МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ КАЗАХСТАН

Казахский национальный исследовательский технический университет имени К.И.Сатпаева

Институт автоматики и информационных технологий

Кафедра кибербезопасность, обработка и хранение информации

Рахимжанова Алтыншаш Сеилхановна

Проектирование системы защиты конфиденциальной информации в банковских системах

ДИПЛОМНАЯ РАБОТА

Специальность 5В070300 – Информационные системы

Алматы, 2022

МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ КАЗАХСТАН

Казахский национальный исследовательский технический университет имени К.И.Сатпаева

Институт автоматики и информационных технологий

Кафедра кибербезопасность, обработка и хранение информации

ДОПУЩЕН К ЗАЩИТЕ
Заведующий кафедрой КОиХИ
к.т.н., ассоц. профессор
_____ Р.Ж.Сатыбалдиева
«19»
05 2022г.

ДИПЛОМНАЯ РАБОТА

На тему: Проектирование системы защиты конфиденциальной информации в банковских системах

Специальность 5В070300 – Информационные системы

Выполнила: Рахимжанова А.С.

Рецензент
Доктор PhD, СНС ИИВТ КН МОН РК
_____ Усатова О.А.
«19» 05 2022 г.

Научный руководитель
Доктор Ph.D, ассоц. профессор
_____ Бегимбаева Е.Е.
«19» 05 2022 г.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН

Казахский национальный исследовательский технический университет имени К.И.Сатпаева

Институт автоматики и информационных технологий

Кафедра кибербезопасность, обработка и хранение информации

5В070300 – Информационные системы

УТВЕРЖДАЮ
Заведующий кафедрой КОиХИ
к.т.н., ассоц. профессор
_____ Р.Ж.Сатыбалдиева
«19» 05 2022г.

ЗАДАНИЕ
на выполнение дипломной работы

Обучающемуся: Рахимжановой Алтыншаш Сеилхановне.

Тема: Проектирование системы защиты конфиденциальной информации в банковских системах.

Утверждена *приказом Ректора Университета № 489-П/Ө от 24.12.2021г.*

Срок сдачи законченной работы *24.05.2022 г.*

Исходные данные к дипломному проекту: сбор теоретического материала, обзор предметной области, результаты преддипломной практики.

Краткое содержание дипломной работы:

а) Обзор и анализ обеспечения информационной безопасности банков РК;
б) Выбор инструментов для разработки системы авторизации;
в) Программная реализация системы авторизации.

Перечень графического материала (с точным указанием обязательных чертежей): *представлены 27 слайдов презентации работы*

Рекомендуемая основная литература: *из 19 наименований*

ГРАФИК

подготовки дипломной работы (проекта)

Наименование разделов, перечень разрабатываемых вопросов	**Сроки представления научному руководителю**	**Примечание**
Исследование банков РК;	13.02.2022	
Анализ технологий, методов защиты конфиденциальной информации;	25.02.2022	
Проектирование формы авторизации;	12.03.2022	
Отладка и тестирование системы.	25.04.2022	

Подписи

консультантов и нормоконтролера на законченную дипломную работу (проект) с указанием относящихся к ним разделов работы (проекта)

Наименование разделов	**Консультанты, Ф.И.О. (уч.степень, звание)**	**Дата подписания**	**Подпись**
Основная часть	Бегимбаева Е.Е. ассоц.проф, PhD	10.05.2022	
Нормоконтроль	Аристомбаева М.Т., маг.тех.наук, лектор	17.05.2022	

Научный руководитель:_____ Бегимбаева Е.Е.

Задание принял к исполнению обучающийся:_____ Рахимжанова А.С.

Дата "20" января 2022

РЕЦЕНЗИЯ

на дипломную работу студентки 4 курса Казахского национального исследовательского технического университета им. К.И.Сатпаева специальности 5В070300 «Информационные системы»
Рахимжанова Алтыншаш Сеилхановна
на тему: «Проектирование системы защиты конфиденциальной информации в банковских системах»

Дипломная работа Рахимжановой А.С. посвящена проектированию системы защиты конфиденциальной информации в банковских системах.

Структура дипломной работы включает в себя: введение, три раздела, заключение, список используемых источников литературы и приложений.

Во введении определяется актуальность выбранной темы, цели и задачи исследования. В работе проведен анализ обеспечения информационной безопасности банковских систем Республики Казахстан. Описаны этапы проектирования системы защиты конфиденциальной информации. Приведена модель компьютерной сети банка, форма авторизации для клиентов банка.

Работа выполнена аккуратно, а также продемонстрировано умение студента применять технические и программные средства. Данная работа содержит некоторые недостатки, например, небольшой объем введения, тем не менее это не влияет на качество работы..

В целом работа представлена завершенной и может быть оценена на «87 Хорошо» а при успешной защите Рахимжанова А.С. достойна присвоению академической степени бакалавра технических наук.

Рецензент
Доктор PhD, главный ученый секретарь, СНС «Института информационных и вычислительных технологий КН МОН РК _____ Усатова О. А.

«18» мая 2022 г.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН

Казахский национальный исследовательский технический университет имени К.И.Сатпаева

Институт автоматики и информационных технологий

Рахимжанова Алтыншаш Сеилхановна

5В070300 – Информационные системы

ОТЗЫВ НАУЧНОГО РУКОВОДИТЕЛЯ

к дипломной работе

Тема: «Проектирование системы защиты конфиденциальной информации в банковских системах»

Рецензируемая дипломная работа Рахимжановой А.С. посвящена проектированию системы защиты конфиденциальной информации в банковских системах.

Автором работы был проведен общирный анализ предметной области, рассмотрены методы защиты информации, меры по защите информационных активов банка, были визулизированы результаты анализа рисков по итогам 2021 года, также была спроектирована модель компьютерной сети, для защиты физических устройств банка. Также был применен метод защиты баз данных банка, методом хеширования паролей. Автор дипломной работы проявлял заинтересованность и активно участвовал в предложениях об улучшении разработки.

По итогам дипломной работы Рахимжанова А.С. выполнила все поставленные задачи, а также участвовала в Республиканском ежегодном конкурсе научно-исследовательских работ студентов НИРС 2022 г.

Дипломная работа выполнена с учетом всех требований, предъевляемых к дипломной работе по специальности 5В070300 – «Информационные системы», работа заслуживает оценки «Отлично», а ее автор Рахимжанова А.С. присвоения академической степени «бакалавра» по специальности 5В070300 – «Информационные системы».

Научный руководитель

Доктор Ph.D, ассоц. профессор Бегимбаева Е.Е.

« 18 » мая 2022 г.

StrikePlagiarism.com

SATBAYEV UNIVERSITY

Дата отчета 5/14/2022
Дата редактирования ---

Отчет не был оценен.

Метаданные

Название
диплом_Рахимжанова_Алтыншаш.docx

Автор
Рахимжанова Алтыншаш Научный руководитель

Подразделение
ИАиИТ

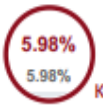
Список возможных попыток манипуляций с текстом

В этом разделе вы найдете информацию, касающуюся манипуляций в тексте, с целью изменить результаты проверки. Для того, кто оценивает работу на бумажном носителе или в электронном формате, манипуляции могут быть невидимы (может быть также целенаправленное вписывание ошибок). Следует оценить, являются ли изменения преднамеренными или нет.

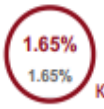
Замена букв	ß	2
Интервалы	A⟶	0
Микропробелы	-	51
Белые знаки	ß	0
Парафразы (SmartMarks)	a	17

Объем найденных подобий

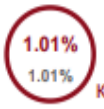
Обратите внимание!Высокие значения коэффициентов не означают плагиат. Отчет должен быть проанализирован экспертом.



КП1



КП2



КЦ

25
Длина фразы для коэффициента подобия 2

4966
Количество слов

40761
Количество символов

Подобия по списку источников

Просмотрите список и проанализируйте, в особенности, те фрагменты, которые превышают КП №2 (выделенные жирным шрифтом). Используйте ссылку «Обозначить фрагмент» и обратите внимание на то, являются ли выделенные фрагменты повторяющимися короткими фразами, разбросанными в документе (совпадающие сходства), многочисленными короткими фразами расположенные рядом друг с другом (парафразирование) или обширными фрагментами без указания источника ("криптоцитаты").

АННОТАЦИЯ

Целью дипломной работы является проектирование системы защиты конфиденциальной информации в банковских системах.

В ходе написания работы, был проведен анализ обеспечения информационной безопасности банковских систем РК, были описаны этапы проектирования системы защиты конфиденциальной информации. Для наглядности примера защиты информации в базе данных, была спроектирована форма авторизации (на языке Java + MySQL). При разработке системы был проведен анализ банков РК, были сравнены технологии и методы защиты информации.

Дипломная работа включает в себя: введение, 3 главы, заключение, список литературы.

АҢДАТПА

Дипломдық жобаның мақсаты - банк жүйелеріндегі құпия ақпаратты қорғау жүйесін жобалау.

Жұмысты жазу барысында ҚР банк жүйелерінің ақпараттық қауіпсіздігін қамтамасыз етуге талдау жүргізілді, құпия ақпаратты қорғау жүйесін жобалау кезеңдері сипатталды. Деректер базасындағы ақпаратты қорғаудың мысалын келтіру үшін авторизация нысаны жасалды (Java + MySQL тілдерінде). Жүйені әзірлеу кезінде ҚР банктеріне талдау жүргізілді, ақпаратты қорғау технологиялары мен әдістері салыстырылды.

Дипломдық жұмыс мыналарды қамтиды: кіріспе, 3 тарау, қорытынды, әдебиеттер тізімі.

ANNOTATION

The purpose of the thesis is to design a system for protecting confidential information in banking systems.

In the course of writing the work, an analysis was carried out to ensure the information security of the banking systems of the Republic of Kazakhstan, the stages of designing a system for protecting confidential information were described. To illustrate an example of protecting information in a database, an authorization form was designed (in Java + MySQL). During the development of the system, an analysis of the banks of the Republic of Kazakhstan was carried out, technologies and methods of information protection were compared.

The thesis includes: introduction, 3 chapters, conclusion, list of references.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

В веке информационных технологий, многие системы и процессы автоматизированы. Банковские системы не являются исключением. Но стоит учесть, что человек принимает участие в автоматизации и системе безопасности банка и прочих организаций. С развитием различных технологий растет рост хакерских и прочих атак. Малейший прокол, малейшая ошибка могут привести к невообразимому ущербу. По этой причине, проектирование информационной системы, является одним из главных этапов защиты информации. Проектируемая система информационной безопасности должна учитывать и обновлять улучшающиеся каждый год технологии и сервисы, а также должна удовлетворять следующим условиям: применение открытых стандартов; использование интегрированных решений; обеспечение масштабирования в широких пределах. С каждым годом растет спрос на «Белых хакеров» и безопасников. Можно с уверенностью заявить, что сфера безопасности данных банка всегда была и будет актуальна.

1 Исследовательский раздел

1.1 Информационная безопасность

Информация – сведения об объектах, лицах, происшествиях, которые происходят вокруг нас и процессах. В обязанности информационной безопасности входит защита информации конфиденциального характера от несанкционированных действий, включая проверку, модификацию, запись и любое нарушение или разрушение, вплоть до уничтожения [1].

В обязанности информационной безопасности входит проектирование комплекса систем предназначенный для конфиденциальной информации, которые будут защищать информационные активы, вне зависимости того, как была отформатирована информация, находится ли она в пути, обрабатывается или находится в состоянии покоя в хранилище. Конфиденциальная информация доступна определённому кругу лиц, обладающих полномочиями на составляющее информации.

Безопасностью автоматизированных систем обработки информации (АСОИ) называют обеспечение безопасности для системы от тех или иных изменений (случайных изменений, преднамеренных искажений, вмешательств) или от несанкционированного доступа к конфиденциальной информации. Информационный доступ может быть санкционированным – удовлетворяющий условиям назначенных правил, так и несанкционированным – не удовлетворяющий условиям назначенных правил. С позиции ИБ информация обладает следующими 3 свойствами [2]:

– конфиденциальность;

– доступность;

– целостность.

Информационная конфиденциальность – доступ к конфиденциальной информации определенным лицам, прошедшие авторизацию и подтвердившие личность и права на доступ к информации. Авторизацию можно пройти при помощи правильного ввода пароля, ПИН-кода, СМС кода, электронной подписи, сгенерированного ключа. Схема процесса авторизации приведен на рисунке 1.1.

Рисунок 1.1 - Авторизация субъекта

Целостность информации – неизмененная информация в первоначальном виде, не подвергшаяся к искажению, изменению.

Доступность информации – доступность информации для правообладателей, авторизованных пользователей.

Виды угроз для безопасности АСОИ [3]:

– Угрозы нарушения конфиденциальности информации – получение информации злоумышленниками, лицами не имеющих прав.

– Нарушения целостности информации – искажение или изменение информации злоумышленниками.

– Нарушения работоспособности системы (DDoS, DoS атаки)

Процессом идентификации называют присвоение абоненту оригинального идентификатора, предъявляющий СЗИ [4]. Воспользовавшись оригинальным пользователю идентификатором, СЗИ удостоверяется в наличии проверяемого пользователя в БД зарегистрированных пользователей и авторизует его в систему. К примеру, можно привести логин пользователя, бесконтактные радиочастотные карты и.т.д. Идентификаторы не несут секретную информацию, по этой причине могут храниться в открытом виде в БД или КС.

Процессом аутентификации называют процесс этапа проверки и подтверждения связи с идентификацией. К примеру, можно отнести пароли, ПИН коды и.т.д.

Главные типы угроз для безопасности парольных систем [3-5]:

– Перебор паролей в интерактивном режиме;

– Преднамеренная передача пароля его владельцем другому лицу;

– Кража базы данных учетных записей с дальнейшим ее анализом, подбором пароля;

– Перехват вводимого пароля путем внедрения в КС программных закладок (клавиатурных шпионов);

– Перехват пароля, передаваемого по сети.

1.2 Банковская безопасность

Банковская безопасность – все меры и мероприятия, для обеспечения защиты деятельности и конфиденциальных данных информационных активов банка [6]. В БД содержится вся конфиденциальная информация о состоянии активов и ресурсов клиентов, личная информация о пользователях и иная информация. Для достижения наибольшей вероятности защиты, банкам необходимо соблюдать все меры по защите информационных, конфиденциальных данных, использовать комплексный подход для виртуальных механизмов также для сетевой безопасности. Подавляющая большинство операций банка или финансового учреждения осуществляется с использованием различных технологий, в том числе через Интернет. Без надежных мер кибербезопасности конфиденциальные данные банка могут

оказаться под угрозой.

Стоит упомянуть, что случаи хакерских атак и прочие небольшие инциденты в отрасли информационной безопасности, являются секретной информацией, которые не подвергаются публичной огласке [7]. Практика показывает, что почти не одна система не может быть идеальна – практически невозможно обеспечить 100% защиту на длительный промежуток времени. Помимо аудита информации, необходимо регулярно тестировать систему (серые хакеры, белые хакеры). В каждой организации должны быть меры по защите конфиденциальной информации согласно стандартам.

При защите данных в банковской отрасли необходимо учитывать следующие пункты [8-9]:

– Анализ, определение угроз;

– проектирование системы защиты информации;

– предупреждение, преждевременное определение угроз;

– рост готовности к последствиям;

– проектирование системы уничтожения последствий разрушающих процессов.

1.2.1 Анализ безопасности банков РК

Сравнительный анализ уровня безопасности 2020 – 2021 годов. Данные были взяты у ЦАРКА по банкам второго уровня РК, вошедшие в периметр анализа, использовавшие технологии WebTotem AI.

Средний показатель степени безопасности банков составил 19.6%. Основной целью исследования был анализ уязвимостей и оценка безопасности банков РК. Оценка уровня безопасности при помощи лучших технологий и стандартов как: OWASP Top 10, ISO27001-2013. Банки оценивались по следующим критериям: репутация домена, шифрование трафика, утечка информации, открытые порты, Security.txt, безопасность email, состав программного обеспечения, скорость работы, HTTPS заголовки и безопасность контента. По результатам показателя защищенности средний показатель составил 70% [10].

Анализ рисков на Python:

1) Импортируем библиотеки: pyplot – для визуализации в виде диаграмм, pandas – для обработки и анализа данных, numpy – для работы с массивами, seaborn - для создания статистических графиков. Список библиотек приведен на рисунке 1.2.1.

```
В [1]: import matplotlib.pyplot as plt
       import pandas as pd
       import numpy as np
       import seaborn as sns
       %matplotlib inline
```

Рисунок 1.2.1 – список библиотек

2) Импортируем xlsx файл в Jupyter, импортируем дата сет, где 1 – «Показатель лучшего результата», -1 – «были обнаружены угрозы», 0 - «средний результат». Xlsx файл изображен на рисунке 1.2.2.

```
В [8]: data = pd.read_excel('анализ банков РК.xlsx')
       data
```

Out[8]:

	Name	security_txt	Software _composition_analysis	Traffic_encryption
0	Altyn Bank	-1	-1	0
1	Bank of China Kazakhstan	-1	-1	0
2	Bank RBK	-1	1	1
3	Capital Bank Kazakhstan	-1	-1	0
4	Citi Bank	-1	1	1
5	First Heartland Jýsan Bank	-1	1	1

Рисунок 1.2.2 – Xlsx файл с данными анализа банков РК

3) Количество банков для анализа, количество параметров по рискам. Используем функцию count (), для подсчета столбцов с названием, функция shape [1] – размерность столбца, для подсчета рисков. Результаты функций count () и shape [] приведены на рисунке 1.2.3.

```
В [32]: #Количество банков для анализа.
        data['Name'].count()
Out[32]: 25

В [46]: #количество параметров по рискам.
        risk = data.loc[:, data.columns != 'Name']
        risk.shape[1]
Out[46]: 8
```

Рисунок 1.2.3 – количество банков, параметров

4) Уязвимость по Security Txt, изображена на рисунке 1.2.4.

```
В [61]: #Уязвимости в security_txt
        data['security_txt'].value_counts()

Out[61]: -1    24
          1     1
         Name: security_txt, dtype: int64

В [62]: data['security_txt'].value_counts().plot(kind='bar')

Out[62]: <AxesSubplot:>
```

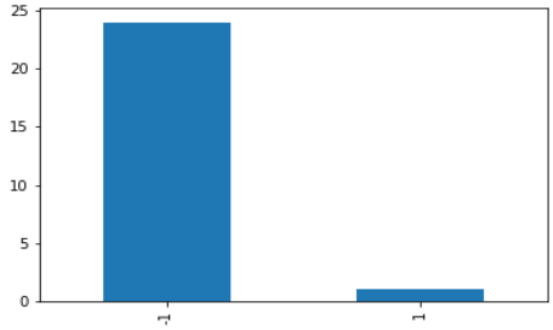


Рисунок 1.2.4 – уязвимость в Security txt

Security txt – стандарт, необходимый для оценки безопасности веб-сайтов. Организациям необходимо размещать security.txt файл в домен веб-сайта. Отсутствие данного файла, говорит о том, что переданные файлы подверглись атаке или изменению. Для защиты организации рекомендуется применять данный стандарт [11].

5) Уязвимость по Software composition analysis, изображён на рисунке 1.2.5.

```
В [63]: #Уязвимости в Software composition analysis
        data['Software _composition_analysis'].value_counts()

Out[63]:  0    11
         -1     9
          1     5
         Name: Software _composition_analysis, dtype: int64

В [64]: data['Software _composition_analysis'].value_counts().plot(kind='bar')

Out[64]: <AxesSubplot:>
```

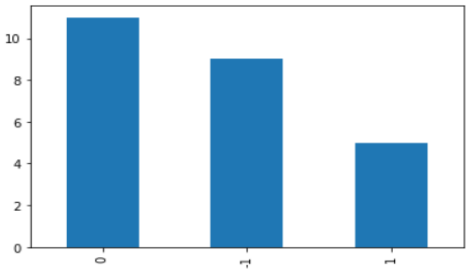


Рисунок 1.2.5 – Уязвимость в Software composition analysis

Software composition analysis – инструменты, необходимые для выявления уязвимостей, несущие угрозу данным банка.

6) Уязвимость по шифрованию трафика, изображен на рисунке 1.2.6.

```
В [65]: #Уязвимости в шифровании трафика
        data['Traffic_encryption'].value_counts()

Out[65]:  0    14
         -1     6
          1     5
         Name: Traffic_encryption, dtype: int64

В [66]: data['Traffic_encryption'].value_counts().plot(kind='bar')

Out[66]: <AxesSubplot:>
```

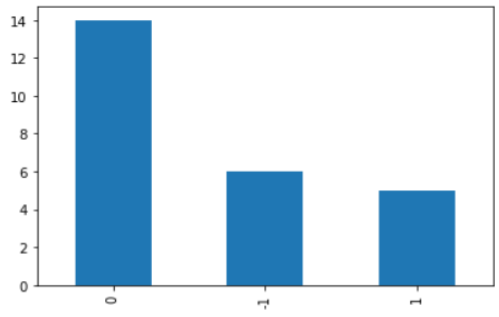


Рисунок 1.2.6 – Уязвимость в шифровании трафика

Уязвимость в шифровании трафика также может привести к краже, изменению, несанкционированному доступу к данным. Рекомендуется применение технологий VPN, OpenVPN, IPsec или покупка VDS-сервера.

7) Уязвимость в утечке данных, изображен на рисунке 1.2.7.

```
В [67]: #Уязвимости в утечке данных
        data['Data_leak'].value_counts()

Out[67]:  0    17
         -1     8
         Name: Data_leak, dtype: int64

В [70]: data['Data_leak'].value_counts().plot(kind='bar')

Out[70]: <AxesSubplot:>
```

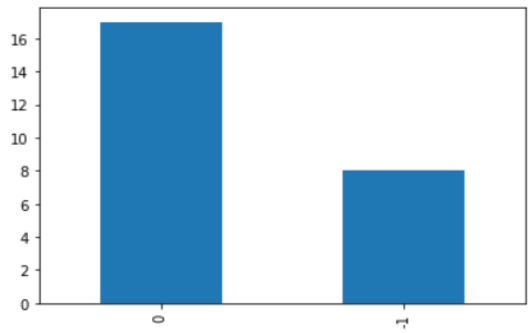


Рисунок 1.2.7 – Уязвимость в утечке данных

Причинами утечки данных могут являться, как и внешние причины, так и внутренние. Проблему с утечкой данных, нужно выполнять комплекс мер по обеспечению данных. Виды сетевых атак и меры по защите данных были подробно описаны в главе 1.2.2. Необходимо шифровать данные, использовать антивирусы, брандмауэры (Firewall), специальные ПО, проводить анализ и.т.д.

8) Уязвимость в Email Security, изображено на рисунке 1.2.8.

```
In [71]: #Уязвимости в Email Security
         data['Email_Security'].value_counts()

Out[71]:  0    18
          1     5
         -1     2
         Name: Email_Security, dtype: int64

In [72]: data['Email_Security'].value_counts().plot(kind='bar')

Out[72]: <AxesSubplot:>
```

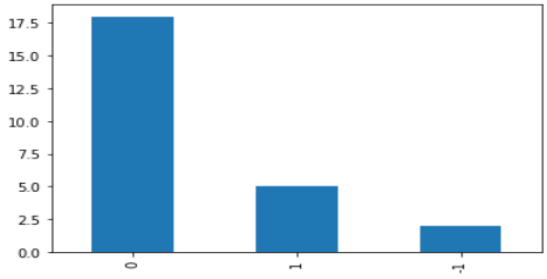


Рисунок 1.2.8 – Уязвимость в Email Security

Уязвимость в почтовом сервере, может привести к утечке данных клиентов банка, клиенты могут подвергнуться фишингу или как минимум спам рассылке. В худшем случае злоумышленники(хакеры) сумеют получить доступ к почтовому серверу банка, что приведет к утечке данных и другим последствиям. Для того, чтобы обезопасить систему банка, сервера необходимо защищать при помощи VPN, который шифрует трафик, или при помощи межсетевых экранов. Также можно использовать такие ПО как: Secure Email Gateway – ПО, предназначенное для отслеживания отправляемых и входящих писем, применение иных технологий.

9) Топ 5 банков по результатам оценки, сортируем массив по убыванию, для подсчета 5 лучших результатов, изображен на рисунке 1.2.9.

Топ 5 банков по результатам оценки

```
In [105]: sizes = data.sum(axis=1) + 10
          names = data['Name']

In [107]: #сумма оценок по банкам
          my_dict = {}
          for A, B in zip(names, sizes):
              my_dict[A] = B

          import operator
          top_5 = sorted(my_dict.items(),key=operator.itemgetter(1),reverse=True)[:5]
          top_5

Out[107]: [('Альфа Банк', 16),
           ('Citi Bank ', 14),
           ('Bank RBK', 13),
           ('First Heartland Jýsan Bank', 13),
           ('Freedom finance Bank', 12)]
```

Рисунок 1.2.9 – Топ 5 банков

10) Диаграмма pie изображена на рисунке 1.2.10.

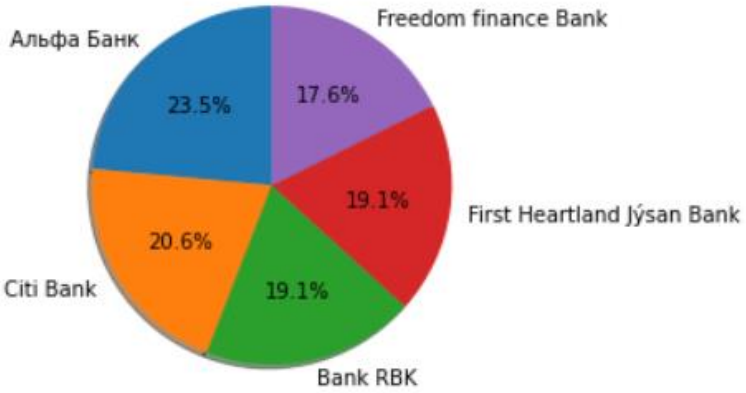


Рисунок 1.2.10 – Топ 5 банков, диаграмма pie

Итоги: По итогам анализа риска банков по 8 критериям, и по итогам анализа программы Bug Bounty лучшие результаты показали: Альфа банк, Bank RBK, Citi Bank, Народный Банк Казахстана, Freedom finance Bank.

1.2.2 Риски в банковских системах

Риск - неопределённое событие, которое может служить последствием наступления неблагоприятных событий. Для банков – возможная потеря, которая может быть нанесена организации в случае использования уязвимостей системы в преступных целях. В банковской сфере чаще всего атакуют платежные системы, инфраструктуры. Чаще всего злоумышленники заражают системы банка, заражают устройства клиентов банка троянскими файлами, атакуют фишингами рассылая спам сообщения.

Причинами возникновения рисков информационным активам банка могут являться: внешние атаки (заражение системы вирусом, отказы в обслуживании), внутренние ошибки (ошибка работников банка). Для совершения хакерской атаки хакеры сканируют для совершения атаки, анализируют известные порты прикладных уровней, далее пытаются пробить уязвимость протоколов [12].

Самые большие угрозы для кибербезопасности банка:

– Незашифрованные данные. Это очень простая, но важная часть кибербезопасности. Все данные, хранящиеся на компьютерах в финансовом учреждении и в интернете, должны быть зашифрованы. Даже если данные украдены хакерами, они не могут быть немедленно использованы ими, если они зашифрованы.

– Вредоносное ПО. Устройства конечных пользователей, такие как

компьютеры и мобильные телефоны, которые были скомпрометированы вредоносным ПО, представляют угрозу для кибербезопасности информации, при подключении к сети. Конфиденциальные данные проходят через это соединение и, если на устройстве конечного пользователя установлено вредоносное ПО без надлежащей защиты, вредоносное ПО может атаковать сети банка.

– Небезопасные сторонние сервисы. Большинство банков и финансовых учреждений используют различные ПО, технологии от других импортеров, для лучшего обслуживания клиентов. Однако, если у этих сторонних поставщиков нет хороших мер кибербезопасности, может пострадать данные.

– Данные, которыми манипулировали. Иногда хакеры не крадут данные, а просто изменяют их. К сожалению, этот тип атаки может быть трудно обнаружить сразу, и финансовые учреждения могут понести убытки в миллионы тенге, поскольку измененные данные практически не отличаются от первоначального вида, может быть сложно определить, что было изменено, а что нет.

– Спуфинг. Новый тип угрозы кибербезопасности — спуфинг, когда хакеры находят способ выдать себя за URL-адрес банковского веб-сайта с веб-сайтом, который выглядит и функционирует аналогично. При введении пользователем личной информацию, информация, крадется и используется хакерами для их личных целей. Еще более тревожным является то, что новые методы спуфинга не используют немного другой, но похожий URL-адрес – они могут нацеливаться на пользователей, которые посетили правильный URL-адрес.

К сетевым атакам можно отнести [13]:

– DoS (denial of service attack) – атаки, которые приводят к отказу в обслуживании. В случае denial of service, злоумышленники отправляют очень большое число запросов жертве. Все эти запросы выводят объект из строя.

– DdoS (distributed denial of service attack) отличается от DoS атаки тем, атака запускается с большинства управляемых злоумышленником устройств, зараженные вредоносным ПО, заставляющий их совершать атаки. Эти зараженные устройства называются BOTNET, которые являются интернетом вещей IoT (internet of things), к примеру умные часы, пылесосы и.т.д.

– СПАМ – рассылка вирусных почтовых сообщений. Вышеперечисленные ботнеты могут также участвовать в пересылке спам сообщений. К примеру: на почту отправляется поддельное письмо от вашего банка с некими документами, при скачивании файла пользователем, злоумышленник получает доступ к вашей системе.

– Фишинг – вид атаки и мошенничества, при котором злоумышленники получают логин и пароль пользователей принимая себя за доверенную организацию. Злоумышленники могут отправлять сообщения от лица банка, где необходимо ввести логин, пароль и прочую информацию.

– Троянские ПО. При заражении злоумышленниками устройства пользователей, могут быть скрыты Backdoor-ы – позволяющие злоумышленнику удаленно управлять девайсом пользователя. Miners – скрытая программа,

добывающая криптовалюту для злоумышленников. Bankers – крадут с девайса имеющуюся информацию, имеющую отношение к онлайн банкингу и иным платежным системам. Spyware – отслеживает действия с клавиатуры, что вводит пользователь, следят что происходит на рабочем столе, могут получить доступ к аудио оборудованию(микрофон), видео устройствам (веб-камере) пользователей. Adware – рекламное ПО, появление рекламного баннера, мешающий работе.

– Вирусы – программы заражающие файлы на ПК, вредоносным кодом, что приводит инфицированию системы.

– Черви – вредоносны ПО, распространяющиеся по системам, используют уязвимые устройства или же сетевые протоколы.

1.2.3 Описание мер по защите конфиденциальной информации

Проектирование системы защиты информации является одним из ключевых мероприятий которых нужно учитывать в первую очередь. Согласно составленному ТЗ, проектируется система защиты информации. Описываются все этапы проектирования, необходимые финансы, ресурсы (трудовые, физические), необходимые технологии и.т.д. Для проектирования системы защиты конфиденциальной информации со стороны безопасников необходимо:

1) Описание бизнес процесса. В этом этапе разрабатываются бизнес планы(модель проектирования), идеи по реализации, документации и стандарты. Организация и учет всех активов (сотрудники, оборудование, сервер, БД, иные ресурсы). Описать функцию, роль каждой фигуры, составляющих.

2) Описание перечня активов подлежащие защите. Формируется список необходимых активов. Также необходимо построить пирамиду важности информации по приоритету защиты, так как есть ограничения в ресурсах, времени, в бюджете и набору технических средств. Ценную информацию могут нести БД с активами банка, пользователей, клиентов, БД с данными клиентов, важные документы организации, доступ к серверам и.т.д. То есть БД с номерами страховки, информацией о наличии/отсутствии кредитов и.т.д. в случае утечки, не сильно навредят отрасли банка.

3) Проектирование модели угроз – выявляются уязвимые точки, недостатки, щели в защищенности информации [14-15]. В сети банка, сегменты разработчиков, сегмент офисных сотрудников, аналитиков, внешних сервисов относятся в внутреннему сегменту, информация которой хранится в БД организации, которые взаимосвязаны с иными серверами. Принцип по сегментного деления происходит по функциональным ролям. Установка средств системы защиты осуществляется по сегментно, контролируется доступ на входе в определенный сегмент по правам доступа.

4) Описать средства защиты от внешних угроз(хакеры, вирусы). Составить матрицу угроз. Подобрать средства защиты по классам.

5) Описать средства защиты от внутренних нарушений(ошибка сотрудников, шпионы и.т.д). Утечка информации, шпионы среди организации, случайные утечки и.т.д.

2. Технический раздел

2.1 Описание бизнес-процесса

Участниками процесса являются сотрудники банка в том числе: отдел по безопасности, hr-менеджеры, сотрудники банка, программисты, руководители, бухгалтера, аудиторы, аналитики, операционисты и. т. д.

Используемые системы для функционирования системы банка: учетная система, CRM, электронная почта, таблицы Excel, БД, сервера, межсетевые экраны, технологии DLP, системы контроля доступа, OpenVPN, антивирусные ПО, стандарты и. т. д.

Описание собранной информации в графическом виде (IDEF3) представлена на рисунке 2.1.

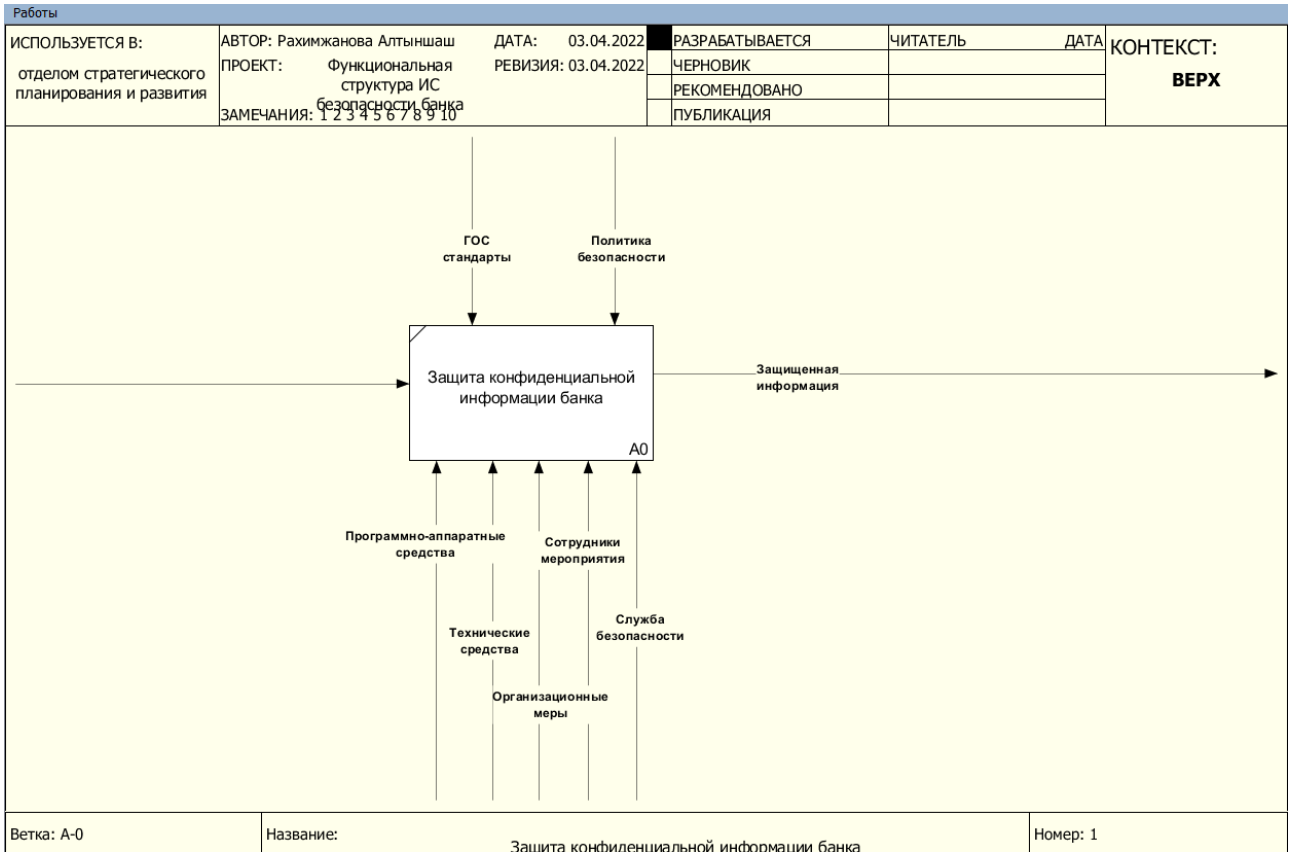


Рисунок 2.1 – Функциональная структура ИС безопасности банка

2.2 Перечень активов для защиты

К информации конфиденциального характера можно отнести : банковская тайна, информация об активах банка, персональные данные клиентов и

работников, информация, защищаемая в соответствии с законодательством о национальной платежной системе, рабочие места администраторов и разработчиков, инсайдерская информация, БД с данными для авторизации, информация, входящая в состав кредитной истории, конфиденциальная корреспонденция, номера счетов, иная информация, доступ к которой ограничен в соответствии с законодательством, в том числе нормативными актами Банка [16].

К информации второстепенного характера можно отнести: данные о платежах, история кредитов, информация о страховках, штрафах, расписания сотрудников, история покупок и.т.д.

2.3 Модель угроз

Проектирование модели угроз позволяет описать угрозы в системе организации. В первую очередь определяются критичные активы банка, анализируются уязвимости в системе, описываются виды угроз. Далее применяются методы защиты информации по определенным угрозам. Модель угроз приведена на рисунке 2.3.

Рисунок 2.3 – Модель угроз ИС безопасности банка

2.4 Описание средств защиты от внешних угроз

– Межсетевой экран – ограничивает сегменты друг от друга, фильтрует информационные потоки. Firewall – ПО для КС от черных хакеров и прочих атак.

– IPS (СОВ, СПВ) – система предотвращения вторжения. Желательно также помещать внутри периметра сети для предотвращения утечки данных.

– Анивирусная защита. Необходимо обеспечить анивирусом не только в ПК, но и в серверах, почтовых серверах(антиспам и.т.д).

– Защита от APT (advanced persistent threat) – защита организации от различных вирусов, троянских программ, червя и других угроз. Среда SandBox – изолирует ПК, систему от вредоносных программ. Нужно тестировать систему в данной среде. SandBox блокирует доступ к вредоносному файлу, программе и.т.д. На SandBox запускают подозрительные или зараженные файлы.

– Система безопасности веб-сайтов WAF (Web App Firewall). Защита сайта организации от несанкционированного доступа, хакерских атак.

– Система мониторинга и контроля функционирования всех средств защиты информационной системы. Необходим SOC (Security Operations Center) – центр реагирования на изменения, неполадки, отвечающие на вопросы по безопасности (безопасники, аналитики).

2.5 Описание средств защиты от внутренних нарушений

– Использование технологий DLP (Data Loss Prevention), которые не позволяют утечке конфиденциальной информации, контролирует информационные потоки. К примеру, предотвращает сотруднику отправлять информацию на другие каналы, потоки.

– Необходима организация удаленного доступа. Необходимо при работе онлайн, дистанционно, для контроля CRM систем. Ниже приведены необходимые меры и программы для защиты конфиденциальной информации.

– Использование программ защиты трафика от перехвата, такие как VPN Client, Open VPN GUI (Для защиты БД) – обеспечивают защищенное соединение между сотрудниками на удаленке и организацией. Необходимо проходить аутентификацию при каждом подключении к сети организации.

– Использвание приложения Authenticator, для 2-х факторной аутентификации. На телефон приходят сгенерированные пин-коды, одноразовые СМС сообщения.

– Авторизация ПК, для сотрудников имеющих доступ к внутренним ресурсам. Подключить проверку через шлюз при подключении в сеть организации. Соблюдать настройки безопасности подключения: проверка подключения межсетевого экрана, обновление антивирусов, контроль использование программ (доступ/запрет).

– Регистрировать события безопасности. Собирать информацию для анализа утечек, возникновения ошибок, неполадок, атак.

– Контроль доступа привилегированных пользователей при помощи технологий Privileged User Management (PUM).

2.6 Проектирование модели КС банка

Компьютерная сеть (КС) – система организации работы с ПК и логическая связь с другими устройствами. Проектирование КС необходима для всех организаций и является обязательной процедурой. Правильное проектирование КС для организаций может защитить данные от утечки, кражи и прочих несанкционированных действий. Модели OSI описывают работу сетевых устройств. Процесс передачи данных происходит на 7 уровнях (физический, канальный, сетевой, транспортный, сеансовый, представления, приложений) [17].

На рисунке 2.6 изображена модель КС банка. Филиал и головной офис банка находятся в разных городах. В головном офисе ПК разных пользователей (директор, программист) имеют разные VLAN, который необходим для обеспечения безопасности данных. К примеру, пользователь ПК “Сотрудник банка”, не имеет доступа к серверу SQL. ПК компьютеры связанны между собой коммутаторами, которые позволяют разбить сеть на сегменты при помощи VLAN – которые шифруют трафик, позволяют управлять доступом данных, защищать данные от утечки, кражи и взлома.

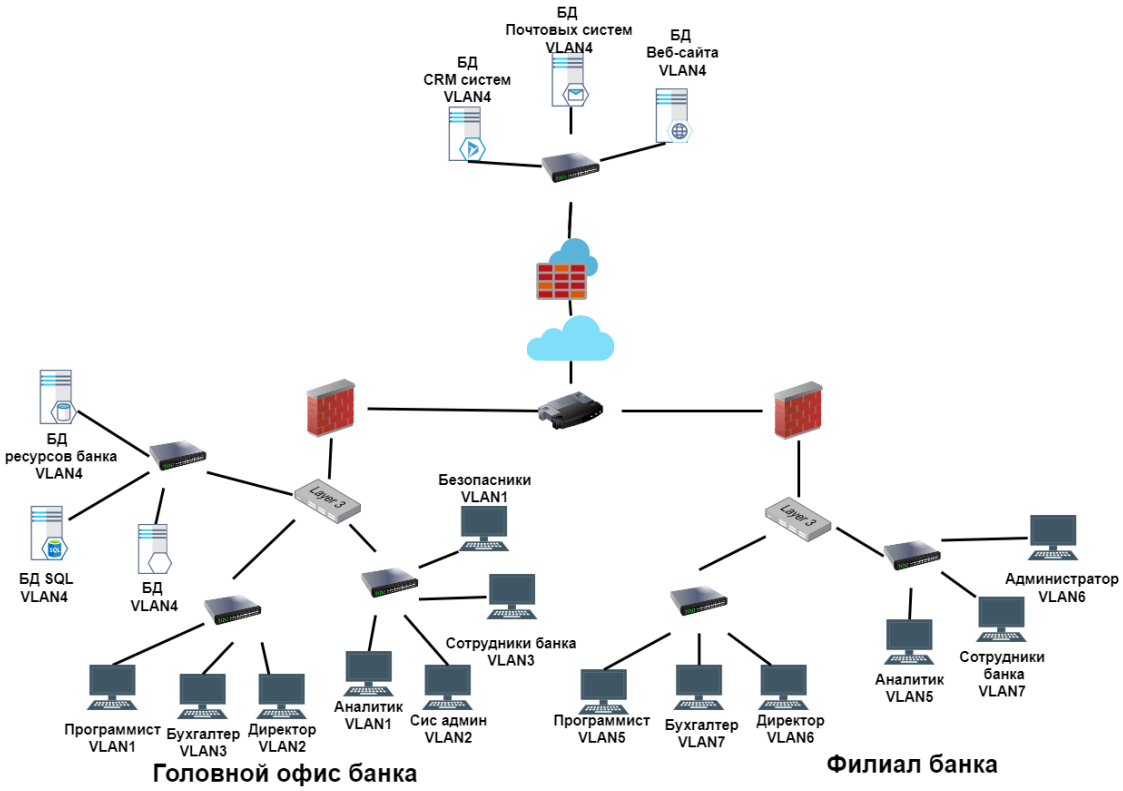


Рисунок 2.6 – Модель КС банка

Коммутаторы типа L2 (канальный уровень) могут быть связаны только при помощи L3 устройств (L3 коммутатор, маршрутизатор). Сервера также

необходимо подключать к коммутаторам, так как коммутаторы (switch) отправляют пакет только в определенный порт (назначенный) за счет использования таблицы MAC-адресов. Эти меры предотвращают утечку данных. Все устройства также необходимо подключать к брандмауэрам (Firewall) при выходе к интернету, так как данные необходимо защитить от хакеров и других внешних угроз. БД облачных хранений также необходимо защищать при помощи брандмауэра. При построении топологии КС организации рекомендуется использование вида “Снежинка” (дерево), так как данная топология самая распространенная (в локальных, глобальных сетях) и эффективная.

3 Экспериментальный раздел

3.1 Проектирование формы авторизации в банковской системе

Защита БД с данными пользователя является одним из ключевых мероприятий, которые нужно проектировать в первую очередь. Все банки имеют IOS, Android приложения, так как ими удобно пользоваться и осуществлять платежи, переводы и прочие действия. Для защиты активов банка и клиентов необходимо защищать сервер с данными при помощи VPN, межсетевых экранов. Но есть и другие способы защиты информации в БД. На рисунке 3.1.1, приведена UML диаграмма для формы авторизации.

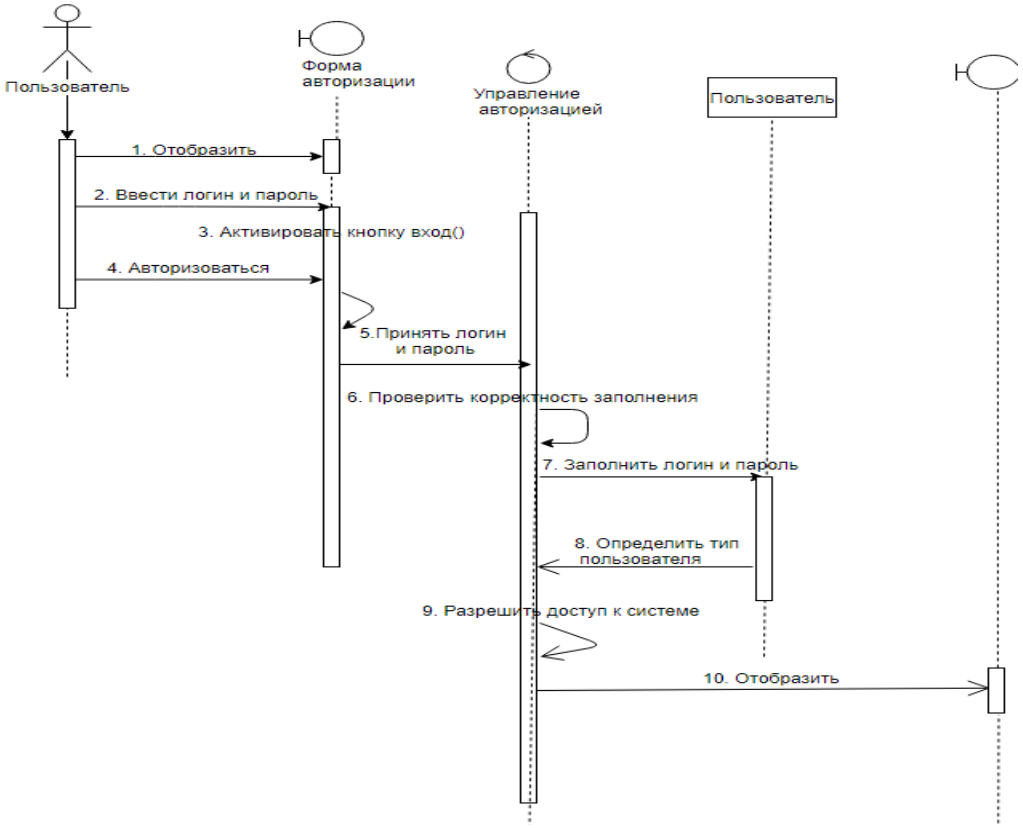


Рисунок 3.1.1 – UML диаграмма формы авторизации

На рисунке 3.1.2 и рисунке 3.1.3 изображены интерфейс формы авторизации и регистрации.

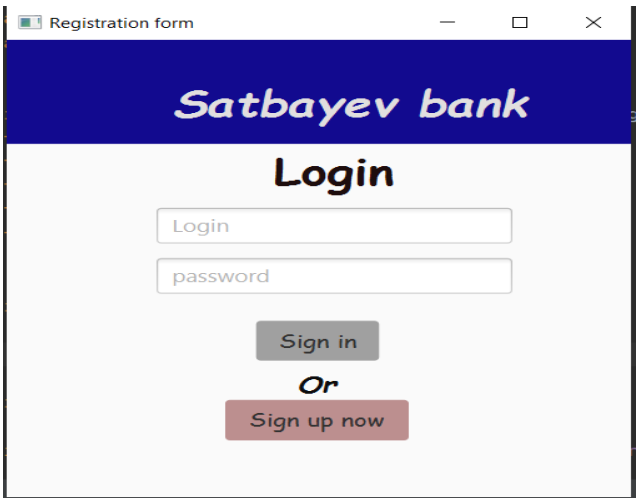


Рисунок 3.1.2 – Интерфейс формы авторизации

Рисунок 3.1.3 – Интерфейс формы регистрации

Этапы проектирования формы авторизации:

1) Интерфейс формы авторизации можно проектировать на таких языках как: Html, CSS, PHP и.т.д. Альтернативой этим языкам можно назвать программу “SceneBuilder” – Шаблон проектирования, где можно создавать формы и приложения. В SceneBuilder можно переносить компоненты (Button, Date Picker) на окно редакции.

2) Соединение Java с MySQL. Форма авторизации была спроектирована в среде IntelijIdea (JavaFX). БД – в среде MySQL. Для начала проектируется схема «test» - в которой будут храниться все данные зарегистрированных клиентов. На языке Java была спроектирован класс Config, который хранит в себе параметры MySQL, такие как хост сервера, название сервера и.т.п, для соединения MySQL с JavaFX.

3) Импортируем библиотеки для SQL, изображенные на рисунке 3.1.4, также через класс BD, соединяем установленные драйвера, изображенные на

рисунке 3.1.5.

```
import  java.sql.Connection;
import  java.sql.DriverManager;
import java.sql.PreparedStatement;
import  java.sql.SQLException;
import java.sql.ResultSet;
```

Рисунок 3.1.4 – Библиотеки для MySQL

```
public class BD extends Configi {
    Connection dbConnection;
    public  Connection  getDbConnection() throws ClassNotFoundException, SQLException{
        String connectionString = "jdbc:mysql://" + dbHost + ":" + dbPort + "/" + dbName +
                "?verifyServerCertificate=false"+
                "&useSSL=false"+
                "&requireSSL=false"+
                "&useLegacyDatetimeCode=false"+
                "&amp"+
                "&serverTimezone=UTC";
        Class.forName("com.mysql.cj.jdbc.Driver");
        dbConnection = DriverManager.getConnection(connectionString,dbUser,dbPass);
        return  dbConnection;
    }
```

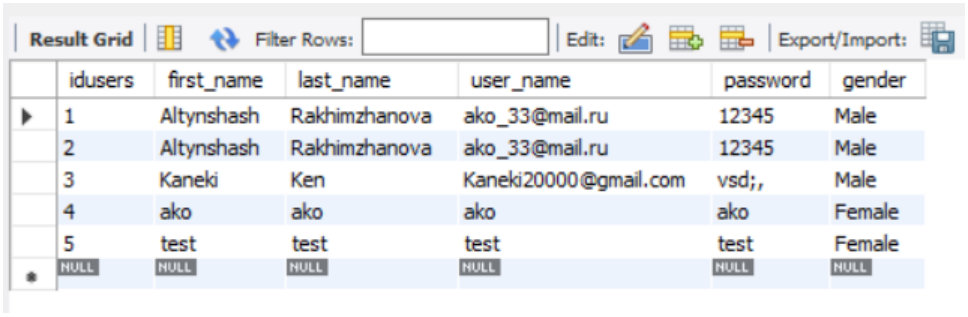
Рисунок 3.1.5 – Класс BD

4) Создание таблицы и столбцов в MySQL. Запросы на языке SQL изображены на рисунке 3.2.6. На рисунке 3.1.6.1 отображено хранение данных в открытом виде. Это небезопасно, необходимо хранить пароли в хешированном виде.

Query 1 | test* | test - Table

```
1  CREATE TABLE `test`.`users` (
2    `idusers` INT NOT NULL,
3    `first_name` VARCHAR(45) NOT NULL,
4    `last_name` VARCHAR(45) NOT NULL,
5    `user_name` VARCHAR(45) NOT NULL,
6    `password` VARCHAR(45) NOT NULL,
7    `gender` VARCHAR(45) NOT NULL,
8    PRIMARY KEY (`idusers`));
```

Рисунок 3.2.6 – Запрос в MySQL для создания столбцов



idusers	first_name	last_name	user_name	password	gender
1	Altynshash	Rakhimzhanova	ako_33@mail.ru	12345	Male
2	Altynshash	Rakhimzhanova	ako_33@mail.ru	12345	Male
3	Kaneki	Ken	Kaneki20000@gmail.com	vsd;,	Male
4	ako	ako	ako	ako	Female
5	test	test	test	test	Female
NULL	NULL	NULL	NULL	NULL	NULL

Рисунок 3.2.6.1 – MySQL хранение паролей в открытом виде

5) Хеширование пароля при помощи встроенной библиотеки java.security. На рисунке 3.1.7 изображено хранение паролей в БД в хешированном виде.

```
private void signUpNewUser() {
    BD dbHandler = new BD();
    sha1pass = DigestUtils.shaHex(String.valueOf(password_field));
    String first_name = SignUpFname.getText();
    String last_name = SignUpLname.getText();
    String user_name = login_field.getText();
    byte[] password = sha1pass.getBytes();
    User user = new User(first_name,last_name,user_name,password,gender);
    dbHandler.signUpUser(user);
}
```

37	Толкын	Муратовна	Tolkyn964@g…	19c10e6ecf62c3488ca1db729759963b	Male
38	Джексон	Алан	Alanjackson@…	9e688c58a5487b8eaf69c9e1005ad0bf	Male
39	Диана	Аскарова	Diaaan08@mai…	8666683506aacd900bbd5a74ac4edf68	Female
41	Michael	Jackson	MichaelJackso…	5baa61e4c9b93f3f0682250b6cf8331b	Male

Рисунок 3.1.7 – MySQL хранение паролей в хешированном виде

Итоги: Сервера с БД лучше всего защищать при помощи технологий и ПО (VPN, Firewall). При незащищенном сервере SQL, небезопасно хранить пароли в открытом виде. При построении защиты баз данных необходимо учитывать угрозы для конфиденциальной безопасности информации.

При соединении по сети аутентификацию должны пройти оба соединяющихся объекта. После установления соединения необходимо выполнить требование защиты при обмене сообщениями [18]:

– получатель должен быть уверен в подлинности источника данных;

– получатель должен быть уверен в подлинности передаваемых данных;
– отправитель должен быть уверен в доставке данных получателю;
– отправитель должен быть уверен в подлинности доставленных данных.

Одним из мер защиты БД, является операторы SQL предоставления и отмены привилегий, которые разрешают или запрещают определенным пользователям изменения в БД. Данные меры необходимы для защиты БД от внутренних утечек. К примеру, можно запретить аналитикам банка изменение таблицы с ресурсами банка, так как они проводят анализ по полученным данным. В языке SQL имеется два оператора GRANT и REVOKE для предоставления и отмены привилегий [19]. Пример реализации предоставления и отмены привилегий изображены на рисунке 3.1.8.

```
5 •   GRANT ALL ON contacts TO 'ako'@'localhost';
6 •   REVOKE DELETE, UPDATE ON contacts FROM 'ako'@'localhost';
7
```

Рисунок 3.1.8 – Операторы предоставления и отмены доступа

6) После регистрации и успешной авторизации, открывается окно интерфейса приложения. Интерфейс приложения приведен на рисунке 3.1.9.

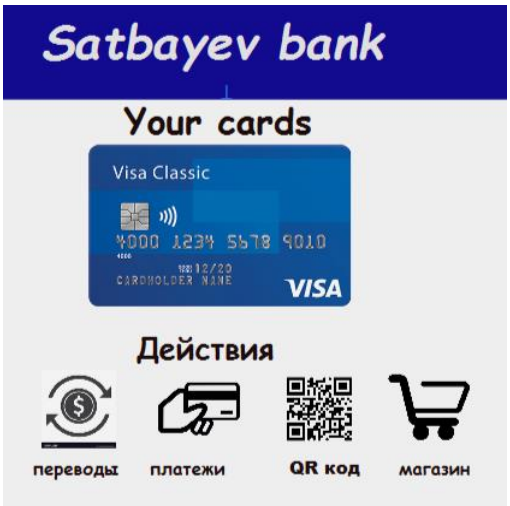


Рисунок 3.1.9 – Интерфейс приложения

ЗАКЛЮЧЕНИЕ

Результатом дипломной работы является проектирование системы защиты конфиденциальной информации в банковских системах. Информационная система, реализована в виде КС банка, формы авторизации. Перед тем, как проектировать систему безопасности, необходимо составить ТЗ, описать и изучить все угрозы, сравнить технологии и методы. При построении модели КС банка, необходимы знания о сетевых угрозах о методах защиты информации. Анализ угроз также необходим в отрасли банка, проанализировав возможные угрозы, можно предотвратить утечку данных и прочие угрозы.

В процессе проектирования авторизации на примере была показана работа MySQL, как хранятся пароли и другие конфиденциальные данные клиентов. Чтобы данные не подверглись хакерской атаке, необходимо защищать сервера. Пароли опасно хранить в открытом виде, их необходимо хешировать или защищать другими способами. Предоставив или отменив привилегии, можно защитить данные от внутренних угроз, утечек информации.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1 Информационная безопасность: Учебник для студентов вузов. — М.: Академический Проект; Гаудеамус, 2-е изд.—s2004. — 544 с.

2 Угрозы информационной безопасности [Электронный ресурс] – Режим доступа: https://searchinform.ru/informatsionnaya-bezopasnost/osnovy-ib/ugrozy-informatsionnoj-bezopasnosti/, свободный.

3 Информационная безопасность и защита информации: учебник / О.В. Прохорова. – Самара: СГАСУ, 2014. – 114 с.

4 Информационная безопасность: Учебное пособие. Авторы: Ясенев В.Н., Дорожкин А.В., Сочков А.Л., Ясенев О.В. Под общей редакцией проф. Ясенева В.Н. – Нижний Новгород: Нижегородский госуниверситет им. Н.И. Лобачевского, 2017. – 198 с.

5 Аникин, И.В. Методы и средства защиты компьютерной информации: [учеб. пособие для студ.] / И.В. Аникин, В.И. Глова. – Казань: Изд. КГТУ им. А.Н. Туполева, 2005.

6 Защита информации в банковских системах: учеб. пособие для бакалавриата и магистратуры / А. А. Внуков. — 2-е изд., испр. и доп. — М.: Издательство Юрайт, 2017. — 246 с. — Серия: Бакалавр и магистр. Академический курс.

7 Дамир Серикпаев. Как банки защищают данные казахстанцев [Электронный ресурс] – Режим доступа: https://forbes.kz/process/internet/kak_banki_zaschischayut_dannyie_kazahstantsev/, свободный.

8 Методы организации защиты информации: учебное пособие для студентов 3–4 курсов всех форм обучения направлений подготовки 230400.55, 230701.51, 090300.65, 220100.55 / Ю. Ю. Громов и др. – Тамбов: Изд-во ФГБОУ ВПО «ТГТУ», 2013. – 80 с. – 100 экз. – ISBN 978-5-8265-1235-7.

9 Кристина Жукова. Утечка данных и риск отзыва лицензии: банки назвали главные угрозы от кибератак [Электронный ресурс] – Режим доступа: https://www.forbes.ru/tehnologii/428155-utechka-dannyh-i-risk-otzyva-licenzii-banki-nazvali-glavnye-ugrozy-kiberatak, свободный.

10 ЦАРКА: Ни один банк в Казахстане не продемонстрировал максимальный уровень защищённости своих веб-ресурсов [Электронный ресурс] – Режим доступа: https://informburo.kz/novosti/ni-odin-bank-v-kazahstane-ne-prodemonstriroval-maksimalnyj-uroven-zashishyonnosti-svoih-veb-resursov, свободный.

11 Есть ли у вашей организации файл Security.txt? [Электронный ресурс] – Режим доступа: https://krebsonsecurity.ru/2021/09/20/does-your-organization-have-a-security-txt-file/, свободный.

12 Информационная безопасность открытых систем [Электронный ресурс]: учебник / Д.а. Мельников. — 2-е изд., стер. — М. : ФлИнта, 2014. — 448 с.

13 Защита информации в компьютерных системах / под ред. д-ра экон. наук Е.В. Стельмашонок, канд. физ.-мат. наук И.Н. Васильевой. – СПб. : Изд-во СПбГЭУ, 2017. – 163 с.

14 Программно-аппаратные средства обеспечения информационной безопасности: Учебное пособие. – М.: Машиностроение-1, 2001.− 126 с.

15 Модели безопасности компьютерных систем. Управление доступом и информационными потоками. Учебное пособие для вузов. − 2-е изд., испр. и доп. – М.: Горячая линия–Телеком, 2013. – 338 с.

16 Обеспечение информационной безопасности организаций банковской системы [Электронный ресурс] – Режим доступа: https://cbr.ru/Crosscut/LawActs/File/445, свободный.

17 Сетевая модель OSI [Электронный ресурс] – Режим доступа: https://ru.wikipedia.org/wiki/%D0%A1%D0%B5%D1%82%D0%B5%D0%B2%D0%B0%D1%8F_%D0%BC%D0%BE%D0%B4%D0%B5%D0%BB%D1%8C_OSI, свободный.

18 Хамидуллин Р.Р., Бригаднов И.А., Морозов А.В. Методы и средства защиты компьютерной информации: Учеб. Пособие. – СПб.: СЗТУ, 2005. – 178 с.

19 Защита информации в базах данных и экспертных системах: пособие для студентов фак. радиофизики и комп. технологий / В. В. Скакун. – Минск: БГУ, 2015. – 140 с.

Приложение А

Листинг программы

/*программа реализована с нескольких классов и единый код разделяется ими*/

```
//код класса BD (Базы Данных)
package sample;
import  java.sql.Connection;
import  java.sql.DriverManager;
import java.sql.PreparedStatement;
import  java.sql.SQLException;
import java.sql.ResultSet;

public class BD extends Configi {
   Connection dbConnection;
   public  Connection  getDbConnection() throws ClassNotFoundException,
SQLException{
       String connectionString = "jdbc:mysql://" + dbHost + ":" + dbPort + "/" +
dbName +
               "?verifyServerCertificate=false"+
               "&useSSL=false"+
               "&requireSSL=false"+
               "&useLegacyDatetimeCode=false"+
               "&amp"+
               "&serverTimezone=UTC";
       Class.forName("com.mysql.cj.jdbc.Driver");
       dbConnection =
DriverManager.getConnection(connectionString,dbUser,dbPass);
       return  dbConnection;
   }

   public  void signUpUser(User user){
       String insert = "INSERT INTO " + Peremennyie.USER_TABLE + "(" +
Peremennyie.USERS_FIRSTNAME + "," + Peremennyie.USERS_LASTNAME
+
               "," + Peremennyie.USERS_USERNAME + "," +
Peremennyie.USERS_PASSWORD + "," + Peremennyie.USERS_GENDER +
")" +
         "VALUES(?,?,?,?,?)";
       try {
          PreparedStatement prst = getDbConnection().prepareStatement (insert);
```

```
            prst.setString(1,user.getFirst_name());
            prst.setString(2,user.getLast_name());
            prst.setString(3,user.getUser_name());
            prst.setString(4,user.getPassword());
            prst.setString(5,user.getGender());
            prst.executeUpdate();
        } catch (SQLException e) {
            e.printStackTrace();
        } catch (ClassNotFoundException e) {
            e.printStackTrace();
        }
    }

    public ResultSet getUser(User user)
    {

        ResultSet resSet = null;
        String select = "select * from users where user_name =? AND password
=?";

        try {
            PreparedStatement prst = getDbConnection().prepareStatement(select);
            prst.setString(1,user.getUser_name());
            prst.setString(2,user.getPassword());

            resSet = prst.executeQuery();
        } catch (SQLException e) {
            e.printStackTrace();
        } catch (ClassNotFoundException e) {
            e.printStackTrace();
        }

        return resSet;
    }
}

/*ПРОГРАММА КЛАССА MAIN*/
//код класса Main:
package sample;
import javafx.application.Application;
import javafx.fxml.FXMLLoader;
```

```
import javafx.scene.Parent;
import javafx.scene.Scene;
import javafx.stage.Stage;

public class Main extends Application {

    @Override
    public void start(Stage primaryStage) throws Exception{
        Parent root = FXMLLoader.load(getClass().getResource("Okno
privetstviya.fxml"));
        primaryStage.setTitle("Registration form");
        primaryStage.setScene(new Scene(root, 400, 400));
        primaryStage.show();
    }

    public static void main(String[] args) {
        launch(args);
    }
}
```