Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение

высшего образования

«Сибирский государственный автомобильно-дорожный университет (СибАДИ)»

Институт Информационные системы, экономика и управление

Кафедра Информационная безопасность

Направление Информационная безопасность

Профиль Безопасность автоматизированных системы

**ПОЯСНИТЕЛЬНАЯ ЗАПИСКА**

**к курсовому проекту**

по дисциплине: «Технология построения защищенных автоматизированных систем»

Тема работы «Проектирование системы защита автоматизированной системы выдачи потребительских кредитов»

Выполнил:

студент группы БИб-21Э1 Чигарев Александр Юрьевич

Курсовой проект сдан на проверку:

«\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_2024 г.

Студент \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Чигарев Александр Юрьевич

(подпись студента)

Курсовой проект допущен к защите:

«\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_2024 г.

Руководитель работы

доцент кафедры, канд. пед. наук \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ А.Г. Анацкая

Курсовой проект защищен с оценкой:

«\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_2024 г.

Руководитель работы

доцент кафедры, канд. пед. наук \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ А.Г. Анацкая

Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение

высшего образования

«Сибирский государственный автомобильно-дорожный университет (СибАДИ)»

Кафедра «Информационная безопасность»

|  |
| --- |
| УТВЕРЖДАЮ |
| И.О., Зав. кафедрой ИБ |
| \_\_\_\_\_\_\_\_\_\_\_\_\_ Д.А. Панков |
| «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 2024 г. |

**ЗАДАНИЕ**

**к курсовому проекту**

студенту группы БИб-21Э1 Чигареву Александру Юрьевичу

1. Тема курсовому проекту: «Проектирование системы защита автоматизированной системы выдачи потребительских кредитов»
2. Содержание пояснительной записки:

* титульный лист;
* задание к курсовому проекту;
* содержание;
* введение;
* анализ объекта защиты;
* требования по обеспечению информационной безопасности;
* техническое задание на создание/моделирование СЗИ;
* заключение;
* список использованных источников.

1. Срок сдачи работы: «\_\_\_» \_\_\_\_\_\_\_\_\_\_ 2024 г.

Задание выдано «\_\_\_» \_\_\_\_\_\_\_\_\_\_ 2024 г.

Руководитель работы: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ А.Г. Анацкая

(подпись преподавателя)

Задание к исполнению принял «\_\_\_» \_\_\_\_\_\_\_\_\_\_ 2024 г.

Студент \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ А. Ю. Чигарев

(подпись студента)

**Содержание**

[**Введение** 4](#_Toc163132929)

[**1. Анализ объекта защиты** 5](#_Toc163132930)

[**1.1 Характеристика объекта защиты** 5](#_Toc163132931)

[**1.2 Технологический процесс обработки информации** 5](#_Toc163132932)

[**1.3 Возможные УБИ** 5](#_Toc163132933)

[**2. Требования по обеспечению информационной безопасности** 6](#_Toc163132934)

[**2.1 Классификация АС** 6](#_Toc163132935)

[**2.2 Состав мер по обеспечению ИБ** 6](#_Toc163132936)

[**3. Техническое задание на создание (моделирование) СЗИ** 7](#_Toc163132937)

[**3.1 Выбор технических СЗИ** 7](#_Toc163132938)

[**3.2 Технико-экономическое обоснование** 7](#_Toc163132939)

[**3.3 Техническое задание** 7](#_Toc163132940)

[**Заключение** 8](#_Toc163132941)

[**Список литературы** 9](#_Toc163132942)

# **Введение**

С развитием технологий и повсеместным использованием интернета, автоматизированные системы выдачи кредитов становятся основным инструментом взаимодействия банков с клиентами, это можно заметить по высокому уровню цифровизации банков [1]. В связи с этим растёт потребность в безопасных и эффективных системах выдачи потребительских.

Однако с увеличением объёма цифровизации, так же увеличивается и объём киберугрроз, а, следовательно, возрастает потребность в защите автоматизированных систем от нарушителей.

Таким образом, разработка эффективной системы защиты автоматизированных систем выдачи кредитов становится приоритетной задачей для финансовых учреждений, обеспечивая безопасность операций и сохранность данных клиентов.

**Цель:**

Исследовать и разработать техническое задание для эффективной системы защиты автоматизированной системы выдачи потребительских кредитов.

**Задачи:**

1. Провести анализ существующих методов и технологий защиты данных в автоматизированных системах выдачи кредитов.
2. Определить критерии эффективности и безопасности системы защиты для последующей оценки их при реализации и эксплуатации.
3. Спроектировать техническое задание.

# **1. Анализ объекта защиты**

## **1.1 Характеристика объекта защиты**

Наименование: …

Назначение: Автоматизированная система "…" предназначена для управления и обработки информации о кредитных операциях, связанных с потребительской областью в банковской среде.

Основная цель системы: эффективное управление выдачей, возвратом и мониторингом кредитов.

## **1.2 Технологический процесс обработки информации**

**Задачи (функции) АС:**

– Регистрация новых кредитных заявок;

– Оценка кредитоспособности клиентов;

– Выдача кредитных решений и формирование договоров;

– Учет и мониторинг выплат и погашений кредитов.

Перечень основных процессов АС указаны в таблице 1.

Таблица 1 – Перечень основных процессов АС.

| **Процесс** | **Вход** | **Поставщик** | **Выход** | **Клиент** |
| --- | --- | --- | --- | --- |
| Регистрация кредитной заявки | Персональные данные клиента, финансовая информация, данные кредита | Клиент банка | Уникальный идентификатор заявки, статус заявки, решение по кредиту | Кредитный аналитик |
| Оценка кредитоспособности | Персональные данные клиента, финансовая информация | Кредитный аналитик | Результат оценки кредитоспособности, рекомендуемая кредитная сумма | Оператор по работе с клиентами |
| Выдача кредита | Решение об оценке кредитоспособности | Кредитный аналитик | Договор кредита, условия, график погашения, уникальный номер кредита | Администратор системы |
| Мониторинг выплат и погашений | Договор кредита, финансовая информация о платежах | Клиент банка | Информация о статусе платежей, остаток задолженности | Оператор по работе с клиентами |

**Состав обрабатываемой информации и её правовой режим:**

– Персональные данные клиентов (ФИО, паспортные данные, адреса);

– Финансовая информация (доходы, расходы, кредитная история клиента);

– Данные кредита (процентная ставка, условия предоставления);

– Данные о статусе кредитов (номер счёта, сумма, статус счёта, дата выдачи, дата закрытия, процентная ставка по кредиту).

**Правовой режим обработки данных соответствует:**

Правовой режим определяется следующими документами:

– ФЗ от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации";

– ФЗ от 27.07.2006 N 152-ФЗ "О персональных данных";

– ФЗ от 02.12.1990 N 395-1 "О банках и банковской деятельности";

В следствии чего можно понять, что правовой режиму соответствует режиму «Коммерческой тайны».

**Схема ИТ-инфраструктуры АС:**

Схема, продемонстрированная на рисунке 1 содержит следующие компоненты:

– Сервер БД;

– Сервер Веб-приложения

– Межсетевой экран;

– Маршрутизаторы;

– Коммутаторы;

– АРМ пользователей.

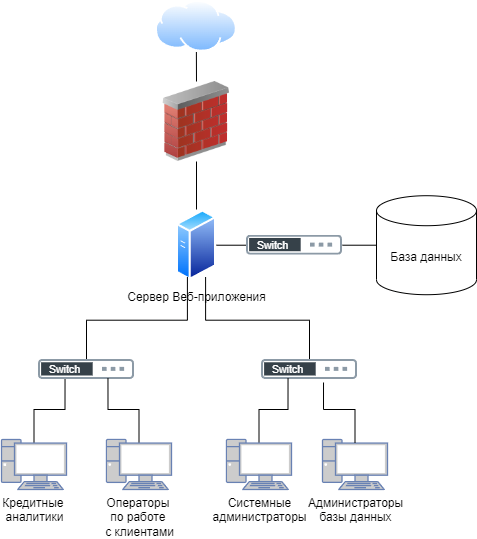


Рисунок 1 – Схема ИТ-инфраструктуры АС.

**Перечень аппаратных и программных средств, в т.ч. используемых средств ЗИ:**

1. Аппаратные средства:
   1. Сервер базы данных;
   2. Сервер веб-приложения;
   3. Системы мониторинга и защиты;
   4. АРМ пользователей;
2. Программные средства:
   1. СУБД (Postgresql);
   2. Среда программирования (Python);
   3. Антивирусная программа (Kaspersky Endpoint Security Cloud Pro);
   4. ОС (AstraLinux);
   5. Веб-приложение (Python (Django)).

**Описание групп внешних и внутренних пользователей:**

* Группы внутренних пользователей:
  1. Администраторы системы:
     + Уровень полномочий: Полный доступ к административным функциям и настройкам системы и сети. (высокий)
     + Типы доступа: Полный доступ к настройкам системы, управление пользователями, установка программного обеспечения, настройка сетевых параметров и обеспечение безопасности.
     + Функции: Мониторинг работы системы и сети, Управление резервным копированием и восстановлением данных, Организация и контроль обновлений программного обеспечения, Управление безопасностью сети и обнаружение угроз.
  2. Администраторы базы данных:
     + Уровень полномочий: Полный доступ к управлению базами данных и их содержимым. (высокий)
     + Типы доступа: Управление структурой баз данных, выполнение запросов, настройка прав доступа к данным, обеспечение безопасности и резервного копирования данных.
     + Функции: Мониторинг производительности баз данных и оптимизация запросов, Разработка и реализация стратегии обеспечения безопасности данных, Создание и настройка резервных копий баз данных, Управление доступом к данным и аудит баз данных.
  3. Кредитные аналитики:
     + Уровень полномочий: Доступ к кредитной информации и аналитическим инструментам. (средний)
     + Типы доступа: Просмотр и анализ кредитных данных, принятие решений о выдаче кредитов, генерация отчетов.
     + Функции: Проведение аналитических исследований для прогнозирования рисков и оценки кредитоспособности клиентов, Формирование рекомендаций по улучшению кредитных процессов и стратегий выдачи кредитов, Создание отчетов и аналитических дашбордов для руководства и аналитических подразделений банка.
  4. Операторы по работе с клиентами:
     + Уровень полномочий: Доступ к клиентской информации и инструментам обслуживания. (низкий)
     + Типы доступа: Обработка запросов клиентов, предоставление информации о счетах и услугах банка, управление жалобами и проблемами клиентов.
     + Функции: Обработка жалоб и обращений клиентов с учетом стандартов обслуживания, Проведение консультаций и предоставление информации о продуктах и услугах банка, Управление клиентскими запросами и координация работы с другими подразделениями банка для решения проблем клиентов
* Группы внешних пользователей:
  1. Клиенты банка:
     + Уровень полномочий: Ограниченный доступ к собственной информации и операциям. (низкий)
     + Типы доступа: Просмотр баланса счета, выполнение транзакций, платежи, запросы на кредиты и другие услуги банка.

## **1.3 Возможные УБИ**

Далее в таблице 2 более подробно рассмотрены виды рисков и негативных последствий, а также в таблице 3 объекты воздействия и виды воздействия на них.

Таблица 2 – Виды рисков (ущерба) и негативных последствий от реализации УИБ для АС по работе с кредитами

|  |  |  |
| --- | --- | --- |
| **№** | **Виды рисков (ущерба)** | **Возможные негативные последствия** |
| 1 | Ущерб физическому лицу | – Нарушение конфиденциальности (утечка) персональных данных.  – Разглашение персональных данных пользователей. |
| 2 | Риски юридическому лицу, индивидуальному предпринимателю, связанные с хозяйственной деятельностью | – Потеря (хищение) денежных средств.  – Потеря клиентов, поставщиков.  – Потеря конкурентного преимущества.  – Нарушение деловой репутации.  – Снижение престижа.  – Утрата доверия.  – Утечка конфиденциальной информации. |

На основе анализа исходных данных и результатов инвентаризации систем и сетей определяются следующие группы информационных ресурсов и компонентов систем и сетей, которые могут являться объектами воздействия:

Сервер веб-приложения, ОС на АРМ сотрудников, Сервер БД, СУБД, Веб-приложение.

Таблица 3 – Объекты воздействия и виды воздействия на них в АС по работе с кредитами

|  |  |  |
| --- | --- | --- |
| **Негативные последствия** | **Объекты воздействия** | **Виды воздействия** |
| Нарушение конфиденциальности (утечка) персональных данных | Сервер БД | Утечка персональных данных пользователей, технический сбой. |
| ОС на АРМ сотрудников | Утечка идентификационной информации сотрудников. |
| Веб-приложение | Несанкционированный доступ к идентификационной информации, содержащейся в веб-приложении. |
| Разглашение персональных данных граждан | Сервер БД | Утечка персональных данных пользователей, технический сбой. |
| ОС на АРМ сотрудников | Утечка идентификационной информации сотрудников. |
| Веб-приложение | Несанкционированный доступ к идентификационной информации, содержащейся в веб-приложении. |
| Потеря (хищение) денежных средств | ОС на АРМ сотрудников | Несанкционированная подмена информации в БД |
| Потеря клиентов, поставщиков | Сервер веб-приложения | Атака по типу «Отказ в обслуживании», технический сбой, утечка идентификационной информации. |
| СУБД | Технический сбой, не санкционированный доступ к системе, утечка идентификационной информации. |
| Потеря конкурентного преимущества | Сервер веб-приложения | Атака по типу «Отказ в обслуживании», технический сбой, утечка идентификационной информации. |
| СУБД | Технический сбой, не санкционированный доступ к системе, утечка идентификационной информации. |
| Нарушение деловой репутации | Сервер веб-приложения | Атака по типу «Отказ в обслуживании», технический сбой, утечка идентификационной информации. |
| СУБД | Технический сбой, не санкционированный доступ к системе, утечка идентификационной информации. |
| Снижение престижа | Сервер веб-приложения | Атака по типу «Отказ в обслуживании», технический сбой, утечка идентификационной информации. |
| СУБД | Технический сбой, не санкционированный доступ к системе, утечка идентификационной информации. |
| Утрата доверия | Сервер веб-приложения | Атака по типу «Отказ в обслуживании», технический сбой, утечка идентификационной информации. |
| СУБД | Технический сбой, не санкционированный доступ к системе, утечка идентификационной информации. |
| Утечка конфиденциальной информации | Сервер БД | Утечка персональных данных пользователей. |
| ОС на АРМ сотрудников | Утечка идентификационной информации сотрудников с АРМ. |
| Веб-приложение | Несанкционированный доступ к идентификационной информации, содержащейся в веб-приложении. |

На основе ранее предоставленных данных были выявлены и представлены в таблице 4 потенциальные нарушители УИБ в автоматизированной системе по работе с потребительскими кредитами, а также в таблице 5 продемонстрированы цели реализации угроз безопасности информации в зависимости от их реализации для автоматизированной системы.

Таблица 4 – Потенциальные нарушители УИБ в АС по работе с кредитами

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№**  **п/п** | **Виды риска и возможные негативные последствия** | **Виды потенциального нарушителя** | **Уровень возможностей нарушителя** | **Возможные цели** |
| 1 | (У1) Нарушение конфиденциальности (утечка)персональных данных. | Преступные группы (криминальные структуры) | Нарушитель, обладающий базовыми повышенными возможностями (Н2) | Получение финансовой или иной материальной выгоды. Желание самореализации (подтверждение статуса) |
| (У1) Разглашение персональных данных граждан. |
| (У2) Потеря клиентов, поставщиков. |
| (У2) Потеря (хищение) денежных средств |
| (У2) Утечка конфиденциальной информации |
| (У2) Нарушение деловой репутации |
| 2 | (У1) Нарушение конфиденциальности (утечка) персональных данных | Отдельные физические лица (хакеры) | Нарушитель, обладающий базовыми возможностями(Н1) | Получение финансовой или иной материальной выгоды.  Любопытство или желание самореализации (подтверждение статуса) |
| (У1) Разглашение персональных данных граждан |
| (У2) Утечка конфиденциальной информации |
| (У2) Нарушение деловой репутации |
| 3 | (У1) Нарушение конфиденциальности (утечка) персональных данных | Конкурирующие организации | Нарушитель, обладающий базовыми повышенными возможностями(Н2) | Получение конкурентных преимуществ. Получение финансовой или иной материальной выгоды |
| (У2) Потеря (хищение) денежных средств |
| (У2) Потеря клиентов, поставщиков |
| (У2) Потеря конкурентного преимущества |
| (У2) Нарушение деловой репутации |
| (У2) Снижение престижа |
| (У2) Утрата доверия |
| 4 | (У1) Нарушение конфиденциальности (утечка) персональных данных | Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора (администрация, охрана, уборщики и т.д.) | Нарушитель, обладающий базовыми возможностями(Н1) | Получение финансовой или иной материальной выгоды.  Непреднамеренные, неосторожные или неквалифицированные действия |
| (У1) Разглашение персональных данных граждан |
| (У2) Нарушение деловой репутации |
| (У2) Утечка конфиденциальной информации |
| 5 | (У1) Нарушение конфиденциальности (утечка) персональных данных | Системные администраторы и администраторы безопасности | Нарушитель, обладающий базовыми повышенными возможностями(Н2) | Получение финансовой или иной материальной выгоды. Любопытство или желание самореализации (подтверждение статуса). Месть за ранее совершенные действия. Непреднамеренные, неосторожные или неквалифицированные действия |
| (У1) Разглашение персональных данных граждан |
| (У2) Нарушение деловой репутации |
| (У2) Утечка конфиденциальной информации |
| 6 | (У1) Нарушение конфиденциальности (утечка) персональных данных | Бывшие работники (пользователи) | Нарушитель, обладающий базовыми возможностями(Н1) | Получение финансовой или иной материальной выгоды. Месть за ранее совершенные действия |
| (У1) Разглашение персональных данных граждан |
| (У2) Нарушение деловой репутации |
| (У2) Утечка конфиденциальной информации |
| 7 | (У1) Нарушение конфиденциальности (утечка) персональных данных | Авторизованные пользователи систем и сетей | Нарушитель, обладающий базовыми возможностями(Н1) | Получение финансовой или иной материальной выгоды. Любопытство или желание самореализации (подтверждение статуса). Месть за ранее совершенные действия. Непреднамеренные, неосторожные или неквалифицированные действия |
| (У1) Разглашение персональных данных граждан |
| (У2) Нарушение деловой репутации |
| (У2) Утечка конфиденциальной информации |

Таблица 5 – Цели реализации нарушителями угроз безопасности информации в зависимости от возможных негативных последствий и видов ущерба от их реализации для АС по работе с кредитами

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Виды нарушителей** | **Возможные цели реализации угроз безопасности информации** | | | **Соответствие целей видам риска и возможным негативным последствиям** |
| **Нанесение ущерба физическому лицу** | **Нанесение ущерба юридическому лицу, индивидуальному предпринимателю** | **Нанесение ущерба государства в области обеспечения обороны страны, безопасности государства и правопорядка, а также в социальной, экономической, политической, экологической сферах деятельности** |
| Преступные группы (криминальные структуры) | +Получение финансовой или иной материальной выгоды. | +Получение финансовой или иной материальной выгоды. Желание самореализации (подтверждение статуса) | – | (У1) Нарушение конфиденциальности (утечка)персональных данных. |
| (У1) Разглашение персональных данных граждан. |
| (У2) Потеря клиентов, поставщиков. |
| (У2) Потеря (хищение) денежных средств |
| (У2) Утечка конфиденциальной информации |
| (У2) Нарушение деловой репутации |
| Отдельные физические лица (хакеры) | +Любопытство или желание самореализации (подтверждение статуса) | +Получение финансовой или иной материальной выгоды. | – | (У1) Нарушение конфиденциальности (утечка) персональных данных |
| (У1) Разглашение персональных данных граждан |
| (У2) Утечка конфиденциальной информации |
| (У2) Нарушение деловой репутации |
| Конкурирующие организации | +Получение финансовой или иной материальной выгоды | +Получение конкурентных преимуществ | – | (У1) Нарушение конфиденциальности (утечка) персональных данных |
| (У2) Потеря (хищение) денежных средств |
| (У2) Потеря клиентов, поставщиков |
| (У2) Потеря конкурентного преимущества |
| (У2) Нарушение деловой репутации |
| (У2) Снижение престижа |
| (У2) Утрата доверия |
| Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора (администрация, охрана, уборщики и т.д.) | +Непреднамеренные, неосторожные или неквалифицированные действия | +Получение финансовой или иной материальной выгоды. | – | (У1) Нарушение конфиденциальности (утечка) персональных данных |
| (У1) Разглашение персональных данных граждан |
| (У2) Нарушение деловой репутации |
| (У2) Утечка конфиденциальной информации |
| Системные администраторы и администраторы безопасности | +Любопытство или желание самореализации (подтверждение статуса). Непреднамеренные, неосторожные или неквалифицированные действия | +Месть за ранее совершенные действия. Получение финансовой или иной материальной выгоды. | – | (У1) Нарушение конфиденциальности (утечка) персональных данных |
| (У1) Разглашение персональных данных граждан |
| (У2) Нарушение деловой репутации |
| (У2) Утечка конфиденциальной информации |
| Бывшие работники (пользователи) | +Получение финансовой или иной материальной выгоды. | +Месть за ранее совершенные действия | – | (У1) Нарушение конфиденциальности (утечка) персональных данных |
| (У1) Разглашение персональных данных граждан |
| (У2) Нарушение деловой репутации |
| (У2) Утечка конфиденциальной информации |
| Авторизованные пользователи систем и сетей | +Любопытство или желание самореализации (подтверждение статуса). Непреднамеренные, неосторожные или неквалифицированные действия | +Месть за ранее совершенные действия. Получение финансовой или иной материальной выгоды. | – | (У1) Нарушение конфиденциальности (утечка) персональных данных |
| (У1) Разглашение персональных данных граждан |
| (У2) Нарушение деловой репутации |
| (У2) Утечка конфиденциальной информации |

**Описание способов реализации угроз безопасности информации, которые могут быть использованы нарушителями разных видов категорий.**

Основными способами реализации (возникновения) угроз безопасности информации являются:

1. Использование уязвимостей;
2. Внедрение вредоносного программного обеспечения;
3. Использование не декларированных возможностей программного обеспечения и (или) программно-аппаратных средств;
4. Ошибочные действия в ходе создания и эксплуатации систем и сетей, в том числе при установке, настройке программных и программно-аппаратных средств.

Условием, позволяющим нарушителям использовать способы реализации угроз безопасности информации, является наличие у них возможности доступа к следующим типам интерфейсов объектов воздействия:

* внутренние сетевые интерфейсы, обеспечивающие взаимодействие (в том числе через промежуточные компоненты) с компонентами систем и сетей, имеющими внешние сетевые интерфейсы (проводные, беспроводные);
* интерфейсы для пользователей (проводные, беспроводные, веб-интерфейсы, интерфейсы удаленного доступа и др.);
* интерфейсы для установки, настройки, испытаний, пусконаладочных работ (в том числе администрирования, управления, обслуживания) обеспечения функционирования компонентов систем и сетей;
* возможность доступа к поставляемым или находящимся на обслуживании, ремонте в сторонних организациях компонентам систем и сетей.

Далее в таблице 6 представлены актуальные способы реализации УИБ в автоматизированной системе по работе с потребительскими кредитами. Также в таблице 7 продемонстрированы возможные УБИ для автоматизированной системы по работе с потребительскими кредитами.

Таблица 6 – Актуальные способы реализации УИБ в АС по работе с кредитами

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **№ п/п** | **Виды нарушителя** | **Категории нарушителя** | **Объект воздействия** | **Доступные интерфейсы** | **Способы реализации** |
| 1 | Преступные группы (криминальные структуры) | Внешний | Сервер веб-приложение | Веб-интерфейс приложения | Использование уязвимостей кода программного обеспечения веб-сервера |
| СУБД | Интерфейс веб-приложения | Использование уязвимостей кода программного обеспечения веб-сервера |
| 2 | Отдельные физические лица (хакеры) | Внешний | Сервер веб-приложение | Веб-интерфейс пользователя | Использование уязвимостей кода программного обеспечения веб-сервера |
| СУБД | Интерфейс веб-приложения | Использование уязвимостей кода программного обеспечения веб-сервера |
| Сервер БД | Веб-интерфейс, консольный интерфейс | Использование уязвимостей кода программного обеспечения веб-сервера |
| 3 | Конкурирующие организации | Внешний | Сервер веб-приложение | Веб-интерфейс приложения | Использование уязвимостей кода программного обеспечения веб-сервера |
| 4 | Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора (администрация, охрана, уборщики и т.д.) | Внутренний | БД | Веб-интерфейс, консольный интерфейс | Использование уязвимостей кода программного обеспечения веб-сервера |
| ОС на АРМ сотрудников | Операционная система. | Использование уязвимостей конфигурации системы. |
| Сервер веб-приложение | Веб-интерфейс приложения | Использование уязвимостей кода программного обеспечения веб-сервера |
| 5 | Системные администраторы и администраторы безопасности | Внутренний | Сервер БД | Веб-интерфейс, консольный интерфейс | Использование уязвимостей кода программного обеспечения веб-сервера |
| АРМ сотрудников | Операционная система. | Использование уязвимостей конфигурации системы. |
| Сервер веб-приложение | Веб-интерфейс приложения | Использование уязвимостей кода программного обеспечения веб-сервера |
| 6 | Бывшие работники (пользователи) | Внешний | Веб-приложение | Веб-интерфейс приложения | Использование уязвимостей кода программного обеспечения веб-сервера |
| 7 | Авторизованные пользователи систем и сетей | Внутренний | Веб-приложение | Веб-интерфейс приложения | Использование уязвимостей конфигурации системы. |
| СУБД | Интерфейс веб-приложения | Использование уязвимостей кода программного обеспечения веб-сервера |

Таблица 7 – Возможные УИБ для АС по работе с кредитами

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **№** | **Угроза БИ** | **Ущерб (негативные последствия)** | **Нарушитель** | **Объект воздействия** | **Способы реализации** |
| 1 | УБИ.008 Угроза восстановления и/или повторного использования аутентификационной информации | Нарушение конфиденциальности (утечка) персональных данных | Системные администраторы и администраторы безопасности | СУБД | Используя SQL команды редактирование данных в БД |
| 2 | УБИ.015 Угроза доступа к защищаемым файлам с использованием обходного пути | Нарушение конфиденциальности (утечка) персональных данных | Преступные группы | Сервер веб-приложения | Использование уязвимостей кода программного обеспечения веб-сервера |
| Отдельные физические лица | Сервер веб-приложения | Использование уязвимостей кода программного обеспечения веб-сервера |
| 3 | УБИ.031 Угроза использования механизмов авторизации для повышения привилегий | Нарушение конфиденциальности (утечка) персональных данных | Преступные группы | СУБД | Используя SQL команды редактирование данных в БД |
| Сервер веб-приложения | Использование уязвимостей кода программного обеспечения веб-сервера |
| Отдельные физические лица | СУБД | Используя SQL команды редактирование данных в БД |
| Сервер веб-приложения | Использование уязвимостей кода программного обеспечения веб-сервера |
| 4 | УБИ.067 Угроза неправомерного ознакомления с защищаемой информацией | Разглашение персональных данных.  Утечка конфиденциальной информации. | Бывшие работники | Веб-приложение | Используя свои данные для авторизации может неправомерно делится информацией |
| Системные администраторы и администраторы безопасности | Веб-приложение | Используя свои данные для авторизации может неправомерно делится информацией |
| 5 | УБИ.068 Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением | Снижение престижа  Нарушение деловой репутации  Утечка конфиденциальной информации | Системные администраторы и администраторы безопасности | Веб-приложение | Неправильное использование приложения приводящие к его ошибкам |
| СУБД | Неправленое создание, редактирование SQL запросов приводящее к сбоям системы |
| Бывшие работники (пользователи) | Веб-приложение | Используя свои данные для авторизации может пользоваться веб-приложением |
| 6 | УБИ.074 Угроза несанкционированного доступа к аутентификационной информации | Нарушение конфиденциальности (утечка) персональных данных  Разглашение персональных данных  Утечка конфиденциальной информации | Преступные группы | СУБД | Используя SQL команды редактирование данных в БД |
| Отдельные физические лица |
| 7 | УБИ.088 Угроза несанкционированного копирования защищаемой информации | Нарушение конфиденциальности (утечка) персональных данных | Системные администраторы и администраторы безопасности | Сервер БД | Копирование данных |
| 8 | УБИ.090 Угроза несанкционированного создания учётной записи пользователя | Нарушение конфиденциальности (утечка) персональных данных  Утрата доверия  Утечка конфиденциальной информации | Системные администраторы и администраторы безопасности | СУБД | Используя SQL команды редактирование данных в БД |
| 9 | УБИ.091 Угроза несанкционированного удаления защищаемой информации | Потеря конкурентного преимущества  Утрата доверия  Потеря клиентов, поставщиков | Системные администраторы и администраторы безопасности | СУБД | Используя SQL команды редактирование данных в БД |
| Преступные группы |
| Отдельные физические лица |
| 10 | УБИ.127 Угроза подмены действия пользователя путём обмана | Потеря (хищение) денежных средств  Потеря клиентов, поставщиков | Авторизованные пользователи систем и сетей | Веб-приложение | Обманув пользователя и используя его авторотационные данные редактировать данные пользователя. |
| 11 | УБИ.140 Угроза приведения системы в состояние «отказ в обслуживании» | Потеря клиентов, поставщиков  Потеря конкурентного преимущества  Нарушение деловой репутации  Снижение престижа  Утрата доверия | Преступные группы | Сервер веб-приложения | DOS, DDOS |
| Конкурирующие организации | Сервер веб-приложения | DOS, DDOS |
| Отдельные физические лица | Сервер веб-приложения | DOS, DDOS |
| Системные администраторы и администраторы безопасности | Сервер веб-приложения | При обслуживании сервера и обновлении веб-приложения ошибки в коде |
| СУБД | Используя SQL неверно выполнив команду, нагрузить сильно систему |
| 12 | УБИ.157 Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации. | Снижение престижа  Потеря клиентов, поставщиков  Потеря конкурентного преимущества | Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора (администрация, охрана, уборщики и т.д.) | АРМ пользователя | Несоблюдение правил эксплуатации устройства, при каком либо взаимодействии с оборудованием |
| Системные администраторы и администраторы безопасности | Сервер веб-приложения | Несоблюдение правил эксплуатации, при работе с оборудованием |
| Сервер БД | Несоблюдение правил эксплуатации, при работе с оборудованием |

# **2. Требования по обеспечению информационной безопасности**

## **2.1 Классификация АС**

## **2.2 Состав мер по обеспечению ИБ**

# **3. Техническое задание на создание (моделирование) СЗИ**

## **3.1 Выбор технических СЗИ**

## **3.2 Технико-экономическое обоснование**

## **3.3 Техническое задание**

# **Заключение**

# **Список литературы**

1. <https://www.banki.ru/news/research/?id=10950478>