 62,5 робочих днів для оцінки 100 ризиків інформаційної системи 10 оцінювачами. Це може бути дуже вигідно для банків, тому що знаємо, що різні оцінювачі повинні виконувати безліч завдань в своїх відповідних відділах. Ця модель допомагає не витрачати багато часу на оцінку залишкових ризиків.

3.2.1 Глобальні результати

Беручи до уваги хорошу ступінь кореляції між модельним і еталонним залишковими ризиками і виграш часу, який забезпечується моделлю, робимо висновок, що наша модель має кілька переваг, які перераховані нижче:

- Автоматичний розрахунок залишкових ризиків інформаційної системи з урахуванням хорошої кореляції між модельними значеннями і еталонними значеннями.
- Зниження похибки оцінки залишкових ризиків за рахунок гармонізації методів і шкал оцінки.

- Скорочення часу на отримання залишкових ризиків з урахуванням виграшу часу, передбаченого моделлю.
- Допомога в підвищенні безпеки банківської інформаційної системи за рахунок автоматизації оцінки зрілості заходів безпеки.
- Сприяння управлінню ризиками за рахунок автоматизації оцінки ризиків і засобів контролю.

Висновок до розділу 3

Проведена апробація пропонованої моделі залишкових ризиків, та визначено, що завдяки неї можливо отримати: зниження похибки під час оцінки залишкових ризиків, скорочення часу на отримання залишкових ризиків, сприяння управління ризиками, підвищення безпеки банківської інформаційної системи.

ВИСНОВКИ

Банківська інформаційна система дуже вразлива для кіберзлочинів і інших атак. З цієї причини оцінка заходів безпеки повинна бути оптимальною для реалізації відповідних заходів контролю щоразу, коли це необхідно. Все ж таки банки працюють з великими об’ємами грошей, що є великою спокусою для злочинців.

Тому в ході дипломної роботи було проаналізовано моделі залишкових ризиків для організацій, вибрано таку модель, яка зможе допомогти та адаптовано для банківської інформаційної системи.

Запропонована модель повинна допомогти та сприяти розвитку безпеки банківської інформаційної системи. Забезпечувати автоматичний розрахунок залишкових ризиків, знижувати частоту помилок оцінки і скорочувати час отримання залишкових ризиків.

Мається на увазі підвищення безпеки банківської інформаційної системи, полегшення управління ризиками і збільшення прибутку банку.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

[1] “Risk management and accreditation of information systems”, 2005р. [Електронний ресур] – Режим доступу до ресурсу: http://osgug.ucaiug.org/conformity/security/Shared%20Documents/Reference/UK%20-%20CPNI%20-%20Risk%20Management%20and%20Accreditation%20of%20IS.pdf

[2] Gary Stoneburner, Alice Goguen, and Alexis Feringa, “Risk Management Guide for Information Technology Systems”, 2002р. [Електронний ресур] – Режим доступу до ресурсу: https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/nist800-30.pdf

[3] «Risk Assessment and Risk Management Methods: Information Packages for Small and Medium Sized Enterprises (SMEs)», 2006 р. [Електронний ресур] – Режим доступу до ресурсу: https://www.enisa.europa.eu/publications/information-packages-for-small-and-medium-sized-enterprises-smes/at_download/fullReport

[4] K. Kohout, “IT Risk Register, faculty of informatics and statistics,”, 2012p.;

[5G. Hardy and J. Heschl, “Aligning CobiT 4.1, ITIL V3 and ISO/IEC 27002 for Business Benefit,”, Інститут управління IT, 2008р. [Електронний ресур] – Режим доступу до ресурсу: https://fdocuments.in/document/aligning-cobit-41-itil-v3-and-isoiec-27002-for-business-benefit.html

[6] A. Syalim, Y. Hori and K. Sakurai, “Comparison of Risk Analysis Methods: Mehari, Magerit, NIST800-30 and Microsoft’s Security Management Guide”, Університет Кюсю [Електронний ресур] – Режим доступу до ресурсу: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.165.6972&rep=rep1&type=pdf

[7] V. Arora, “Comparing different information security
standards: COBIT v s. ISO 27001” [Електронний ресур] – Режим доступу до ресурсу: https://vdocuments.mx/cobit-v-s-iso-27001.html
[8] M. Gehrmann, “Combining ITIL, COBIT and ISO/IEC
27002 for structuring comprehensive information
technology for management in organizations”, ISSN 2237-4558, 2012р. [Електронний ресур] – Режим доступу до ресурсу: https://dialnet.unirioja.es/descarga/articulo/5168701.pdf
[9] I. Mukherjee, “Cloud Security Through COBIT,
ISO 27001 ISMS CONTROLS, ASSURANCE AND
COMPLIANCE,” ISACA, RSA Conference ASIA PACIFIC, 2013р. [Електронний ресур] – Режим доступу до ресурсу: https://docplayer.net/2576394-Cloud-security-through-cobit-iso-27001-isms-controls-assurance-and-compliance.html
[10] " Organisation Resilience: Business Continuity, Incident
and Corporate Crisis Management", Інститут управління безперервністю бізнесу, 2012р. [Електронний ресур] – Режим доступу до ресурсу: https://www.continuitycentral.com/OrganisationResilience.pdf
[11] C. Periou, “New players and new banking models for Africa”, 2013р. [Електронний ресур] – Режим доступу до ресурсу: https://www.proparco.fr/en/ressources/new-players-and-new-banking-models-africa
[12] “Payments 101: Credit and Debit Card Payments,” 2010р. [Електронний ресур] – Режим доступу до ресурсу: http://euro.ecom.cmu.edu/resources/elibrary/epay/Payments-101.pdf
[13] P. Dulany, H. Gong and K. Shah, “CA Technologies, Advanced Analytics and Data Science: 3D-Secure Authentication with Advanced Models”, 2014р. [Електронний ресур] – Режим доступу до ресурсу: https://docs.broadcom.com/doc/3-d-secure-authentication-using-advanced-models

[14] «Card-Not-Present Fraud Working Committee White
Paper», 2015p. [Електронний ресур] – Режим доступу до ресурсу: https://www.emv-connection.com/wp-content/uploads/2015/04/CNP-Solutions-White-Paper-FINAL.pdf
[15] R. Anderson, “Risk and Privacy Implications of
Consumer Payment Innovation” Cambridge University [Електронний ресур] – Режим доступу до ресурсу: https://www.cl.cam.ac.uk/~rja14/Papers/anderson-frb-kansas-mar27.pdf
[16] «Review of the Risk Assessment Process for Payment Systems», 2013p. [Електронний ресур] – Режим доступу до ресурсу: http://createdev.net/bpfi-old/wp-content/uploads/2014/10/Review_of_the_Risk_Assessment_Process_for_Payment_Systems.pdf
[17] J. Conroy, “3D Secure: The Force for CNP Fraud Prevention Awakens”, 2016p.
[18] P. Kellogg, “Evolving Operational Risk Management for Retail Payments”, 2003p. [Електронний ресур] – Режим доступу до ресурсу: https://www.chicagofed.org/~/media/publications/occasional-papers/2003/eps-2003-1e-pdf.pdf
[19] A. L. Pereira and A. M. de Alba, “Understanding the new payment methods, their risks and opportunities”, 2014p. [Електронний ресур] – Режим доступу до ресурсу: https://www.lexisnexis.com/risk/intl/en/resources/whitepaper/Understanding-The-New-Payment-Methods-CSMB.pdf
[20] P. Burns and A. Stanley, “Fraud Management in the
Credit Card Industry” 2002p. [Електронний ресур] – Режим доступу до ресурсу: https://poseidon01.ssrn.com/delivery.php?ID=682025021087127099027005078114076121029022041052070026086029023005003010120001080121054013022125049112043073117022125066099117059075089079105114012123113077084039055079085109110004120118089104084097127017065070026013001029005005097080087003069021&EXT=pdf&INDEX=TRUE

[21] C. Periou, “New players and new banking models for Africa”, 2013р. [Електронний ресур] – Режим доступу до ресурсу: https://www.proparco.fr/en/ressources/new-players-and-new-banking-models-africa

[22] W. S. Koffi, “The Fintech Revolution: An Opportunity for the West African Financial Sector”, 2016р. [Електронний ресур] – Режим доступу до ресурсу: https://www.researchgate.net/publication/309273233_The_Fintech_Revolution_An_Opportunity_for_the_West_African_Financial_Sector

[23] «Net Losses: Estimating the Global Cost of Cybercrime», 2014р. [Електронний ресур] – Режим доступу до ресурсу: https://www.combattingcybercrime.org/files/virtual-library/phenomena-challenges-cybercrime/net-losses%E2%80%93estimating-the-global-cost-of-cybercrime-%28economic-impact-of-cybercrime-ii%29.pdf

[24] D. Weese, “Overview of risk assessment methods and applications”, 2006р. [Електронний ресур] – Режим доступу до ресурсу: https://cdn.ymaws.com/www.casss.org/resource/resmgr/imported/CMC_July_09_Dan_Weese.pdf

[25] A. Ho, “Integration and use of Enterprise Risk Management (ERM) information», 2013р. [Електронний ресур] – Режим доступу до ресурсу: https://web.actuaries.ie/sites/default/files/erm-resources/integration_and_use_of_enterprise_risk_management_information.pdf

[26] N. Mathur, H. Mathur and T. Pandya, “Risk Management in Information System of Organisation: A Conceptual Framework”, 2015р.

[27] O. Pastor, L. J. G. Villalba and D. Lpez, “DYNAMIC RISK ASSESSMENT IN INFORMATION SYSTEMS: STATE-OF-THE-ART” 2013р. [Електронний ресур] – Режим доступу до ресурсу: http://icit.zuj.edu.jo/icit13/Papers%20list/Camera_ready/Software%20Engineering/772.pdf

[28] B. Jenkins, “Risk Analysis helps establish a good security posture; Risk Management keeps it that way”, 1998р. [Електронний ресур] – Режим доступу до ресурсу: https://nr.no/~abie/RA_by_Jenkins.pdf

[29 M. Ndaw, G. Mendy and S. Ouya, “A quantification model of internal control impact on banking risks using FMECA”, 2016р. [Електронний ресур] – Режим доступу до ресурсу: https://publications.waset.org/10003851/improving-the-quantification-model-of-internal-control-impact-on-banking-risks

[30] M. Ndaw, G. Mendy and S. Ouya, “Quantify the Maturity of Internet Banking Security Measures in WAEMU (West African Economic and Monetary Union) Banks”, 2017р. [Електронний ресур] – Режим доступу до ресурсу: https://eudl.eu/doi/10.1007/978-3-319-72965-7_11

[31] “Risk Assessment Process Information Security”, 2014р. [Електронний ресур] – Режим доступу до ресурсу: https://www.digital.govt.nz/dmsdocument/3~Risk-Assessment-Process-Information-Security.pdf

[32] L. Lipol and J. Haq, “Risk Analysis Method: FMEA/FMECA in the Organizations”, 2011р. [Електронний ресур] – Режим доступу до ресурсу: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.419.7912&rep=rep1&type=pdf#:~:text=Failure%20Mode%20and%20Effects%20Analysis%20(FMEA)%20is%20a%20methodology%20designed,for%20a%20product%20or%20process.&text=Assess%20the%20risk%20associated%20with,prioritize%20issues%20for%20corrective%20action.&text=Identify%20and%20carry%20out%20corrective%20actions%20to%20address%20the%20most%20serious%20concerns.

[33] V. Dumbrav, T. Maiorescu and V. S. Iacob, “Using Probability Impact Matrix in Analysis and Risk Assessment,” 2013р. [Електронний ресур] – Режим доступу до ресурсу: https://ru.scribd.com/document/252573910/07-Dumbrava-Iacob-USING-PROBABILITY-IMPACT-MATRIX-IN-ANALYSIS-AND-RISK-ASSESSMENT-PROJECTS-pdf

[34] B. Nikoli and L. R. Dimitrijevi, “Risk Assessment of Information Technology Systems», 2009р. [Електронний ресур] – Режим доступу до ресурсу: http://iisit.org/Vol6/IISITv6p595-615Nikolic673.pdf

[35] K. Sahu, Rajshree and R. Kumar, “Risk Management Perspective in SDLC” 2014р. [Електронний ресур] – Режим доступу до ресурсу: https://www.academia.edu/11101776/Risk_Management_Perspective_in_SDLC

[36] Інструкція з організації внутрішнього контролю в системі Міністерства юстиції України [Електронний ресур] – Режим доступу до ресурсу: https://minjust.gov.ua/m/instruktsiya-z-organizatsii-vnutrishnogo-kontrolyu-v-sistemi-ministerstva-yustitsii-ukraini

[37] [Електронний ресур] – Режим доступу до ресурсу: https://art-audit.net/yakist-poslug/sistema-kontrolyu-yakosti/vikonannya/#:~:text=%D0%92%D0%A0%20%E2%80%94%20%D0%B2%D0%BB%D0%B0%D1%81%D1%82%D0%B8%D0%B2%D0%B8%D0%B9%20(%D0%BD%D0%B5%D0%B2%D1%96%D0%B4'%D1%94%D0%BC%D0%BD%D0%B8%D0%B9)%20%D1%80%D0%B8%D0%B7%D0%B8%D0%BA%20(IR)%2C&text=%D0%A0%D0%B8%D0%B7%D0%B8%D0%BA%20%D0%BD%D0%B5%D0%B2%D0%B8%D1%8F%D0%B2%D0%BB%D0%B5%D0%BD%D0%BD%D1%8F%20%E2%80%94%20%D1%86%D0%B5%20%D1%80%D0%B8%D0%B7%D0%B8%D0%BA%20%D1%82%D0%BE%D0%B3%D0%BE,%D0%B2%20%D1%81%D1%83%D0%BA%D1%83%D0%BF%D0%BD%D0%BE%D1%81%D1%82%D1%96%20%D0%B7%20%D1%96%D0%BD%D1%88%D0%B8%D0%BC%D0%B8%20%D0%B2%D0%B8%D0%BA%D1%80%D0%B8%D0%B2%D0%BB%D0%B5%D0%BD%D0%BD%D1%8F%D0%BC%D0%B8

[38] Sean Boran, «IT Security Cookbook», 2003[Електронний ресур] – Режим доступу до ресурсу: http://www.boran.com/security/

[39] Dillon G. “Information Security Management: Global Challenges in the New Millennium” Idea Group Publishing House, 2001.

[40] Bo Bergman & Bengt Klefsjö, 2010, ISBN 978-91-44–05942-6, 3, [rev.] Ed., “Quality: from customer needs to customer satisfaction, Lund: Student literature.“

[41] Donald W. Benbow, Roger W. Berger, Ahmad K. Elshennawy, H. Fred Walker, 2002, the Certified Quality Engineer Handbook by ASQ.

[42] “Failure Modes and Effects Analysis (FMEA) and Failure Modes, Effects and Criticality Analysis (FMECA)”, 2011. [Електронний ресур] – Режим доступу до ресурсу: http://sce.uhcl.edu/goodwin/Ceng5334/downLoads/FMEA%20Basics.pdf

[43] Hot Wire, “the eMagazine for the Reliability Professional” by ReliaSoft, 2004 [Електронний ресур] – Режим доступу до ресурсу: www.weibull.com/hotwire/issue46/relbasics46.htm

[44] Fiorenzo Franceschini and Marizio Galetto, VOL. 39, NO. 13, 2991-3002; “A new approach for evaluation of risk priorities of failure modes in FMEA” by International Journal of Production Research, 2001 [Електронний ресур] – Режим доступу до ресурсу: https://www.researchgate.net/publication/261578433_A_new_approach_for_evaluation_of_risk_priorities_of_failure_modes_in_FMEA

[45] Luca Bencini and Steve Pautz, “FMEA Can Add Value in Various Project Stages”, 2011 [Електронний ресур] – Режим доступу до ресурсу: https://www.isixsigma.com/tools-templates/fmea/fmea-can-add-value-various-project-stages/

[46] ICH, Guidance for industry “Q9 quality Risk Managemen”t, 2006 [Електронний ресур] – Режим доступу до ресурсу: http://www.fda.gov/downloads/Drugs/GuidanceComplianceRegulatoryInformation/Guidances/UCM073511.pdf.

[47]
David C.Dunkle, ITT Industries- Systems Division, NASA Risk Management Conference, “Prioritizing Human Interface Design Issues for Range Safety Systems using Human Factors Process Fmea” by NASA, 2005

[48]
Dr. Deborah L. Smith, “FMEA: Preventing a Failure before Any Harm Is”, 2011 [Електронний ресур] – Режим доступу до ресурсу: https://www.isixsigma.com/tools-templates/fmea/fmea-preventing-failure-any-harm-done/

[49] А.А. Семкина, А.М. Цыбулин “ОЦЕНКА УРОВНЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ПРЕДПРИЯТИЯ ЧЕРЕЗ ОСТАТОЧНЫЙ РИСК”, 2012. [Електронний ресур] – Режим доступу до ресурсу: https://cyberleninka.ru/article/n/otsenka-urovnya-informatsionnoy-bezopasnosti-predpriyatiya-cherez-ostatochnyy-risk/viewer

[50] Wijnhoven, F. “Information Management: An Informing Approach”, 2009 [Електронний ресур] – Режим доступу до ресурсу: https://onesearch.library.uwa.edu.au/discovery/fulldisplay?vid=61UWA_INST:UWA&tab=Everything&docid=alma99584213902101&lang=en&context=L&adaptor=Local%20Search%20Engine

[51] Makhijani, N., Creelman, J. “Creating a Balanced Scorecard for a Financial Services Organization”, 2011 [Електронний ресур] – Режим доступу до ресурсу: https://onlinelibrary.wiley.com/doi/book/10.1002/9781119199274