Министерство науки и высшего образования Российской Федерации
федеральное государственное автономное образовательное учреждение
высшего образования «Национальный исследовательский университет
ИТМО»

Факультет инфокоммуникационных технологий

Основы кибербезопасности

Практическая работа №6

Выполнил:

студент группы К34211

Фисенко Максим Вячеславович

Проверил:

преподаватель практики, КТН

Назаров Михаил Сергеевич

Санкт-Петербург

2024

Содержание

Введение

Цель работы

Изучить типовой алгоритм проектирования системы защиты информации в информационных системах. Приобрести практические навыки в классификации автоматизированных систем. Научиться подбирать средства защиты информации для защищаемых систем.

В данной работе необходимо было спроектировать систему защиты информации информационной систем, а также подобрать средства защиты информации для нее. В качестве такой информационной системы была выбрана *система интернет-банкинга*. Интернет-банкинг работает с конфиденциальными данными пользователей, которые могут оказаться под угрозой, а также включает в себя данные, представляющие коммерческую тайну, и информацию, доступную только сотрудникам.

Содержание отчета

Описание системы

В первую очередь необходимо определить, из чего будет состоять информационная система. В данную информационную систему входят следующие компоненты:

- **Серверная часть**. Включает в себя сервера баз данных, веб-сервера, сервера обработки платежей, сервера авторизации;
- **Рабочие станции сотрудников**. Включает в себя рабочие станции для операторов службы поддержки, системных администраторов и разработчиков;
- **Клиентская часть**. Включает в себя как веб-интерфейс, так и мобильные приложения для доступа пользователей;

Таким образом, можно сказать, что система состоит из нескольких частей, при этом как одну из частей стоит рассматривать и рабочие станции пользователей банка. В дополнение можно отметить, что данная информационная система обеспечивает доступ клиентов к своим финансовым данным и сервисам банка через *HTTPS*-запросы, так как безопасность и шифрование данных крайне важны при передачи чувствительных данных, которых в данной системе будет много в силу ее области. Также можно отметить, что разработчики и системные администраторы могут подключаться к серверной части через защищенный протокол *VPN*.

Очень важной частью полноценного функционирования интернет-банкинга является интеграция с внешними системами. Для работы интернет-банкинга требуется интеграция с такими системами, включая системы процессинга платежей, онлайн-эквайринга и межбанковских переводов.

Далее необходимо сказать о том, что будет храниться в базе данных. Основная информация, которая будет храниться в базе данных системы интернет-банкинга, это:

- Данные клиентов (персональная информация, история операций, остатки на счетах);

- Информация о кредитах и депозитах;
- Внутренние данные банка (отчеты, финансовая статистика).

В системе будет несколько ролей:

- **Пользователи (клиенты банка)**. Данные пользователи должны иметь доступ к своим счетам, платежам и другим сервисам через веб-интерфейс или мобильное приложение;
- **Сотрудники банка:**

1. Операторы службы поддержки. Данные пользователи помогают с решением проблем у клиентов банка;
2. Системные администраторы. Обслуживают серверную часть системы;
3. Разработчики. Создают и обновляют программное обеспечение системы.

Основные функциональные требования к системе таковы:

- Обеспечение доступа клиентов к их счетам 24/7 через веб-интерфейс и мобильное приложение;
- Возможность совершать переводы, оплачивать услуги, оформлять кредиты;
- Защита персональных данных клиентов от утечек;
- Доступ сотрудников к внутренним данным в соответствии с их ролями;
- Интеграция с внешними платежными системами.

В данной системе, как и во всех других, данные должны быть защищены. Ниже приведен список требований к защите информации в системе интернет-банкинга:

- Конфиденциальность

1. Шифрование персональных данных клиентов и информации о транзакциях;
2. Ограничение доступа сотрудников к данным по принципу минимальных привилегий.

- Целостность

1. Обеспечение защиты данных от несанкционированного изменения;
2. Логирование всех операций для их последующего анализа.

- Доступность:

1. Гарантия работы сервиса 24/7;
2. Защита от *DDoS*-атак;
3. Организация резервного копирования данных.

Архитектура информационной системы должна включать в себя такие компоненты, как:

- **Аутентификация и авторизация**: использование двухфакторной аутентификации (*2FA*), разделение прав доступа по ролям;
- **Защита каналов связи**: шифрование *HTTPS* и использование *VPN* для сотрудников;
- **Защита серверов**: использование веб-аппликационных экранов (*WAF*), ограничение доступа через файрвол, регулярное обновление ПО;
- **Защита базы данных**: шифрование данных на уровне хранения, логирование доступа к базе.

Локальная сеть организации состоит из серверной части и рабочих станций сотрудников. Серверы подключены к изолированной сети, доступ к которой возможен только через *VPN*. Рабочие станции сотрудников имеют ограниченный доступ к интернету для предотвращения утечек информации.

Программно-технические средства ИБ будут следующими:

- Брандмауэр;
- Антивирусное ПО;
- Системы обнаружения вторжений (*IDS/IPS*);
- Системы резервного копирования;
- Программное обеспечение для управления правами доступа (*IAM*).

Циркулирующая в системе информация будет следующей:

- **Персональные данные клиентов**: ФИО, адрес, номер телефона, email, паспортные данные;
- **Финансовые данные**: остатки на счетах, история операций, данные о кредитах и депозитах;
- **Технические данные**: логи операций, данные мониторинга системы.

Информационная система будет состоять из следующих сегментов:

- **Серверная часть**: сервер баз данных (например, *PostgreSQL*), веб-сервер (например, *nginx*), сервер авторизации, сервер обработки платежей, тестовый сервер, сервер резервного копирования;
- **Рабочие станции сотрудников**: операторы службы поддержки, системные администраторы, разработчики;
- **Внешние пользователи**: доступ через веб и мобильные приложения.

Ниже описаны основные функции физической безопасности:

- Серверное оборудование размещено в дата-центре с ограниченным доступом;
- Доступ сотрудников в офис осуществляется через систему пропусков;
- Рабочие станции сотрудников защищены паролями, экранами конфиденциальности.

Перечень ОТСС (объектов технических средств и систем):

- Серверы баз данных (*PostgreSQL*);
- Веб-сервер (*Nginx*);
- Серверы обработки платежей;
- Рабочие станции сотрудников;
- Каналы связи (*HTTPS, VPN*).

Перечень ВТСС (вспомогательных технических средств и систем):

- Резервные серверы;

- Системы мониторинга и логирования;
- Системы резервного копирования;
- Сетевое оборудование (маршрутизаторы, коммутаторы).

На основе описания информационной системы, представленного выше, была составлена диаграмма графического представления системы, представленная ниже на рисунке 1.

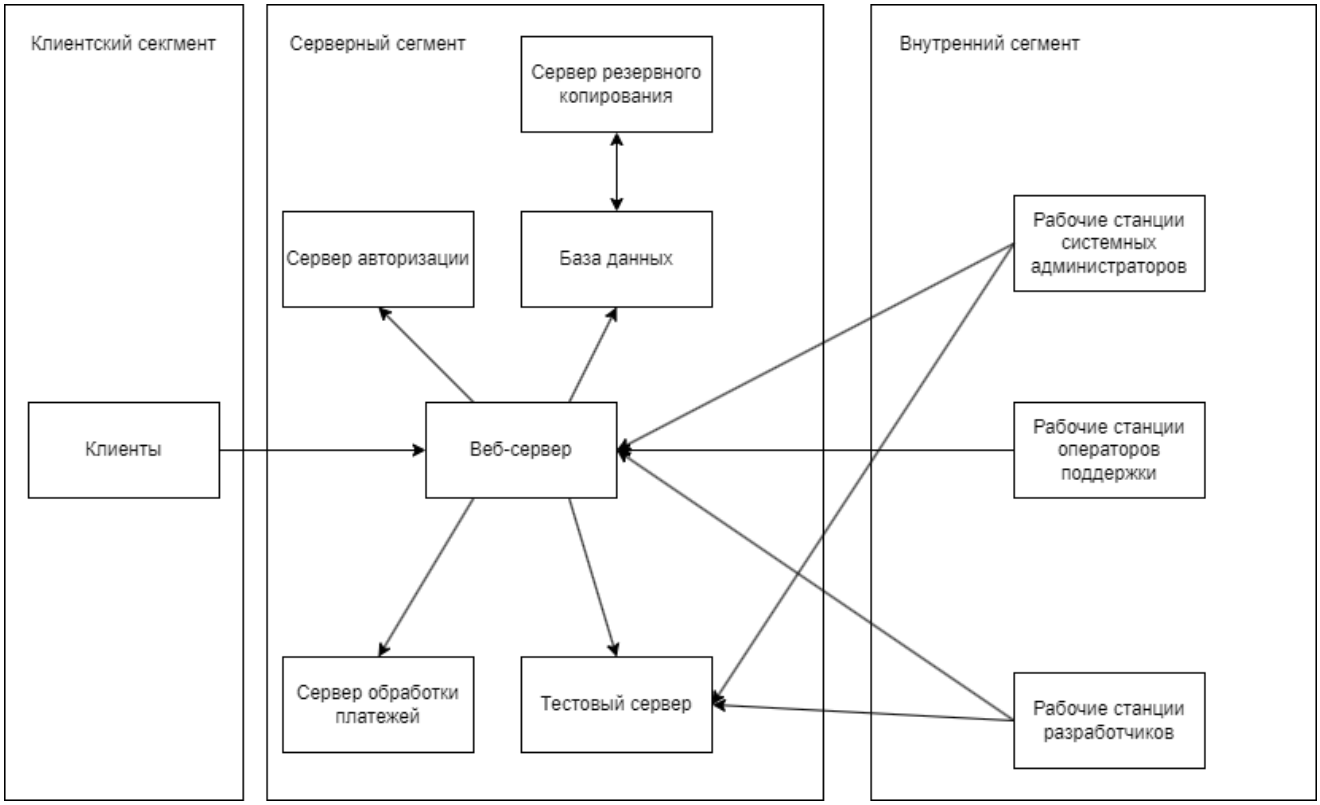

Рисунок 1 - Графическое представление системы

Класс защищаемой системы

В данной системе есть два подконтрольных сегмента – это внутренний и серверный сегменты.

На рабочих станциях обрабатываются персональные данные, коммерческая информация (например, сведения о транзакциях), а также данные внутренней инфраструктуры. Это относится к категории конфиденциальной информации. Доступ имеют сотрудники банка (операторы, менеджеры) и системные администраторы. Обычно число пользователей составляет менее 1000 человек. На рабочих станциях внедрены механизмы разграничения прав: операторы имеют минимальные привилегии (например, доступ к части

банковских операций), а системные администраторы управляют настройкой инфраструктуры. С учетом объема обрабатываемой информации, количества пользователей и разграничения прав доступа, сегмент рабочих станций соответствует классу 2Б.

В серверном сегменте хранится критически важная информация: персональные данные клиентов, финансовые операции, логи авторизации, а также резервные копии базы данных. Эта информация относится к категории особо важной конфиденциальной информации. Число пользователей сегмента минимально — только системные администраторы. Сегмент использует строгие политики доступа (*VPN*, разграничение доступа по ролям). Можно сделать вывод, что серверный сегмент соответствует классу 1Г.

Таблица 1 – Требования к сегментам по классам

№	**Подсистема и требование**	**Класс 1Г**	**Класс 2Б**
1	Подсистема управления доступом		
1.1	Идентификация, проверка подлинности и контроль доступа субъектов:		
	- в систему	+	+
	- к терминалам, ЭВМ, узлам сети ЭВМ	+	-
	- к программам	+	-
	- к томам, каталогам, файлам, записям, полям записей	+	-
1.2	Управление потоками информации	-	-
2	Подсистема регистрации и учета		
2.1	Регистрация и учет:		
	- входа (выхода) субъектов доступа в (из) систему (узел сети)	+	+
	- выдачи выходных документов	+	-
	- запуска (завершения) программ и процессов	+	-
	- доступа программ к защищенным файлам	+	-
	- доступа программ к терминалам, ЭВМ, узлам сети ЭВМ	+	-
	- изменения полномочий субъектов доступа	-	-
	- создаваемых защищаемых объектов доступа	-	-
2.2	Учет носителей информации	+	+
2.3	Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей	+-	-
2.4	Сигнализация попыток нарушения защиты		-
3	Криптографическая подсистема		
3.1	Шифрование конфиденциальной информации	-	-

3.2	Шифрование информации, принадлежащей различным субъектам доступа (группам субъектов) на разных ключах	-	-
3.3	Использование аттестованных криптографических средств	-	-
4	Подсистема обеспечения целостности		
4.1	Обеспечение целостности программных средств и обрабатываемой информации	+	+
4.2	Физическая охрана средств вычислительной техники и носителей информации	+	+
4.3	Наличие администратора (службы) защиты информации в АС	-	-
4.4	Периодическое тестирование СЗИ НСД	+	+
4.5	Наличие средств восстановления СЗИ НСД	+	+
4.6	Использование сертифицированных средств защиты	-	-

Системы защиты информации

Внутренний сегмент:

- *Astra Linux* на рабочих станциях сотрудников и системных администраторов: использование сертифицированной ОС, соответствующей требованиям российского законодательства в области информационной безопасности, обеспечивающей защиту рабочих станций сотрудников;
- Антивирусное ПО с сертификатом ФСТЭК: установлено на рабочих станциях сотрудников, администраторов и разработчиков для защиты от вредоносных программ и предотвращения утечек данных;
- Доступ к ресурсам через *VPN*: для безопасного подключения сотрудников и системных администраторов к серверам организации, защищая передаваемые данные от несанкционированного перехвата;
- Тестовый сервер: используется для проверки новых версий приложений в изолированной и безопасной среде, что позволяет избежать рисков компрометации боевой системы.

Серверный сегмент:

- Серверная версия *Astra Linux*: установлена на всех серверах (веб-сервер, сервер авторизации, сервер обработки платежей, база данных,

резервный сервер). Соответствует требованиям российского законодательства по защите серверных данных;

- *WAF (Web Application Firewall)*: обеспечивает защиту веб-сервера и сервера авторизации от попыток сетевых атак, включая *SQL*-инъекции и *XSS*-атаки;
- Протоколы *HTTPS* и *TLS*: обеспечивают шифрование данных, передаваемых между клиентским сегментом, веб-сервером и другими серверами системы, исключая возможность их перехвата;
- Система мониторинга и логирования: позволяет оперативно выявлять сетевые аномалии, фиксировать подозрительные события и анализировать их, чтобы минимизировать риски утечки данных.

Клиентский сегмент

- Многофакторная аутентификация (*2FA*): обеспечивает безопасность доступа клиентов к интернет-банкингу, требуя дополнительное подтверждение (например, одноразовый код по *SMS*);
- Мобильные приложения с встроенной защитой: использование защищённых мобильных приложений с обязательной проверкой цифровых сертификатов серверов;
- Шифрование данных на устройствах клиентов: шифрование пользовательских данных в мобильных и веб-приложениях интернет-банкинга для предотвращения их утечки в случае компрометации устройства.

Вывод по работе

В ходе выполнения практической работы была спроектирована система защиты информации информационной системы интернет-банкинга. Итоговый вид данной системы представлен ниже на рисунке 2.

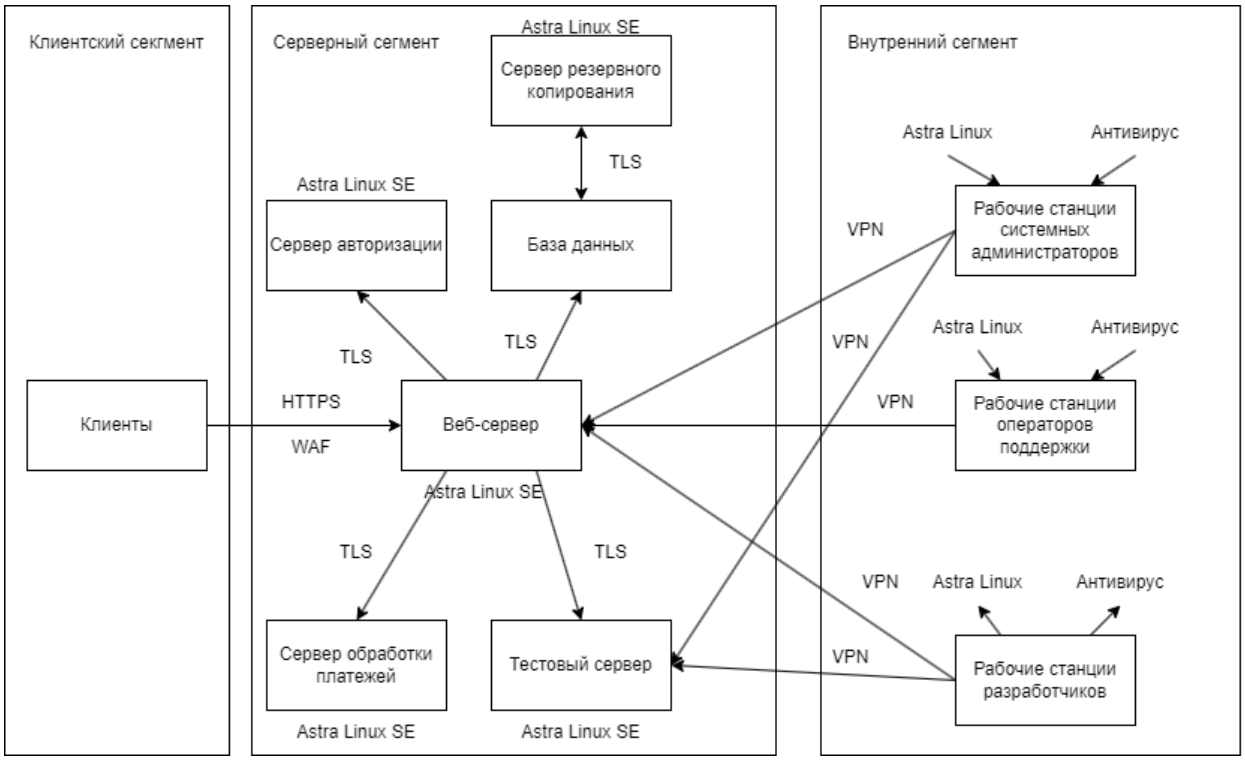

Рисунок 2 - Итоговый вид системы