

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение

высшего образования

**«МИРЭА – Российский технологический университет»**

**РТУ МИРЭА**

ИКБ направление «Киберразведка и противодействие угрозам с применением технологий искусственного интеллекта» 10.04.01

Кафедра КБ-4 «Интеллектуальные системы информационной безопасности»

**Практическая работа №3**

по дисциплине: «Управление информационной безопасностью»   
На тему:

«Разработка модели угроз»

Группа:

ББМО-01-22

Выполнил:

Гребенник Г.С

Проверил:

Пимонов Р.В.

Москва, 2023

УТВЕРЖДАЮ

Директор АО «Россети»

\_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_ /

«\_\_\_» \_\_\_\_\_\_\_\_\_\_ 20\_\_г.

**Модель угроз безопасности информации, защищенной автоматизированной информационной системы** **АО «Россети»**

Москва 2023

**Содержание**

[**ПЕРЕЧЕНЬ ПРИНЯТЫХ СОКРАЩЕНИЙ** 4](#_Toc156847541)

[**1 ОБЩИЕ ПОЛОЖЕНИЯ** 4](#_Toc156847542)

[**1.1 Назначение Модели угроз** 4](#_Toc156847543)

[**1.2 Нормативные правовые акты, методические документы, национальные стандарты, используемые для оценки угроз безопасности информации и разработки модели угроз** 4](#_Toc156847544)

[**2 ОПИСАНИЕ СИСТЕМ И СЕТЕЙ И ИХ ХАРАКТЕРИСТИКА КАК ОБЪЕКТОВ ЗАЩИТЫ** 6](#_Toc156847545)

[**2.1 Наименование систем и сетей, для которых разработана модель угроз безопасности информации** 7](#_Toc156847546)

[**2.2 Класс защищенности, категория значимости систем и сетей, уровень защищенности персональных данных** 7](#_Toc156847547)

[**2.3 Нормативные правовые акты Российской Федерации, в соответствии с которыми создаются и (или) функционируют системы и сети** 7](#_Toc156847548)

[**2.4 Назначение, задачи (функции) систем и сетей, состав обрабатываемой информации и ее правовой режим** 7](#_Toc156847549)

[**2.5 Основные процессы обладателя информации, для обеспечения которых создаются (функционируют) системы** 8](#_Toc156847550)

[**2.6 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)** 8](#_Toc156847551)

[**2.7 Описание функционирования систем и сетей на базе информативно-телекоммуникационной инфраструктуры центра обработки данных или облачной инфраструктуры** 9](#_Toc156847552)

[**2.8 Описание модели предоставления вычислительных услуг, распределения ответственности за защиту информации между обладателями информации, оператором и поставщиком вычислительных услуг** 9](#_Toc156847553)

[**2.9 Описание условий использования информационно-телекоммуникационной инфраструктуры обработки данных или облачной инфраструктуры поставщика услуг (при наличии)** 10](#_Toc156847554)

[**3 ВОЗМОЖНЫЕ ОБЪЕКТЫ ВОЗДЕЙСТВИЯ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ. ВОЗМОЖНЫЕ НЕГАТИВНЫЕ ПОСЛЕДСТВИЯ РЕАЛИЗАЦИИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ** 10](#_Toc156847555)

[**4 ИСТОЧНИКИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ. СПОСОБЫ РЕАЛИЗАЦИИ УГРОЗ БЕЗОПАСНОТИ ИНФОРМАЦИИ** 11](#_Toc156847556)

[**5 СПОСОБЫ РЕАЛИЗАЦИИ (ВОЗНИКНОВЕНИЯ) УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ** 12](#_Toc156847557)

[**6 АКТУАЛЬНЫЕ УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ** 15](#_Toc156847558)

## **ПЕРЕЧЕНЬ ПРИНЯТЫХ СОКРАЩЕНИЙ**

|  |  |
| --- | --- |
| АИС | Автоматизированная информационная система |
| БД | База данных |
| ИБ | Информационная безопасность |
| ИСПДн | Информационная система персональных данных |
| НСД | Несанкционированный доступ |
| ПДн | Персональные данные |
| ПО | Программное обеспечение |
| СЗИ | Средство защиты информации |
| УБИ | Угроза безопасности информации |
| ФСТЭК России | Федеральная служба по техническому и экспортному контролю |

**1 ОБЩИЕ ПОЛОЖЕНИЯ**

**1.1 Назначение Модели угроз**

Разработка модели угроз безопасности информации выполняется для определения актуальных угроз безопасности защищаемой информации, обрабатываемой в АИС АО «Россети» (далее «Россети»).

Результаты определения актуальных угроз безопасности защищаемой информации предназначены для формирования обоснованных требований к составу и содержанию мер по обеспечению информационной безопасности АИС Россети.

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

Оценка угроз безопасности информации и разработка модели угроз осуществляются на основании нормативно правовых актов Российской Федерации. В перечень используемых нормативных источников входят:

– Федеральный закон от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

– Федеральный закон от 27 июля 2006 г. N 152-ФЗ «О персональных данных»;

– Постановление Правительства Российской Федерации от 01 ноября 2012 г. N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– Указ Президента Российской Федерации от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»;

– Приказ ФСТЭК России от 18 февраля 2013 г. N 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

– Методика оценки угроз безопасности информации ФСТЭК России, утвержденная ФСТЭК России 5 февраля 2021 г;

– «Требования к средствам антивирусной защиты» (утвержден приказом ФСТЭК России от 20.03.2012 N 28. ДСП);

– «Требования к межсетевым экранам» (утвержден приказом ФСТЭК России от 09.02.2016 N 9. ДСП);

– «Требованиям безопасности информации к операционным системам» (утвержден приказом ФСТЭК России от 19.08.2016 N 119. ДСП);

– «Требования к средствам контроля съёмных машинных носителей информации» (утвержден приказом ФСТЭК России от 28.07.2014 N 87. ДСП).

– ГОСТ Р 51624-2000 «Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования»;

– ГОСТ Р 56545-2015 «Защита информации. Уязвимости информационных систем. Правила описания уязвимостей».

– Приказ ФСБ России № 416, ФСТЭК России № 489 от 31 августа 2010 г. «Об утверждении требований о защите информации, содержащейся в информационных системах общего пользования».

**1.3 Область применения настоящей Модели угроз**

Областью применения настоящей модели угроз является совокупность информационных и программно-аппаратных средств, а также информационных технологий, применяемых при обработке информации в АИС Россети.

В область применения входит:

– информация от заказчика, как совокупность информации и её носителей, используемых в АИС Россети,

– информационные технологии, применяемые при обработке информации,

– технологические средства, осуществляющие обработку информации (средства вычислительной техники, информационно-вычислительные комплексы сети, средства и системы хранения, передачи, приема и обработки информации),

– программные средства инфраструктурного уровня (операционные системы),

–средства защиты информации,

– подсистемы и сервисы АИС Россети.

Информационная система персональных данных (ИСПДн) Россети обрабатывает разнообразные персональные данные.

Эти данные включают:

−  Персональные данные сотрудников. В них входят данные о сотрудниках организации, такие как имена, даты рождения, адреса, номера паспортов, контактная информация, информация о трудоустройстве, налоговые и страховые данные, медицинская информация и т. д.

−  Данные клиентов/заказчиков и партнеров. ИСПДн содержит информацию о клиентах и партнерах предприятия, включая контактные данные, проекты, историю заказов материалов, финансовую информацию и другие данные, необходимые для ведения деловых отношений.

− Бухгалтерская и финансовая информация. ИСПДн включает в себя данные о доходах, расходах, налогообложении, финансовых операциях и другие финансовые параметры предприятия.

− Другие специфические данные: ИСПДн содержит другие специфические данные, связанные с деятельностью предприятия.

Модель угроз включает в себя данные по угрозам, связанные с несанкционированным, в том числе случайным доступом в ИСПДн Россети с целью изменения, хищения, неправомерного распространения информации или деструктивных воздействий на элементы ИСПДн и обрабатываемых в них информации с использованием программных и программно-аппаратных средств с целью уничтожения или блокирования защищаемой информации.

В Модели угроз представлена оценка исходного уровня защищенности защищаемой информации в Россети, а также анализ возможных угроз безопасности информации.

Анализ угроз безопасности информации включает: описание угроз; оценку вероятности возникновения угроз; оценку реализуемости угроз; оценку опасности угроз; определение актуальности угроз.

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

 Обладателем информации является АО «Россети».

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

Ответственными за обеспечение защиты информации и отвечающие за обеспечение защиты информации (безопасности) считаются:

– руководитель подразделения Россети,

– отдел информационной безопасности (ИБ). Отдел ИБ включает в себя руководителя информационной безопасности,

– работники, выполняющие следующие функции: администратор информационных систем, администратор локальной вычислительной сети, администратор по обеспечению безопасности информации и инженеры по безопасности (отвечают за настройку и обслуживание технических систем и сетей с учетом безопасности, устанавливают антивирусное программное обеспечение, брандмауэры, системы мониторинга безопасности и другие технические средства для защиты информации).

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

Отсутствует, разработка произведена собственными силами.

**2 ОПИСАНИЕ СИСТЕМ И СЕТЕЙ И ИХ ХАРАКТЕРИСТИКА КАК ОБЪЕКТОВ ЗАЩИТЫ**

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

– объект 1 – информационная система персональных данных АСИ Россети,

– объект 2 – ЛВС, в рамках которой работники обеспечивают обмен информацией,

– объект 3 – сервер, на котором хранятся БД ИСПДн, АСИ Россети.

**2.2 Класс защищенности, категория значимости систем и сетей, уровень защищенности персональных данных**

Класс защищенности, категория значимости систем и сетей, а также уровень защищенности персональных данных в организации зависят от специфики деятельности, объема обрабатываемых данных и требований законодательства. В России, для определения этих параметров, могут использоваться ряд нормативных актов, включая ГОСТы и Федеральный закон «О персональных данных». Класс защищенности: Класс защищенности систем и сетей определяет уровень и глубину мер безопасности, которые должны быть применены к информационным ресурсам.

В России классы защищенности могут определяться согласно ГОСТ ИСО/МЭК 27001-2012 и другим нормативам.

Обычно они имеют следующие обозначения:

* КС1 (критический класс защищенности).
* КС2 (высокий класс защищенности).
* КС3 (средний класс защищенности).
* КС4 (низкий класс защищенности).

Уровень защищенности ИСПДн АСИ Россети – КС3 (средний класс защищенности).

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

АСИ Россети разработана в соответствии с положениями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», а также иными подзаконными нормативно-правовыми актами в сфере персональных данных.

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

ИСПДн Россети предназначена для обработки информации о сотрудниках и заказчиках, поставщиков и других физических лиц, связанных с деятельностью организации, с целью обеспечения безопасности от несанкционированного доступа на объект посторонних людей, порчи имущества, а также хранение всей информации на сервере.

В ИСПДн Россети могут обрабатываться следующие персональные данные:

– фамилия, имя, отчество работника,

– серия и номер документа, удостоверяющего личность работника, кем и когда выдан,

– дата рождения работника,

– адрес проживания работника,

– реквизиты ИНН,

– реквизиты страхового номера Индивидуального лицевого счета в Пенсионном фонде РФ,

– сведения о доходах работника (номер банковской карты, номер лицевого счета, размер оклада, размер надбавок, премий),

– сведения о начислениях работников.

Основные задачи (функции) ИСПДн Россети:

* Сбор и хранение персональные данных, включая данные сотрудников, заказчиков и других заинтересованных сторон;
* Обеспечение контроля над доступом к персональным данным и информационным ресурсам в соответствии с уровнем доступа сотрудников;
* Обработка персональных данных, включая обновление, анализ и создание отчетов на основе этих данных;
* Обеспечение безопасности персональных данных, включая защиту от несанкционированного доступа, утечек и взломов;
* Обеспечение соблюдения законодательства о защите персональных данных и других нормативных актов.

Правовой режим информации определяется законодательством о защите персональных данных и включает в себя требования к сбору, обработке, хранению и передаче персональных данных.

**2.5 Основные процессы обладателя информации, для обеспечения которых создаются (функционируют) системы**

Обладатель информации Россети должен регулярно проводить следующие процессы для обеспечения безопасности и эффективности обработки персональных данных:

* Сбор и регистрации данных;
* Управление доступом;
* Обеспечение конфиденциальности;
* Обучение и осведомленность;
* Реагирование на инциденты безопасности и уведомление о нарушениях;
* Соблюдение законодательства.

**2.6 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)**

Описание групп внешних и внутренних пользователей систем и сетей, уровней их полномочий и типов доступа представлены в таблице 1.

Таблица 1 – Описание групп пользователей

|  |  |  |
| --- | --- | --- |
| **Типовая роль** | **Уровень доступа к ИСПДн** | **Разрешенные действия по отношению к ИСПДн** |
| Администраторы систем и сетей | Обладает полной правами права на управление и настройку системы, полные права на настройку и конфигурацию системы, полный мониторинг и аудит системы, полное управление резервными копия и восстановлением данные | Полный доступ к управлению, настройкам и обслуживаниям информационных систем и сетей организации. Полный доступ для администрирования |
| Пользователи ИСПДн | Обладают полной информацией о системном и прикладном программном обеспечении ИСПДн | Сбор, систематизация, хранение, уточнение, использование, распространение, обезличивание, блокирование, уничтожение |
| Менеджеры и руководители | Обладают полномочиями для настройки и мониторинга безопасности данных | Имеют доступ к данным и ресурсам, необходимым для принятия решений и управления бизнес-процессами |
| Финансовый отдел | Доступ к финансовым данным, бухгалтерской информации и другим финансовым ресурсам организации | Доступ к отчетам, договорам компании |
| Пользователи, являющиеся внешними по отношению к ИСПДн | Информация относящееся к самому субъекту | Уточнение |
| Поставщики | Отсутствует | Отсутствует |
| Заказчики | Отсутствует | Отсутствует |

**3 ВОЗМОЖНЫЕ ОБЪЕКТЫ ВОЗДЕЙСТВИЯ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ. ВОЗМОЖНЫЕ НЕГАТИВНЫЕ ПОСЛЕДСТВИЯ РЕАЛИЗАЦИИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ**

Возможные негативные последствия реализации (возникновения) угроз безопасности информации, способы реализации угроз отображены в таблице 2.

Таблица 2 – Возможные негативные последствия и объекты воздействия

|  |  |  |
| --- | --- | --- |
| **Негативные последствия** | **Объекты воздействия** | **Виды воздействия** |
| Потеря, изменение или хищение данных | Сервер, база данных информационной системы, содержащая конфиденциальную информацию | Подмена данных, содержащихся на сервере |
| АРМы сотрудников организации | - Подмена данных, содержащих платёжную информацию, информацию о проектах  - Отправка электронных писем с недостоверной информацией или доступ к системе, с последующими заказами материалов |
| Нарушение работоспособности программно-аппаратных средств обработки, передачи и хранения информации | Программно-аппаратные средства обработки и хранения информации | Несанкционированный доступ к составляющим с последующим хищением жёсткого диска, либо добавление своего USB-носителя |
| Хищение денежных средств со счета организации (У2) | Банк-клиент | Несанкционированная подмена данных, содержащихся в реквизитах платежного поручения |
| АРМ главного бухгалтера | Подмена данных, содержащих реквизиты платежных поручений и другой платежной информации на АРМ главного бухгалтера |
| Срыв запланированной сделки с партнером/заказчиком (У2) | АРМ руководителя организации | Модификация информации и отправка электронных писем с недостоверной информацией от имени руководителя организации |
| Электронный почтовый ящик руководителя организации | Модификация информации и отправка электронных писем с недостоверной информацией от имени руководителя организации |
| Недоступность данных | Сервер и хранилище данных | Несанкционированная отправка команд, приводящая к несрабатыванию средств аварийной защиты |
| Программно-аппаратные средства | Несанкционированный доступ к источнику бесперебойного питания |
| Утечка персональных данных | Веб-приложение информационной системы | Несанкционированный доступ к идентификационной информации граждан, содержащейся в веб-приложении информационной системы |

**4 ИСТОЧНИКИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ. СПОСОБЫ РЕАЛИЗАЦИИ УГРОЗ БЕЗОПАСНОТИ ИНФОРМАЦИИ**

Были определены источники угроз безопасности, собрана модель нарушителя, а также определены возможные цели реализации угроз в организации. Всё это представлено в таблице 3.

Таблица 3 – Возможные цели реализации угроз безопасности информации нарушителями

|  |  |  |  |
| --- | --- | --- | --- |
| **№ вида** | **Вид нарушителя** | **Категории нарушителя** | **Возможные цели реализации угроз безопасности информации** |
| 1 | Отдельные физические лица (хакеры) | Внешний | Получение финансовой или иной материальной выгоды |
| 2 | Конкурирующие организации (шпионы) | Внешний | - Получение конкурентных преимуществ  - Получение финансовой или иной материальной выгоды |
| 3 | Разработчики программных, программно-аппаратных средств | Внутренний | - Получение финансовой или иной материальной выгоды  - Непреднамеренные, неосторожные или неквалифицированные действия |
| 4 | Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора (администрация, охрана, уборщики и т.д.) | Внутренний | Непреднамеренные, неосторожные или неквалифицированные действия |
| 5 | Авторизованные пользователи систем и сетей АО «Россети» | Внутренний | - Получение финансовой или иной материальной выгоды  - Непреднамеренные, неосторожные или неквалифицированные действия  - Месть за ранее совершенные действия |
| 6 | Системные администраторы и администраторы безопасности | Внутренний | - Получение финансовой или иной материальной выгоды  - Месть за ранее совершенные действия  - Непреднамеренные, неосторожные или неквалифицированные действия |
| 7 | Бывшие (уволенные) работники (пользователи) АО «Россети» | Внешний | - Получение финансовой или иной материальной выгоды  - Месть за ранее совершенные действия |

**5 СПОСОБЫ РЕАЛИЗАЦИИ (ВОЗНИКНОВЕНИЯ) УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ**

Способы реализации угроз безопасности информации указаны в таблице 4.

Таблица 4 – Определение актуальных способов реализации угроз безопасности информации и соответствующие им виды нарушителей и их возможности

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **№**  **п/п** | **Вид нарушителя** | **Категория нарушителя** | **Объект воздействия** | **Доступные интерфейсы** | **Способы реализации** |
| 1 | Отдельные физические лица (хакеры) | Внешний | Доступ к базам данных | Веб-интерфейс удаленного администрирования базы данных  информационной системы | Использование уязвимостей конфигурации системы управления базами данных |
| Удаленное рабочее место пользователя | Доступ через локальную вычислительную сеть организации | Внедрение вредоносного ПО; использование уязвимостей системы |
| 2 | Конкурирующие организации (шпионы) | Внешний | Доступ к базам данных | Веб-интерфейс удаленного администрирования базы данных информационной системы  Пользовательский веб-интерфейс доступа к базе данных информационной системы | Использование уязвимостей конфигурации системы управления базами данных |
| АРМ сотрудника бухгалтерии Россети | Съемные машинные носители информации, содержащие  аутентификационную информацию | Извлечение аутентификационной информации из постоянной памяти носителя |
| 3 | Разработчики программных, программно-аппаратных средств | Внутренний | АРМ сотрудников | Съемные машинные носители информации, содержащие  аутентификационную информацию | Извлечение аутентификационной информации из постоянной памяти носителя;  Внедрение вредоносного ПО |
| 4 | Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора (администрация, охрана, уборщики и т.д.) | Внутренний | Доступ к базам данных | Веб-интерфейс удаленного администрирования базы данных информационной системы  Пользовательский веб-интерфейс доступа к базе данных информационной системы | Использование уязвимостей конфигурации системы управления базами данных |
| Коммутационный контроллер | Удаленный канал управления коммутационным контроллером  Съемные машинные носители информации, содержащие  аутентификационную информацию | Использование уязвимостей кода; кража аутентификационной информации из постоянной памяти носителя |
| 5 | Системные администраторы и администраторы безопасности | Внутренний | Доступ к базам данных | Веб-интерфейс удаленного администрирования базы данных информационной системы  Пользовательский веб-интерфейс доступа к базе данных информационной системы | Использование уязвимостей конфигурации системы управления базами  данных |
| Удаленное рабочее место пользователя | Доступ через локальную вычислительную сеть организации  Съемные машинные носители информации, подключаемые к АРМ пользователя | Использование уязвимостей конфигурирования системы; установка вредоносного ПО |
|  | Линия связи между сервером основного центра обработки  данных и сервером резервного центра обработки данных: | Канал передачи данных между сервером основного центра обработки данных и сервером резервного центра обработки  данных | Установка закладок |
| 6 | Бывшие (уволенные) работники/сотрудники (пользователи) АО«Россети» | Внешний | Доступ к базам данных | Веб-интерфейс удаленного администрирования базы данных информационной системы  Пользовательский веб-интерфейс доступа к базе данных информационной  системы | Использование уязвимостей конфигурации системы управления базами  данных |
| Удаленное рабочее место пользователя | Доступ через локальную вычислительную сеть организации | Внедрение вредоносного ПО; использование уязвимостей системы |
| АРМ сотрудника бухгалтерии Россети | Доступ к базам данных, информация о клиентах | Извлечение/ кража информации из постоянной памяти носителя |

**6 АКТУАЛЬНЫЕ УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

Актуальной считается угроза, которая может быть реализована в ИСПДн и представляет опасность для ПДн.

Актуальность угрозы определяется следующими параметрами: уровень исходной защищенности ИСПДн и частота (вероятность) реализации рассматриваемой угрозы.

Исходная степень защищенности определяется следующим образом:

1. ИСПДн имеет высокий уровень исходной защищенности, если не менее 70% характеристик ИСПДн соответствуют уровню «высокий» (суммируются положительные решения по первому столбцу, соответствующему высокому уровню защищенности), а остальные – среднему уровню защищенности (положительные решения по второму столбцу).
2. ИСПДн имеет средний уровень исходной защищенности, если не выполняются условия по пункту 1 и не менее 70% характеристик ИСПДн соответствуют уровню не ниже «средний» (берется отношение суммы положительные решений по второму столбцу, соответствующему среднему уровню защищенности, к общему количеству решений), а остальные – низкому уровню защищенности.
3. ИСПДн имеет низкую степень исходной защищенности, если не выполняются условия по пунктам 1 и 2.

Под частотой (вероятностью) реализации угрозы понимается определяемый экспертным путём показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности ПДн для данной ИСПДн в складывающихся условиях обстановки.

Вводятся четыре вербальных градации этого показателя:

маловероятно – отсутствуют объективные предпосылки для осуществления угрозы (например, угроза хищения носителей информации лицами, не имеющими легального доступа в помещение, где последние хранятся);

низкая вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (например, использованы соответствующие средства защиты информации);

средняя вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны;

высокая вероятность - объективные предпосылки для реализации угрозы существуют, и меры по обеспечению безопасности ПДн не приняты.

При составлении перечня актуальных угроз безопасности ПДн каждой градации вероятности возникновения угрозы ставится в соответствие числовой коэффициент, а именно:

0 – для маловероятной угрозы;

2 – для низкой вероятности угрозы;

5 – для средней вероятности угрозы;

10 – для высокой вероятности угрозы.

С учетом изложенного коэффициент реализуемости угрозы Y будет определяться соотношением.

По значению коэффициента реализуемости угрозы Y формируется вербальная интерпретация реализуемости угрозы.

Далее оценивается опасность каждой угрозы. При оценке опасности 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.

При составлении перечня актуальных угроз безопасности персональных данных каждой степени исходного уровня защищенности ИСПДн ставится в соответствие числовой коэффициент Y₁, а именно:

0 – для высокой степени исходной защищенности;

5 – для средней степени исходной защищенности;

10 – для низкой степени исходной защищенности.

Правила актуальности представлены в таблице 5.

Таблица 5 - Правила отнесения угрозы безопасности к актуальной

|  |  |  |  |
| --- | --- | --- | --- |
| Возможность реализации угрозы | Показатель опасности угрозы | | |
| Низкая | Средняя | Высокая |
| Низкая | неактуальна | неактуальная | актуальная |
| Средняя | неактуальная | актуальная | актуальная |
| Высокая | актуальная | актуальная | актуальная |
| Очень высокая | актуальная | актуальная | актуальная |

Для выявления из всего перечня угроз безопасности персональных данных актуальных для информационной системы персональных данных оцениваются два показателя: уровень исходной защищенности информационной системы персональных данных и частота (вероятность) реализации рассматриваемой угрозы.

Под уровнем исходной защищенности информационной системы персональных данных (ИСПДн) понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПДн, а именно:

* территориальное размещение,
* наличие соединения сетями общего пользования,
* встроенные (легальные) операции с записями баз персональных данных,
* разграничение доступа к персональным данным,
* наличие соединений с другими базами персональных данных иных ИСПДн,
* уровень обобщения (обезличивания) персональных данных,
* объем персональных данных, который предоставляется сторонним пользователям ИСПДн без предварительной обработки.

Показатели исходной защищенности отображены в таблице 6.

Таблица 6 – Показатели исходной защищенности ИСПДн Россети

|  |  |  |  |
| --- | --- | --- | --- |
| **Технические и эксплуатационные характеристики ИСПДн** | **Уровень защищенности** | | |
| **Высокий** | **Средний** | **Низкий** |
| **1. По территориальному размещению:** |  | + |  |
| распределенная ИСПДн, которая охватывает несколько областей, краев, округов или государство в целом; | – | – | – |
| городская ИСПДн, охватывающая не более одного населенного пункта (города, поселка); | – | – | – |
| корпоративная распределенная ИСПДн, охватывающая многие подразделения одной организации; | – | – | – |
| локальная (кампусная) ИСПДн, развернутая в пределах нескольких близко расположенных зданий; | – | – | – |
| локальная ИСПДн, развернутая в пределах одного здания | – | + | – |
| **2. По наличию соединения с сетями общего пользования:** |  | + |  |
| ИСПДн, имеющая многоточечный выход в сеть общего пользования; | – | – | – |
| ИСПДн, имеющая одноточечный выход в сеть общего пользования; | – | + | – |
| ИСПДн, физически отделенная от сети общего пользования | – | – | – |
| **3. По встроенным (легальным) операциям с записями баз персональных данных:** |  |  | + |
| чтение, поиск; | – | – | + |
| запись, удаление, сортировка; | – | + | – |
| модификация, передача | – | – | + |
| **4.По разграничению доступа к персональным данным:** |  | + |  |
| ИСПДн, к которой имеют доступ определенные перечнем сотрудники организации, являющейся владельцем ИСПДн, либо субъект ПДн; | – | + | – |
| ИСПДн, к которой имеют доступ все сотрудники организации, являющейся владельцем ИСПДн; | – | + | – |
| ИСПДн с открытым доступом | – | – | – |
| **5. По наличию соединений с другими базами ПДн иных ИСПДн:** |  | + |  |
| интегрированная ИСПДн (организация использует несколько баз ПДн ИСПДн, при этом организация не является владельцем всех используемых баз ПДн); | – | + | – |
| ИСПДн, в которой используется  одна база ПДн, принадлежащая организации – владельцу данной ИСПДн | – | – | – |
| **6. По уровню обобщения (обезличивания) ПДн:** |  |  | + |
| ИСПДн, в которой предоставляемые пользователю данные являются обезличенными (на уровне организации, отрасли, области, региона и т.д.); | – | – | – |
| ИСПДн, в которой данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации; | – | – | + |
| ИСПДн, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта ПДн) | – | – | – |
| **7. По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки:** | + |  |  |
| ИСПДн, предоставляющая всю базу данных с ПДн; | – | – | – |
| ИСПДн, предоставляющая часть ПДн; | – | – | – |
| ИСПДн, не предоставляющая никакой информации. | + | – | – |

Числовой коэффициент исходной защищенности (Y1) соответствует значению 5 – средняя степень исходной защищенности.

Для каждой угрозы определяется вероятность реализации угрозы Y2 и соответствующий коэффициент:

2 - для низкой вероятности угрозы;

5 - для средней вероятности угрозы;

10 - для высокой вероятности угрозы.

С учетом этого реализуемость каждой угрозы Y рассчитывается по формуле:

Y = (Yl+Y2)/20.

По значению коэффициента реализуемости угрозы Y формируется вербальная интерпретация реализуемости угрозы следующим образом:

если О < 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.

Типовая модель реализации следующих угроз безопасности ПДн (табл. 7).

Таблица 7 – Таблица угроз и коэффициент возможной реализации

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Наименование угрозы** | **Описание угрозы** | **Возможность реализации угрозы (Y2)** | **Показатель опасности угрозы (0-1)** | **Коэффициент защищенности**  **(Y)** |
| УБИ 8. Угроза нарушения функционирования (работоспособности) | Угроза заключается в частичной или полной утрате работоспособности или функциональности компонента или информационной системы в целом. | 5 | 1 | 0,5 |
| УБИ 1. Угроза утечки информации | Общая угроза, связанная с утечкой, компрометацией, кражей, разглашением информации, специальной (умышленной) или случайной. | 2 | 0,5 | 0,35 |
| Угроза изменения компонентов информационной (автоматизированной) системы | Угроза заключается в возможности получения нарушителем доступа к сети, файлам, внедрения закладок и т.п. путём несанкционированного изменения состава программных или аппаратных средств информационной системы. | 2 | 1 | 0,35 |
| УБИ 2. Угроза несанкционированного доступа | Угроза заключается в получении доступа к информационным ресурсам, нарушающего установленные в информационной системе правила разграничения доступа. Например, несанкционированный доступ к информации, хранимой на файловом хранилище | 10 | 0,5 | 0,75 |
| УБИ 5. Угроза удаления информационных ресурсов | Угроза заключается в несанкционированном удалении обрабатываемой в информационной системе информации. Например, удаление информации, обрабатываемой в базе данных, в обход существующих механизмов разграничения доступа | 2 | 1 | 0,35 |
| УБИ 6. Угроза отказа в обслуживании | Угроза заключается в недоступности информационной системы или ее компонентов и (или) приостановлении оказания услуг. | 5 | 1 | 0,5 |

По результатам, ИСПДн Россети соответствует среднему уровню защищенности.