|  |  |  |  |
| --- | --- | --- | --- |
|  | НИЯУ МИФИ | | |
|  | |  |  |
| Мисикс  Модель угроз информационной безопасности  Версия 1.00 | | | |
| **СОГЛАСОВАНО** | |  | **Представители организации Разработчика** |
| Должность  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Х.Х. ХХХХ  (личная подпись) (расшифровка подписи)  «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_2021 г | |  | Должность  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Х.Х. ХХХХ  (личная подпись) (расшифровка подписи)  «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_2021 г |
|  | |  |  |
|  | |  |  |
|  | |  |  |
| 2021 | | | |

|  |  |
| --- | --- |
|  |  |
|  | |
| Мисикс  Модель угроз информационной безопасности  Листов 66  Версия 1.00 | |
| 2021 | |

**Аннотация**

В данном документе описывается модель угроз и модель нарушителя информационной безопасности информационной системы управления правами на результаты интеллектуальной деятельности (ИС).

Модель угроз информационной безопасности является основой для определения состава необходимых режимных, организационно-технических и технических мер защиты ИС.

Модель угроз информационной безопасности ИС содержит:

* описание ИС;
* описание модели нарушителя информационной безопасности ИС;
* перечень угроз информационной безопасности (с привязкой к потенциальным нарушителям) ИС;
* меры по противодействию угрозам информационной безопасности в ИС.

**СОДЕРЖАНИЕ**

[1. Общие сведения 11](#_Toc70703207)

[1.1. Перечень документов на основании которых создается модель угроз информационно безопасности 11](#_Toc70703208)

[1.2. Назначение модели угроз информационной безопасности 11](#_Toc70703209)

[2. сведения оБ объекте защите 11](#_Toc70703210)

[2.1. Назначение создаваемой Системы 11](#_Toc70703211)

[2.2. Структура Системы и ее основные характеристики 11](#_Toc70703212)

[2.2.1. Структура создаваемой Системы 12](#_Toc70703213)

[2.2.2. Местонахождение технических средств Системы и перечень физических лиц, имеющих к ним доступ 13](#_Toc70703214)

[2.2.3. Режим разграничения прав доступа пользователей Системы 13](#_Toc70703215)

[2.2.4. Подключение Системы к сетям связи общего пользования и (или) сетям международного информационного обмена 14](#_Toc70703216)

[2.3. Информация, обрабатываемая в Системе 14](#_Toc70703217)

[2.3.1. Персональные данные 15](#_Toc70703218)

[2.3.2. Конфиденциальная информация 15](#_Toc70703219)

[2.4. Перечень защищаемых ресурсов Системы и их уровень конфиденциальности 15](#_Toc70703220)

[2.5. Исходный уровень защищенности Системы 17](#_Toc70703221)

[2.6. Основные данные о создаваемой системе 18](#_Toc70703222)

[3. Модель нарушителей информационной безопасности 20](#_Toc70703223)

[3.1. Внешние нарушители 20](#_Toc70703224)

[3.2. Внутренние нарушители 20](#_Toc70703225)

[3.2.1. Категории ввнутреннего нарушителя информационной безопасности 20](#_Toc70703226)

[3.2.2. Предположения о средствах реализации угроз внутренним нарушителем 21](#_Toc70703227)

[3.2.3. Каналы, используемые внутренним нарушителем для доступа к защищаемым ресурсам Системы и способы атак 21](#_Toc70703228)

[4. Модель угроз информационной безопасности 22](#_Toc70703229)

[4.1. Потенциальные угрозы безопасности 22](#_Toc70703230)

[4.2. Детальное описание угроз 23](#_Toc70703231)

[4.2.1. Источник угроз: Внутренние. Угроза: субъективная. Возможная деятельность потенциальных внутренних нарушителей 23](#_Toc70703232)

[4.3. Необходимые мероприятия для противодействия угрозам 24](#_Toc70703233)

[5. ВЫВОДЫ 24](#_Toc70703234)

[Список использованных источников 25](#_Toc70703235)

[Список изменений 26](#_Toc70703236)

[Приложение 1. Возможная деятельность потенциальных внутренних И ВНЕШНИХ нарушителей 27](#_Toc70703237)

[Приложение 2. Необходимые мероприятия для противодействия угрозам 43](#_Toc70703238)

[Приложение 3. правила отнесения способа реализации угрозы информационной безопасности к актуальному 66](#_Toc70703239)

**Термины и определения**

|  |  |
| --- | --- |
| **АкТУАЛЬНАЯ УГРОЗА** | Совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного доступа к персональным данным, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия при их обработке в информационной системе персональных данных (ИСПДн) |
| **АТАКА** | Целенаправленные действия нарушителя с использованием технических и (или) программных средств, с целью нарушения заданных характеристик безопасности защищаемой информации или с целью создания условий для этого |
| **Безопасность персональных данных (Пдн)** | Состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность ПДн при их обработке в информационных системах персональных данных |
| **Внешний нарушитель информационной безопасности (ИБ)** | Нарушитель, который не имеет непосредственного доступа к техническим средствам и ресурсам системы, находящимся в пределах контролируемой зоны |
| **Внутренний нарушитель иб** | Физические лица, имеющие право пребывания на территории контролируемой зоны, в пределах которой размещается оборудование системы |
| **Доступ к информации** | Возможность получения информации и ее использования |
| **Закладочное устройство** | Элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации) |
| **Источник угрозы иб** | Субъект, материальный объект или физическое явление, создающий угрозу безопасности защищаемой информации |
| **Контролируемая зона** | Пространство, в пределах которого осуществляется контроль за пребыванием и действиями лиц и/или транспортных средств |
| **Конфидециальность пдн** | Обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя |
| **Нарушитель** | Физическое лицо (лица), случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности ПДн при их обработке техническими средствами в информационных системах |
| **ПОЛЬЗОВАТЕЛИ СИСТЕМЫ** | Администраторы, архитекторы, разработчики, бизнес аналитики, системные аналитики, руководители проекта |
| **Ресурс ИСпдн** | Именованный элемент системного, прикладного или аппаратного обеспечения функционирования ИСПДн |
| **СИСТЕМА** | Комплекс, состоящий из процессов, технических и программных средств, устройств и персонала, обладающий возможностью удовлетворять установленным потребностям и целям. Совокупность элементов, объединенная связями между ними и обладающая определенной целостностью |
| **Специальная ИСПДн** | ИСПДн, в которой вне зависимости от необходимости обеспечения конфиденциальности ПДн требуется обеспечить хотя бы одну из характеристик безопасности ПДн, отличную от конфиденциальности (защищенность от уничтожения, изменения, блокирования, а также иных несанкционированных действий) |
| **Технический канал утечки информации** | Совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация |
| **Типовая испдн** | ИСПДн, в которой требуется обеспечение только конфиденциальности ПДн |
| **Угроза безопасности Пдн** | Совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к ПДн, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение ПДн, а также иных несанкционированных действий при их обработке в информационной системе ПДн |
| **удаленный доступ** | Доступ к функциям и данным информационной системы, получаемый по каналам или линиям связи и осуществляемый при помощи программных средств |
| **Физический доступ** | Непосредственный доступ к техническим средствам информационной системы, а также к функциям и данным информационной системы при помощи аппаратных устройств управления (консоли), непосредственно подключенных к техническим средствам |
| **целостность информации** | Состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право |
| **Эксперт** | Специалист в области защиты информации |
| **Back-end сервер** | Cервер системы, предназначенный для обработки и хранения информации и не имеющий непосредственного взаимодействия с рабочими местами пользователей системы |
| **Front-end сервер** | Cервер системы, обеспечивающий непосредственный интерфейс взаимодействия с рабочими местами пользователей или иными информационными системами и предназначенный для обработки запросов пользователей на получение информации и передачи им результатов запроса. Front-end сервер может также хранить и обрабатывать общедоступную информацию |

**Обозначения и сокращения**

|  |  |
| --- | --- |
| **АРМ** | Автоматизированное рабочее место |
| **АС** | Автоматизированная система |
| **БД** | База данных |
| **БМИ** | Базовая межведомственная инфраструктура |
| **ГК** | Государственный контракт |
| **ГОСТ** | Государственный стандарт |
| **ЕРЗ** | Единый реестр застрахованных лиц |
| **ЗУ** | Закладочное устройство |
| **ЗСПД** | Защищенная сеть передачи данных |
| **ИБ** | Информационная безопасность |
| **ИНН** | Идентификационный номер налогоплательщика |
| **ИСПДн** | Информационная система персональных данных |
| **КСИБ** | Комплексная система безопасности межведомственного взаимодействия, в том числе посредством защищенных каналов связи |
| **КЦОД** | Коммерческий центр обработки данных |
| **ЛВС** | Локальная вычислительная сеть |
| **МИСИКС** | Система управления требованиями на производственном предприятии |
| **НИЯУ МИФИ** | Национальный исследовательский ядерный университет «Московский инженерно-физический институт» |
| **НСИ** | Нормативно-справочная информация |
| **ОС** | Операционная система |
| **ОУЗ** | Орган управления здравоохранения |
| **ПО** | Программное обеспечение |
| **РД** | Руководящий документ |
| **СЗИ** | Средства защиты информации |
| **СЗПДн** | Средства защиты персональных данных |
| **СНИЛС** | Страховой номер индивидуального лицевого счета |
| **СХД** | Система хранения данных |
| **ТС** | Технические средства |
| **ТЗ** | Техническое задание |
| **УЭК** | Универсальная электронная карта |
| **ФЗ** | Федеральный закон |
| **ФСБ** | Федеральная служба безопасности Российской Федерации |
| **ФСТЭК** | Федеральная служба по техническому и экспортному контролю |
| **ЦТО** | Центр телефонного обслуживания |
| **ЦОД** | Центр обработки данных |
| **DDoS** | Distributed Denial of Service - распределённая атака типа «отказ в обслуживании» |
| **DNS** | Domain Name System - система доменных имён |
| **PIN** | Personal Identification Number - личный опознавательный номер |
| **USB** | Universal Serial Bus - Универсальная последовательная шина |
| **VM** | Virtual Machine - Виртуальная машина |

1. Общие сведения

Общие сведения о разрабатываемой Системе представлены в документе «ТЗ. МИСИКС. Техническое задание».

* 1. Перечень документов на основании которых создается модель угроз информационно безопасности

«Модель угроз информационной безопасности» на Систему «*МИСИКС*» разработана в соответствии с документами [1-9].

* 1. Назначение модели угроз информационной безопасности

Модель угроз информационной безопасности предназначена для:

* анализа защищенности Системы «*МИСИКС*» от угроз безопасности ПДн;
* организации и выполнения работ по обеспечению безопасности Системы «*МИСИКС*» от угроз безопасности ПДн;
* разработки системы защиты ПДн, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты ПДн;
* проведения мероприятий, направленных на предотвращение несанкционированного доступа к ПДн и (или) передачи их лицам, не имеющим права доступа к такой информации;
* недопущения воздействия на технические средства Системы «*МИСИКС*» в результате которого может быть нарушено их функционирование;
* контроля обеспечения уровня защищенности ПДн.

1. сведения оБ объекте защите
   1. Назначение создаваемой Системы

Назначение создаваемой Системы представлено в документе «ТЗ. МИСИКС. Техническое задание».

* 1. Структура Системы и ее основные характеристики

В данном подразделе структура Системы не приводится в явном виде, а оформляется ссылкой на документы: ТЗ или Паспорт системы и «Описание комплекса технических средств». В подразделе также указывается тип структуры.

По типам структуры создаваемые системы могут подразделяются на:

* автономные (не подключенные к иным информационным системам) комплексы технических и программных средств, предназначенные для обработки персональных данных (автоматизированные рабочие места);
* на комплексы автоматизированных рабочих мест, объединенных в единую информационную систему средствами связи без использования технологии удаленного доступа (локальные информационные системы);
* на комплексы автоматизированных рабочих мест и (или) локальных информационных систем, объединенных в единую информационную систему средствами связи с использованием технологии удаленного доступа (распределенные информационные системы).

В подразделе описывается:

* местонахождение технических средств информационной системы и перечень физических лиц, имеющие к ним доступ;
* режим разграничения прав доступа пользователей информационной системы;
* наличие подключений информационной системы к сетям связи общего пользования и (или) сетям международного информационного обмена.

Информационные системы в зависимости от местонахождения их технических средств подразделяются на системы, все технические средства которых находятся в пределах Российской Федерации, и системы, технические средства которых частично или целиком находятся за пределами Российской Федерации.

По наличию подключений к сетям связи общего пользования и (или) сетям международного информационного обмена информационные системы подразделяются на системы, имеющие подключения, и системы, не имеющие подключений.

По разграничению прав доступа пользователей информационные системы подразделяются на системы без разграничения прав доступа и системы с разграничением прав доступа.

* + 1. Структура создаваемой Системы

Перечень подсистем Системы «*МИСИКС*» представлен в документе «ТЗ. МИСИКС. Техническое задание».

Система «*МИСИСК*» использует архитектурное решение: Браузер клиента – Web-сервер – Сервер приложений – Сервер баз данных (БД).

Описание структуры комплекса технических средств Системы «*МИСИКС*» представлено в документе «МИСИКС. Описание комплекса технических средств».

Структура Системы представляет собой комплекс автоматизированных рабочих мест и (или) локальных информационных систем, объединенных в единую информационную систему средствами связи с использованием технологии удаленного доступа (распределенные информационные системы)

* + 1. Местонахождение технических средств Системы и перечень физических лиц, имеющих к ним доступ

Все серверные компоненты системы и технические средства размещаются в помещении, предоставленном Кафедрой 12, в центре обработки данных (ЦОД). На выделенной площадке могут присутствовать технические средства прочих информационных систем, не имеющих отношения к Системе «*МИСИКС*».

В помещения Кафедры 12 возможен доступ руководства Кафедры 12, пользователей системы и прочих лиц, получающих доступ от руководства Кафедры 12.

* + 1. Режим разграничения прав доступа пользователей Системы

Возможности пользователя по взаимодействию с Системой и доступу к информации определяются интерфейсом, разработанным для каждой роли пользователей. В таблице 1 представлены категории ролей пользователей системы, имеющих доступ к ее ресурсам.

*Таблица* *1 – Перечень ролей пользователей, имеющих доступ к ресурсам Системы*

| **Категория** | **Тип доступа** | **Описание** |
| --- | --- | --- |
| Администратор системы | Физический доступ к автоматизированному рабочему месту (АРМ) и техническим средствам Системы «*МИСИКС*» / Удаленный. Имеет полный доступ к функциональности и информационным ресурсам Системы | Пользователи системы, обеспечивающие эксплуатацию комплекса программно-технических средств Системы «*МИСИКС*» |
| Администратор ИБ системы | Физический /Удаленный доступ к АРМ. Имеет полный доступ к функциям безопасности Системы | Сотрудники Кафедры 12, осуществляющие управление функциями безопасности в системе |
| Пользователи системы | Физический доступ к АРМ/Удаленный доступ к функциям Системы. Имеют ограниченный доступ к web-интерфейсу системы и предоставляемым им функциям | Пользователи системы получают доступ к информации проектов и требований в рамках НИЯУ МИФИ |

Идентификация и аутентификация пользователей при доступе к ресурсам системы осуществляется при помощи сервиса «*Сервис авторизации*», за исключением доступа к ресурсу нормативно-справочной информации (НСИ).

Доступ к ресурсу НСИ осуществляется путем идентификации пользователя при помощи локальных учетных записей на сервере НСИ и аутентификации с помощью штатных механизмов операционной системы (ОС). АРМ оператора НСИ расположен в защищенном окружении ЦОД.

* + 1. Подключение Системы к сетям связи общего пользования и (или) сетям международного информационного обмена

Информационный обмен между компонентами Системы, расположенными на различных объектах, осуществляется с использованием общедоступных каналов связи, в том числе при помощи сети Интернет.

Работа Системы зависит от доступности внешних информационных сервисов: «*Интеграционный сервис»*. Взаимодействие с сервисом «*Интеграционный сервис»* осуществляется через систему «*МИСИКС»*. Подключение к системе «*Подсистема управления тестированием»* осуществляется при помощи защищенных каналов связи, организованных в рамках данной системы. Взаимодействие с сервисом «*Интеграционный сервис»* осуществляется с использованием сети общего доступа Интернет.

* 1. Информация, обрабатываемая в Системе

Система «*МИСИКС*» поддерживает многопользовательскую обработку ПДн.

В ИС обрабатывается информация следующих категорий:

* Персональные данные, позволяющие идентифицировать субъекта персональных данных и получить дополнительную информацию;
* информация, составляющая коммерческую тайну;
* сведения, составляющие служебную информацию ограниченного распространения (служебная тайна);

В ИС кроме информации, размещаемой в БД, ведется обработка и хранение документов различных форматов и электронных образов печатных документов.

В ИС обработка речевой и видео информации не осуществляется.

* + 1. Персональные данные

Персональные данные включают в себя, в частности следующую информацию:

* Фамилию, имя, отчество (ФИО).
* Имя учетной записи пользователя.
* Должность пользователя системы.
  + 1. Конфиденциальная информация

К конфиденциальной информации, обрабатываемой в ИС, относится:

* Сведения, раскрывающие вопросы по проектам
* Сведения, раскрывающие информацию о требованиях
  1. Перечень защищаемых ресурсов Системы и их уровень конфиденциальности

Защищаемыми ресурсами Системы являются:

* обрабатываемая и защищаемая в системе информация (файлы, записи БД);
* системное и прикладное программное обеспечение;
* технические средства обработки (АРМ пользователей и виртуальные машины серверных компонентов, коммутационное оборудование);
* каналы связи, используемые для взаимодействия компонентов системы;
* внешние информационные сервисы, необходимые для работы системы.

Критичность каждого ресурса определяется по степени ущерба (негативных последствий) в случае нарушения состояния информационной безопасности, по оценке экспертов. Для оценки критичности ресурса используется показатели, указанные в таблице 2.

*Таблица 2 – Показатели критичности ресурсов*

| **Критичность ресурса** | **Описание показателя** | **Числовая оценка показателя** |
| --- | --- | --- |
| Низкая | Затраты на восстановление ресурса и последствия от нарушения его безопасности не приятны, но фактически не сказываются на организации, ответственную за работу системы | 1 |
| Средняя | Затраты на восстановление ресурса и последствия от нарушения его безопасности достаточно чувствительны и требуют привлечения дополнительных ресурсов и затрат на устранение последствий | 2 |
| Высокая | Затраты на восстановление ресурса и последствия от нарушения его безопасности значительны и существенно влияют на деятельность организации, ответственную за работу системы, в течении длительного времени, требуют больших усилий и затрат на устранение последствий | 3 |
| Очень высокая | Затраты на восстановление ресурса очень велики или восстановление ресурса невозможно, а последствия от нарушения его безопасности могут представлять угрозу для дальнейшего существования организации | 4 |

Описание и характеристики защищаемых ресурсов Системы приведены в таблице 3.

*Таблица* *3 – Описание защищаемых ресурсов Системы*

| **Ресурс** | **Описание** | **Требования безопасности: К – конфиденциальность; Д – доступ к информации; Ц - целостность** | **Критичность ресурса / Числовая оценка показателя** |
| --- | --- | --- | --- |
| **Ресурсы, размещаемые в помещениях Кафедры 12** | | | |
| ПДн пользователей системы | Описание представлено в п. 2.3 настоящего документа | (К) Необходимо обеспечить конфиденциальность данных в соответствии с требованиями законодательства. Доступ к данным должен предоставляться только пользователям Системы в необходимом объеме | Высокая (для всей совокупности персональных данных) / 3 |
| (Д) Необходимо обеспечить доступность данных в целях возможности изучения информации по проектам и требованиям | Высокая / 3 |
| (Ц) Необходимо обеспечить целостность данных для предотвращения ошибок при внесении изменений в проекты и требования | Средняя / 2 |

* 1. Исходный уровень защищенности Системы

В соответствии с [5], уровень исходной защищенности Системы определяется, исходя из уровня защищенности технических и эксплуатационных характеристик Системы, представленных в таблице 4.

*Таблица 4 – Показатели исходной защищенности Системы*

| **№** | **Технические и эксплуатационные  характеристики Системы** | **Уровень защищенности** |
| --- | --- | --- |
|  | По территориальному размещению | Низкий |
|  | По наличию соединения с сетями общего пользования | Средний |
|  | По встроенным (легальным) операциям с записями баз персональных данных | Средний |
|  | По разграничению доступа к персональным данным | Средний |
|  | По наличию соединений с другими базами ПДн иных ИСПДн | Высокий |
|  | По уровню обобщения (обезличивания) ПДн | Высокий |
|  | По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки | Низкий |

Уровень исходной защищенности Системы средний, поскольку не менее 70% характеристик ИСПДн соответствуют уровню не ниже "средний", а остальные – низкому уровню защищенности.

Исходя из полученного значения уровня защищенности и в соответствии с рекомендациями [5], значение числового коэффициента  = 5 (для средней степени исходной защищенности).

* 1. Основные данные о создаваемой системе

При разработке модели угроз должны учитываться исходные данные о Системе, представленные в таблице 5.

*Таблица 5 – Исходные данные о создаваемой Системе*

|  |  |  |
| --- | --- | --- |
|  | Категория обрабатываемых в информационной системе персональных данных | Категория 2. Персональные данные, позволяющие идентифицировать субъекта персональных данных, и получить о нем дополнительную информацию |
|  | Объем обрабатываемых персональных данных | Группа 2. Одновременно обрабатываются персональные данные от 1 000 до 100 000 субъектов персональных данных, работающих в отрасли экономики РФ, в органе государственной власти, проживающих в пределах муниципального образования |
|  | Заданные оператором характеристики безопасности персональных данных, обрабатываемых в информационной системе | Система относиться к специальным информационным системам, в которых обрабатываются персональные данные, касающиеся проектов и требований |
|  | Структура создаваемой автоматизированной системы | Структура Системы есть распределенная информационная система. Система включает комплексы автоматизированных рабочих мест и (или) локальных информационных систем, объединенных в единую информационную систему средствами связи с использованием технологии удаленного доступа |
|  | Наличие подключений информационной системы к сетям связи общего пользования и (или) сетям международного информационного обмена | Система имеет подключения к сетям связи общего пользования и (или) сетям международного информационного обмена информационные системы подразделяются на системы, имеющие подключения |
|  | Режим обработки персональных данных | Система является многопользовательской системой |
|  | Режим разграничения прав доступа пользователей информационной системы | Система является системой с разграничением прав доступа |
|  | Местонахождение технических средств информационной системы | Технические средства Системы находятся в пределах Российской Федерации |
|  | Исходная защищенность Системы | Уровень защищенности Системы средний |

1. Модель нарушителей информационной безопасности
   1. Внешние нарушители

Предполагается, что внешний нарушитель не может воздействовать на защищаемую информацию для целей нарушения безопасности ПДн, так как объем информации, хранимой и обрабатываемой в Системе, является недостаточным для возможной мотивации внешнего нарушителя к осуществлению действий, направленных на нарушение безопасности ПДн.

* 1. Внутренние нарушители
     1. Категории ввнутреннего нарушителя информационной безопасности

Перечень категорий внутренних нарушителей информационной безопасности и имеющейся у них информации об объектах реализации угроз Системы приведен в таблице 6.

*Таблица 6 – Категории внутренних нарушителей безопасности информации*

|  |  |  |
| --- | --- | --- |
| **Категория** | **Описание** | **Имеющаяся у нарушителя информация об объектах реализации угроз** |
| Категория I | Администратор системы | Информация по системе (например, алгоритмы, протоколы, реализуемые и используемые в конкретных подсистемах, принципы и концепции безопасности, информационное обеспечение системы и т.п.) |
| Категория II | Администратор ИБ системы | Полная информация по защите информации от несанкционированного доступа |
| Категория III | Пользователи системы | Информация о проектах и требованиях |

К лицам категорий I и II ввиду их исключительной роли в системе должен применяться комплекс особых организационных мер по их подбору, принятию на работу, назначению на должность и контролю выполнения функциональных обязанностей.

Предполагается, что в число лиц категорий I и II будут включаться только доверенные лица и поэтому указанные лица исключаются из числа вероятных нарушителей.

Предполагается, что лица категории III относятся к вероятным нарушителям.

* + 1. Предположения о средствах реализации угроз внутренним нарушителем

Состав имеющихся у нарушителя средств, которые он может использовать для реализации угроз ИБ, а также возможности по их применению зависят от многих факторов, включая реализованные на объектах НИЯУ МИФИ конкретные организационные меры, финансовые возможности и компетенцию нарушителей. Поэтому объективно оценить состав имеющихся у нарушителя средств реализации угроз в общем случае практически невозможно.

Поэтому, для создания устойчивых средств защиты персональных данных (СЗПДн) предполагается, что вероятный нарушитель имеет все необходимые для реализации угроз средства, возможности которых не превосходят возможности аналогичных средств реализации угроз на информацию, содержащую сведения, не составляющие государственную тайну, и технические и программные средства, обрабатывающие эту информацию.

Внутренний нарушитель может использовать доступные в свободной продаже технические средства и программное обеспечение, специально разработанные технические средства и программное обеспечение. Внутренний нарушитель может иметь штатные средства.

Вместе с тем предполагается, что нарушитель не имеет:

* средств воздействия через цепи заземления;
* средств активного воздействия на технические средства (средств облучения).
  + 1. Каналы, используемые внутренним нарушителем для доступа к защищаемым ресурсам Системы и способы атак

Для осуществления доступа к ресурсам Системы внутренний нарушитель может использовать следующие каналы атак:

* физический доступ к штатным программно-аппаратным средствам из состава системы;
* носители информации, в том числе съемные.

Возможны следующие способы атак:

* негласное (скрытое) временное изъятие или хищение съемных носителей защищаемой информации, аутентифицирующей или ключевой информации;
* вызывание сбоев технических средств;
* внесение неисправностей в технические средства.

1. Модель угроз информационной безопасности
   1. Потенциальные угрозы безопасности

В таблице 7 представлено описание потенциальных угроз безопасности Системы.

*Таблица 7 – Потенциальные угрозы безопасности Системы*

| **Источники угроз** | **Объективные** | **Субъективные** |
| --- | --- | --- |
| **Внутренние** | * передача информации по линиям связи; * побочные электромагнитные излучения и наводки; * дефекты, сбои и отказы аппаратных или программных средств обработки информации (в том числе и средств защиты информации) | * ненамеренные действия лиц, имеющих доступ к защищаемой информации, по ее разглашению; * ошибочные действия лиц, имеющих доступ к защищаемой информации и техническим средствам (ТС); * возможная деятельность потенциальных внутренних нарушителей |
| **Внешние** | * явления техногенного характера (радиационное облучение, непреднамеренное электромагнитное облучение и т.п.); * природные явления, стихийные бедствия (пожары, наводнения, землетрясения и т.п.) | * возможная деятельность потенциальных внешних нарушителей |

Вопросы защиты от природных катастроф и чрезвычайных ситуаций, угроз социально-политического характера не являются предметом для рассмотрения в рамках данной модели. Это связано с тем, что масштаб их возможного деструктивного воздействия, превосходит возможности системы защиты информации Системы. Защита от данного вида угроз организуется на уровне ЦОД в целом.

* 1. Детальное описание угроз
     1. Источник угроз: Внутренние. Угроза: субъективная. Возможная деятельность потенциальных внутренних нарушителей

Детальное описание угрозы «Возможная деятельность потенциальных внутренних внешних нарушителей» представлено в приложении 1.

Угрозы делятся на следующие группы:

* Угроза утечки видовой информации
* Угрозы утечки с использованием закладочных устройств
* Угроза НСД за счет непосредственного физического доступа
* Угроза НСД с применением программно-аппаратных или программных средств
* Угроза НСД при передаче информации по каналам связи

Защита от внедрение закладочного устройства (ЗУ) в ТС, размещаемых в ЦОД, обеспечивается Комплексной системой безопасности межведомственного взаимодействия, в том числе посредством защищенных каналов связи (КСИБ).

Защита от угрозы НСД за счет непосредственного физического доступа обеспечивается КСИБ. Утеря мобильного телефона не рассматривается, так как приложение не предусматривает мобильную версию.

Защита от угрозы НСД с применением программно-аппаратных или программных средств обеспечивается КСИБ за исключением:

* эксплуатации уязвимостей ПО back-end серверов;
* получения доступа к персональным данным с использованием web интерфейса доступа к серверу приложений;
* получение персональных данных лицами, которые не должны иметь к ним доступ, в результате ошибок в реализации системы разграничения доступа в прикладных компонентах.

Защита при эксплуатации уязвимостей ПО back-end серверов и при получении доступа к персональным данным с использованием web интерфейса доступа к серверу приложений поддерживается КСИБ частично. В КСИБ используется IDS прикладного уровня. На уровне прикладной системы необходимо использовать методы безопасного программирования для минимизации ошибок в программном коде.

Защита от перехвата персональных данных в результате прослушивания трафика информационного взаимодействия пользователей с сервером приложений поддерживается КСИБ частично. Если для работы прикладного сервиса используется сеть интернет или другой открытый канал (например, сотовая сеть) то нужно исключать передачу персональных данных в информационном обмене.

В рамках КСИБ создана ЗСПД предназначенная для защиты пользователей НИЯУ МИФИ.

* 1. Необходимые мероприятия для противодействия угрозам

Перечень мероприятий для противодействия угрозам предполагает использование мер как технического, так и организационного порядка в отношении угроз, степень опасности которых не ниже высокой. Предлагаемые мероприятий направлены на обеспечение защиты ресурсов в целях снижения негативных последствий при реализации способов угроз.

Для способов реализации угрозы, степень опасности которых не выше высокой, предполагается использование организационных мер, как наименее затратных.

Детальное описание угрозы «Необходимые мероприятия для противодействия угрозам» представлено в приложении 2.

1. ВЫВОДЫ

В соответствии с предоставленной информацией о Системе и технологиях обработки информации средства защиты информации, применяемые в системе, должны удовлетворять требованиям, предъявляемым к методам и способам защиты информации, изложенным в НМД ФСТЭК России применительно к автоматизированным системам (АС) класса защищенности 1Г.

В соответствии с «Порядком проведения классификации информационных систем персональных данных» (утвержден Приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 13 февраля 2008 г. № 55/86/20) и настоящей Моделью, в которой определены условия обработки персональных данных и категории потенциальных нарушителей информационной безопасности, Система является специальной информационной системой. С учетом приведенного перечня актуальных угроз ИБ для Системы должен быть обеспечен уровень защищённости персональных данных в соответствии с требованиями для информационной системы ПДн (ИСПДн) класса К2.

Список использованных источников

1. Федеральный закон Российской Федерации от 27.07.2006 № 149-ФЗ Об информации, информационных технологиях и о защите информации - (ред. от 06.04.2011, с изм. от 21.07.2011)
2. Федеральный закон Российской Федерации от 27.07.2006 № 152-ФЗ О персональных данных - (ред. от 25.07.2011)
3. ГОСТ Р 51275–2006. Защита информации. Объект автоматизации. Факторы, воздействующие на информацию. Общие положения
4. ГОСТ Р 52863-2007. Защита информации. Автоматизированные системы в защищенном исполнении. Испытания на устойчивость к преднамеренным силовым электромагнитным воздействиям. Общие требования
5. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утв. ФСТЭК РФ 14.02.2008 г.)
6. Базовая модель угроз безопасности персональных данных при их обработке, в информационных системах персональных данных (утв. ФСТЭК РФ 15.02.2008 г.)
7. Положение о методах и способах защиты информации в информационных системах персональных данных, утвержденное Приказом ФСТЭК от 5 февраля 2010 года №58 (зарегистрирован Минюстом России 19 февраля 2011 г. N 16456)
8. Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации (утв. ФСБ РФ 21 февраля 2008 г. N 149/54-144)
9. ГОСТ 2.105-95 Межгосударственный стандарт. Единая система конструкторской документации. Общие требования к текстовым документам

Список изменений

|  |  |  |  |
| --- | --- | --- | --- |
| **Дата** | **Версия** | **Описание изменений** | **Автор** |
| 23.04.2021 | 1.00 | Начальная версия документа | Симанович К.О. |

1. Возможная деятельность потенциальных внутренних И ВНЕШНИХ нарушителей

Детальное описание угрозы «Возможная деятельность потенциальных внутренних нарушителей» представлено в таблице 0.

*Таблица 0 – Возможная деятельность потенциальных внутренних нарушителей Детальное описание угрозы утечки видовой информации*

| **Способ реализации угрозы** | **Источник угрозы** | **Совокупность ресурсов, на которые угроза может воздействовать** | **Уязвимости ресурсов, которые приводят к реализации угрозы** | **Результат воздействия угрозы и нарушаемое свойство безопасности информации** |
| --- | --- | --- | --- | --- |
| **Угроза утечки видовой информации** | | | | |
| Утечка данных, отображаемых на экранах мониторов АРМ пользователей | Лицо, способное осуществлять перехват информации по техническим каналам утечки | Персональные данные пользователей системы;  Аутентификационная информация пользователя | Возможность наблюдения за мониторами пользователей через оконные проемы  Отображение паролей в открытом виде при их вводе в систему;  Размещение в общедоступном месте | (К) Перехват пароля пользователя или некоторого количества персональных данных пользователей системы в зависимости от роли пользователя |
| **Угрозы утечки с использованием закладочных устройств** | | | | |
| Утечка с использованием закладочных устройств | Внутренний нарушитель (III категория) | Персональные данные пользователей системы;  Информация о проектах и требованиях;  Аутентификационная информация | Отсутствие ограничения физического доступа к оборудованию системы | (К) Перехват пароля пользователя и персональных данных множества пользователей системы, а также прочих данных |
| **Угроза НСД за счет непосредственного физического доступа** | | | | |
| Восстановление защищаемой информации путем анализа выведенных из употребления для утилизации или ремонта носителей информации ТС | Лицо, способное получить доступ к ТС (носителям информации) предназначенных для утилизации или ремонта | Персональные данные пользователей системы, сохраняемые на жестких дисках серверов БД и носителях резервных копий | Отсутствие штатных гарантированных механизмов удаления информации с магнитных носителей;  Отсутствие регламентированного порядка очистки носителей информации | Восстановление и компрометация персональных данных  пользователей системы, содержащихся в БД системы |
| Недоверенная загрузка серверов и АРМ пользователей системы | Внутренний нарушитель (I и II категорий) | Персональные данные пользователей системы, сохраняемые на жестких дисках АРМ | Возможность загрузки сторонней ОС на компьютер с помощью съемного носителя;  Сохранение пользователем результатов обработки запросов на локальный жесткий диск АРМ | (К) Получение полного доступа к данным на жестком диске или получения доступа в ЛВС.  Получение доступа к некоторому количеству персональных данных пользователей системы в зависимости от роли пользователя |
| Использование чужого сеанса доступа к рабочему столу ОС АРМ пользователя / администратора | Внутренний нарушитель | Персональные данные пользователей системы;  Информация о проектах и требованиях; | Отсутствие автоматического завершения сеанса пользователя к сервису | (К) Получение доступа к сервису и персональным данным пользователей системы с правами пользователя  (Ц) Внесение искажений в информацию |
| Утрата, компрометация пользователем ИС ключевой, парольной и аутентифицирующей информации, любой другой защищаемой информации, а также несообщение о фактах компрометации и утраты такой информации. | Внутренний нарушитель | Персональные данные пользователей системы;  Информация о проектах и требованиях; | Использование пользователем слабых паролей;  Использование электронной карты без PIN кода;  Прозрачная аутентификация в поле регистрации на АРМ | (К) Получение доступа к сервису и персональным данным пользователей системы с правами пользователя.  (Ц) Внесение искажений в информацию |
| Кража носителей резервных копий содержимого базы данных | Внутренний нарушитель (I и II категорий) | Персональные данные пользователей системы, содержащиеся в БД; | Наличие не контролируемого доступа к носителям резервных копий посторонних лиц | (К) Компрометация персональных пользователей системы, содержащихся в БД системы |
| Несанкционированное подключение во внутреннюю локальную сеть | Внутренний нарушитель (I и II категорий) | Персональные данные пользователей системы; | Наличие не контролируемого доступа посторонних лиц к коммутационному оборудованию;  Использование медных межстоечных кабелей в ЦОД | Прослушивание трафика информационного обмена, перехват персональных данных, передаваемых по внутренней сети.  Получение возможности организовать атаки на сервера системы |
| Отключение штатных ТС и СЗИ | Внутренний нарушитель (I и II категорий) | Технические средства | Наличие не контролируемого доступа посторонних лиц к оборудованию | (Д) Нарушение функционирования системы на срок от нескольких минут до нескольких часов |
| Несанкционированный вывод персоналом Кафедры 12 защищаемой информации на устройство, подключаемое к Universal Serial Bus (USB) порту на АРМ пользователя | Внутренний нарушитель (III категория) | Информация о проектах и требованиях | Наличие USB портов на АРМ пользователя | Конфиденциальность. Компрометация некоторого числа персональных данных лиц, имеющих отношение к проектам и требованиям |
| **Угроза НСД с применением программно-аппаратных или программных средств** | | | | |
| Эксплуатации уязвимостей ПО back-end серверов | Пользователи иных информационных систем, размещенных в ЦОД или сотрудники КЦОД;  Разработчики прикладных систем | Системное или прикладное ПО back-end серверов (приложений, БД и пр.) | Отсутствие сегментации ЛВС (включая среду виртуализации);  Несвоевременная установка обновлений безопасности | (К) Получение расширенных прав управления серверами с возможностью последующего получения доступа непосредственно к содержанию БД.  (Ц) Внесение искажений в информацию  (Д) Нарушение функционирования системы |
| Эксплуатация уязвимостей системного ПО front – end серверов | Пользователи сети интернет;  Внутренний нарушитель | Системное или прикладное ПО front – end серверов (web, proxy, терминальные и пр.) | Отсутствие ограничения сетевого доступа к сетевым службам и сервисам сервера.  Несвоевременная установка обновлений безопасности | Получение расширенных прав управления сервером с возможностью последующего получения доступа к внутренним серверам.  (Д) Нарушение функционирования |
| Получение доступа к персональным данным с использованием web интерфейса доступа к серверу приложений | Пользователи сети интернет;  Внутренний нарушитель | Прикладное ПО серверов приложений | Ошибки программирования прикладного ПО | (К) Получение доступа к записям БД в обход установленных правил получения доступа. |
| Блокирование работы сервиса путем организации атаки типа «DDoS». | Пользователи сети интернет | Front-end и сервера приложений | Ограниченная производительность и системные ресурсы серверов | (Д) Блокировка работы системы и невозможность использования сервисов пользователями на длительный срок. |
| Получение прямого доступа к БД системы в обход прикладного ПО за счет использования штатных средств администрирования ПО СУБД | Пользователи иных информационных систем, размещенных в ЦОД;  Внутренний нарушитель;  Разработчики прикладных систем | Прикладное ПО сервера БД системной шины;  Прикладное ПО сервера БД;  Прикладное ПО сервера БД НСИ | Отсутствие сегментации ЛВС (включая виртуализированную среду).  Ошибки в конфигурировании СУБД | (К) Получение доступа к записям БД в обход установленных правил получения доступа.  (Ц) Внесение искажений в информацию |
| Внедрение сетевого вредоносного ПО в серверные компоненты системы | Пользователи иных информационных систем, размещенных в ЦОД;  Внутренний нарушитель;  Пользователи сети Интернет | Системное ПО серверов | Отсутствие сегментации и ограничения сетевого доступа к сетевым службам и сервисам серверов в ЛВС (включая виртуализированную среду).  Несвоевременная установка обновлений безопасности | (Д) Снижение производительности серверов.  (Ц) Реализация «черного хода» в систему |
| Сканирование сетевых адресов и служб серверов системы | Пользователи иных информационных систем, размещенных в ЦОД;  Внутренний нарушитель;  Пользователи сети Интернет | Системное и прикладное ПО серверов | Отсутствие сегментации и ограничения сетевого доступа к сетевым службам и сервисам серверов в ЛВС (включая виртуализированную среду).  Несвоевременная установка обновлений безопасности | (К) Получение нарушителем чувствительной информации, позволяющей организовать атаки на систему |
| Подбор пароля администратора сервера (ОС, СУБД) с использованием встроенных функций удаленного администрирования системного и прикладного ПО | Пользователи иных информационных систем, размещенных в ЦОД;  Внутренний нарушитель;  Внутренний нарушитель | Системное и прикладное ПО серверов | Отсутствие сегментации ЛВС (включая виртуализированную среду).  Использование слабых паролей администраторами | (К) Получение нарушителем полного контроля над сервером, возможность получения доступа к защищаемым данным и организации атак на другие сервера  (Ц) Внесение искажений в информацию |
| Загрузка и запуск пользователями на АРМ постороннего ПО, содержащего вредоносный код или являющегося инструментом проведения атак | Внутренний нарушитель | Информация, используемая для аутентификации пользователей | Наличие внешней почты, доступа к сети Интернет у пользователя.  Возможность использования съемных носителей | (К) Компрометация пароля пользователя и возможность получения доступа к персональным данным в системе от имени пользователя |
| Подключение к портам управления коммутационного оборудования | Внутренний нарушитель | Коммутационное оборудование ЛВС ЦОД и ЛПУ | Отсутствие сегментации ЛВС;  Использование паролей, установленных производителем по умолчанию | (К) Изменение маршрутной информации, позволяющей перехватывать и анализировать трафик в целях получения защищаемой информации |
| Получение персональных данных лицами, которые не должны иметь к ним доступ, в результате ошибок в реализации системы разграничения доступа в прикладных компонентах | Пользователи сети Интернет; Внутренний нарушитель | Персональные данные пользователей системы, содержащихся в БД | Ошибки в реализации механизмов разграничения доступа в прикладных компонентах | (К) Получение доступа к персональным или иным защищаемым данным, находящихся в базах данных, доступ к которым не предназначался для данной категории пользователей |
| **Угроза НСД при передаче информации по каналам связи** | | | | |
| Отправка некорректного запроса веб-сервису со стороны смежных систем | Пользователи смежных информационных систем | Прикладное ПО серверов, обеспечивающих взаимодействие со смежными системами | Отсутствие контроля параметров запроса и соответствия запроса запрашивающей системе. | (Д) Нарушение функционирования системы  (К) Получение расширенных или не предназначенных пользователю данных |
| Получение доступа к внутренней сети в результате подмены IP адреса источника (спуффинг) | Пользователи сети интернет;  Внутренний нарушитель | Системное и прикладное ПО серверов | Объединение трафика из различных источников на одном централизованном сетевом устройстве | (К) Получение сетевого доступа к внутренней сети с возможностью дальнейшего проведения атак на серверные компоненты системы |
| Перехват и внедрение в сессию доступа к сервисам легального пользователя | Пользователи сети интернет | Персональные данные пользователей системы, содержащихся в БД | Использование http сессий при организации взаимодействия пользователя с сервисами | (К) Получение доступа к сервисам с правами пользователя системы |
| Перехват аутентификационных данных при авторизации пользователей и администраторов | Пользователи сети интернет | Информация, используемая для аутентификации пользователей / администраторов | Использование не защищенного канала связи;  Использование слабых паролей | (К) Перехват и возможность восстановления пароля пользователя для получения доступа в систему |
| Перехват персональных данных в результате прослушивания трафика информационного взаимодействия пользователей с сервером приложений | Пользователи сети интернет | Персональные данные пользователей системы, содержащихся в БД | Использование http сессий при организации взаимодействия пользователя с сервисами | (К) Прослушивание канала связи, перехват и компрометация некоторого количества персональных данных |
| Перехват и модификация данных информационного взаимодействия пользователей с сервером приложений в результате навязывания ложного маршрута во внешних сетях | Пользователи сети интернет | Персональные данные пользователей системы, содержащихся в БД;  Информация, используемая для аутентификации пользователей | Использование http сессий при организации взаимодействия пользователя с сервисами;  Отсутствие авторизации сессии на стороне сервера | (К) Перенаправление трафика информационного взаимодействия пользователей через компьютер нарушителя с возможностью перехвата и контроля трафика |
| **Угроза НСД, связанная с неправомерными действиями пользователей** | | | | |
| Внесение заведомо ложной информации в проекты и требования | Внутренний нарушитель (III категории) | Персональные данные пользователей системы | Невозможность установления авторства изменений;  Отсутствие механизмов контроля целостности электронных записей | (Ц) Ошибки в предоставлении неверной информации по проекту и требованиям |
| Отключение средств защиты информации на АРМ пользователя | Внутренний нарушитель | Файлы настроек и конфигураций безопасности | Доступ пользователя к функциям управления или файлам конфигурации средств обеспечения безопасности | (Ц) Нарушение работы или отключение средств обеспечения безопасности, что может привести к реализации различных угроз ИБ |
| Несанкционированный вывод персоналом Кафедры 12 на печать защищаемой информации или запись ее на неучтенные съемные носители | Внутренний нарушитель | Информация по проектам и требованиям;  Персональные данный пользователей системы | Наличие USB портов на АРМ пользователя | (К) Компрометация некоторого числа персональных данных |
| Внесение вредоносного ПО при обновлении системного и прикладного ПО серверов и АРМ | Внутренний нарушитель (I и II категории) | Системное и прикладное ПО серверов | Недостаточная квалификация персонала в вопросах ИБ | (Ц) Внедрение троянских программ  (Д) Нарушение функционирования работы серверных компонентов системы |
| Ошибки персонала администрирования по эксплуатации прикладного ПО и оборудования | Внутренний нарушитель (I и II категории) | Файлы настроек и конфигураций безопасности;  Системное и прикладное ПО серверов | Низкая квалификация персонала;  Отсутствие документированных требований по настройке ПО;  Отсутствие резервного копирования. | (К) Несанкционированный доступ к защищаемой информации  (Д) Ошибки в конфигурации системы или удаление необходимых для работы системы файлов приводящих к отказу в работе компонентов системы и недоступности сервисов для всех пользователей  (Ц) Ошибочное удаление данных |
| **Угроза техногенного характера** | | | | |
| Сбой в работе ТС связанный с дефектами аппаратного обеспечения | Технический дефект аппаратного обеспечения | ТС серверов | Использование ненадежного оборудования | (Д) Недоступность сервисов для всех пользователей системы на значительный срок |
| Сбой в программных средствах в результате ошибок программного кода в пакетах обновлений | Ошибки программного кода | Прикладное и системное ПО серверов | Отсутствие процедур тестирования работы ПО при обновлении | (Д) Недоступность сервисов для всех пользователей системы на срок несколько часов |
| Отказ коммутационного оборудования ЛВС | Технический дефект аппаратного обеспечения | Коммутационное оборудование ЛВС ЦОД | Использование ненадежного оборудования | (Д) Недоступность сервисов для всех пользователей системы на срок несколько часов |
| Превышение расчетной нагрузки на систему | Внутренний нарушитель | Сервера | Использование не масштабируемой архитектуры | (Д) Замедление отклика сервиса или полный отказ в предоставлении сервиса множеству пользователей в течении длительного времени |
| Отключение или нарушение параметров электропитания на объекте размещения ТС системы | Различные аварии в сетях электропитания | Сервера, размещенные в ЦОД | Отсутствие резервных источников питания | (Д) Недоступность сервисов для всех пользователей системы на срок несколько часов |

1. Необходимые мероприятия для противодействия угрозам

Организационные и технические меры по противодействию угрозам информационной безопасности, на основании которых должны определяться требования к системе обеспечения информационной безопасности (СОИБ) ИС, в структурированном виде представлены в таблице 0.

*Таблица 0 – Модель защиты информации ИС от угроз, не являющихся атаками*

| **Описание** | **Меры по противодействию** | |
| --- | --- | --- |
| **Технические** | **Организационные** |
| **Угроза утечки видовой информации** | | |
| Утечка данных, отображаемых на экранах мониторов АРМ пользователей | Блокировка пользователя по истечению действия пароля.  Ввод пароля в специальном поле, которое будет отображаться специальными символами, заменяя символы пароля. | Наличие на предприятии службы информационной безопасности как выделенной структурной единицы.  Использование на предприятии единых регламентирующих документов (если их нет, должны быть разработаны):   * Памятка по информационной безопасности пользователя ИС. * Процедура предоставления доступа к информационным ресурсам. * Процедура предоставления доступа к внешним сетевым ресурсам. * Инструкция пользователя по безопасной работе в сети Интернет. |
| **Угрозы утечки с использованием закладочных устройств** | | |
| Утечка с использованием закладочных устройств | Использование для анализа сетевого трафика, электронной почты, защиты серверов и АРМ антивирусное ПО разных производителей. | Наличие на предприятии службы информационной безопасности как выделенной структурной единицы.  Ограничения физического доступа посторонних лиц к АРМ.  Использование на предприятии единых регламентирующих документов (если их нет, должны быть разработаны):   * Памятка по информационной безопасности пользователя ИС. * Процедура предоставления доступа к информационным ресурсам. * Процедура предоставления доступа к внешним сетевым ресурсам. * Инструкция пользователя по безопасной работе в сети Интернет. |
| **Угроза НСД за счет непосредственного физического доступа** | | |
| Восстановление защищаемой информации путем анализа выведенных из употребления для утилизации или ремонта носителей информации ТС | Данный тип мер противодействия не применим для рассматриваемой угрозы. | Использование на предприятии единых регламентирующих документов (если их нет, должны быть разработаны):   * Процедура очистки носителей информации. |
| Недоверенная загрузка серверов и АРМ пользователей системы | Применение сертифицированных средств, обеспечивающих невозможность несанкционированной установки ОС.  Применение сертифицированных средств, обеспечивающих невозможность несанкционированной установки пользователем ОС.  Запрет на сохранение информации на локальный жесткий диск.  Чистка дисков от лишних файлов. |  |
| Использование чужого сеанса доступа к рабочему столу ОС АРМ пользователя / администратора | Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу.  Ограничение числа параллельных сеансов до-ступа для каждой учетной записи пользователя информационной системы. | Наличие на предприятии службы информационной безопасности как выделенной структурной единицы.  Использование на предприятии единых регламентирующих документов (если их нет, должны быть разработаны):   * Памятка по информационной безопасности пользователя ИС. * Процедура предоставления доступа к информационным ресурсам. * Процедура предоставления доступа к внешним сетевым ресурсам. * Инструкция пользователя по безопасной работе в сети Интернет. |
| Утрата, компрометация пользователем ИС ключевой, парольной и аутентифицирующей информации, любой другой защищаемой информации, а также несообщение о фактах компрометации и утраты такой информации | Данный тип мер противодействия не применим для рассматриваемой угрозы. | Наличие на предприятии службы информационной безопасности как выделенной структурной единицы.  Использование на предприятии единых регламентирующих документов (если их нет, должны быть разработаны):   * Памятка по информационной безопасности пользователя ИС. * Процедура предоставления доступа к информационным ресурсам. * Процедура предоставления доступа к внешним сетевым ресурсам.   Инструкция пользователя по безопасной работе в сети Интернет. |
| Кража носителей резервных копий содержимого базы данных | Данный тип мер противодействия не применим для рассматриваемой угрозы. | Ограничение доступа к техническим помещениям.  Использование на предприятии единых регламентирующих документов (если их нет, должны быть разработаны):   * Процедура очистки носителей информации. |
| Несанкционированное подключение во внутреннюю локальную сеть | Использование сертифицированных средств антивирусной защиты.  Использование для анализа сетевого трафика, электронной почты, защиты серверов и АРМ антивирусное ПО разных производителей. | Наличие на предприятии службы информационной безопасности как выделенной структурной единицы.  Использование на предприятии единых регламентирующих документов (если их нет, должны быть разработаны):   * Политика антивирусной защиты; * Инструкция по антивирусной защите; * Инструкция пользователя по безопасной работе в сети Интернет; * Памятка по информационной безопасности пользователя ИС.   Проведение мероприятий по повышению осведомленности пользователей ИС в вопросах защиты информации. |
| Отключение штатных ТС и СЗИ | Данный тип мер противодействия не применим для рассматриваемой угрозы. | Ограничение доступа к техническим помещениям.  Использование на предприятии единых регламентирующих документов (если их нет, должны быть разработаны):   * Процедура очистки носителей информации. |
| Несанкционированный вывод персоналом Кафедры 12 защищаемой информации на устройство, подключаемое к Universal Serial Bus (USB) порту на АРМ пользователя | Использование сертифицированных средств антивирусной защиты.  Отключение или отсутствие USB-портов. | Наличие на предприятии службы информационной безопасности как выделенной структурной единицы.  Использование на предприятии единых регламентирующих документов (если их нет, должны быть разработаны):   * Политика антивирусной защиты; * Инструкция по антивирусной защите; * Инструкция пользователя по безопасной работе в сети Интернет; * Памятка по информационной безопасности пользователя ИС.   Проведение мероприятий по повышению осведомленности пользователей ИС в вопросах защиты информации. |
| **Угроза НСД с применением программно-аппаратных или программных средств** | | |
| Эксплуатации уязвимостей ПО back-end серверов | Использование сертифицированных средств антивирусной защиты.  Использование для анализа сетевого трафика, электронной почты, защиты серверов и АРМ антивирусного ПО разных производителей. | Данный тип мер противодействия не применим для рассматриваемой угрозы. |
| Эксплуатация уязвимостей системного ПО front – end серверов | Использование сертифицированных средств антивирусной защиты.  Использование для анализа сетевого трафика, электронной почты, защиты серверов и АРМ антивирусного ПО разных производителей. | Данный тип мер противодействия не применим для рассматриваемой угрозы. |
| Получение доступа к персональным данным с использованием web интерфейса доступа к серверу приложений | Использование сертифицированных средств антивирусной защиты.  Использование для анализа сетевого трафика, электронной почты, защиты серверов и АРМ антивирусного ПО разных производителей. | Данный тип мер противодействия не применим для рассматриваемой угрозы. |
| Блокирование работы сервиса путем организации атаки типа «DDoS» | Блокировка сервисов, которые отправляют слишком много запросов. | Данный тип мер противодействия не применим для рассматриваемой угрозы. |
| Получение прямого доступа к БД системы в обход прикладного ПО за счет использования штатных средств администрирования ПО СУБД | Использование сертифицированных средств антивирусной защиты.  Использование для анализа сетевого трафика, электронной почты, защиты серверов и АРМ антивирусного ПО разных производителей. | Использование на предприятии единых регламентирующих документов (если их нет, должны быть разработаны):   * Политика смены пароля; |
| Внедрение сетевого вредоносного ПО в серверные компоненты системы | Использование сертифицированных средств антивирусной защиты.  Использование для анализа сетевого трафика, электронной почты, защиты серверов и АРМ антивирусного ПО разных производителей. | Наличие на предприятии службы информационной безопасности как выделенной структурной единицы.  Использование на предприятии единых регламентирующих документов (если их нет, должны быть разработаны):   * Политика антивирусной защиты; * Инструкция по антивирусной защите; * Инструкция пользователя по безопасной работе в сети Интернет; * Памятка по информационной безопасности пользователя ИС.   Проведение мероприятий по повышению осведомленности пользователей ИС в вопросах защиты информации. |
| Сканирование сетевых адресов и служб серверов системы | Ограничение сетевого доступа к сетевым службам и сервисам серверов.  Использование сертифицированных средств антивирусной защиты.  Использование для анализа сетевого трафика, электронной почты, защиты серверов и АРМ антивирусного ПО разных производителей. | Данный тип мер противодействия не применим для рассматриваемой угрозы. |
| Подбор пароля администратора сервера (ОС, СУБД) с использованием встроенных функций удаленного администрирования системного и прикладного ПО | Ограничение доступа удаленного администрирования.  Использование сертифицированных средств антивирусной защиты.  Использование для анализа сетевого трафика, электронной почты, защиты серверов и АРМ антивирусного ПО разных производителей. | Наличие на предприятии службы информационной безопасности как выделенной структурной единицы.  Использование на предприятии единых регламентирующих документов (если их нет, должны быть разработаны):   * Политика антивирусной защиты; * Инструкция по антивирусной защите; * Инструкция пользователя по безопасной работе в сети Интернет; * Памятка по информационной безопасности пользователя ИС. |
| Загрузка и запуск пользователями на АРМ постороннего ПО, содержащего вредоносный код или являющегося инструментом проведения атак | Использование сертифицированных средств антивирусной защиты.  Использование для анализа сетевого трафика, электронной почты, защиты серверов и АРМ антивирусного ПО разных производителей. | Наличие на предприятии службы информационной безопасности как выделенной структурной единицы.  Использование на предприятии единых регламентирующих документов (если их нет, должны быть разработаны):   * Политика антивирусной защиты; * Инструкция по антивирусной защите; * Инструкция пользователя по безопасной работе в сети Интернет; * Памятка по информационной безопасности пользователя ИС. |
| Подключение к портам управления коммутационного оборудования | Использование сертифицированных средств антивирусной защиты.  Использование для анализа сетевого трафика, электронной почты, защиты серверов и АРМ антивирусного ПО разных производителей. | Наличие на предприятии службы информационной безопасности как выделенной структурной единицы.  Использование на предприятии единых регламентирующих документов (если их нет, должны быть разработаны):   * Политика антивирусной защиты; * Инструкция по антивирусной защите; * Инструкция пользователя по безопасной работе в сети Интернет;   Памятка по информационной безопасности пользователя ИС. |
| Получение персональных данных лицами, которые не должны иметь к ним доступ, в результате ошибок в реализации системы разграничения доступа в прикладных компонентах | Разграничение доступа к записям и экранам.  Настройки доступа на всех уровнях, включая СУБД. | Данный тип мер противодействия не применим для рассматриваемой угрозы. |
| **Угроза НСД при передаче информации по каналам связи** | | |
| Отправка некорректного запроса веб-сервису со стороны смежных систем | Использование для анализа сетевого трафика антивирусное ПО разных производителей.  Ограничение на использование веб-сервисов. | Данный тип мер противодействия не применим для рассматриваемой угрозы. |
| Получение доступа к внутренней сети в результате подмены IP адреса источника (спуффинг) | Ограничение доступа к внутренней сети.  Проверка местоположения пользователя.  Использование сертифицированных средств антивирусной защиты.  Использование для анализа сетевого трафика, электронной почты, защиты серверов и АРМ антивирусного ПО разных производителей. | Данный тип мер противодействия не применим для рассматриваемой угрозы. |
| Перехват и внедрение в сессию доступа к сервисам легального пользователя | Ограничение доступа к внутренней сети.  Проверка местоположения пользователя.  Использование сертифицированных средств антивирусной защиты.  Использование для анализа сетевого трафика, электронной почты, защиты серверов и АРМ антивирусного ПО разных производителей. | Данный тип мер противодействия не применим для рассматриваемой угрозы. |
| Перехват аутентификационных данных при авторизации пользователей и администраторов | Использование защищённого канала связи.  Использование сертифицированных средств антивирусной защиты.  Использование для анализа сетевого трафика, электронной почты, защиты серверов и АРМ антивирусного ПО разных производителей. | Наличие на предприятии службы информационной безопасности как выделенной структурной единицы.  Использование на предприятии единых регламентирующих документов (если их нет, должны быть разработаны):   * Политика антивирусной защиты; * Инструкция по антивирусной защите; * Инструкция пользователя по безопасной работе в сети Интернет;   Памятка по информационной безопасности пользователя ИС. |
| Перехват и модификация данных информационного взаимодействия пользователей с сервером приложений в результате навязывания ложного маршрута во внешних сетях | Ограничение на использование веб-сервисов.  Использование сертифицированных средств антивирусной защиты.  Использование для анализа сетевого трафика, электронной почты, защиты серверов и АРМ антивирусного ПО разных производителей. | Использование на предприятии единых регламентирующих документов (если их нет, должны быть разработаны):   * Политика антивирусной защиты; * Инструкция по антивирусной защите; * Инструкция пользователя по безопасной работе в сети Интернет;   Памятка по информационной безопасности пользователя ИС. |
| Перехват персональных данных в результате прослушивания трафика информационного взаимодействия пользователей с сервером приложений | Использование защищённого канала связи. | Наличие на предприятии службы информационной безопасности как выделенной структурной единицы.  Использование на предприятии единых регламентирующих документов (если их нет, должны быть разработаны):   * Политика антивирусной защиты; * Инструкция по антивирусной защите; * Инструкция пользователя по безопасной работе в сети Интернет;   Памятка по информационной безопасности пользователя ИС. |
| **Угроза НСД, связанная с неправомерными действиями пользователей** | | |
| Внесение заведомо ложной информации в проекты и требования | Отслеживание авторов изменений.  Валидация всех полей на правильность значений. | Данный тип мер противодействия не применим для рассматриваемой угрозы. |
| Отключение средств защиты информации на АРМ пользователя | Доступ к конфигурационным файлам есть только у администраторов.  Ограничения доступа как к папкам с конфигурационными файлами, так и к самим файлам | Наличие на предприятии службы информационной безопасности как выделенной структурной единицы.  Использование на предприятии единых регламентирующих документов (если их нет, должны быть разработаны):   * Политика антивирусной защиты; * Инструкция по антивирусной защите; * Инструкция пользователя по безопасной работе в сети Интернет;   Памятка по информационной безопасности пользователя ИС. |
| Несанкционированный вывод персоналом Кафедры 12 на печать защищаемой информации или запись ее на неучтенные съемные носители | Ограничение на использование веб-сервисов.  Использование сертифицированных средств антивирусной защиты.  Использование для анализа сетевого трафика, электронной почты, защиты серверов и АРМ антивирусного ПО разных производителей.  Ограничение на печать и скачивание данных на локальный компьютер | Наличие на предприятии службы информационной безопасности как выделенной структурной единицы.  Использование на предприятии единых регламентирующих документов (если их нет, должны быть разработаны):   * Политика антивирусной защиты; * Инструкция по антивирусной защите; * Инструкция пользователя по безопасной работе в сети Интернет;   Памятка по информационной безопасности пользователя ИС. |
| Внесение вредоносного ПО при обновлении системного и прикладного ПО серверов и АРМ | Использование сертифицированных средств антивирусной защиты.  Использование для анализа сетевого трафика, электронной почты, защиты серверов и АРМ антивирусного ПО разных производителей.  Резервное копирование. | Повышение квалификации администраторов. |
| Ошибки персонала администрирования по эксплуатации прикладного ПО и оборудования | Использование сертифицированных средств антивирусной защиты.  Использование для анализа сетевого трафика, электронной почты, защиты серверов и АРМ антивирусного ПО разных производителей.  Резервное копирование. | Повышение квалификации администраторов. |
| **Угроза техногенного характера** | | |
| Сбой в работе ТС связанный с дефектами аппаратного обеспечения | Данный тип мер противодействия не применим для рассматриваемой угрозы. | Повышение качества аппаратного обеспечения.  Наличие готового резервного аппаратного обеспечение, на которое можно будет переключиться при сбое. |
| Сбой в программных средствах в результате ошибок программного кода в пакетах обновлений | Резервное копирование. | Выделение специального времени обновления, когда систему никому не нужна.  Повышение квалификации администраторов.  Иметь несколько сред тестирования, на которые будет производится накат до поставки в рабочую среду. |
| Отказ коммутационного оборудования ЛВС | Данный тип мер противодействия не применим для рассматриваемой угрозы. | Повышение качества коммутационного оборудования.  Иметь запасные коммутационные оборудования. |
| Превышение расчетной нагрузки на систему | Резервное копирование | Нагрузочное тестирование на тестовых средах. |
| Отключение или нарушение параметров электропитания на объекте размещения ТС системы | Данный тип мер противодействия не применим для рассматриваемой угрозы. | Наличие резервных генераторов.  Наличие на предприятии эксплуатационной службы.  Работа с облачными серверами. |
| Блокирование внешних каналов связи на объектах системы |  |  |

1. правила отнесения способа реализации угрозы информационной безопасности к актуальному

Для отнесения способа реализации угрозы безопасности ПДн к актуальному используются правила, представленные в таблице 0.

*Таблица 0 – Правила отнесения способа реализации угрозы безопасности ПДн к актуальному*

|  |  |  |  |
| --- | --- | --- | --- |
| **Возможность реализации способа** | **Показатель опасности способа** | | |
| **Низкая** | **Средняя** | **Высокая** |
| Низкая | неактуальный | неактуальный | актуальный |
| Средняя | неактуальный | актуальный | актуальный |
| Высокая | актуальный | актуальный | актуальный |
| Очень высокая | актуальный | актуальный | актуальный |