УТВЕРЖДАЮ

Президент-председатель правления ПАО «РОСНЕФТЬ»

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

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

**МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ПРИ ЕЕ ОБРАБОТКЕ В ИНФОРМАЦИОННОЙ СИСТЕМЕ ПЕРСОНАЛЬНЫХ ДАННЫХ «ПАО РОСНЕФТЬ»**

**Публичное акционерное общество «РОСНЕФТЬ»**

Москва 2023

СОДЕРЖАНИЕ

[1 ОБЩИЕ ПОЛОЖЕНИЯ 5](#_Toc148354719)

[1.1. Назначение Модели угроз 5](#_Toc148354720)

[1.2. Нормативно-правовые акты, методические документы, используемые для оценки угроз безопасности информации и разработки Модели угроз 5](#_Toc148354721)

[1.3. Область применения настоящей Модели угроз 6](#_Toc148354722)

[1.4. Наименование обладателя информации, заказчика, оператора систем и сетей 7](#_Toc148354723)

[1.5. Подразделения, должностные лица, ответственные за обеспечение защиты информации (безопасности) систем и сетей 8](#_Toc148354724)

[1.6. Наименование организации, привлекаемой для разработки модели угроз безопасности информации (при наличии) 8](#_Toc148354725)

[2 ОПИСАНИЕ СИСТЕМ И СЕТЕЙ И ИХ ХАРАКТЕРИСТИКА КАК ОБЪЕКТОВ ЗАЩИТЫ 9](#_Toc148354726)

[2.1. Наименование систем и сетей, для которых разработана модель угроз безопасности информации: 9](#_Toc148354727)

[2.2. Класс защищенности, категория значимости систем и сетей, уровень защищенности персональных данных 9](#_Toc148354728)

[2.3. Нормативно правовые акты Российской Федерации, в соответствии с которыми создаются и (или) функционируют системы и сети 10](#_Toc148354729)

[2.4. Назначение, задачи (функции) систем и сетей, состав обрабатываемой информации и ее правовой режим; основные процессы обладателя информации, для обеспечения которых создаются (функционируют) системы и сети 10](#_Toc148354730)

[2.5. Основные процессы обладателя информации, для обеспечения которых создаются (функционируют) системы и сети 11](#_Toc148354731)

[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 12](#_Toc148354732)

[2.7 Описание функционирования систем и сетей на базе информативно-телекоммуникационной инфраструктуры центра обработки данных или облачной инфраструктуры 12](#_Toc148354733)

[2.8 Описание модели предоставления вычислительных услуг, распределения ответственности за защиту информации между обладателями информации, оператором и поставщиком вычислительных услуг 13](#_Toc148354734)

[2.9 Описание условий использования информационно-телекоммуникационной инфраструктуры обработки данных или облачной инфраструктуры поставщика услуг (при наличии) 13](#_Toc148354735)

[3. ВОЗМОЖНЫЕ ОБЪЕКТЫ ВОЗДЕЙСТВИЯ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ. ВОЗМОЖНЫЕ НЕГАТИВНЫЕ ПОСЛЕДСТВИЯ РЕАЛИЗАЦИИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ 14](#_Toc148354736)

[4. ИСТОЧНИКИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ. СПОСОБЫ РЕАЛИЗАЦИИ УГРОЗ БЕЗОПАСНОТИ ИНФОРМАЦИИ 15](#_Toc148354737)

[5. СПОСОБЫ РЕАЛИЗАЦИИ (ВОЗНИКНОВЕНИЯ) УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ 17](#_Toc148354738)

[6. АКТУАЛЬНЫЕ УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 19](#_Toc148354739)

Перечень принятых сокращений

АИС – Автоматизированная информационная система

БД – База данных

ИСПДн – Информационная система персональных данных

ЛВС – Локальная вычислительная сеть

НСД – Несанкционированный доступ

ОС – Операционная система

ПДн – Персональные данные

ПО – Программное обеспечение

# 1 ОБЩИЕ ПОЛОЖЕНИЯ

# 1.1. Назначение Модели угроз

Разработка Модели угроз выполняется для определения актуальных угроз безопасности защищаемой информации, обрабатываемой в АИСПД ПАО Роснефть.

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

# 1.2. Нормативно-правовые акты, методические документы, используемые для оценки угроз безопасности информации и разработки Модели угроз

Нормативной основой настоящей модели являются законодательство Российской Федерации и нормы права в части обеспечения информационной безопасности, требования нормативных актов Российской Федерации, Федерального органа исполнительной власти, уполномоченного в области безопасности, Федерального органа исполнительной власти, уполномоченного в области противодействия техническим разведкам и технической защиты информации, и основывается, в том числе

− Федеральный закон от 27.06.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

− Федеральный закон от 27.06.2006 г. № 152-ФЗ «О персональных данных»;

− Федеральный закон "О связи" № 126-ФЗ

− Распоряжение Правительства РФ "О мерах по обеспечению информационной безопасности Российской Федерации" от 09.06.2008 № 538

− Методические рекомендации по обеспечению информационной безопасности:

## 1.3. Область применения настоящей Модели угроз

Информационная система персональных данных (ИСПДн) предназначена для обработки, хранения и управления персональными данными сотрудников, клиентов, партнеров и других физических лиц, которые могут быть связаны с деятельностью ПАО "РОСНЕФТЬ"

В контексте ПАО "РОСНЕФТЬ" ИСПДн выполняет следующие основные функции и цели

- правление персональными данными сотрудников;

- Учет и администрирование доступа;

- Соблюдение законодательства:

- Конфиденциальность и безопасность данных

- Повышение эффективности управления персоналом и другие задачи.

- Упрощение процессов взаимодействия с клиентами и партнерами:

- Автоматизация процессов отчетности:

В соответствии с актом классификации ИСПДн ПАО Роснефть от 15.10.2021 №555-о утверждённым президентом и по результатам анализа исходных данных ИСПДн Роснефть имеет 2 уровень защищенности персональных данных (УЗ 2).

Информационная система персональных данных (ИСПДн) промышленного предприятия обрабатывает разнообразные персональные данные в соответствии с целями и задачами этой организации.

ИСПДн ПАО Роснефть обрабатывает следующие категории данных:

− Персональные данные сотрудников. Это включает в себя данные о сотрудниках предприятия, такие как имена, даты рождения, адреса, номера паспортов, контактная информация, информация о трудоустройстве, налоговые и страховые данные, медицинская информация и т. д.

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

− Данные посетителей и поставщиков. ИСПДн содержит информацию о посетителях и поставщиках, включая данные о въезде и выезде, договорах и контактной информации.

− 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 содержит данные по угрозам, связанным с несанкционированным, в том числе случайным. доступом в ИСПДн Роснефть с целью изменения, 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, а также анализ 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

ПАО “Роснефть”

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

Подразделениями, отвечающими за обеспечение защиты информации, выступают:

- Отдел информационной безопасности (ИБ). Отдел ИБ может включать в себя руководителя информационной безопасности и его команду, включая администраторов безопасности, аналитиков информационной безопасности и специалистов по защите данных.

- Системные администраторы 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 «Роснефть»;

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

– объект 3 – сервер, на котором хранятся БД ИСПДн, «ПАО Роснефть».

# 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 на промышленном предприятии 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 Р 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).

Категория значимости систем и сетей: Категория значимости определяет важность информационных систем и сетей для деятельности предприятия и определяет необходимый уровень защиты. В России категории значимости также могут быть определены согласно ГОСТ Р ИСО/МЭК 27001-2012 и другим стандартам.

Категории значимости могут быть такими, как "критическая," "высокая," "средняя," "низкая" и т. д.

Уровень защищенности ИСПДн ПАО Роснефть – третий.

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

Настоящая Модель угроз разработана в соответствии с положениями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее в тексте – Закон № 152-ФЗ), 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; основные процессы обладателя информации, для обеспечения которых создаются (функционируют) системы и сети

ИСПДн Роснефти предназначены для обработки, хранения и защиты персональных данных сотрудников, клиентов, поставщиков и других физических лиц, связанных с деятельностью предприятия.

В ИСПДн Роснефти могут обрабатываться следующие персональные данные:

Основные задачи (функции) ИСПДн Роснефти:

* Сбор и хранение персональные данных, включая данные сотрудников, клиентов 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.

Состав обрабатываемой информации включает в себя персональные данные, такие как имена, даты рождения, адреса, номера паспортов, данные о трудоустройстве, налоговые и страховые данные, медицинская информация и другие данные, связанные с работой и взаимодействием сотрудников, клиентов и партнеров предприятия.

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 и сети

Обладатель информации ПАО Роснефти 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

Таблица 1 – Описание групп пользователей

|  |  |  |
| --- | --- | --- |
| Типовая роль | Уровень доступа к ИСПДн | Разрешенные действия в ИСПДн |
| Сотрудники отдела IT | Обладают полным функционалом для технической поддержки и для обслуживания информационных систем | расширенные полномочия для управления технической инфраструктурой |
| 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 предприятия. полный доступ для администрирования. |
| 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 |
| Отдел кадров | имеет доступ к данным сотрудников, включая информацию о трудоустройстве, заработной плате и другие данные. | Доступ к данным сотрудником, их персональные данные и т.п. |
| Финансовый отдел | Доступ к финансовым данным, бухгалтерской информации и другим финансовым ресурсам предприятия. | Доступ к отчетам, договорам компании |
| Специалисты по безопасности | Ответственные за обеспечение информационной безопасности и управление доступом. | Отслеживание различных активностей пользователей |
| Поставщики | доступ к системам предприятия для взаимодействия в рамках поставок и заказов. | Просмотр заказов |
| Аудиторы и ревизоры | Имеют временный доступ к системам и данным предприятия для проверки соблюдения нормативов и стандартов. | Доступ ко всему объекту для проверки соблюдения требований |

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

Не реализовано.

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

Не реализовано.

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

Не реализовано.

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

Таблица 2 – Описание групп пользователей

|  |  |  |
| --- | --- | --- |
| Негативные последствия | Объекты воздействия | Виды воздействия |
| Потеря (хищение) данных | Серверы и хранилища данных | Несанкционированная подмена данных, содержащихся на серверах |
| АРМы бухгалтерии | Подмена данных, содержащих реквизиты платежных поручений и другой платежной информации на АРМ главного бухгалтера |
| АРМы финансового департамента | Подмена данных, переделанная информации в платежных распоряжениях и отправка недостоверных распоряжений от имени финансового директора |
| Нарушение штатного режима функционирования автоматизированной системы управления и управляемого объекта и/или процесса | АРМы отдела Информационной безопасности | Модификация информации и отправка электронных писем с недостоверной информацией от имени руководителя организации |
| АРМ главного инженера/администратора | Несанкционированная отправка команд, приводящая к несрабатыванию средств аварийной защиты и (или) к изменению логики ПЛК |
| Недоступность данных | Серверы и хранилища данных | Несанкционированная отправка команд, приводящая к несрабатыванию средств аварийной защиты |
| Программное обеспечение | Несанкционированная отправка команд, приводящая к остановке бизнес процессов |
| Сетевая инфраструктура | Несанкционированная модификация (изменение) логики работы или установок коммутационного контроллера, которая приводит к остановке бизнес-процессов |
| Утечка персональных данных | Серверы и хранилища данных | Нарушение безопасности может привести к утечке персональных данных, что может вызвать ущерб репутации предприятия и привести к юридическим последствиям. |

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

Таблица 3 – Возможные цели реализации угроз безопасности информации нарушителями

|  |  |  |  |
| --- | --- | --- | --- |
| № вида | Виды нарушителя | Категории нарушителя | Возможные цели реализации угроз ИБ |
| 1 | Системные администраторы и администраторы безопасности | Внутренний | Получение финансовой выгоды. Любопытство или желание самореализации. Непреднамеренные, неосторожные или неквалифицированные действия |
| 2 | Хакеры | Внешний | Уничтожение данных в системе, в том числе ИС предприятия. Выкладывание в сеть различные ПДн сотрудников и партнеров предприятия. Кража конфиденциальной информации |
| 3 | Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ | Внутренний | Получение финансовой или иной материальной выгоды. Непреднамеренные, неосторожные или неквалифицированные действия. Получение конкурентных преимуществ |
| 4 | Бывшие(уволенные) сотрудники ПАО Роснефть | Внешний | Получение финансовой выгоды. Месть за прошлый опыт. Финансовые и репутационные убытки для компании |
| 5 | Рэнсомвареры | Внешний | Получение финансовой выгоды |
| 6 | Шпионы и конкуренты | Внешний | Получение финансовой выгоды. Финансовые и репутационные убытки для компании |

Таблица 4 – Оценка целей реализации нарушителями угроз безопасности информации в зависимости от возможных негативных последствий и видов ущерба от их реализации

|  |  |  |
| --- | --- | --- |
| Виды нарушителей | Возможные цели реализации угроз безопасности информации | Соответствие целей видам риска (ущерба) и возможным негативным последствиям |
| **Риски юридическому лицу,**  **вязанные с**  **хозяйственной деятельностью** |
| Системные администраторы и администраторы безопасности | +  (получение финансовой или иной материальной выгоды при вступлении в сговор с преступной группой) | У2 (хищение денежных средств ПАО Роснефть) |
| Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ | +  (дестабилизация деятельности предприятия ПАО Роснефть) | У2 (остановка бизнес-процессов; нарушение штатного режима функционирования объекта) |
| Хакеры | +  (дестабилизация деятельности предприятия ПАО Роснефть) | У2 (утечка коммерческой тайны; причинение имущественного ущерба; уничтожение данных |
| Бывшие(уволенные) сотрудники ПАО Роснефть | +  (получение финансовой или иной материальной выгоды при вступлении в сговор с преступной группой) | У2 (хищение денежных средств ПАО Роснефть, утечка персональных данных) |
| Рэнсомвареры | +  (дестабилизация деятельности предприятия ПАО Роснефть) | У2 (утечка коммерческой тайны; причинение имущественного ущерба; уничтожение данных) |
| Шпионы и конкуренты | +  (получение финансовой или иной материальной выгоды при вступлении в сговор с преступной группой) | У2 (хищение денежных средств ПАО Роснефть, утечка персональных данных) |

# 5. СПОСОБЫ РЕАЛИЗАЦИИ (ВОЗНИКНОВЕНИЯ) УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Таблица 5 – 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 | 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 |
| 2 | Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ | 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 |
| АРМ оператора | Съемные машинные носители информации, содержащие аутентификационную информацию | Извлечение аутентификационной информации из постоянной памяти носителя |
| Коммутационный контроллер: | Удаленный канал управления коммутационным контроллером  Съемные машинные носители информации, содержащие аутентификационную информацию | Использование уязвимостей кода; кража аутентификационной информации из постоянной памяти носителя |
| 3 | 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 |
| 4 | Бывшие(уволенные) сотрудники ПАО Роснефть | 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 работника бухгалтерии Роснефти | Доступ к базам данных, информация о клиентах | Извлечение/ кража информации из постоянной памяти носителя |
| АРМ работника финансового департамента | Доступ к базе данных, содержащие информации о финансовых сделках компании | Извлечение/ кража информации из постоянной памяти носителя |
| 5 | Рэнсомвареры | 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 |
| 6 | Шпионы и конкуренты | 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 |
| АРМ работника бухгалтерии Роснефти | Съемные машинные носители информации, содержащие аутентификационную информацию | Извлечение аутентификационной информации из постоянной памяти носителя |
| АРМ работника финансового департамента | Съемные машинные носители информации, содержащие аутентификационную информацию | Извлечение/ кража информации из постоянной памяти носителя |

# 6. АКТУАЛЬНЫЕ УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

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.

При составлении перечня актуальных угроз безопасности ПДн каждой степени исходной защищенности ставится в соответствие числовой коэффициент, а именно:

0 – для высокой степени исходной защищенности;

5 – для средней степени исходной защищенности;

10 – для низкой степени исходной защищенности.

Под частотой (вероятностью) реализации угрозы понимается определяемый экспертным путем 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 следующим образом:

если, то возможность реализации угрозы признается низкой;

если, то возможность реализации угрозы признается средней;

если, то возможность реализации угрозы признается высокой;

если, то возможность реализации угрозы признается очень высокой.

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

Таблица 6 – Правила отнесения угрозы безопасности ПДн 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;
* 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 соединению 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.

Таблица 7 – Показатели исходной защищенности ИСПДн

|  |  |  |  |
| --- | --- | --- | --- |
| **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.** | + | – | – |

По результатам, **ИСПДн ПАО Роснефти** соответствует **среднему** уровню защищенности.