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 (работе)**

по дисциплине: «Технология построения защищенных автоматизированных систем»

Название работы «Проектирование системы защиты 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](#_Toc167224431)

[**1. Анализ объекта защиты** 5](#_Toc167224432)

[**1.1 Характеристика объекта защиты** 5](#_Toc167224433)

[**1.2 Технологический процесс обработки информации** 5](#_Toc167224434)

[**1.3 Возможные угрозы безопасности информации** 10](#_Toc167224435)

[**2. Требования по обеспечению информационной безопасности** 24](#_Toc167224436)

[**2.1 Классификация АС** 24](#_Toc167224437)

[**2.2 Состав мер по обеспечению ИБ** 24](#_Toc167224438)

[**3. Техническое задание на проектирование СЗИ АС** 43](#_Toc167224439)

[**3.1 Выбор технических СЗИ** 43](#_Toc167224440)

[**3.2 Техническое задание** 43](#_Toc167224441)

[**Заключение** 44](#_Toc167224442)

[**Список литературы** 45](#_Toc167224443)

# **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: Потребительское кредитование

Назначение: Автоматизированная система (далее АС) потребительских кредитов 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 за потребительскими кредитами.

## **1.2 Технологический процесс обработки информации**

Задачи и функции АС:

1. Регистрация новых кредитных заявок;
2. Выдача кредитных решений и формирование договоров;
3. Учет и мониторинг выплат и погашений кредитов.

Данные задачи можно считать бизнес-процессами данной АС, содержание (описание) данных бизнес-процессов предоставлено в таблице 1.

Таблица 1 – Описание бизнес-процессов

| **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 |
| 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 |

В данной АС обрабатывается следующие данные, используемые в бизнес-процессах:

1. Персональные данные клиентов (ФИО, паспортные данные, адреса);
2. Финансовая информация (доходы, расходы, кредитная история клиента);
3. Данные кредита (процентная ставка, условия предоставления);
4. Данные о статусе кредитов (номер счёта, сумма, статус счёта, дата выдачи, дата закрытия, процентная ставка по кредиту).

Правовой режим определяется следующими документами:

1. ФЗ от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации";
2. ФЗ от 27.07.2006 N 152-ФЗ "О персональных данных";
3. ФЗ от 02.12.1990 N 395-1 "О банках и банковской деятельности".

Правовой режиму соответствует режиму «Коммерческой тайны». Это означает, что определенная информация или материал защищены законом как коммерческая тайна, а следовательно, информация не может быть раскрыта, использована или распространена без согласия владельца без нарушения закона.

Режим "Коммерческой тайны" обеспечивает защиту конфиденциальной информации, которая имеет ценность для бизнеса и может принести прибыль или предоставить конкурентное преимущество. Это может включать в себя такую информацию, которая не должна быть доступна для конкурентов или других лиц без разрешения владельца.

**Схема ИТ-инфраструктуры АС:**

Схема, продемонстрированная на рисунке 1 содержит следующие компоненты:

– Сервер БД;

– Сервер Веб-приложения

– Межсетевой экран;

– Маршрутизаторы;

– АРМ пользователей.

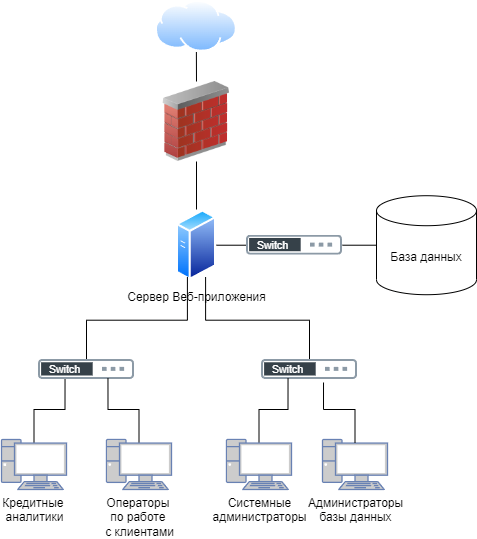


Рисунок 1 – Схема ИТ-инфраструктуры АС.

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

Аппаратные средства:

* 1. Сервер базы данных;
  2. Сервер веб-приложения;
  3. Системы мониторинга и защиты;
  4. АРМ пользователей;

Программные средства:

* 1. СУБД (Postgresql);
  2. Среда программирования (Python);
  3. Антивирусная программа (Kaspersky Endpoint Security Cloud Pro);
  4. ОС (Windows 10);
  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 угрозы безопасности информации**

Угрозы безопасности информации (далее УБИ) – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения информационной безопасности.

УБИ определяется на основе методического документа «Федеральной службы по техническому и экспортному контролю» (далее ФСТЭК) от 5 февраля 2021 г. «Методика оценки угроз безопасности информации».

На основе данного документа была написана таблица 2 в которой рассмотрены виды рисков УБИ характерные АС по выдаче кредитов, а также возможные негативные последствия, которые характерны перечисленным видам.

Таблица 2 – Виды рисков и негативных последствий

| **№** | **Виды рисков (ущерба)** | **Возможные негативные последствия** |
| --- | --- | --- |
| У1 | Ущерб физическому лицу | – Нарушение конфиденциальности (утечка) персональных данных.  – Разглашение персональных данных пользователей. |
| У2 | 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:

1. Сервер веб-приложения;
2. ОС на АРМ сотрудников;
3. Сервер БД;
4. СУБД;
5. Веб-приложение.

Для данных объектов воздействия в таблице 3 предоставлены сведения об видах воздействия на них.

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, несанкционированный доступ. |
| 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. |
| Сервер БД | Несанкционированная подмена информации. |
| Потеря клиентов, поставщиков | Сервер веб-приложения | Нарушение доступности, технический сбой, утечка идентификационной информации. |
| СУБД | Технический сбой, не санкционированный доступ к системе, утечка идентификационной информации. |
| Потеря конкурентного преимущества | Сервер веб-приложения | Нарушение доступности, технический сбой, утечка идентификационной информации. |
| СУБД | Технический сбой, не санкционированный доступ к системе, утечка идентификационной информации. |
| Нарушение деловой репутации | Сервер веб-приложения | Нарушение доступности, технический сбой, утечка идентификационной информации. |
| СУБД | Технический сбой, не санкционированный доступ к системе, утечка идентификационной информации. |
| Снижение престижа | Сервер веб-приложения | Нарушение доступности, технический сбой, утечка идентификационной информации. |
| СУБД | Технический сбой, не санкционированный доступ к системе, утечка идентификационной информации. |
| Утрата доверия | Сервер веб-приложения | Нарушение доступности, 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.

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

| **Виды риска и возможные негативные последствия** | **Виды потенциального нарушителя** | **Уровень возможностей нарушителя** | **Возможные цели** |
| --- | --- | --- | --- |
| (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 |
| (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 |
| (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 |
| (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 |
| (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 |
| (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 |
| (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 |

Далее в таблице 5, основываясь на видах угроз, выявленных в таблице 4, демонстрируются цели реализации угроз безопасности информации в зависимости от их реализации для автоматизированной системы.

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.

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

| **Виды нарушителя** | **Категории нарушителя** | **Объект воздействия** | **Доступные интерфейсы** | **Способы реализации** |
| --- | --- | --- | --- | --- |
| 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 |
| 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 |
| Конкурирующие организации | Внешний | Сервер веб-приложение | Веб-интерфейс приложения | Использование уязвимостей кода программного обеспечения веб-сервера |
| 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 |
| 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 |
| Бывшие работники (пользователи) | Внешний | Веб-приложение | Веб-интерфейс приложения | Использование уязвимостей кода программного обеспечения веб-сервера |
| 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 |

В таблице 7 продемонстрированы возможные УБИ для автоматизированной системы по работе с потребительскими кредитами.

Таблица 7 – Возможные УИБ для АС по работе с кредитами

| **Угроза БИ** | **Ущерб (негативные последствия)** | **Нарушитель** | **Объект воздействия** | **Способы реализации** |
| --- | --- | --- | --- | --- |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| УБИ.088 Угроза несанкционированного копирования защищаемой информации | Нарушение конфиденциальности (утечка) персональных данных | Системные администраторы и администраторы безопасности | Сервер БД | Копирование данных |
| 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 |
| 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 |
| 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. |
| 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 |
| 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 |

(Нужно здесь что-то написать… Только вот что?)

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

## **2.1 Классификация АС**

Для АС: «…» был определён средний (УЗ 3) уровень значимости т.к., если в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны незначительные негативные последствия в социальной, политической, международной, экономической, финансовой или иных областях деятельности и (или) информационная система и (или) оператор (обладатель информации) могут выполнять возложенные на них функции с недостаточной эффективностью или выполнение функций воз-можно только с привлечением дополнительных сил и средств.

Информационная система имеет объектовый масштаб т.к., функционирует на объектах одного федерального органа государственной власти, органа государственной власти субъекта Российской Федерации, муниципального образования и (или) организации и не имеет сегментов в территориальных органах, представительствах, филиалах, подведомственных и иных организациях.

Класс защищенности информационной системы, определённый в соответствии с таблицей: К3.

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

Таблица 8 – Меры защиты информации в информационных системах.

| **Условное обозначение и номер меры** | **Меры защиты информации в информационных системах** |
| --- | --- |
|
| **I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)** | |
| ИАФ.1 | Идентификация и аутентификация пользователей, являющихся работниками оператора |
| ИАФ.3 | Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов |
| ИАФ.4 | Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации |
| ИАФ.5 | Защита обратной связи при вводе аутентификационной информации |
| ИАФ.6 | Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей) |
| **II. Управление доступом субъектов доступа к объектам доступа (УПД)** | |
| УПД.1 | Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей |
| УПД.2 | Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа |
| УПД.3 | Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами |
| УПД.4 | Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы |
| УПД.5 | Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы |
| УПД.6 | Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе) |
| УПД.10 | Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу |
| УПД.11 | Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации |
| УПД.13 | Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети |
| УПД.14 | Регламентация и контроль использования в информационной системе технологий беспроводного доступа |
| УПД.15 | Регламентация и контроль использования в информационной системе мобильных технических средств |
| УПД.16 | Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы) |
| **III. Ограничение программной среды (ОПС)** | |
| ОПС.3 | Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов |
| **IV. Защита машинных носителей информации (ЗНИ)** | |
| ЗНИ.1 | Учет машинных носителей информации |
| ЗНИ.2 | Управление доступом к машинным носителям информации |
| ЗНИ.8 | Уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) |
| **V. Регистрация событий безопасности (РСБ)** | |
| РСБ.1 | Определение событий безопасности, подлежащих регистрации, и сроков их хранения |
| РСБ.2 | Определение состава и содержания информации о событиях безопасности, подлежащих регистрации |
| РСБ.3 | Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения |
| РСБ.4 | Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти |
| РСБ.5 | Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них |
| РСБ.6 | Генерирование временных меток и (или) синхронизация системного времени в информационной системе |
| РСБ.7 | Защита информации о событиях безопасности |
| **VI. Антивирусная защита (АВЗ)** | |
| АВЗ.1 | Реализация антивирусной защиты |
| АВЗ.2 | Обновление базы данных признаков вредоносных компьютерных программ (вирусов) |
| **VIII. Контроль (анализ) защищенности информации (АНЗ)** | |
| АНЗ.1 | Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей |
| АНЗ.2 | Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации |
| АНЗ.3 | Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации |
| АНЗ.4 | Контроль состава технических средств, программного обеспечения и средств защиты информации |
| АНЗ.5 | Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе |
| **IX. Обеспечение целостности информационной системы и информации (ОЦЛ)** | |
| ОЦЛ.3 | Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций |
| **XI. Защита среды виртуализации (ЗСВ)** | |
| ЗСВ.1 | Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации |
| ЗСВ.2 | Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин |
| ЗСВ.3 | Регистрация событий безопасности в виртуальной инфраструктуре |
| ЗСВ.9 | Реализация и управление антивирусной защитой в виртуальной инфраструктуре |
| ЗСВ.10 | Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки информации отдельным пользователем и (или) группой пользователей |
| **XII. Защита технических средств (ЗТС)** | |
| ЗТС.2 | Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования |
| ЗТС.3 | Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы и помещения и сооружения, в которых они установлены |
| ЗТС.4 | Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр |
| **XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)** | |
| ЗИС.3 | Обеспечение защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи |
| ЗИС.5 | Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств |
| ЗИС.20 | Защита беспроводных соединений, применяемых в информационной системе |
| ЗИС.30 | Защита мобильных технических средств, применяемых в информационной системе |

В процессе адаптации из базового набора мер исключаются:

Таблица 9 – Исключённые базовые меры

| **Условное обозначение и номер меры** | **Причина исключения** |
| --- | --- |
| УПД.11 | До проведения идентификации и аутентификации пользователю запрещены любые действия, кроме ввода идентификационной и аутентификационной информации |
| УПД.14 | В данной АС: «Регламентация и контроль использования в информационной системе технологий беспроводного доступа» не требуется т.к., методы беспроводного доступа к АС отсутствуют. |
| ЗСВ.1 | Отсутствуют средства виртуализации |
| ЗСВ.2 | Отсутствуют средства виртуализации |
| ЗСВ.3 | Отсутствуют средства виртуализации |
| ЗСВ.9 | Отсутствуют средства виртуализации |
| ЗСВ.10 | Отсутствуют средства виртуализации |
| ЗИС.20 | Отсутствуют беспроводные соединения в системе. |

Таблица 10 – Уточнение мер противодействия

| **УБИ** | **Меры противодействия** |
| --- | --- |
| УБИ.008 Угроза восстановления и/или повторного использования аутентификационной информации | ИАФ.1, ИАФ.3, ИАФ.4, ИАФ.5, ИАФ.6 |
| УБИ.015 Угроза доступа к защищаемым файлам с использованием обходного пути | УПД.1, УПД.2, УПД.3, УПД.4, УПД.5, АВЗ.1, АВЗ.2, АНЗ.1, |
| УБИ.031 Угроза использования механизмов авторизации для повышения привилегий | УПД.1, УПД.2, УПД.3, УПД.4, УПД.5, УПД.6, УПД.10, УПД.13, УПД.15, УПД.16 |
| УБИ.067 Угроза неправомерного ознакомления с защищаемой информацией | ЗТС.2, ЗТС.3, ЗТС.4, ЗИС.3 |
| УБИ.068 Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением | ОПС.3, УПД.6, УПД.10, УПД.13 |
| УБИ.074 Угроза несанкционированного доступа к аутентификационной информации | УПД.1, УПД.2, УПД.3, УПД.4, УПД.5, УПД.6, УПД.10, УПД.13, УПД.15, УПД.16 |
| УБИ.088 Угроза несанкционированного копирования защищаемой информации | ЗНИ.1, ЗНИ.2, ЗНИ.8 |
| УБИ.090 Угроза несанкционированного создания учётной записи пользователя | УПД.1, УПД.2, УПД.3, УПД.4, УПД.5, УПД.6, УПД.10, УПД.13, УПД.15, УПД.16 |
| УБИ.091 Угроза несанкционированного удаления защищаемой информации | РСБ.1, РСБ.2, РСБ.3, РСБ.4, РСБ.5, РСБ.6, РСБ.7 |
| УБИ.127 Угроза подмены действия пользователя путём обмана | ИАФ.1, ИАФ.3, ИАФ.4, ИАФ.5, ИАФ.6 |
| УБИ.140 Угроза приведения системы в состояние «отказ в обслуживании» | РСБ.1, РСБ.2, РСБ.3, РСБ.4, РСБ.5, РСБ.6, РСБ.7, АВЗ.1, АВЗ.2, АНЗ.1, АНЗ.2, АНЗ.3, АНЗ.4, ОЦЛ.3 |
| УБИ.157 Угроза физического вы-ведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации | ЗТС.2, ЗТС.3, ЗТС.4 |

Дополнительные меры противодействия не требуются т.к., базовый набор удовлетворяет требованиям.

Таблица 11 – Сравнение мер в приказах 17 и 21

| **По приказу ФСТЭК России №17 (КЗ)** | | **По приказ ФСТЭК России №21 (4 УЗ)** | |
| --- | --- | --- | --- |
| **Идентификатор** | **Название меры** | **Идентификатор** | **Название меры** |
| **I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)** | | | |
| ИАФ.1 | Идентификация и аутентификация пользователей, являющихся работниками оператора | ИАФ.1 | Идентификация и аутентификация пользователей, являющихся работниками оператора |
|  |  | ИАФ.2 | Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных |
| ИАФ.3 | Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов | ИАФ.3 | Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов |
| ИАФ.4 | Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации | ИАФ.4 | Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации |
| ИАФ.5 | Защита обратной связи при вводе аутентификационной информации | ИАФ.5 | Защита обратной связи при вводе аутентификационной информации |
| ИАФ.6 | Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей) | ИАФ.6 | Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей) |
| **II. Управление доступом субъектов доступа к объектам доступа (УПД)** | | | |
| УПД.1 | Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей | УПД.1 | Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей |
| УПД.2 | Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа | УПД.2 | Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа |
| УПД.3 | Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами | УПД.3 | Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами |
| УПД.4 | Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы | УПД.4 | Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы |
| УПД.5 | Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы | УПД.5 | Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы |
| УПД.6 | Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе) | УПД.6 | Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе) |
| УПД.10 | Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу | УПД.10 | Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу |
|  |  | УПД.11 | Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации |
| УПД.13 | Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети | УПД.13 | Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети |
|  |  | УПД.14 | Регламентация и контроль использования в информационной системе технологий беспроводного доступа |
| УПД.15 | Регламентация и контроль использования в информационной системе мобильных технических средств | УПД.15 | Регламентация и контроль использования в информационной системе мобильных технических средств |
| УПД.16 | Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы) | УПД.16 | Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы) |
|  |  | УПД.17 | Обеспечение доверенной загрузки средств вычислительной техники |
| **III. Ограничение программной среды (ОПС)** | | | |
|  |  | ОПС.2 | Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения |
| ОПС.3 | Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов |  |  |
| **IV. Защита машинных носителей информации (ЗНИ)** | | | |
| ЗНИ.1 | Учет машинных носителей информации | ЗНИ.1 | Учет машинных носителей персональных данных |
| ЗНИ.2 | Управление доступом к машинным носителям информации | ЗНИ.2 | Управление доступом к машинным носителям персональных данных |
| ЗНИ.8 | Уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) | ЗНИ.8 | Уничтожение (стирание) или обезличивание персональных данных на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) или обезличивания |
| **V. Регистрация событий безопасности (РСБ)** | | | |
| РСБ.1 | Определение событий безопасности, подлежащих регистрации, и сроков их хранения | РСБ.1 | Определение событий безопасности, подлежащих регистрации, и сроков их хранения |
| РСБ.2 | Определение состава и содержания информации о событиях безопасности, подлежащих регистрации | РСБ.2 | Определение состава и содержания информации о событиях безопасности, подлежащих регистрации |
| РСБ.3 | Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения | РСБ.3 | Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения |
| РСБ.4 | Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти |  |  |
| РСБ.5 | Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них | РСБ.5 | Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них |
| РСБ.6 | Генерирование временных меток и (или) синхронизация системного времени в информационной системе |  |  |
| РСБ.7 | Защита информации о событиях безопасности | РСБ.7 | Защита информации о событиях безопасности |
| **VI. Антивирусная защита (АВЗ)** | | | |
| АВЗ.1 | Реализация антивирусной защиты | АВЗ.1 | Реализация антивирусной защиты |
| АВЗ.2 | Обновление базы данных признаков вредоносных компьютерных программ (вирусов) | АВЗ.2 | Обновление базы данных признаков вредоносных компьютерных программ (вирусов) |
| **VII. Обнаружение вторжений (СОВ)** | | | |
|  |  | СОВ.1 | Обнаружение вторжений |
|  |  | СОВ.2 | Обновление базы решающих правил |
| **VIII. Контроль (анализ) защищенности информации (АНЗ)** | | | |
| АНЗ.1 | Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей | АНЗ.1 | Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей |
| АНЗ.2 | Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации | АНЗ.2 | Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации |
| АНЗ.3 | Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации | АНЗ.3 | Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации |
| АНЗ.4 | Контроль состава технических средств, программного обеспечения и средств защиты информации | АНЗ.4 | Контроль состава технических средств, программного обеспечения и средств защиты информации |
| АНЗ.5 | Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе | АНЗ.5 | Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в информационной системе |
| **IX. Обеспечение целостности информационной системы и информации (ОЦЛ)** | | | |
|  |  | ОЦЛ.1 | Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации |
| ОЦЛ.3 | Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций |  |  |
|  |  | ОЦЛ.4 | Обнаружение и реагирование на поступление в информационную систему незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы (защита от спама) |
| **X. Обеспечение доступности персональных данных (ОДТ)** | | | |
|  |  | ОДТ.4 | Периодическое резервное копирование персональных данных на резервные машинные носители персональных данных |
|  |  | ОДТ.5 | Обеспечение возможности восстановления персональных данных с резервных машинных носителей персональных данных (резервных копий) в течение установленного временного интервала |
| **XI. Защита среды виртуализации (ЗСВ)** | | | |
|  |  | ЗСВ.1 | Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации |
|  |  | ЗСВ.2 | Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин |
|  |  | ЗСВ.3 | Регистрация событий безопасности в виртуальной инфраструктуре |
|  |  | ЗСВ.6 | Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных |
|  |  | ЗСВ.7 | Контроль целостности виртуальной инфраструктуры и ее конфигураций |
|  |  | ЗСВ.8 | Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры |
|  |  | ЗСВ.9 | Реализация и управление антивирусной защитой в виртуальной инфраструктуре |
|  |  | ЗСВ.10 | Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки персональных данных отдельным пользователем и (или) группой пользователей |
| **XII. Защита технических средств (ЗТС)** | | | |
| ЗТС.2 | Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования |  |  |
| ЗТС.3 | Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы и помещения и сооружения, в которых они установлены | ЗТС.3 | Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены |
| ЗТС.4 | Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр | ЗТС.4 | Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр |
| **XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)** | | | |
| ЗИС.3 | Обеспечение защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи | ЗИС.3 | Обеспечение защиты персональных данных от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи |
| ЗИС.5 | Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств |  |  |
|  |  | ЗИС.11 | Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов |
|  |  | ЗИС.15 | Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки персональных данных |
|  |  | ЗИС.17 | Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы |
|  |  | ЗИС.20 | Защита беспроводных соединений, применяемых в информационной системе |
| ЗИС.30 | Защита мобильных технических средств, применяемых в информационной системе |  |  |
| **XIV. Выявление инцидентов и реагирование на них (ИНЦ)** | | | |
|  |  | ИНЦ.1 | Определение лиц, ответственных за выявление инцидентов и реагирование на них |
|  |  | ИНЦ.2 | Обнаружение, идентификация и регистрация инцидентов |
|  |  | ИНЦ.3 | Своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе пользователями и администраторами |
|  |  | ИНЦ.4 | Анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий |
|  |  | ИНЦ.5 | Принятие мер по устранению последствий инцидентов |
|  |  | ИНЦ.6 | Планирование и принятие мер по предотвращению повторного возникновения инцидентов |
| **XV. Управление конфигурацией информационной системы и системы защиты персональных данных (УКФ)** | | | |
|  |  | УКФ.1 | Определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и системы защиты персональных данных |
|  |  | УКФ.2 | Управление изменениями конфигурации информационной системы и системы защиты персональных данных |
|  |  | УКФ.3 | Анализ потенциального воздействия планируемых изменений в конфигурации информационной системы и системы защиты персональных данных на обеспечение защиты персональных данных и согласование изменений в конфигурации информационной системы с должностным лицом (работником), ответственным за обеспечение безопасности персональных данных |
|  |  | УКФ.4 | Документирование информации (данных) об изменениях в конфигурации информационной системы и системы защиты персональных данных |

После всех анализов итоговый набор мер для обеспечения ЗИ в рассматриваемой АС собран в таблице 12.

Таблица 12 – Итоговый набор мер для обеспечения ЗИ в АС

| **Идентификатор мер** | **Название меры** | |
| --- | --- | --- |
| **I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)** | | |
| ИАФ.1 | Идентификация и аутентификация пользователей, являющихся работниками оператора | |
| ИАФ.2 | Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных | |
| ИАФ.3 | Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов | |
| ИАФ.4 | Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации | |
| ИАФ.5 | Защита обратной связи при вводе аутентификационной информации | |
| **II. Управление доступом субъектов доступа к объектам доступа (УПД)** | | |
| УПД.1 | Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей | |
| УПД.2 | Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа | |
| УПД.3 | Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами | |
| УПД.4 | Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы | |
| УПД.5 | Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы | |
| УПД.6 | Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе) | |
| УПД.10 | Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу | |
| УПД.13 | Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети | |
| УПД.15 | Регламентация и контроль использования в информационной системе мобильных технических средств | |
| УПД.16 | Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы) | |
| УПД.17 | Обеспечение доверенной загрузки средств вычислительной техники | |
| **III. Ограничение программной среды (ОПС)** | |
|  | | |
| ОПС.2 | Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения | |
| ОПС.3 | Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов | |
| **IV. Защита машинных носителей информации (ЗНИ)** | | |
| ЗНИ.1 | Учет машинных носителей персональных данных | |
| ЗНИ.2 | Управление доступом к машинным носителям персональных данных | |
| ЗНИ.8 | Уничтожение (стирание) или обезличивание персональных данных на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) или обезличивания | |
| **V. Регистрация событий безопасности (РСБ)** | | |
| РСБ.1 | Определение событий безопасности, подлежащих регистрации, и сроков их хранения | |
| РСБ.2 | Определение состава и содержания информации о событиях безопасности, подлежащих регистрации | |
| РСБ.3 | Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения | |
| РСБ.4 | Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти | |
| РСБ.5 | Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них | |
| РСБ.6 | Генерирование временных меток и (или) синхронизация системного времени в информационной системе | |
| РСБ.7 | Защита информации о событиях безопасности | |
| **VI. Антивирусная защита (АВЗ)** | | |
| АВЗ.1 | Реализация антивирусной защиты | |
| АВЗ.2 | Обновление базы данных признаков вредоносных компьютерных программ (вирусов) | |
| **VII. Обнаружение вторжений (СОВ)** | | |
| СОВ.1 | Обнаружение вторжений | |
| СОВ.2 | Обновление базы решающих правил | |
| **VIII. Контроль (анализ) защищенности информации (АНЗ)** | | |
| АНЗ.1 | Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей | |
| АНЗ.2 | Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации | |
| АНЗ.3 | Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации | |
| АНЗ.4 | Контроль состава технических средств, программного обеспечения и средств защиты информации | |
| АНЗ.5 | Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в информационной системе | |
| **IX. Обеспечение целостности информационной системы и информации (ОЦЛ)** | | |
| ОЦЛ.1 | Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации | |
| ОЦЛ.3 | Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций | |
| ОЦЛ.4 | Обнаружение и реагирование на поступление в информационную систему незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы (защита от спама) | |
| **X. Обеспечение доступности персональных данных (ОДТ)** | | |
| ОДТ.4 | Периодическое резервное копирование персональных данных на резервные машинные носители персональных данных | |
| ОДТ.5 | Обеспечение возможности восстановления персональных данных с резервных машинных носителей персональных данных (резервных копий) в течение установленного временного интервала | |
| **XI. Защита среды виртуализации (ЗСВ)** | | |
| ЗСВ.6 | Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных | |
| ЗСВ.7 | Контроль целостности виртуальной инфраструктуры и ее конфигураций | |
| ЗСВ.8 | Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры | |
| **IX. Обеспечение целостности информационной системы и информации (ОЦЛ)** | | |
| ОЦЛ.1 | Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации | |
| ОЦЛ.3 | Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций | |
| ОЦЛ.4 | Обнаружение и реагирование на поступление в информационную систему незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы (защита от спама) | |
| **X. Обеспечение доступности персональных данных (ОДТ)** | | |
| ОДТ.4 | Периодическое резервное копирование персональных данных на резервные машинные носители персональных данных | |
| ОДТ.5 | Обеспечение возможности восстановления персональных данных с резервных машинных носителей персональных данных (резервных копий) в течение установленного временного интервала | |
| **XII. Защита технических средств (ЗТС)** | | |
| ЗТС.2 | Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования | |
| ЗТС.3 | Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы и помещения и сооружения, в которых они установлены | |
| ЗТС.4 | Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр | |
| **XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)** | | |
| ЗИС.3 | Обеспечение защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи | |
| ЗИС.5 | Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств | |
| ЗИС.11 | Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов | |
| ЗИС.15 | Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки персональных данных | |
| ЗИС.17 | Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы | |
| ЗИС.30 | Защита мобильных технических средств, применяемых в информационной системе | |
| **XIV. Выявление инцидентов и реагирование на них (ИНЦ** | | |
| ИНЦ.1 | Определение лиц, ответственных за выявление инцидентов и реагирование на них | |
| ИНЦ.2 | Обнаружение, идентификация и регистрация инцидентов | |
| ИНЦ.3 | Своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе пользователями и администраторами | |
| ИНЦ.4 | Анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий | |
| ИНЦ.5 | Принятие мер по устранению последствий инцидентов | |
| ИНЦ.6 | Планирование и принятие мер по предотвращению повторного возникновения инцидентов | |
| **XV. Управление конфигурацией информационной системы и системы защиты персональных данных (УКФ)** | | |
| УКФ.1 | Определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и системы защиты персональных данных | |
| УКФ.2 | Управление изменениями конфигурации информационной системы и системы защиты персональных данных | |
| УКФ.3 | Анализ потенциального воздействия планируемых изменений в конфигурации информационной системы и системы защиты персональных данных на обеспечение защиты персональных данных и согласование изменений в конфигурации информационной системы с должностным лицом (работником), ответственным за обеспечение безопасности персональных данных | |
| УКФ.4 | Документирование информации (данных) об изменениях в конфигурации информационной системы и системы защиты персональных данных | |

(Тут надо что-то написать… Только вот что?)

# **3. Техническое задание на проектирование СЗИ АС**

## **3.1 Выбор технических СЗИ**

## **3.2 Техническое задание**

# **Заключение**

# **Список литературы**

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