|  |
| --- |
| Национальный медицинский исследовательский центр  имени В. А. Алмазова  Федеральное государственное бюджетное учреждение  «НМИЦ им. В. А. Алмазова» Минздрава России |
| Модель угроз безопасности информации  «НМИЦ им. В. А. Алмазова» |
|  |
| г. Москва  2023 г. |

Содержание

[1. ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ 4](#_Toc154515405)

[2. ОБЩИЕ ПОЛОЖЕНИЯ 5](#_Toc154515406)

[2.1. Назначение и область действия документа 5](#_Toc154515407)

[2.2. Нормативные правовые акты, методические документы, национальные стандарты, используемые для оценки угроз безопасности информации и разработки модели угроз 6](#_Toc154515408)

[3. Наименование обладателя информации, заказчика, оператора систем и сетей 7](#_Toc154515409)

[Правомерными обладателями информации, средствами обработки и хранения информации являются акционеры 7](#_Toc154515410)

[3.1. Подразделения, должностные лица, ответственные за обеспечение защиты информации (безопасности) систем и сетей 7](#_Toc154515411)

[Ответственность за обеспечение защиты информации (безопасности) систем и сетей возлагается на руководителей должностных подразделений Управления Информационной Безопасностью; работников, ответственных за администрирование сегментов информационной телекоммуникационной системы 7](#_Toc154515412)

[3.2. Наименование организации, привлекаемой для разработки модели угроз безопасности информации (при наличии) 7](#_Toc154515413)

[Сотрудники сторонних организаций к разработке модели угроз не привлекаются. 7](#_Toc154515414)

[4. ОПИСАНИЕ СИСТЕМ И СЕТЕЙ И ИХ ХАРАКТЕРИСТИКА КАК ОБЪЕКТОВ ЗАЩИТЫ 8](#_Toc154515415)

[4.1. Наименование систем и сетей, для которых разработана модель угроз безопасности информации 8](#_Toc154515416)

[4.2. Класс защищенности, категория значимости систем и сетей, уровень защищенности персональных данных 8](#_Toc154515417)

[4.3. Нормативные правовые акты Российской Федерации, в соответствии с которыми создаются и (или) функционируют системы и сети 8](#_Toc154515418)

[4.4. Назначение, задачи (функции) систем и сетей, состав обрабатываемой информации и ее правовой режим 8](#_Toc154515419)

[4.5. Основные процессы обладателя информации, для обеспечения которых создаются (функционируют) системы и сеты 12](#_Toc154515420)

[4.6. Описание групп внешних и внутренних пользователей систем и сетей, уровней их полномочий и типов доступа (в состав групп пользователей включается все пользователи, для которых требуется авторизация при доступе к информационным ресурсам, и пользователи, для которых не требуется авторизация) 13](#_Toc154515421)

[4.7. Описание функционирования систем и сетей на базе информативно-телекоммуникационной инфраструктуры центра обработки данных или облачной инфраструктуры 14](#_Toc154515422)

[4.8. Описание модели предоставления вычислительных услуг, распределения ответственности за защиту информации между обладателями информации, оператором и поставщиком вычислительных услуг 15](#_Toc154515423)

[4.9. Описание условий использования информационно-телекоммуникационной инфраструктуры обработки данных или облачной инфраструктуры поставщика услуг (при наличии) 15](#_Toc154515424)

[5. ВОЗМОЖНЫЕ НЕГАТИВНЫЕ ПОСЛЕДСТВИЯ РЕАЛИЗАЦИИ (ВОЗНИКНОВЕНИЯ) УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ. ВОЗМОЖНЫЕ ОБЪЕКТЫ ВОЗДЕЙСТВИЯ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ. ИСТОЧНИКИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ. СПОСОБЫ РЕАЛИЗАЦИИ (ВОЗНИКНОВЕНИЯ) УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАИИ 16](#_Toc154515425)

[6. АКТУАЛЬНЫЕ УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ 18](#_Toc154515426)

[7. ПЕРЕЧЕНЬ АКТУАЛЬНЫХ УГРОЗ И ВЕКТОРЫ АТАКИ 19](#_Toc154515427)

# ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

|  |  |  |
| --- | --- | --- |
| АИС | – | Автоматизированная информационная система |
| БД | – | База данных |
| ИСПДн | – | Информационная система персональных данных |
| ЛВС | – | Локальная вычислительная сеть |
| НСД | – | Несанкционированный доступ |
| ОС | – | Операционная система |
| ПДн | – | Персональные данные |
| ПО | – | Программное обеспечение |

# ОБЩИЕ ПОЛОЖЕНИЯ

# Назначение и область действия документа

Документ модели угроз Организации ФГБУ «НМИЦ им. В. А. Алмазова» Минздрава России (далее — Центра) определяет потенциальные уязвимости и риски информационной безопасности, а также предлагает стратегии и меры по их минимизации. Он служит руководством для разработки, внедрения и поддержания системы управления информационной безопасностью в Центре.

Область действия документа может включать все информационные системы, ресурсы и данные Центра, включая физические, цифровые и сетевые активы. Это может включать информацию, хранящуюся на компьютерах, серверах, мобильных устройствах, в базах данных, в облачных сервисах и в других местах.

Документ также описывает специфические угрозы, характерные для отрасли или сферы деятельности Центра, и предлагать специфические подходы к защите информации, соответствующие этим угрозам. Кроме того, документ может содержать рекомендации по обучению персонала, формированию культуры информационной безопасности и проведению аудита безопасности.

Автоматизированная информационная среда организации включает в себя множество элементов, таких как:

1. Информационные системы — программное обеспечение, которое используется для хранения, обработки и передачи информации. Примеры включают системы управления базами данных, ERP-системы, CRM-системы и другие;
2. Информационные технологии — это технологии, которые используются для обработки, передачи и хранения информации. Примеры включают компьютеры, сервера, сети, мобильные устройства и т.д.;
3. Данные — это информация, которая хранится в информационных системах. Это могут быть текстовые файлы, изображения, видео, аудио и другие форматы;
4. Процессы — последовательность действий, которые выполняются для достижения определенной цели. Примеры включают процессы управления, процессы разработки программного обеспечения, процессы поддержки клиентов и т.д.;
5. Люди — это сотрудники организации, которые работают с информационными системами и технологиями. Они могут быть администраторами, разработчиками, пользователями и другими;
6. Политика безопасности — правила и процедуры, которые регулируют использование информационных систем и технологий в организации;
7. Физическая инфраструктура — здания, помещения, оборудование и другие элементы, которые обеспечивают функционирование информационной среды организации.

# Нормативные правовые акты, методические документы, национальные стандарты, используемые для оценки угроз безопасности информации и разработки модели угроз

Разработка технологических, организационных требований к информационной безопасности Организации осуществляется на основании следующих нормативных документов Российской Федерации:

1. Федеральный закон от 27 июля 2006 г. N 149-ФЗ “Об информации, информационных технологиях и о защите информации”;
2. Федеральный закон от 27 июля 2006 г. N 152-ФЗ “О персональных данных”;
3. Методика оценки угроз безопасности информации ФСТЭК России, утвержденная ФСТЭК России 5 февраля 2021 г;
4. “Требования к системам обнаружения вторжений” (ФСТЭК России от 06.12.2011 N 638. ДСП);
5. “Требования к средствам антивирусной защиты” (ФСТЭК России от 20.03.2012 N 28. ДСП);
6. “Требования к средствам доверенной загрузки” (ФСТЭК России от 27.09.2013 N 119. ДСП);
7. “Требования к межсетевым экранам” (ФСТЭК России от 09.02.2016 N 9. ДСП);

# **Наименование обладателя информации, заказчика, оператора систем и сетей**

Правомерными обладателями информации, средствами обработки и хранения информации являются акционеры Центра.

# **Подразделения, должностные лица, ответственные за обеспечение защиты информации (безопасности) систем и сетей**

Ответственность за обеспечение защиты информации (безопасности) систем и сетей возлагается на руководителей должностных подразделений Управления Информационной Безопасностью; работников, ответственных за администрирование сегментов информационной телекоммуникационной системы Центра; работников службы мониторинга информационной безопасности; сотрудников организации.

# **Наименование организации, привлекаемой для разработки модели угроз безопасности информации (при наличии)**

Сотрудники сторонних организаций к разработке модели угроз не привлекаются.

# ОПИСАНИЕ СИСТЕМ И СЕТЕЙ И ИХ ХАРАКТЕРИСТИКА КАК ОБЪЕКТОВ ЗАЩИТЫ

# Наименование систем и сетей, для которых разработана модель угроз безопасности информации

Модель угроз безопасности информации разработана для следующих систем и сетей:

* Система управления предприятием (ERP);
* Система управления взаимоотношениями с клиентами (CRM);
* Информационная система управления проектами (PM);
* Электронная почта и обмен сообщениями.

# Класс защищенности, категория значимости систем и сетей, уровень защищенности персональных данных

Для каждой из перечисленных в п. 4.1 систем и сетей определен класс защищенности, категория значимости и уровень защищенности персональных данных. Эти параметры определяются в соответствии с требованиями законодательства и нормативных актов в области информационной безопасности.

# Нормативные правовые акты Российской Федерации, в соответствии с которыми создаются и (или) функционируют системы и сети

Модель угроз Центра разработана в соответствии с положениями Федерального закона от 27.07.2006 № 152-ФЗ “О персональных данных”.

# Назначение, задачи (функции) систем и сетей, состав обрабатываемой информации и ее правовой режим

Назначение и задачи систем и сетей определяются их функциональностью и целями, для которых они были созданы. Состав обрабатываемой информации также определяется функциональностью систем и может включать различные типы данных, такие как текстовые, графические, аудио- и видеофайлы, а также различные форматы документов. Правовой режим информации определяется законодательством и нормативными актами в области защиты информации.

Система управления предприятием предназначена для автоматизации процессов управления предприятием, включая управление ресурсами, планирование, контроль выполнения задач, анализ результатов и принятие решений на основе полученных данных.

Функции системы управления предприятием включают:

* Управление ресурсами: планирование, распределение и контроль использования ресурсов предприятия;
* Планирование: разработка планов и стратегий развития предприятия, а также контроль их выполнения;
* Контроль выполнения задач: мониторинг выполнения задач и проектов, выявление отклонений и принятие мер по их устранению;
* Анализ результатов: оценка эффективности работы предприятия, анализ данных и принятие решений на основе полученной информации;
* Принятие решений: формирование и реализация решений на основе анализа данных и оценки результатов деятельности предприятия.

Система управления предприятием (ERP) обрабатывает следующие типы информации:

* Данные о ресурсах предприятия (сотрудники, оборудование, материалы и т.д.);
* Планы и бюджеты предприятия;
* Заказы и контракты с клиентами;
* Отчеты о выполнении планов и проектов;
* Информация о финансовых операциях и учете;
* Данные об управлении качеством продукции и процессов;
* Интеграционные процессы с другими системами и партнерами.

Система управления взаимоотношениями с клиентами предназначена для автоматизации процесса управления отношениями с клиентами, включая сбор и анализ информации о клиентах, управление контактами, продажами и маркетинговыми кампаниями.

Основные функции системы управления взаимоотношениями с клиентами:

* Сбор и анализ информации о клиентах: система позволяет собирать информацию о клиентах из различных источников и анализировать ее для принятия решений о стратегии взаимодействия с каждым клиентом;
* Управление контактами: система предоставляет инструменты для управления контактной информацией о клиентах, включая контактные данные, историю взаимодействия и предпочтения клиентов;
* Продажи и маркетинг: система помогает автоматизировать процесс продаж и маркетинговых кампаний, предоставляя инструменты для планирования и анализа результатов маркетинговых активностей, а также для управления продажами;
* Интеграция с другими системами: система может быть интегрирована с другими бизнес-системами, такими как системы управления ресурсами предприятия или системы управления проектами, для обеспечения более эффективного управления взаимоотношениями с клиентами.

Система управления взаимоотношения с клиентами (CRM) обрабатывает следующую информацию:

* Данные о клиентах (имя, адрес, телефон, email и т.д.);
* История взаимодействия с клиентами (звонки, письма, встречи и т.д.);
* Информация о сделках и продажах (сумма, дата, товар и т.д.);
* Маркетинговые данные (акции, скидки, рекламные кампании и т.д.);
* Аналитика по продажам и маркетингу (отчеты, графики, статистика и т.д.).

Информационная система управления проектами предназначена для автоматизации управления проектами, включая планирование, контроль и анализ выполнения проектов.

Система предоставляет следующие функции:

* Планирование проектов: позволяет создавать планы проектов, определять этапы и задачи, устанавливать сроки и ресурсы;
* Контроль выполнения проектов: обеспечивает мониторинг хода выполнения проектов, отслеживание задач и ресурсов, выявление проблем и отклонений от плана;
* Анализ результатов проектов: предоставляет инструменты для оценки эффективности проектов, анализа затрат и выгод, выявления резервов и возможностей улучшения;
* Интеграция с другими системами: позволяет интегрироваться с другими информационными системами, такими как ERP, CRM и др., для обеспечения эффективного обмена данными и совместной работы над проектами.

Информационная система управления проектами (PM) обрабатывает информацию о следующих аспектах:

* Данные о проектах: название, цель, сроки, бюджет, участники и т.д.;
* Планы проектов: этапы, задачи, ресурсы, риски и т.д.;
* Ход выполнения проектов: статус задач, проблемы, отклонения и т.д.;
* Результаты проектов: достигнутые цели, затраты, выгоды и т.д.;
* Интеграция с другими системами для обмена данными и координации работы.

Система электронной почты и обмена сообщениями обеспечивает пользователям возможность обмениваться электронными письмами и другими видами сообщений, такими как текстовые сообщения, мгновенные сообщения, файлы и т. д.

Основными функциями системы являются:

* Отправка и получение электронных писем: пользователи могут отправлять и получать электронные письма, используя различные адреса электронной почты;
* Хранение и организация сообщений: система хранит все отправленные и полученные сообщения, позволяя пользователям легко находить и организовывать их;
* Шифрование и защита данных: система обеспечивает шифрование сообщений для защиты конфиденциальной информации от несанкционированного доступа;
* Поддержка различных протоколов: система поддерживает различные протоколы обмена сообщениями, что позволяет пользователям взаимодействовать с другими системами и сервисами;
* Интеграция с другими системами: систему можно интегрировать с другими приложениями и сервисами для обмена сообщениями и совместной работы.

Система электронной почты и обмена сообщениями обрабатывает следующую информацию:

* Электронные письма: текст, вложения, адреса отправителя и получателя;
* Текстовые сообщения: текст, время отправки и получения;
* Мгновенные сообщения: текст, участники беседы, история сообщений;
* Файлы: документы, изображения, аудио и видео файлы;
* Настройки пользователей и системы: параметры почты, аккаунты, пароли.

# Основные процессы обладателя информации, для обеспечения которых создаются (функционируют) системы и сеты

Определены следующие процессы работы внутри Центра, для обеспечения которых внедряются и функционируют существующие и новые ИС:

* Заключение договоров страхования

Процесс включает в себя сбор информации о страхователе, объекте страхования и рисках, оценку рисков и заключение договора страхования;

* Обработка страховых случаев и андеррайтинг  
  Процесс начинается с получения заявления от страхователя, проведения расследования и принятия решения о выплате страхового возмещения или отказе в выплате;
* Управление активами  
  Инвестирование страховых резервов и обеспечение их доходности;
* Маркетинг и продажи  
  Этот процесс включает разработку и реализацию маркетинговых стратегий, привлечение новых клиентов и продажу страховых продуктов;
* Управление персоналом  
  Набор, обучение и развитие сотрудников, а также управление корпоративной культурой и мотивацией персонала;
* Финансовый учет и отчетность  
  Этот процесс включает подготовку финансовой отчетности в соответствии с международными стандартами финансовой отчетности и предоставление ее регуляторам и акционерам;
* Внутренний контроль и аудит  
  Процесс направлен на обеспечение эффективности и результативности деятельности страховой компании, а также на предотвращение мошенничества и других нарушений;
* Юридическая поддержка  
  Обеспечивает юридическое сопровождение деятельности компании, включая консультирование по вопросам законодательства, представительство в судах и разрешение споров.

# Описание групп внешних и внутренних пользователей систем и сетей, уровней их полномочий и типов доступа (в состав групп пользователей включается все пользователи, для которых требуется авторизация при доступе к информационным ресурсам, и пользователи, для которых не требуется авторизация)

Таблица 1 – Описание основных групп пользователей

|  |  |  |
| --- | --- | --- |
| **Группа пользователей** | **Уровень полномочий** | **Тип доступа к ИР** |
| Администраторы ИСПДн | Полный технический доступ к ИСПДн | Полный доступ - пользователь имеет возможность выполнять все операции в системе |
| Операторы ИСПДн | Согласно ранее утвержденной модели разграничения доступа в соответствующей ИСПДн | Ограниченный доступ - пользователь может выполнять только определенные операции, указанные в его правах доступа |
| Потребители ИСПДн | Согласно ранее утвержденной модели разграничения доступа в соответствующей ИСПДн | Ограниченный доступ - пользователь может выполнять только определенные операции, указанные в его правах доступа |
| Сотрудники служб ИБ | По согласованию с владельцами ИСПДн и других заинтересованных лиц | Временный доступ - доступ предоставляется на определенный период времени и автоматически прекращается по истечении этого срока |
| Обслуживающий персонал | По согласованию с владельцами ИСПДн и других заинтересованных лиц | Гостевой доступ - предоставляет пользователю ограниченный набор возможностей для просмотра информации |
| Клиенты Организации | Не предусмотрено | Не предусмотрено |

# Описание функционирования систем и сетей на базе информативно-телекоммуникационной инфраструктуры центра обработки данных или облачной инфраструктуры

Системы и сети, работающие на базе ЦОД и облачной инфраструктур, функционируют следующим образом:

* Система управления предприятием: осуществляет сбор, обработку и анализ данных о работе предприятия, планирует ресурсы и контролирует выполнение задач. Размещение в ЦОД Организации;
* Система управления взаимоотношениями с клиентами: собирает и анализирует информацию о клиентах, управляет контактами и продажами, проводит маркетинговые кампании. Размещение в ЦОД;
* Информационная система управления проектами: планирует проекты, контролирует их выполнение и анализирует результаты. Размещение в ЦОД Организации;
* Система электронной почты: обеспечивает обмен электронными сообщениями между пользователями. Размещение в ЦОД Организации.

# Описание модели предоставления вычислительных услуг, распределения ответственности за защиту информации между обладателями информации, оператором и поставщиком вычислительных услуг

Обладатель информации (Центр) заключает договор с оператором (компанией, предоставляющей вычислительные услуги), который, в свою очередь, заключает договор с поставщиком вычислительных услуг (ЦОД или облачной инфраструктурой).

Обладатель информации несет ответственность за защиту конфиденциальной информации, оператор - за предоставление вычислительных услуг и интеграцию с информационными системами обладателя информации, поставщик вычислительных услуг - за обеспечение функционирования инфраструктуры и выполнение требований по защите информации.

# Описание условий использования информационно-телекоммуникационной инфраструктуры обработки данных или облачной инфраструктуры поставщика услуг (при наличии)

Размещение ИСПДн или систем хранения ПД в облачной инфраструктуре компаний-провайдеров облачных решение должно строго регулировать и согласовываться с управлением информационной безопасности на этапе планирования проектов.

# ВОЗМОЖНЫЕ НЕГАТИВНЫЕ ПОСЛЕДСТВИЯ РЕАЛИЗАЦИИ (ВОЗНИКНОВЕНИЯ) УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ. ВОЗМОЖНЫЕ ОБЪЕКТЫ ВОЗДЕЙСТВИЯ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ. ИСТОЧНИКИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ. СПОСОБЫ РЕАЛИЗАЦИИ (ВОЗНИКНОВЕНИЯ) УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Таблица 2 – Описание внешних и внутренних нарушителей ИБ Центра

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **№ п/п** | **Группа нарушителей** | **Функциональные обязанности** | **Вид/категория нарушителя/возможности нарушителя** | **Виды воздействия/негативные последствия** | **Угрозы** | **Цели реализации угроз** | **Описание способов реализации угроз (описание интерфейсов объектов воздействия)** |
| 1 | Администраторы ИСПДн | Поддержание системы в рабочем состоянии, разрешение типовых и нетиповых проблем, формирование отчетов, проведение анализа и проверки работоспособности ПО | Внутренний нарушитель.  Владение прямым полным доступом. Обладает полной технической информацией о системе. | Возможное нарушение целостности, конфиденциальности и доступности ИС. | Несанкционированное применение прав для нанесения вреда Организации. Передача данных третьи лицам. Ошибки при использовании, настройке и эксплуатации ИС. | Непреднамеренные, неосторожные или неквалифицированные действия. Личная обида. | Внедрение ВПО, извлечение данных, нарушение целостности данных, повреждение ИС, реализация уязвимостей ИС. |
| 2 | Операторы ИСПДн | Ведение непосредственной рабочей деятельности в ПО, внесение/изменение/удаление данных, согласно должностной инструкции | Внутренний нарушитель. Обладает ограниченным доступом. Владеет технической информацией о системе. | Возможное нарушение конфиденциальности данных ИС. | Несанкционированное применение прав для нанесения вреда Организации.  Передача данных третьи лицам. Ошибки при использовании, настройке и эксплуатации ИС. | Непреднамеренные, неосторожные или неквалифицированные действия. Личная обида. | Извлечение данных, нарушение целостности данных, повреждение ИС, реализация уязвимостей ИС. |
| 3 | Потребители ИСПДн | Группа лиц, использующих данные, передаваемые и обрабатываемые ИС | Внутренний нарушитель.  Может обладать информацией, согласно согласованному временному доступу. | Возможное нарушение конфиденциальности данных ИС. | Передача данных третьи лицам. Ошибки при использовании, настройке и эксплуатации ИС. | Непреднамеренные, неосторожные или неквалифицированные действия. Личная обида. | Извлечение данных, нарушение целостности данных, повреждение ИС, реализация уязвимостей ИС. |
| 4 | Сотрудники служб ИБ | Обеспечение соблюдения норм ИБ, нормативных актов на должном уровне | Внутренний нарушитель.  Может обладать информацией, согласно согласованному временному доступу. | Возможное нарушение целостности, конфиденциальности и доступности ИС. | Несанкционированное применение прав для нанесения вреда Организации.  Передача данных третьи лицам. Ошибки при использовании, настройке и эксплуатации ИС. | Непреднамеренные, неосторожные или неквалифицированные действия. Личная обида. | Извлечение данных, нарушение целостности данных, повреждение ИС. |
| 5 | Обслуживающий персонал | Обеспечение физической работоспособности ИС, поддержка рабочего пространства и посещения | Внутренний нарушитель.  Не обладает доступом и технической информацией. | Нарушение целостности, доступности данных ИС. | Ошибки при использовании, настройке и эксплуатации ИС. | Непреднамеренные, неосторожные или неквалифицированные действия. Личная обида. | Извлечение данных, нарушение целостности данных, повреждение ИС. |
| 6 | Клиенты Организации | Потребление готовых данных без непосредственного доступа в ИС | Внешний нарушитель.  Не обладает доступом и технической информацией. | Возможное нарушение целостности, конфиденциальности и доступности ИС. | Ошибки при использовании, настройке и эксплуатации ИС. | Непреднамеренные, неосторожные или неквалифицированные действия. Личная обида. | Повреждение целостности данных. |
| 7 | Злоумышленники | Нанесение вреда Организации с целью извлечения материальной выгоды | Внешний нарушитель.  Не обладает доступом и технической информацией. | Возможное нарушение целостности, конфиденциальности и доступности ИС. | Несанкционированное направленное действие для нанесения вреда Организации. | Направленные действия, направленные на извлечение личной выгоды. | Внедрение ВПО, извлечение данных, нарушение целостности данных, повреждение ИС, реализация уязвимостей ИС. |

# АКТУАЛЬНЫЕ УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Согласно п.6 Требований к защите персональных данных при их обработке в ИСПДн, утвержденных постановлением Правительства РФ от 01.11.2012 №1119, установлены 3 типа актуальных угроз безопасности персональных данных. Самый низкий тип угроз – третий, самый высокий – первый.

Актуальной считается угроза, которая может быть реализована в ИСПДн и представляет опасность для персональных данных. Подход к составлению перечня актуальных угроз состоит в следующем. Для оценки возможности реализации угрозы применяются два показателя:

Y₁ - уровень исходной защищенности ИСПДн;

Y₂ - частота (вероятность) реализации рассматриваемой угрозы.

Коэффициент реализуемости угрозы Y определяться соотношением:

Y = (Y₁ + Y₂ )/ 20 .

если 0 ≤ Y ≤ 0.3, то возможность реализации угрозы признается низкой;

если 0.3 < Y ≤ 0.6, то возможность реализации угрозы признается средней;

если 0.6 < Y ≤ 0.8, то возможность реализации угрозы признается высокой;

если Y < 0.8, то возможность реализации угрозы признается очень высокой.

Далее оценивается опасность каждой угрозы. При оценке опасности угроз безопасности персональных данных на основе опроса экспертов (специалистов в области защиты информации) определяется вербальный показатель опасности для рассматриваемой ИСПДн. Этот показатель имеет три значения:

* Низкая опасность – если реализация угрозы может привести к незначительным негативным последствиям для субъектов персональных данных;
* Средняя опасность – если реализация угрозы может привести к негативным последствиям для субъектов персональных данных;
* Высокая опасность – если реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных.

Таблица 3 – Описание актуальных угроз информационной безопасности

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Угроза | Вероятность | Реализуемость | Опасность | Актуальность |
| Угроза использования альтернативных путей доступа к ресурсам | Низкая (1) | Низкая (2) | Низкая | Неактуальна |
| Угроза использования слабостей протоколов сетевого/локального обмена данными | Средняя (3) | Низкая (1) | Низкая | Неактуальна |
| Угроза исчерпания вычислительных ресурсов хранилища больших данных | Средняя (5) | Низкая (1) | Средняя | Неактуальна |
| Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети | Низкая (0.5) | Низкая (0) | Низкая | Неактуальна |
| Угроза межсайтовой подделки запроса | Средняя (5) | Средняя (6) | Средняя | Актуальна |
| Угроза использования уязвимых версий программного обеспечения | Высокая (7) | Высокая (9) | Очень высокая | Актуальна |
| Угроза «фишинга» | Высокая (7) | Высокая (9) | Очень высокая | Актуальна |
| Угроза «кражи» учётной записи доступа к сетевым сервисам | Средняя (5) | Высокая (7) | Высокая | Актуальна |
| Угроза повышения привилегий | Низкая (2) | Низкая (2) | Низкая | Неактуальна |
| Угроза определения топологии вычислительной сети | Низкая (1) | Низкая (0) | Низкая | Неактуальна |
| Угроза определения типов объектов защиты | Низкая (2) | Низкая (0) | Низкая | Неактуальна |
| Угроза утечки пользовательских данных при использовании функций автоматического заполнения аутентификационной информации в браузере | Средняя (6) | Средняя (6) | Высокая | Актуальна |
| Угроза хищения обучающих данных | Средняя (4) | Низкая (2) | Средняя | Неактуальна |
| Угроза использования скомпрометированного доверенного источника обновлений программного обеспечения | Средняя (5) | Низкая (2) | Средняя | Неактуальна |
| Угроза обхода многофакторной аутентификации | Низкая (3) | Средняя (4) | Средняя | Актуальна |
| Угроза подмены модели машинного обучения | Низкая (2) | Низкая (1) | Низкая | Неактуальна |

# ПЕРЕЧЕНЬ АКТУАЛЬНЫХ УГРОЗ И ВЕКТОРЫ АТАКИ

Ниже перечислены все обозначенные актуальными угрозы информационной безопасности по спецификации ФСТЭК, а также приведены векторов атаки из рекомендаций OWASP.

1. **Угроза межсайтовой подделки запроса (УБИ. 042)**Угроза заключается в возможности отправки нарушителем дискредитируемому пользователю ссылки на содержащий вредоносный код веб-ресурс, при переходе на который автоматически будут выполнены неправомерные вредоносные действия от имени дискредитированного пользователя.

Данная угроза обусловлена уязвимостями браузеров, которые позволяют выполнять действия без подтверждения или аутентификации со стороны дискредитируемого пользователя.

Реализация угрозы возможна в случае, если дискредитируемый пользователь сохраняет аутентификационную информацию с помощью браузера.  
Атаки типа "межсайтовый скриптинг" (XSS) возникают, когда:

Данные попадают в веб-приложение через недоверенный источник, чаще всего через веб-запрос.

Эти данные включаются в динамическое содержимое, которое отправляется пользователю без проверки на наличие вредоносного содержимого.

Вредоносное содержимое, отправляемое в браузер, часто имеет вид фрагмента JavaScript, но может включать и HTML, Flash или любой другой код, который может быть выполнен браузером. Разнообразие атак, основанных на XSS, практически безгранично, но обычно они включают в себя передачу злоумышленнику приватных данных, таких как Cookies или другой информации о сеансе, перенаправление жертвы на контролируемый злоумышленником веб-контент или выполнение других вредоносных операций на машине пользователя под видом уязвимого сайта.

1. **Угроза использования уязвимых версий программного обеспечения (УБИ 192)**Угроза заключается в возможности осуществления нарушителем деструктивного воздействия на систему путём эксплуатации уязвимостей программного обеспечения. Данная угроза обусловлена слабостями механизмов анализа программного обеспечения на наличие уязвимостей. Реализация данной угрозы возможна при отсутствии проверки перед применением программного обеспечения на наличие в нем уязвимостей или использованием программного обеспечения, поддержка которого была прекращена производителе.

Компоненты, как правило, работают с теми же привилегиями, что и само приложение, поэтому дефекты в любом компоненте могут привести к серьезным последствиям. Такие недостатки могут быть как случайными (например, ошибка в кодировании), так и преднамеренными (например, наличие "черного хода" в компоненте). В качестве примеров обнаруженных уязвимостей компонентов можно привести следующие:

Существуют автоматизированные инструменты, помогающие злоумышленникам находить непропатченные или неправильно сконфигурированные системы. Например, поисковая система Shodan IoT поможет найти устройства, которые все еще страдают от уязвимости Heartbleed, исправленной в апреле 2014 года.

1. **Угроза “фишинга” (УБИ 175)**  
   Угроза заключается в возможности неправомерного ознакомления нарушителем с защищаемой информацией (в т.ч. идентификации/аутентификации) пользователя путём убеждения его с помощью методов социальной инженерии (в т.ч. посылкой целевых писем (т.н. spear-phishing attack), с помощью звонков с вопросом об открытии вложения письма, имитацией рекламных предложений (fake offers) или различных приложений (fake apps)) зайти на поддельный сайт (выглядящий одинаково с оригинальным), на котором от дискредитируемого пользователя требуется ввести защищаемую информацию или открыть заражённое вложение в письме.

Данная угроза обусловлена недостаточностью знаний пользователей о методах и средствах «фишинга».

Реализация данной угрозы возможна при условии наличия у нарушителя:

сведений о конкретных сайтах, посещаемых пользователем, на которых требуется ввод защищаемой информации; средств создания и запуска поддельного сайта; сведений о контактах пользователя с доверенной организацией (номер телефона, адрес электронной почты и др.).

Для убеждения пользователя раскрыть информацию ограниченного доступа (или открыть вложение в письмо) наиболее часто используются поддельные письма от администрации какой-либо организации, с которой взаимодействует пользователь.  
Фишинг предполагает кражу данных, например пароля пользователя, которые злоумышленник может использовать для проникновения в сеть. Злоумышленники получают доступ к этим данным, обманом вынуждая жертву раскрыть их. Фишинг остается одним из наиболее часто используемых векторов атак - например, многие атаки с целью получения выкупа начинаются с фишинговой кампании против организации-жертвы.

1. **Угроза “кражи” учётной записи доступа к сетевым сервисам (УБИ 168)**  
   Угроза заключается в возможности неправомерного ознакомления нарушителем с защищаемой информацией пользователя путём получения информации идентификации/аутентификации, соответствующей учётной записи доступа пользователя к сетевым сервисам (социальной сети, облачным сервисам и др.), с которой связан неактивный/несуществующий адрес электронной почты.

Данная угроза обусловлена недостаточностью мер контроля за активностью/существованием ящиков электронной почты.

Реализация данной угрозы возможна при условиях: наличия статуса «свободен для занимания» у адреса электронной почты, с которым связана учётная запись доступа пользователя к сетевым сервисам (например, если пользователь указал при регистрации несуществующий адрес или долго не обращался к почтовому ящику, вследствие чего, его отключили); наличия у нарушителя сведений об адресе электронной почты, с которым связана учётная запись дискредитируемого пользователя для доступа к сетевым сервисам.  
Злоумышленник приобретает имена пользователей и пароли в результате взлома сайта, фишинговой атаки, на сайте "дампа" паролей.

1. С помощью автоматизированных инструментов злоумышленник проверяет украденные учетные данные на многих сайтах (например, в социальных сетях, на онлайн-площадках или в веб-приложениях).
2. Если вход в систему проходит успешно, злоумышленник понимает, что у него есть набор действительных учетных данных.
3. Теперь злоумышленник знает, что у него есть доступ к учетной записи. Возможные дальнейшие действия включают:
4. Снятие с украденного счета накопленных ценностей или совершение покупок.
5. Получение доступа к конфиденциальной информации, такой как номера кредитных карт, личные сообщения, фотографии или документы.
6. Использование учетной записи для рассылки фишинговых сообщений или спама.

Продажа известных валидных учетных данных одного или нескольких взломанных сайтов для использования другими злоумышленниками.

1. **Угроза утечки пользовательских данных при использовании функций автоматического заполнения аутентификационной информации в браузере (УБИ 201)**Угроза заключается в возможности утечки пользовательских данных за счет использования реализованной в браузерах функции автоматического заполнение форм авторизации.

Реализация данной угрозы обусловлена хранением в браузерах в открытом виде пользовательских данных, используемых для автозаполнения форм авторизации.

Реализация данной угрозы возможна при условии, что пользователь использует браузер, в котором реализована и активирована функция автоматического заполнения форм авторизации.

1. **Угроза обхода многофакторной аутентификации (УБИ 213)**Угроза заключается в возможности обхода многофакторной аутентификации путем внедрения вредоносного кода в дискредитируемую систему и компоненты, участвующие в процедуре многофакторной аутентификации.

Данная угроза обусловлена: наличием уязвимостей программного обеспечения; слабостями мер антивирусной защиты и разграничения доступа.

Реализация данной угрозы возможна: в случае работы дискредитируемого пользователя с файлами, поступающими из недоверенных источников; при наличии у него привилегий установки программного обеспечения.