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. Исходные данные
   * БДУ ФСТЭК;
   * Реестр Российского программного обеспечения;
   * Федеральные законы Российской Федерации;
   * Приказы Российской Федерации;
   * Методика определения угроз.
3. 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](#_Toc167820530)

[**1. Анализ объекта защиты** 5](#_Toc167820531)

[**1.1 Характеристика объекта защиты** 5](#_Toc167820532)

[**1.2 Технологический процесс обработки информации** 5](#_Toc167820533)

[**1.3 Возможные угрозы безопасности информации** 12](#_Toc167820534)

[**2. Требования по обеспечению информационной безопасности** 26](#_Toc167820535)

[**2.1 Классификация АС** 26](#_Toc167820536)

[**2.2 Состав мер по обеспечению ИБ** 27](#_Toc167820537)

[**3. Техническое задание на проектирование средств защиты информации автоматизированной системы потребительских кредитов** 49](#_Toc167820538)

[**3.1 Классификация и выбор технических средств защиты информации** 49](#_Toc167820539)

[**3.2 Техническое задание** 57](#_Toc167820540)

[**Заключение** 59](#_Toc167820541)

[**Список литературы** 60](#_Toc167820542)

[**Приложение А** 62](#_Toc167820543)

# **Введение**

Автоматизация бизнес-процессов играет ключевую роль в повышении эффективности и безопасности работы современных организаций [13]. В контексте банковского сектора, где обрабатываются большие объемы конфиденциальной информации, защита данных становится особенно важной. В 2024 году кибербезопасность остается приоритетом для бизнеса, требующим использования передовых технологий и стратегий [15].

Одной из основных задач в проектировании автоматизированных систем кредитования является обеспечение надежной защиты данных клиентов и предотвращение киберугроз [16]. Статистика Центрального Банка РФ показывает, что количество инцидентов информационной безопасности продолжает расти, что подчеркивает необходимость внедрения комплексных защитных мер [17]. Современные системы мониторинга и предотвращения утечек данных, такие как Solar Dozor, предлагают эффективные решения для управления информационными рисками [18].

Для успешного проектирования системы защиты необходимо учитывать множество факторов, включая требования к шифрованию, контроль доступа и мониторинг событий безопасности [19]. Применение интегрированных подходов к управлению идентификацией и доступом позволяет создавать надежные и устойчивые к атакам информационные системы.

**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**

Одним из ключевых аспектов применения АС является автоматизация. Далее предоставлен перечень основных задач, которые должна выполнять АС потребительских кредитов, которые могут быть автоматизированы:

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 |

Таким образом на основе данных таблицы 1 можно построить диаграммы IDEF0 которые предоставлены на рисунках 1 и 2 где, рисунок 1 свёрнутая схема IDEF0, рисунок 2 развёрнутая схема IDEF0.



Рисунок 1 – Свёрнутая схема бизнес-процесса



Рисунок 2 – Развёрнутая схема бизнес-процесса

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

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.

Определим правовой режим используя следующие документы:

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.

Для эффективного функционирования систем автоматизации и бизнес-процессов необходима ИТ-инфраструктура. На рисунке 3 приведена схема ИТ-инфраструктуры, которая показывает взаимосвязь и взаимодействие компонентов системы, таких как:

* сервер БД;
* сервер Веб-приложения
* межсетевой экран;
* маршрутизаторы;
* АРМ пользователей.

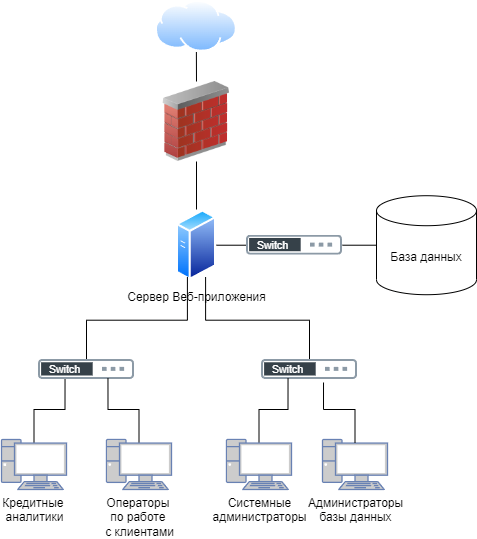


Рисунок 3 – Схема ИТ-инфраструктуры АС.

Для обеспечения работы АС необходима использовать соответствующие аппаратные и программные средства. Далее приведен перечень аппаратных и программных средств, которые используются в данной АС, в том числе используемы средств защиты информации (далее СЗИ):

Аппаратные средства:

* + сервер базы данных;
  + сервер веб-приложения;
  + системы мониторинга и защиты;
  + АРМ пользователей;

Программные средства:

* + СУБД Postgresql;
  + среда программирования Python;
  + антивирусная программа Kaspersky Endpoint Security Cloud Pro;
  + операционная система (далее ОС) Windows 10;
  + веб-приложение Python фреймворк Django.

Системы автоматизации и бизнес-процессы являются важными компонентами любой организации и взаимодействуют с различными группами пользователей. Для успешного функционирования систем автоматизации и бизнес-процессов необходимо учитывать интересы и потребности всех заинтересованных сторон. Далее приведено описание групп внешних и внутренних пользователей, которые взаимодействуют с АС.

Группы внутренних пользователей:

* 1. Администраторы системы:
     + уровень полномочий: Полный доступ к административным функциям и настройкам системы и сети;
     + 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;
     + 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;
     + 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;
     + 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 и негативных последствий от реализации УБИ характерные АС по выдаче кредитов.

Таблица 2 – Виды рисков и негативных последствий от реализации УБИ

| **№** | **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 ИТ инфраструктуры определяются следующие группы информационных ресурсов, 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 УБИ в автоматизированной системе по работе с потребительскими кредитами.

Таблица 4 – Потенциальные нарушители УБИ 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 |

Для того, чтобы обеспечить безопасность и целостность данных, необходимо знать, какие угрозы могут возникнуть и как можно им противостоять. Для этого далее предоставлен список основных способов реализации (возникновения) угроз безопасности информации.

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.

На основе этого в таблице 6 представлены актуальные способы реализации УБИ в автоматизированной системе по работе с потребительскими кредитами.

Таблица 6 – Актуальные способы реализации УБИ 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 |

Для более полного понимания возможных УБИ, которые могут возникнуть при работе с АС потребительских кредитов, далее предоставлена таблица 7. В ней перечислены возможные УБИ, негативные последствия, нарушители, которые могут реализовать определённую УБИ, объект на который нарушители могут воздействовать, и способы, как нарушители могут воздействовать на объект.

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 |

Анализ АС потребительских кредитов позволил выявить основные бизнес-процессы, которые могут быть автоматизированы, и определить информацию, которая обрабатывается в этих процессах, а также режим использования этой информации, ИТ-инфраструктуру с перечнем аппаратных и программных средств, возможных нарушителей и перечень УБИ, которые могут быть реализованы.

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

## **2.1 Классификация АС**

Класс защищенности информационной системы определяется в зависимости от уровня значимости информации, обрабатываемой в этой информационной системе, и масштаба информационной системы, который определяется по приказу правительства №1119.

Для АС потребительских кредитов был определён средний уровень защищённости (далее УЗ 2) т.к., по приказу правительства №1119 АС необходимость обеспечения 2-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из перечисленных в приказе условий. В данном случае это:

1. для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает общедоступные персональные данные более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

А также, если в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны умеренные негативные последствия в социальной, политической, международной, экономической, финансовой или иных областях деятельности и (или) информационная система и (или) оператор (обладатель информации) не могут выполнять хотя бы одну из возложенных на них функций.

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.

На основе приказа ФСТЭК России от 11 февраля 2013 г. N 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах». Класс защищенности информационной системы: К2.

Также при составлении итогового набора мер следует учитывать приказ ФСТЭК России от 18 февраля 2013 г. N 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» т.к. в АС потребительских кредитов использует персональные данные клиентов.

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

Исходя из ранее установленного уровня защищенности и класса защищённости по приказу ФСТЭК России от 11 февраля 2013 г. N 17 Был определён базовый набор мер в АС, который предоставлен в таблице 8.

Таблица 8 – Базовый набор мер защиты информации в АС

| **Идентификатор** | **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.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 |
| 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) |
| 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.2 | Управление доступом к машинным носителям информации |
| ЗНИ.5 | Контроль использования интерфейсов ввода (вывода) информации на машинные носители 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) |
| 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 доступом, 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 информации (ОДТ) | |
| ОДТ.3 | Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование |
| ОДТ.4 | Периодическое резервное копирование информации на резервные машинные носители информации |
| ОДТ.5 | Обеспечение возможности восстановления информации с резервных машинных носителей информации (резервных копий) в течение установленного временного интервала |
| ОДТ.7 | Контроль состояния и качества предоставления уполномоченным лицом вычислительных ресурсов (мощностей), в том числе по передаче информации |
| 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.4 | Управление (фильтрация, маршрутизация, контроль соединения, однонаправленная передача) потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры |
| 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 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.1 | Разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты информации, функций по обработке информации и иных функций информационной системы |
| 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.7 | Контроль санкционированного и исключение несанкционированного использования технологий мобильного кода, в том числе регистрация событий, связанных с использованием технологий мобильного кода, их анализ и реагирование на нарушения, связанные с использованием технологий мобильного кода |
| ЗИС.8 | Контроль санкционированного и исключение несанкционированного использования технологий передачи речи, в том числе регистрация событий, связанных с использованием технологий передачи речи, их анализ и реагирование на нарушения, связанные с использованием технологий передачи речи |
| ЗИС.9 | Контроль санкционированной и исключение несанкционированной передачи видеоинформации, в том числе регистрация событий, связанных с передачей видеоинформации, их анализ и реагирование на нарушения, связанные с передачей видеоинформации |
| ЗИС.11 | Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов |
| ЗИС.12 | Исключение возможности отрицания пользователем факта отправки информации другому пользователю |
| ЗИС.13 | Исключение возможности отрицания пользователем факта получения информации от другого пользователя |
| ЗИС.15 | Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки информации |
| 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.22 | Защита информационной системы от угроз безопасности информации, направленных на отказ в обслуживании информационной системы |
| ЗИС.23 | Защита периметра (физических и (или) логических границ) информационной системы при ее взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями |
| ЗИС.24 | Прекращение сетевых соединений по их завершении или по истечении заданного оператором временного интервала неактивности сетевого соединения |
| ЗИС.30 | Защита мобильных технических средств, применяемых в информационной системе |

Так же в целях адаптации базового набора мер были исключены некоторые меры, которые предоставлены в таблице 9

Таблица 9 – Исключённые базовые меры в целях адаптации.

| **Идентификатор** | **Причина исключения** |
| --- | --- |
| УПД.11 | В АС пользователям до идентификации и аутентификации запрещены любые действия кроме ввода пароля и логина |
| УПД.14 | В АС не подразумевается использование технологии беспроводного доступа |
| УПД.15 | В АС не подразумевается использование мобильных технических устройств |
| ЗСВ.1 | В АС отсутствует виртуальная среда |
| ЗСВ.2 | В АС отсутствует виртуальная среда |
| ЗСВ.3 | В АС отсутствует виртуальная среда |
| ЗСВ.4 | В АС отсутствует виртуальная среда |
| ЗСВ.6 | В АС отсутствует виртуальная среда |
| ЗСВ.7 | В АС отсутствует виртуальная среда |
| ЗСВ.8 | В АС отсутствует виртуальная среда |
| ЗСВ.9 | В АС отсутствует виртуальная среда |
| ЗСВ.10 | В АС отсутствует виртуальная среда |
| ЗИС.5 | Удаленная активация видеокамер, микрофонов и тп не предусмотрена |
| ЗИС.7 | Использование мобильного кода не предусмотрено |
| ЗИС.8 | Использование технологий передачи речи не предусмотрено |
| ЗИС.9 | Удаленная активация видеокамер не предусмотрено |
| ЗИС.20 | В АС отсутствуют беспроводные соединения |
| ЗИС.24 | В АС отсутствуют беспроводные соединения |
| ЗИС.30 | В АС отсутствуют мобильные технические средства |

После адаптации для поддержания эффективной защиты объекта от возможных угроз безопасности информации провелось уточнение мер противодействий. Результат данного уточнения приведён в таблице 10.

Таблица 10 – Уточнение мер противодействия

| **УБИ** | **Меры противодействия** |
| --- | --- |
| УБИ.008 Угроза восстановления и/или повторного использования аутентификационной информации | ИАФ.4; ИАФ.5; УПД.6; РСБ.1; РСБ.2; РСБ.3; АНЗ.5 |
| УБИ.015 Угроза доступа к защищаемым файлам с использованием обходного пути | УПД.2; УПД.3; ЗНИ.2; ЗНИ.5; АНЗ.1 |
| УБИ.031 Угроза использования механизмов авторизации для повышения привилегий | УПД.4; УПД.5; УПД.10; РСБ.1; РСБ.2; РСБ.3; АНЗ.5 |
| УБИ.067 Угроза неправомерного ознакомления с защищаемой информацией | УПД.2; УПД.3; ЗНИ.2; ЗНИ.5; АНЗ.1 |
| УБИ.068 Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением | УПД.2; УПД.3; АНЗ.1 |
| УБИ.074 Угроза несанкционированного доступа к аутентификационной информации | ИАФ.4; ИАФ.5; УПД.6; РСБ.1; РСБ.2; РСБ.3; АНЗ.5 |
| УБИ.088 Угроза несанкционированного копирования защищаемой информации | УПД.2; УПД.3; ЗНИ.2; ЗНИ.5; РСБ.1; РСБ.2; РСБ.3; АНЗ.1 |
| УБИ.090 Угроза несанкционированного создания учётной записи пользователя | УПД.1; УПД.4; УПД.5; РСБ.1; РСБ.2; РСБ.3; АНЗ.5 |
| УБИ.091 Угроза несанкционированного удаления защищаемой информации | УПД.2; УПД.3; ОЦЛ.1; ОЦЛ.3; РСБ.1; РСБ.2; РСБ.3; АНЗ.1 |
| УБИ.127 Угроза подмены действия пользователя путём обмана | УПД.2; УПД.3; ЗИС.11; АНЗ.1 |
| УБИ.140 Угроза приведения системы в состояние «отказ в обслуживании» | ЗИС.20; ЗИС.22; РСБ.1-3; АНЗ.1 |
| УБИ.157 Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации | ЗТС.2-4; ОДТ.3-5; РСБ.1-3; АНЗ.1 |

После проведения уточнения мер противодействия было выявлено, что набор мер, предоставленный по итогу адаптации, удовлетворяет всем требованиям и не требует дополнений. Однако, т.к. автоматизированная система (АС) потребительских кредитов обрабатывает персональные данные, было проведено дополнительное сравнение нормативных актов, которые регламентируют требования к защите персональных данных.

В частности, был проведен анализ Приказа ФСТЭК России от 11 февраля 2013 г. N 17 и Приказа ФСТЭК России от 18 февраля 2013 г. N 21 Этот анализ был проведен для того, чтобы проверить достаточность мер и полноту базового набора мер. Таблица 11 содержит результаты этого сравнения

Таблица 11 – Сравнение мер в приказах ФСТЭК №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.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.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.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 | 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.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 | 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.5 | Контроль использования интерфейсов ввода (вывода) информации на машинные носители 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) | 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.1 | Обнаружение вторжений |
| СОВ.2 | Обновление базы решающих правил | 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.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) | 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 информации (ОДТ)** | | | |
| ОДТ.3 | Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование |  |  |
| ОДТ.4 | Периодическое резервное копирование информации на резервные машинные носители информации | ОДТ.4 | Периодическое резервное копирование персональных данных на резервные машинные носители персональных данных |
| ОДТ.5 | Обеспечение возможности восстановления информации с резервных машинных носителей информации (резервных копий) в течение установленного временного интервала | ОДТ.5 | Обеспечение возможности восстановления персональных данных с резервных машинных носителей персональных данных (резервных копий) в течение установленного временного интервала |
| ОДТ.7 | Контроль состояния и качества предоставления уполномоченным лицом вычислительных ресурсов (мощностей), в том числе по передаче информации |  |  |
| **XI. Защита среды виртуализации (ЗСВ)** | | | |
| **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.1 | Разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты информации, функций по обработке информации и иных функций информационной системы |  |  |
| 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.11 | Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов | ЗИС.11 | Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов |
| ЗИС.12 | Исключение возможности отрицания пользователем факта отправки информации другому пользователю |  |  |
| ЗИС.13 | Исключение возможности отрицания пользователем факта получения информации от другого пользователя |  |  |
| ЗИС.15 | Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки информации | 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.17 | Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы |
| ЗИС.22 | Защита информационной системы от угроз безопасности информации, направленных на отказ в обслуживании информационной системы |  |  |
| ЗИС.23 | Защита периметра (физических и (или) логических границ) информационной системы при ее взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями |  |  |
| **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 |

В результате сравнения было выявлено что некоторые необходимые меры защиты отсутствуют в приказе ФСТЭК России от 11 февраля 2013 г. N 17, а следовательно, в таблице 12 был приведён дополненный набор мер мерами из приказа ФСТЭК России от 18 февраля 2013 г. N 21 для обеспечения защиты информации в рассматриваемой АС. Дополнение было произведено в целях увеличения защищённости АС и персональных данных, в частности.

Таблица 12 – Итоговый набор мер для обеспечения ЗИ в АС

| **Идентификатор** | **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.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 |
| 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.13 | Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети |
| 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.2 | Управление доступом к машинным носителям информации |
| ЗНИ.5 | Контроль использования интерфейсов ввода (вывода) информации на машинные носители 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) |
| 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 доступом, 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 информации (ОДТ) | |
| ОДТ.3 | Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование |
| ОДТ.4 | Периодическое резервное копирование информации на резервные машинные носители информации |
| ОДТ.5 | Обеспечение возможности восстановления информации с резервных машинных носителей информации (резервных копий) в течение установленного временного интервала |
| ОДТ.7 | Контроль состояния и качества предоставления уполномоченным лицом вычислительных ресурсов (мощностей), в том числе по передаче информации |
| XI. Защита среды виртуализации (ЗСВ) | |
| 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.1 | Разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты информации, функций по обработке информации и иных функций информационной системы |
| 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.11 | Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов |
| ЗИС.12 | Исключение возможности отрицания пользователем факта отправки информации другому пользователю |
| ЗИС.13 | Исключение возможности отрицания пользователем факта получения информации от другого пользователя |
| ЗИС.15 | Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки информации |
| ЗИС.17 | Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы |
| ЗИС.22 | Защита информационной системы от угроз безопасности информации, направленных на отказ в обслуживании информационной системы |
| ЗИС.23 | Защита периметра (физических и (или) логических границ) информационной системы при ее взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями |
| 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 |

В данной главе проведен анализ и определен уровень значимости и класс защищенности для автоматизированной системы потребительских кредитов. На основе приказа ФСТЭК России от 11 февраля 2013 г. N 17 был определен средний уровень значимости (УЗ 2) и класс защищенности К2.

Был определен базовый набор мер для обеспечения информационной безопасности в АС, который был адаптирован с учетом особенностей системы. После адаптации были проведены уточнения мер противодействия для защиты объекта от возможных угроз безопасности информации.

В результате анализа приказов ФСТЭК России от 11 февраля 2013 г. № 17 и от 18 февраля 2013 г. № 21 был выявлен ряд необходимых мер защиты, отсутствующих в приказе ФСТЭК России от 11 февраля 2013 г. № 17. В целях увеличения защищенности АС и персональных данных, в частности, был приведен дополненный набор мер мерами из приказа ФСТЭК России №21 для обеспечения защиты информации в рассматриваемой АС.

# **3. Техническое задание на проектирование средств защиты информации автоматизированной системы потребительских кредитов**

## **3.1 Классификация и выбор технических средств защиты информации**

Любая автоматизированная система, которая используется для обработки и хранения информации, требует надежной защиты от несанкционированного доступа и других угроз безопасности. Для обеспечения защиты информации применяются специальные средства, которые называются средствами защиты информации (СЗИ).

К каждому виду СЗИ существуют определенные требования, которые необходимо учитывать при их выборе и применении. Для классификации и последующего выбора технических СЗИ используется специальный документ - приказ Минкомсвязи России от 22.09.2020 №486 "Об утверждении классификатора программ для электронных вычислительных машин и баз данных".

В соответствии с этим приказом, все программные средства, используемые в сфере информационных технологий, разделены на 12 разделов:

1. Встроенное программное обеспечение.
2. Системное программное обеспечение.
3. Средства обеспечения информационной безопасности.
4. Средства разработки программного обеспечения.
5. Прикладное программное обеспечение.
6. Офисное программное обеспечение.
7. Лингвистическое программное обеспечение.
8. Промышленное программное обеспечение.
9. Средства управления процессами организации.
10. Средства обработки и визуализации массивов данных.
11. Средства анализа данных.
12. Отраслевое прикладное программное обеспечение.

В данной работе будет использоваться раздел "Средства обеспечения информационной безопасности", который содержит в себе следующие классы:

1. Средства защиты от несанкционированного доступа к информации
   * Программы, которые должны предотвращать несанкционированный доступ к информации не криптографическими методами и обеспечивать: идентификацию и аутентификацию, управление доступом, целостность, аудит (регистрацию и учет). Включает программы управления средствами (устройствами) защиты от несанкционированного доступа к информации
2. Средства управления событиями информационной безопасности
   * Программы, которые должны обеспечивать выявление и предотвращение кибератак за счет анализа в режиме реального времени событий (данных) с целью определения потенциальных угроз безопасности
3. Межсетевые экраны
   * Программы, которые должны осуществлять контроль и фильтрацию проходящих через него сетевых пакетов (в том числе в виртуальной среде) в соответствии с заданными правилами
4. Средства фильтрации негативного контента:
   * Программное обеспечение, которое должно позволять управлять доступом к различным категориям веб-сайтов, для ограничения определенного нежелательного контента, средства защиты от спама и нежелательной корреспонденции.
5. Средства защиты сервисов онлайн-платежей и дистанционного банковского обслуживания:
   * Программное обеспечение, которое должно позволять выявлять, анализировать и предотвращать мошенничество.
6. Средства антивирусной защиты:
   * Программное обеспечение, которое должно позволять обнаруживать, перехватывать и обезвреживать вредоносное программное обеспечение как в памяти устройства, так и во входящем/исходящем трафике.
7. Средства выявления и предотвращения целевых атак:
   * Программное обеспечение, которое должно обнаруживать атаки (в том числе DDoS атаки) на конкретную организацию, страну или индустрию с целью кражи данных, получения контроля над ресурсами или блокирования их работы; должно противодействовать таким атакам.
8. Средства гарантированного уничтожения данных:
   * Программное обеспечение, которое должно использовать специальные методики многократной перезаписи определенными паттернами, для минимизации вероятности восстановления информации с носителей на базе жестких магнитных дисков (HDD). Должно быть ограниченно применимо к твердотельным накопителям (SSD).
9. Средства обнаружения и предотвращения утечек информации:
   * Программы, которые должны обнаруживать утечки и предотвращать распространения охраняемой законом компьютерной информации.
10. Средства криптографической защиты информации и электронной подписи:
    * Программы, которые должны предотвращать несанкционированный доступ к информации криптографическими методами, а также управлять ключевой информацией, включая ключи электронной подписи, ключи проверки электронной подписи и ключи шифрования информации; программное обеспечение, которое предназначено для изготовления сертификатов открытых ключей и управления ими (аннулирование, приостановление, возобновление), включая служебные функции (управление списками сертификатов, подтверждение статусов сертификатов открытых ключей, сервисы доверенного времени).
11. Средства защиты каналов передачи данных, в том числе криптографическими методами:
    * Программы, которые должны обеспечивать конфиденциальность информации, передаваемой через общедоступные каналы связи.
12. Средства управления доступом к информационным ресурсам:
    * Совокупность программных или программно-аппаратных технических средств безопасности, которые должны ограничивать и регистрировать доступ к ресурсам информационной системы.
13. Средства резервного копирования:
    * Программное обеспечение, которое должно обеспечивать создание копии данных на носителе (жестком диске, твердотельных накопителях и иных носителях) и которое должно обеспечивать их восстановление в оригинальном или новом месте в случае их повреждения или утраты.
14. Средства обнаружения и/или предотвращения вторжений (атак):
    * Системы, которые должны позволять обнаруживать вторжения уровня сети, уровня узла.
15. Средства обнаружения угроз и расследования сетевых инцидентов:
    * Программное обеспечение, которое должно выявлять вредоносную активность, присутствие злоумышленников, нецелевое использование ресурсов, халатность администраторов и должно позволять расследовать сетевые инциденты информационной безопасности.
16. Средства администрирования и управления жизненным циклом ключевых носителей:
    * Программное обеспечение, которое должно обеспечивать связь между учетными записями пользователей, средствами аутентификации, приложениями и регламентами информационной безопасности.
17. Средства автоматизации процессов информационной безопасности:
    * Средства, которые должны автоматизировать процессы управления и обеспечения информационной безопасности, включая менеджмент инцидентов информационной безопасности, учет и контроль безопасности ИТ-активов, контроль соблюдения требований по безопасности, моделирование угроз и управление рисками информационной безопасности, получение и анализ данных об актуальных угрозах с целью прогнозирования вероятных кибератак и их предотвращения.
18. Средства защиты почтовых систем:
    * Программы, осуществляющие контроль и фильтрацию почтовых сообщений на наличие в них вредоносного содержания.
19. Средства защиты виртуальных сред:
    * Программы, осуществляющие защиту виртуальных машин путем контроля их операций на основном виртуальном сервере.
20. Средства защиты систем промышленной автоматизации (автоматизированных систем управления технологическими процессами):
    * Программное обеспечение, осуществляющее защиту сред управления критическими процессами и обеспечивающее безопасную передачу данных напрямую с промышленного оборудования, используя для этого общепринятые стандарты протоколов во внешние и локальные информационные системы посредством использования вычислительных ресурсов локального средства вычислительной техники.

Кроме того, в работе будут рассмотрены некоторые пункты раздела "Средства разработки программного обеспечения", которые также имеют отношение к обеспечению информационной безопасности:

1. Средства версионного контроля исходного кода:

* Программное обеспечение, которое должно позволять хранить несколько версий одного и того же документа и при необходимости возвращать к более ранним версиям и определять кем и когда были сделаны те или иные изменения.

1. Среды разработки, тестирования и отладки:

* Интегрированные программы, которые должны быть необходимыми для разработки программного обеспечения, включающие специализированное программное обеспечение, процедуры и документы.

1. Средства анализа исходного кода на закладки и уязвимости:

* Средства, которые должны позволять проводить аудит безопасности исходного кода с использованием автоматизированных средств и ручной обработки данных.

1. Системы предотвращения анализа и восстановления исполняемого кода программ:

* Программное обеспечение, которое должно позволять защищать готовые исполняемые коды программ или исходные тексты программ от их анализа и восстановления.

1. Средства обратной инженерии кода программ:

* Программное обеспечение, предназначенное для решения задач восстановления, анализа, трансформации и визуализации реализованных в программном обеспечении архитектурных решений, алгоритмов и форматов данных.

Таким образом, с помощью классификатора программ, предоставленного Минкомсвязи России, можно систематизировать и выбрать наиболее подходящие технические средства защиты информации для конкретной автоматизированной системы. Это и было сделано и представлено в таблице 13 в которой на основе данной классификации и с использованием Реестра российского программного обеспечения и Государственного реестра сертифицированных средств защиты информации были выбраны технические СЗИ.

Таблица 13 – Список технических СЗИ, классифицированных по различным подсистемам

| **Подсистема СЗИ** | **Средства ЗИ и их стоимость** | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **В1** | **Руб.** | **В2** | **Руб.** | **В3** | **Руб.** |
| Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ) | CRADLE ID (ПАО «Газпром нефть») | Договорная | CRADLE ID (ПАО «Газпром нефть») | Договорная | CRADLE ID (ПАО «Газпром нефть») | Договорная |
| Управление доступом субъектов доступа к объектам доступа (УПД) | СЗИ DALLAS LOCK 8.0‑С | 10 000 | Positive Technologies Application Firewall (PT AF) | Договорная | Аура 1.2.4 | Договорная |
| Ограничение программной среды (ОПС) | KPI MONITOR Basic | от 55 тыс  до 350 тыс | KPI MONITOR Basic | от 55 тыс  до 350 тыс | KPI MONITOR Basic | от 55 тыс  до 350 тыс |
| Защита машинных носителей информации (ЗНИ) | Блокхост-Сеть 4 (ПАО «Газпром нефть») | 10 000 | Блокхост-Сеть 4 (ПАО «Газпром нефть») | 10 000 | Блокхост-Сеть 4 (ПАО «Газпром нефть») | 10 000 |
| Регистрация событий безопасности (РСБ) | ПО Sentinel R | Договорная | EYECONT | 6000 | ПО Sentinel R | Договорная |
| Антивирусная защита (АВЗ) | Kaspersky Standard | 1709 | Kaspersky Plus | 2069 | Kaspersky Premium | 1959 |
| Обнаружение вторжений (СОВ) | Kaspersky Standard | 1709 | Kaspersky Plus | 2069 | Kaspersky Premium | 1959 |
| Контроль (анализ) защищенности информации (АНЗ) | Security Vision | от 75 000  до 240 000 | Security Vision | от 75 000  до 240 000 | Security Vision | от 75 000  до 240 000 |
| Обеспечение целостности информационной системы и информации (ОЦЛ) | SafeInspect | от 37 500  до 225 000 | SMIKS | Договорная | SMIKS | Договорная |
| Обеспечение доступности персональных данных (ОДТ) | Модуль ID | от 15 000 | ElVirtualWalking | от 8000 | Mind tracker BCI | От 20 000 |
| Защита технических средств (ЗТС) | Аккорд-АМДЗ | От 15 000 | СПРУТ! | От 25 000 | Eplat4m «Управление классификацией объектов защиты. САПУИБ-И» | От 30 000 |
| Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС) | SafeInspect | От 50 000 | SafeInspect | От 50 000 | SafeInspect | От 50 000 |
| Выявление инцидентов и реагирование на них (ИНЦ) | Integris TMS | От 70 000 | Integris TMS | От 70 000 | Integris TMS | От 70 000 |
| Управление конфигурацией информационной системы и системы защиты персональных данных (УКФ) | — | — | — | — | — | — |

После анализа и классификации технических средств защиты информации, примененных в рамках данного проекта, были выбраны наиболее эффективные средства для обеспечения безопасности системы.

Эти меры обеспечивают надежную защиту от несанкционированного доступа и утечек конфиденциальной информации, что соответствует современным стандартам безопасности данных.

Выбранные средства защиты информации не только эффективно предотвращают несанкционированный доступ к системе, но и обеспечивают контроль за целостностью и конфиденциальностью данных. Это позволяет минимизировать риски утечек информации и сохранять высокий уровень доверия пользователей к системе. Такой подход соответствует современным требованиям безопасности данных и обеспечивает стабильную и защищенную работу автоматизированной системы.

Выбранные технические средства защиты информации также обеспечивают возможность быстрого реагирования на потенциальные угрозы и инциденты безопасности. Их системы мониторинга и реагирования позволяют оперативно выявлять аномалии в работе системы и предпринимать необходимые меры по устранению уязвимостей. Такой комплексный подход гарантирует непрерывную и эффективную защиту информации.

## **3.2 Техническое задание**

В данном разделе рассматриваются основные моменты необходимые для написания технического задания, представленного в приложении А.

Цель проекта — разработка и внедрение автоматизированной системы управления кредитными операциями, которая будет обеспечивать эффективную обработку и управление информацией о кредитах в потребительском банковском секторе.

Система будет включать следующие ключевые компоненты:

* Серверная часть: Серверы для хранения и обработки данных.
* Защитные механизмы: Межсетевой экран, антивирусное ПО.
* Пользовательские интерфейсы: Рабочие станции для администраторов и операторов, а также веб-интерфейс.

Система должна предоставлять следующие функции:

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

Система должна обеспечивать высокую производительность. Также система будет построена на базе PostgreSQL для управления базами данных и будет использовать Kaspersky для защиты от вирусов и других угроз.

Реализация проекта позволит повысить эффективность обработки кредитных операций, улучшить качество обслуживания клиентов и обеспечить высокий уровень безопасности данных. Успешность проекта будет оцениваться по критериям скорости обработки заявок, надежности системы и удовлетворенности клиентов.

# **Заключение**

Анализ существующих методов и технологий защиты данных показал, что для обеспечения безопасности в автоматизированных системах выдачи кредитов необходимо использовать многоуровневый подход. Современные решения включают в себя комплексные меры для решения проблем. Наиболее эффективными являются решения, которые обеспечивают всестороннюю защиту данных как на уровне хранения, так и на уровне передачи информации.

Критерии эффективности и безопасности системы защиты были определены на основе анализа стандартов в области информационной безопасности. Основными критериями стали конфиденциальность, целостность, доступность, простота управления и мониторинга, соответствие требованиям законодательства. Эти критерии позволили провести последующую оценку безопасности и эффективности системы.

На основе проведенного анализа и определенных критериев эффективности и безопасности было спроектировано техническое задание. В техническом задании описаны требования к системе защиты данных, включая функциональные и нефункциональные требования, а также методы и средства защиты, которые будут использованы.

Выполнение поставленных задач позволило провести комплексный анализ методов и технологий защиты данных, определить ключевые критерии эффективности и безопасности, а также спроектировать техническое задание для системы защиты данных в автоматизированной системе выдачи кредитов. Эти шаги обеспечат надежную защиту информации.

# **Список литературы**

1. "ГОСТ 34.602-2020. Межгосударственный стандарт. Информационные технологии. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы // КонсультантПлюс URL: https://ac-mos.ru/about/price-expert/chatbot/market-price/download/estimate/223-ФЗ/Методика18-Р/НПА/10.%20ГОСТ%2034.602-2020.%20Межгосударственный%20стандарт.%20Информационны.pdf (дата обращения: 28.05.2024).
2. Методический документ от 5 февраля 2021 г. "МЕТОДИКА ОЦЕНКИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ" // ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ URL: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g (дата обращения: 28.05.2024).
3. Постановление Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных" // КонсультантПлюс URL: https://www.consultant.ru/document/cons\_doc\_LAW\_137356/8c86cf6357879e861790a8a7ca8bea4227d56c72/ (дата обращения: 28.05.2024).
4. Приказ № 486 «Об утверждении классификатора программ для электронных вычислительных машин и баз данных» // Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации URL: https://digital.gov.ru/ru/documents/7362/ (дата обращения: 28.05.2024).
5. Приказ ФСБ России от 10 июля 2014 г. N 378 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности" // ГАРАНТ URL: https://ivo.garant.ru/#/document/70727118/paragraph/1:0 (дата обращения: 28.05.2024).
6. Приказ ФСТЭК России от 11 февраля 2013 г. N 17 "ОБ УТВЕРЖДЕНИИ ТРЕБОВАНИЙ О ЗАЩИТЕ ИНФОРМАЦИИ, НЕ СОСТАВЛЯЮЩЕЙ ГОСУДАРСТВЕННУЮ ТАЙНУ, СОДЕРЖАЩЕЙСЯ В ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ" // ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ URL: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-11-fevralya-2013-g-n-17 (дата обращения: 28.05.2024).
7. Приказ ФСТЭК России от 18 февраля 2013 г. N 21 "ОБ УТВЕРЖДЕНИИ СОСТАВА И СОДЕРЖАНИЯ ОРГАНИЗАЦИОННЫХ И ТЕХНИЧЕСКИХ МЕР ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ" // ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ URL: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21 (дата обращения: 28.05.2024).
8. Федеральный закон "О коммерческой тайне" от 29.07.2004 N 98-ФЗ // КонсультантПлюс URL: https://www.consultant.ru/document/cons\_doc\_LAW\_48699/ (дата обращения: 28.05.2024).
9. Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ // КонсультантПлюс URL: https://www.consultant.ru/document/cons\_doc\_LAW\_61798/ (дата обращения: 28.05.2024).
10. Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ // КонсультантПлюс URL: https://www.consultant.ru/document/cons\_doc\_LAW\_61801/ (дата обращения: 28.05.2024).
11. Федеральный закон "О банках и банковской деятельности" от 02.12.1990 N 395-1 // КонсультантПлюс URL: https://www.consultant.ru/document/cons\_doc\_LAW\_5842/ (дата обращения: 28.05.2024).
12. IDEF0. Знакомство с нотацией и пример использования // trinion URL: https://www.trinion.org/blog/idef0-znakomstvo-s-notaciey-i-primer-ispolzovaniya (дата обращения: 28.05.2024).
13. Автоматизация процессов: кому нужна, кто её проводит и какие системы для неё использовать // Skillbox URL: https://skillbox.ru/media/management/avtomatizatsiya-protsessov-komu-nuzhna-kto-eye-provodit-i-kakie-sistemy-dlya-neye-ispolzovat/ (дата обращения: 28.05.2024).
14. Банк данных угроз безопасности информации // Федеральная служба по техническому и экспортному контролю URL: https://bdu.fstec.ru/threat (дата обращения: 28.05.2024).
15. Как обеспечить кибербезопасность своего бизнеса в 2024 году // РБК Компании URL: https://companies.rbc.ru/news/wUFvbgOC3l/kak-obespechit-kiberbezopasnost-svoego-biznesa-v-2024-godu/ (дата обращения: 28.05.2024).
16. Методология разработки и архитектура кредитного конвейера АПИКС в Банке ДОМ.РФ // ХАБР URL: https://habr.com/ru/companies/domrf/articles/673628/ (дата обращения: 28.05.2024).
17. Обзор отчетности об инцидентах информационной безопасности при переводе денежных средств // Банк России URL: http://cbrf.forwardsoft.ru/statistics/ib/review\_1q\_2023/ (дата обращения: 28.05.2024).
18. Как банкам защитить свои данные // SOLAR URL: https://rt-solar.ru/products/solar\_dozor/blog/3541/ (дата обращения: 28.05.2024).
19. Разработка автоматизированной информационной системы 'Выдача банком кредита' Источник: https://www.bibliofond.ru/view.aspx?id=656456 © Библиофонд // Библиофонд URL: https://www.bibliofond.ru/view.aspx?id=656456 (дата обращения: 28.05.2024).
20. РЕЕСТР РОССИЙСКОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ // РЕЕСТР РОССИЙСКОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ URL: https://reestr.digital.gov.ru/ (дата обращения: 28.05.2024).

# **Приложение А**

УТВЕРЖДАЮ:

Начальник Управления информационных технологий

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

\_\_\_\_\_\_\_\_\_\_\_ 2021 г.

**ТЕХНИЧЕСКОЕ ЗАДАНИЕ**

**на создание комплексной системы информационной безопасности ИТ инфраструктуры согласно требованиям Приказа №17 «ОБ УТВЕРЖДЕНИИ ТРЕБОВАНИЙ О ЗАЩИТЕ ИНФОРМАЦИИ, НЕ СОСТАВЛЯЮЩЕЙ ГОСУДАРСТВЕННУЮ ТАЙНУ, СОДЕРЖАЩЕЙСЯ В ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ»**

**1. Заказчик** – Кредитная организация «KsaCredit» (г. Омск, ул. Петра Некрасова, д. 10).

**2. Исполнитель договора** на создание комплексной системы информационной безопасности ИТ инфраструктуры согласно требованиям Приказа №17 «ОБ УТВЕРЖДЕНИИ ТРЕБОВАНИЙ О ЗАЩИТЕ ИНФОРМАЦИИ, НЕ СОСТАВЛЯЮЩЕЙ ГОСУДАРСТВЕННУЮ ТАЙНУ, СОДЕРЖАЩЕЙСЯ В ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ», определяется по итогам проведения конкурсных процедур.

**3. Период действия договора** – до момента исполнения обязательств по договору.

**4. Цель и основные требования:**

4.1. В целях предотвращения неправомерного доступа к информации, обрабатываемой объектами критической информационной инфраструктуры Кредитной организации «KsaCredit»:

* создание в Кредитной организации «KsaCredit» подсистемы информационной безопасности значимых объектов автоматизированной системы (далее по тексту ПИБ АС);
* соблюдение требования действующего законодательства Российской Федерации к защите АС.

**5. Состав и содержание работ (действий)**

Создание ПИБ АС должны включать в себя следующие работы (действия):

* разработка проектной и эксплуатационной документации на ПИБ АС;
* внедрение ПИБ АС;
* разработка внутренней документации, регламентирующей вопросы обеспечения информационной безопасности АС;
* аттестация ПИБ АС.

**6. Порядок оформления и предъявления Заказчику результатов работ (действий).**

По завершении работ (действий), указанных в п. 4.1. настоящего технического задания, Исполнитель предоставляет Заказчику необходимую отчетную документацию. Полный перечень отчетных документов представлен в разделе 11 настоящего технического задания.

Сдача отчетной документации осуществляется путем предоставления в согласованный срок результата работ в бумажном виде в 1 экземпляре и оформляется сторонами актом приема-передачи документации или накладной о передаче документации.

Вся документация должна быть выполнена на русском языке.

6.1. Объект информатизации Кредитная организация «KsaCredit» эксплуатирует АС по следующим адресам:

г. Омск, ул. Петра Некрасова, д. 10.

**7. Назначение и цели создания системы**

7.1. Цели создания ПИБ АС

Основными целями создания ПИБ АС являются:

* выполнение требований нормативных правовых актов Российской Федерации, руководящих документов ФСТЭК России, ФСБ России, регламентирующих вопросы защиты информации;
* защита АС и иной конфиденциальной информации, обрабатываемых техническими средствами, от хищения, утраты, утечки, уничтожения, искажения, подделки и блокирования доступа за счёт комплексного использования организационных, программных, программно-аппаратных средств и мер защиты;
* обнаружение вторжений и предотвращение инцидентов в области информационной безопасности;
* реагирование на компьютерные инциденты и принятие мер по ликвидации последствий компьютерных атак на объекты АС в соответствии с требованиями нормативно-правовых актов и Российской Федерации по взаимодействию субъектов АС с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

7.2. Цели проектирования ПИБ АС

Целью разработки проектной и эксплуатационной документации является определение вида и структуры ПИБ АС её количественных и качественных показателей, параметров настройки СЗИ, а также разработка необходимой документации для последующей эксплуатации ПИБ.

7.3. Цели аттестации ПИБ АС

Целью аттестации ПИБ АС является оценка эффективности реализованных в рамках подсистемы информационной безопасности мер защиты информации.

**8. Общая характеристика АС КО «KsaCredit»**

К АС КО «KsaCredit» подключены автоматизированные рабочие места (далее по тексту АРМ) различных информационных и автоматизированных систем, представляющие из себя IBM PC - совместимый компьютер. Данные АРМ могут быть выполнены в следующих исполнениях:

* системный блок форм-фактора ATX, mATX;

В качестве операционной системы (далее по тексту ОС) АРМ могут выступать все ОС семейства Windows для рабочих станций.

Также к АС КО «KsaCredit» подключены серверы (не более 15 шт.), функционирующие как в режиме физических серверов, так и виртуальных.

АС КО «KsaCredit» установлен 2 (второй) уровень значимости. Категорирование осуществлялось в соответствии с требованиями Приказа №17 «ОБ УТВЕРЖДЕНИИ ТРЕБОВАНИЙ О ЗАЩИТЕ ИНФОРМАЦИИ, НЕ СОСТАВЛЯЮЩЕЙ ГОСУДАРСТВЕННУЮ ТАЙНУ, СОДЕРЖАЩЕЙСЯ В ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ».

Для целей защиты информации КО «KsaCredit» использует следующие СЗИ, имеющие сертификат, выданный Федеральной службы по техническому и экспортному контролю (далее по тексту ФСТЭК):

1. С целью обеспечения защиты от несанкционированного доступа эксплуатируются СЗИ «DALLAS LOCK 8.0‑С» (Х шт.) подключенные к единому серверу безопасности СЗИ «DALLAS LOCK 8.0‑С»

2. Антивирусную защиту обеспечивает СЗИ «Kaspersky Standard» (лицензия на Х узлов)

**9. Требования к созданию АС**

9.1. Требования руководящих документов ФСТЭК России, ФСБ России.

В соответствии с «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утвержденными приказом ФСТЭК России №17, при установленном 2 уровне защищенности, итоговым набором мер по обеспечению безопасности для АС будут являться меры, приведённые в таблице 9.1.

**Таблица 9.1** – Итоговый набор мер для 2 уровня значимости

| **Идентификатор** | **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.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 |
| 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.13 | Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети |
| 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.2 | Управление доступом к машинным носителям информации |
| ЗНИ.5 | Контроль использования интерфейсов ввода (вывода) информации на машинные носители 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) |
| 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 доступом, 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 информации (ОДТ) | |
| ОДТ.3 | Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование |
| ОДТ.4 | Периодическое резервное копирование информации на резервные машинные носители информации |
| ОДТ.5 | Обеспечение возможности восстановления информации с резервных машинных носителей информации (резервных копий) в течение установленного временного интервала |
| ОДТ.7 | Контроль состояния и качества предоставления уполномоченным лицом вычислительных ресурсов (мощностей), в том числе по передаче информации |
| XI. Защита среды виртуализации (ЗСВ) | |
| 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.1 | Разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты информации, функций по обработке информации и иных функций информационной системы |
| 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.11 | Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов |
| ЗИС.12 | Исключение возможности отрицания пользователем факта отправки информации другому пользователю |
| ЗИС.13 | Исключение возможности отрицания пользователем факта получения информации от другого пользователя |
| ЗИС.15 | Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки информации |
| ЗИС.17 | Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы |
| ЗИС.22 | Защита информационной системы от угроз безопасности информации, направленных на отказ в обслуживании информационной системы |
| ЗИС.23 | Защита периметра (физических и (или) логических границ) информационной системы при ее взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями |
| 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 |

9.2. Требования к системе в целом

Для реализации дополненного уточненного адаптированного базового набора мер по обеспечению защиты информации Исполнитель должен создать ПИБ АС и выполнить ряд дополнительных технических мероприятий.

9.3. Требования к структуре и функционированию ПИБ АС

9.3.1. Требования к составу

Для создания ПИБ АС, необходимо дополнить, актуализировать и, при необходимости, создать следующие подсистемы, используя поставляемый Исполнителем Товар (см. раздел 12):

* + - Идентификация и аутентификация (ИАФ);
    - Управление доступом (УПД);
    - Ограничение программной среды (ОПС);
    - Защита машинных носителей информации (ЗНИ);
    - Регистрация событий безопасности (РСБ);
    - Антивирусная защита (АВЗ);
    - Обнаружение вторжений (СОВ);
    - Контроль (анализ) защищенности информации (АНЗ);
    - Обеспечение целостности информационной системы и информации (ОЦЛ);
    - Обеспечение доступности информации (ОДТ);
    - Защита технических средств (ЗТС);
    - Защита информационной (автоматизированной) системы и ее компонентов (ЗИС);
    - Выявление инцидентов и реагирование на них (ИНЦ);
    - Управление конфигурацией информационной системы и системы защиты персональных данных (УКФ).

9.3.2. Требования к взаимосвязи между подсистемами и компонентами, смежными подсистемами являются:

* + - внешние сети передачи данных;
    - внешние информационные системы.

Решения по подключению смежных подсистем должны соответствовать действующим государственным стандартам в области связи и телекоммуникаций и требованиями ФСТЭК России и ФСБ России.

9.3.3. Перспективы развития, модернизации ПИБ АС

ПИБ должна позволять, не снижая свою функциональность, поэтапно увеличивать количество защищаемых АРМ, серверов и сетевых устройств.

9.3.4. Требования к режимам функционирования системы

Компоненты ПИБ АС должны функционировать одновременно с функционированием АС.

9.3.5. Требования к надёжности

Элементы ПИБ АС должны удовлетворять условию круглосуточной работы, а также иметь возможность восстановления в случаях сбоев.

9.4. Требования безопасности

9.4.1. Требования по обеспечению радиоэлектронной безопасности

Требования по обеспечению радиоэлектронной безопасности при монтаже, наладке, эксплуатации, обслуживании и ремонте технических средств определяются ГОСТ-12.1.006-84 «Система стандартов безопасности труда. Электромагнитные поля радиочастот».

9.4.2. Требования к эргономике и технической эстетике

Разрабатываемая ПИБ не должна вносить значительных задержек в работу пользователей АРМ и серверов КО «KsaCredit».

Программные и программно-аппаратные СЗИ должны обладать интуитивно-понятным интерфейсом управления.

9.5. Требования к эксплуатации, техническому обслуживанию

Климатические условия в помещениях с размещенными техническими средствами, на которых функционирует ПИБ АС должны соответствовать климатическим условиям, установленным производителями технических средств.

Эксплуатация и техническое обслуживание средств защиты информации в составе ПИБ АС должны осуществляться в соответствии с эксплуатационной и технической документацией.

9.6. Требования к патентной чистоте

Программные и аппаратно-программные средства, приобретаемые у сторонних организаций, должны сопровождаться документацией, подтверждающей правомочность этих организаций поставлять данную продукцию и сопровождаться лицензионным соглашением.

9.7. Требования по стандартизации

Используемые в составе ПИБ средства защиты информации должны иметь соответствующие сертификаты ФСТЭК и/или ФСБ России.

В качестве схемы сертификации указанных ниже компонент защитных подсистем должна быть выбрана схема серийной сертификации.

9.8. Требования к организационному обеспечению

Должна быть разработана проектная и эксплуатационная документация, а также документы, регламентирующие организационные и организационно-технические вопросы информационной безопасности (перечень необходимых документов приведён в разделе 9).

9.9. Требования к лингвистическому обеспечению

Язык взаимодействия пользователей и администраторов с компонентами ПИБ АС должен быть русским.

9.10. Требования к выполнению организационных мероприятий

Дополнительные организационные и технические мероприятия должны включать в себя разработку регламентов по обеспечению информационной безопасности.

9.11. Требования к разработке регламентов по обеспечению информационной безопасности

Регламенты по обеспечению информационной безопасности должны быть разработаны в соответствии со следующими нормативными документами:

* + - Приказ ФСТЭК России от 11 февраля 2013 г. N 17 «ОБ УТВЕРЖДЕНИИ ТРЕБОВАНИЙ О ЗАЩИТЕ ИНФОРМАЦИИ, НЕ СОСТАВЛЯЮЩЕЙ ГОСУДАРСТВЕННУЮ ТАЙНУ, СОДЕРЖАЩЕЙСЯ В ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ»;
    - Приказ ФСТЭК России от 18 февраля 2013 г. N 21 «ОБ УТВЕРЖДЕНИИ СОСТАВА И СОДЕРЖАНИЯ ОРГАНИЗАЦИОННЫХ И ТЕХНИЧЕСКИХ МЕР ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ»;
    - Федеральный закон от 27 июля 2006 г. N 149-ФЗ «ОБ ИНФОРМАЦИИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЯХ И О ЗАЩИТЕ ИНФОРМАЦИИ»;
    - Федеральный закон от 27 июля 2006 г. N 152-ФЗ «О ПЕРСОНАЛЬНЫХ ДАННЫХ»;
    - Постановление Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных".

При разработке регламентов должны учитываться индивидуальные особенности информационных систем Заказчика.

**10. ТРЕБОВАНИЯ К СОЗДАНИЮ ПИБ АС**

10.1. Общие требования

При создании ПИБ АС:

* определяются типы субъектов доступа и объектов доступа, являющихся объектами защиты;
* определяются методы управления доступом, типы доступа и правила разграничения доступа субъектов доступа к объектам доступа, подлежащие реализации в АС;
* адаптируется базовый набор мер по обеспечению безопасности для АС. При этом допускается исключение из базового набора мер защиты информации тех мер, которые связаны с обеспечением защиты технологий, не используемых Заказчиком;
* уточняется адаптированный набор мер по обеспечению безопасности для АС. При этом, в данный набор мер могут быть включены меры из изначального списка мер, которые не были отмечены базовыми для третьей категории значимости объекта КИИ (таблица 10.1);
* дополняется уточнённый адаптированный набор мерами, определяемыми иными нормативно-правовыми актами или необходимостью усиления данного набора;
* выбираются меры защиты информации, подлежащие реализации в подсистеме защиты информации АС;
* определяются виды и типы средств защиты информации, обеспечивающие реализацию технических мер защиты информации;
* определяется структура подсистемы защиты информации АС включая состав (количество) и места размещения её элементов;
* осуществляется выбор средств защиты информации, сертифицированных на соответствие требованиям по безопасности информации, с учётом их стоимости, совместимости с информационными технологиями и техническими средствами, функций безопасности этих средств и особенностей их реализации, а также класса защищенности АС;
* определяются параметры настройки программного обеспечения, включая программное обеспечение средств защиты информации, обеспечивающие реализацию мер защиты информации, а также устранение возможных уязвимостей АС, приводящих к возникновению угроз безопасности информации;
* определяются меры защиты информации при информационном взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями.

**11.Требования к документированию**

11.1. Требования к документированию работ (действий) по разработке проектной и эксплуатационной документации на ПИБ АС.

Результаты проектирования ПИБ АС должны быть отражены в проектной документации (техническом проекте) на АС, разрабатываемой с учетом ГОСТ 34.201 «Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем» (далее – ГОСТ 34.201). Эксплуатационная документация на ПИБ АС должна быть разработана с учетом ГОСТ 34.601, ГОСТ 34.201 и ГОСТ Р 51624 и должна, в том числе, содержать описание:

* структуры ПИБ АС;
* состава, мест установки, параметров и порядка настройки средств защиты информации, программного обеспечения и технических средств;
* правил эксплуатации ПИБ АС.

11.2 Требования к документированию работ (действий) по разработке внутренней документации, регламентирующей вопросы обеспечения информационной безопасности

При разработке внутренней документации, регламентирующей вопросы обеспечения информационной безопасности, должны быть выполнены работы (действия) по:

1. Регламентации правил и процедур ИАФ.
2. Регламентации правил и процедур УПД.
3. Регламентации правил и процедур ОПС.
4. Регламентации правил и процедур ЗНИ.
5. Регламентации правил и процедур РБС.
6. Регламентации правил и процедур АВЗ.
7. Регламентации правил и процедур СОВ.
8. Регламентации правил и процедур АНЗ.
9. Регламентации правил и процедур ОЦЛ.
10. Регламентации правил и процедур ОДТ.
11. Регламентации правил и процедур ЗТС.
12. Регламентации правил и процедур ЗИС.
13. Регламентации правил и процедур ИНЦ.
14. Регламентации правил и процедур УКФ.

Результатом данных работ должны стать проекты соответствующих нормативных документов.

11.3 Требования к документированию работ (действий) по аттестации ПИБ АС

В результате выполнения работ по аттестации ПИБ АС должны быть разработаны следующие документы:

* технический паспорт;
* программа и методики аттестационных испытаний;
* протокол аттестационных испытаний;
* заключение по результатам аттестации;
* аттестат соответствия.

Указанные документы должны быть разработаны с учётом требования ГОСТ РО 0043-003-2012 Защита информации. Аттестация объектов информатизации.

**12.СОСТАВ И СОДЕРЖАНИЕ ПОСТАВЛЯЕМОГО ТОВАРА**

12.1. Товар, поставляемый для дополнения и актуализации существующей системы защиты информации для построения ПИБ АС:

Таблица 12.1 – Товар, поставляемый для дополнения и актуализации существующей СЗИ.

|  |  |  |  |
| --- | --- | --- | --- |
| № | Наименование | Ед. изм. | Кол-во |
| ПИБ АС | | | |
| 1 | Positive Technologies Application Firewall | шт | 1 |
| 2 | KPI MONITOR Basic | шт | 1 |
| 3 | EYECONT | шт | 1 |
| 4 | Kaspersky Plus | шт | 16 |
| 5 | Security Vision | шт | 1 |
| 6 | SafeInspect | шт | 1 |
| 7 | Windows | шт | 16 |

12.2 Описание Positive Technologies Application Firewall

Специализированное программное или аппаратное решение, предназначенное для защиты веб-приложений от различных видов кибератак и обеспечения безопасности данных.

Основные функции:

* Защита от OWASP Top 10: PT AF обеспечивает защиту от наиболее распространённых угроз веб-приложений, перечисленных в OWASP Top 10, включая SQL-инъекции, XSS-атаки, CSRF и другие;
* Анализ трафика: Система анализирует весь входящий и исходящий трафик в режиме реального времени, выявляя и блокируя подозрительные запросы;
* Контроль доступности: PT AF помогает обеспечивать доступность веб-приложений, предотвращая атаки типа DDoS;
* Проверка данных: Решение проверяет входные данные на наличие вредоносного кода, предотвращая эксплуатацию уязвимостей.

Архитектура и компоненты:

* Модуль защиты веб-приложений: Основной компонент, который отвечает за анализ и фильтрацию трафика, а также за выявление и блокировку атак;
* Логирование и отчетность: PT AF ведет детальный журнал всех событий безопасности, что позволяет отслеживать инциденты и анализировать их причины;
* Интеграция с SIEM: Система может интегрироваться с решениями для управления событиями и информацией безопасности (SIEM) для более эффективного мониторинга и реагирования на инциденты;
* Поддержка различных протоколов: PT AF поддерживает множество веб-протоколов и технологий, таких как HTTP, HTTPS, SOAP, REST и другие.

Преимущества:

* Высокая производительность: PT AF разработан для работы в условиях высоких нагрузок, обеспечивая минимальную задержку и высокую скорость обработки трафика;
* Легкость в развертывании: Решение легко интегрируется в существующую инфраструктуру, не требуя значительных изменений;
* Обновления и поддержка: Positive Technologies регулярно выпускает обновления для PT AF, включая новые правила и сигнатуры для защиты от новых видов атак;
* Поддержка пользовательских правил: Администраторы могут создавать и настраивать собственные правила безопасности для удовлетворения специфических требований организации.

12.3 Описание KPI MONITOR Basic

Программное решение для мониторинга ключевых показателей эффективности (KPI) бизнеса, предназначенное для упрощения процесса сбора, анализа и визуализации данных.

Основные функции:

* Сбор данных: Автоматический сбор данных из различных источников, включая базы данных, CRM-системы, ERP-системы и другие бизнес-приложения;
* Анализ показателей: Возможность проведения анализа KPI в режиме реального времени для оценки текущего состояния бизнеса;
* Визуализация данных: Интерактивные дашборды и отчеты, которые позволяют пользователям визуализировать данные в удобном для восприятия виде;
* Настройка KPI: Пользователи могут настраивать и добавлять свои собственные ключевые показатели эффективности в зависимости от потребностей бизнеса;
* Уведомления и оповещения: Настраиваемые уведомления о достижении определенных KPI или при возникновении отклонений от плановых показателей.

Архитектура и компоненты:

* Модуль сбора данных: отвечает за интеграцию с различными источниками данных и их автоматический сбор;
* Модуль анализа: обеспечивает обработку и анализ собранных данных для вычисления KPI;
* Модуль визуализации: предоставляет инструменты для создания дашбордов и отчетов, а также для интерактивного анализа данных;
* Модуль уведомлений: позволяет настраивать и отправлять уведомления пользователям при достижении критических значений KPI.

Преимущества:

* Простота использования: интуитивно понятный интерфейс позволяет быстро освоить работу с системой даже неподготовленным пользователям;
* Гибкость и масштабируемость: Система легко адаптируется под нужды различных организаций и может масштабироваться по мере роста бизнеса;
* Снижение затрат: Автоматизация процесса мониторинга KPI позволяет сократить затраты на ручной сбор и анализ данных;
* Улучшение принятия решений: Регулярный мониторинг и анализ ключевых показателей эффективности помогают руководству принимать обоснованные решения.

12.4 Описание EYECONT

Система для мониторинга и анализа видеонаблюдения, предназначенная для повышения уровня безопасности и улучшения управления объектами.

Основные функции:

* Видеомониторинг в реальном времени: EYECONT обеспечивает возможность просмотра видеопотоков с камер наблюдения в реальном времени, что позволяет оперативно реагировать на происходящие события;
* Анализ видеоданных: Система использует алгоритмы искусственного интеллекта для анализа видеоданных, выявления подозрительных действий и распознавания лиц;
* Архивирование видео: Запись видеопотоков и их хранение в архиве для последующего анализа и расследования инцидентов;
* Уведомления и оповещения: Настраиваемые уведомления и оповещения о выявленных инцидентах, отправляемые через SMS, email или другие средства связи;
* Интеграция с другими системами: Возможность интеграции с системами управления доступом, пожарной сигнализацией и другими системами безопасности.

Архитектура и компоненты:

* Модуль видео захвата: отвечает за получение видеопотоков с камер наблюдения и их передачу в систему;
* Модуль анализа: использует алгоритмы машинного обучения и компьютерного зрения для анализа видеоданных и выявления аномалий;
* Модуль архивирования: обеспечивает запись и хранение видеопотоков, а также быстрый доступ к архивным записям;
* Модуль уведомлений: настраиваемая система уведомлений, позволяющая оперативно информировать ответственных лиц о выявленных инцидентах;
* Интерфейс пользователя: интуитивно понятный интерфейс для управления системой, просмотра видеопотоков, анализа данных и настройки параметров.

Преимущества:

* Высокий уровень безопасности: EYECONT позволяет оперативно выявлять и реагировать на подозрительные действия, предотвращая возможные угрозы;
* Интеллектуальный анализ: Использование передовых алгоритмов искусственного интеллекта для анализа видеоданных обеспечивает высокую точность выявления инцидентов;
* Гибкость и масштабируемость: Система может быть адаптирована под нужды различных организаций и легко масштабируется по мере роста количества камер и объема данных;
* Экономия времени и ресурсов: Автоматизация процесса мониторинга и анализа видеоданных снижает нагрузку на сотрудников службы безопасности и повышает их эффективность.

12.5 Описание Kaspersky Plus

Многофункциональное антивирусное программное обеспечение, предоставляемое компанией Kaspersky Lab, которое обеспечивает комплексную защиту от различных видов киберугроз. Основные функции и возможности Kaspersky Plus включают:

Антивирусная защита:

* Обнаружение и удаление вирусов, троянов, червей, шпионского ПО, рекламного ПО и других типов вредоносных программ;
* Проактивная защита от новых и неизвестных угроз с использованием облачных технологий и машинного обучения.

Защита интернет-серфинга:

* Блокировка опасных веб-сайтов, фишинговых ссылок и загрузок вредоносного ПО;
* Расширения для браузеров, которые предупреждают о подозрительных сайтах и блокируют их.

Защита электронной почты:

* Проверка входящих и исходящих сообщений на наличие вредоносных вложений и фишинговых ссылок;
* Фильтрация спама и нежелательных писем.

Защита конфиденциальных данных:

* Функции шифрования данных и файлов для предотвращения несанкционированного доступа;
* Инструменты для безопасного удаления данных без возможности их восстановления.

Менеджер паролей:

* Хранение паролей в зашифрованном виде и автоматическое заполнение форм авторизации;
* Генерация надежных паролей для различных учетных записей.

Сетевой экран (файрволл):

* Защита компьютера от сетевых атак и несанкционированного доступа;
* Контроль сетевого трафика и предотвращение утечек данных.

Преимущества Kaspersky Plus:

* Высокий уровень обнаружения и блокировки угроз;
* Интуитивно понятный интерфейс и простота в использовании;
* Низкая нагрузка на систему, что обеспечивает быструю работу компьютера;
* Интеграция с облачными сервисами для повышения эффективности защиты.

12.6 Описание Security Vision

Интегрированное программное обеспечение для мониторинга безопасности информационных систем и реагирования на угрозы в реальном времени. Основной целью Security Vision является обеспечение комплексной защиты информации и выявление потенциальных угроз для оперативного реагирования на них.

Мониторинг безопасности:

* Security Vision осуществляет непрерывный мониторинг событий и активности в информационной системе, включая аудит доступа, сетевой трафик, аномалии в поведении пользователей и уязвимости системы;
* Он анализирует данные с различных источников, таких как журналы событий, сенсоры безопасности, системы регистрации и аутентификации, чтобы выявлять подозрительные действия.

Обнаружение угроз:

* Security Vision использует алгоритмы машинного обучения и анализ поведения для выявления потенциально опасных сценариев и атак;
* Он определяет аномальное поведение пользователей, необычные сетевые пакеты, попытки несанкционированного доступа и другие угрозы.

Анализ уязвимостей:

* Программное обеспечение Security Vision проводит сканирование и анализ уязвимостей в системе, включая открытые порты, необходимость обновлений программного обеспечения и конфигурационные ошибки;
* Оно предоставляет отчеты о выявленных уязвимостях и рекомендации по их устранению для повышения уровня безопасности.

Управление инцидентами:

* Security Vision автоматически классифицирует инциденты по уровню угрозы и приоритету;
* Он предоставляет средства для быстрого реагирования на инциденты, включая оповещения, блокировку атак, изоляцию уязвимых устройств и сбор доказательств для дальнейшего анализа.

Аналитика и отчетность:

* Программное обеспечение обеспечивает аналитику событий и трендов в области безопасности для выявления улучшений и оптимизации стратегий защиты;
* Оно генерирует отчеты о происшествиях, статистику по уровню безопасности, эффективность действий по обнаружению и реагированию на угрозы.

Интеграция с другими системами:

* Security Vision интегрируется с другими системами безопасности, такими как межсетевые экраны, системы обнаружения вторжений (IDS), антивирусные программы и системы аутентификации для обеспечения единой и централизованной защиты.

12.7 Описание SafeInspect

Программное обеспечение для обеспечения безопасности и контроля качества в производственных и промышленных предприятиях. Оно предоставляет инструменты для мониторинга производственных процессов, выявления потенциальных угроз и опасностей, а также обеспечения соответствия стандартам безопасности и качества. Вот основные аспекты и возможности SafeInspect:

Инспекции и аудиты:

* Проведение регулярных инспекций и аудитов по стандартам безопасности, качества и соблюдению нормативных требований;
* Оценка состояния оборудования, рабочих мест, производственных процессов и соблюдения правил безопасности труда.

Управление рисками:

* Оценка рисков и угроз для работников, оборудования и окружающей среды;
* Разработка и реализация мер по снижению рисков и предотвращению несчастных случаев.

Мониторинг и анализ данных:

* Отслеживание параметров производственных процессов и сбор данных о безопасности и качестве;
* Анализ данных для выявления тенденций, аномалий и потенциальных проблем.

Управление инцидентами:

* Регистрация и анализ инцидентов, несчастных случаев и аварий;
* Разработка планов действий по реагированию на инциденты и минимизации последствий.

Обучение и тренинги:

* Проведение обучающих мероприятий и тренингов по безопасности, качеству и соблюдению стандартов;
* Подготовка сотрудников к правильной работе с оборудованием и соблюдению процедур безопасности.
* Соблюдение нормативов и стандартов:
* Обеспечение соответствия производственных процессов и условий труда требованиям законодательства, стандартов качества и безопасности;
* Поддержка сертификации и аттестации предприятия по стандартам безопасности и качества.

SafeInspect является важным инструментом для обеспечения безопасности труда, контроля качества и соблюдения стандартов в производственных и промышленных компаниях. Он помогает снижать риски производственных аварий, повышать эффективность работы и обеспечивать безопасные условия труда для сотрудников.

12.8 Возможности операционной системы Windows

Операционная система Windows предоставляет ряд возможностей в области информационной безопасности (ИБ), включая:

Аутентификация и управление учетными записями:

* Возможности управления пользователями и группами для ограничения доступа к ресурсам;
* Встроенные средства аутентификации, такие как пароли, PIN-коды, Windows Hello для биометрической аутентификации.

Шифрование данных:

* BitLocker для шифрования дисков и защиты данных на уровне диска;
* Encrypting File System (EFS) для шифрования отдельных файлов и папок.

Брандмауэр и сетевая безопасность:

* Встроенный брандмауэр для контроля сетевого трафика и защиты от внешних атак;
* Средства управления сетевыми подключениями и настройки безопасности Wi-Fi.

Антивирусная защита и защита от вредоносного ПО:

* Windows Security (ранее Windows Defender) для защиты от вирусов, троянов, шпионского ПО и других угроз;
* Защита от нежелательных приложений и приложений с подозрительным поведением.

Обновления и патчи безопасности:

* Автоматические обновления операционной системы и приложений для исправления уязвимостей безопасности;
* Центр обновлений для управления обновлениями и патчами безопасности.

Управление политиками безопасности:

* Групповые политики (Group Policies) для установки требований безопасности на уровне домена или компьютера;
* Windows Defender Application Control (ранее Device Guard) для управления запуском приложений и предотвращения выполнения вредоносного ПО.

Аудит безопасности и мониторинг событий:

* Средства аудита безопасности для записи событий аудита и мониторинга действий пользователей и системы;
* Windows Event Viewer для анализа журналов событий и выявления потенциальных угроз.

Виртуализация и изоляция приложений:

* Windows Sandbox для запуска приложений в изолированной среде и безопасного тестирования;
* Windows Virtual Desktop для виртуализации рабочих окружений и обеспечения безопасного доступа к приложениям.

Средства управления и мониторинга устройств:

* Microsoft Intune для управления мобильными устройствами и применения политик безопасности;
* Windows Defender Advanced Threat Protection (ATP) для обнаружения и реагирования на угрозы на уровне конечных точек.

Эти возможности позволяют организациям и пользователям Windows обеспечивать высокий уровень информационной безопасности и защиты от различных угроз.

ПРОВЕРИЛ:

Начальник службы информационной безопасности и системного администрирования

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

ПОДГОТОВИЛ:

Начальник отдела информационной безопасности

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_