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

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:

− Управление 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.

1.7. Особенности пересмотра Модели угроз

Модель угроз может быть пересмотрена в следующих случаях:

– по решению на основе периодически проводимых анализа и оценки угроз безопасности ПДн с учетом особенностей и (или) изменений на объекте информатизации;

– в случае возникновения (обнаружения) новых уязвимостей и угроз безопасности информации;

– в случае изменения федерального законодательства в части оценки угроз безопасности информации;

– в случае появления новых угроз в используемых источниках данных об угрозах безопасности информации;

– в случае изменения структурно-функциональных характеристик, применяемых информационных технологий или особенностей функционирования АИСПДн ПАО “Роснефть”;

– в случае появления сведений и (или) фактов о новых возможностях потенциальных нарушителей;

– в случаях выявления инцидентов информационной безопасности на объекте информатизации и (или) взаимодействующих (смежных) системах.

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 – Возможные негативные последствия для ПАО “Роснефть”

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

В процессе оценки угроз безопасности информации были выявлены информационные ресурсы и компоненты системы ИСПДН ПАО “Роснефть”, доступ или воздействие на которые, при реализации угроз безопасности информации, могут вызвать негативные последствия, т.е. стать объектами воздействия.

Для выявления потенциальных объектов воздействия использовались следующие исходные данные:

1) Общий перечень угроз безопасности информации из банка данных угроз ФСТЭК России, модели угроз безопасности информации, создаваемые ФСТЭК России в соответствии с утвержденным Указом Президента Российской Федерации, и отраслевые модели угроз безопасности информации.

2) Дополнительно к указанным данным, также рассматривались документация по сетям и системам, включающая информацию о составе и архитектуре, группах пользователей, их полномочиях, типах доступа, а также внешних и внутренних интерфейсах. Негативные последствия от реализации угроз безопасности информации также учитывались при определении возможных объектов воздействия.

На основе проведенного анализа и инвентаризации систем и сетей были выделены следующие категории информационных ресурсов и компонентов систем и сетей, которые могут подвергаться воздействию: информация (данные), хранящиеся в системах и сетях; программно-аппаратные средства обработки и хранения информации (сервера); машинные носители информации.

Для каждого выявленного объекта воздействия были определены виды воздействия, которые могут привести к негативным последствиям.

Выделяют следующие виды воздействия:

1) Воздействие 1 (В1) – утечка (перехват) конфиденциальной информации или отдельных данных;

2) Воздействие 2 (В2) – несанкционированный доступ к компонентам, защищаемой информации, системным, конфигурационным, иным служебным данным;

3) Воздействие 3 (В3) – Отказ в обслуживании компонентов;

4) Воздействие 4 (В4) – Несанкционированная модификация, подмена, искажение защищаемой информации;

5) Воздействие 5 (В5) – Несанкционированное использование вычислительных ресурсов систем и сетей в интересах решения несвойственных им задач;

6) Воздействие 6 (В6) – Нарушение функционирования программно-аппаратных средств обработки, передачи и хранения информации.

Исходными данными для определения возможных актуальных нарушителей являются:

а) общий перечень угроз безопасности информации, содержащихся в банке данных угроз безопасности информации ФСТЭК России (bdu.fstec.ru), модели угроз безопасности информации, разрабатываемые ФСТЭК России в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085, а также отраслевые (ведомственные, корпоративные) модели угроз безопасности информации;

б) документация на сети и системы (в части сведений о составе и архитектуре, о группах пользователей и уровне их полномочий, типах доступа, внешних и внутренних интерфейсах);

в) негативные последствия от реализации (возникновения) угроз безопасности информации;

г) объекты воздействия угроз безопасности информации и виды воздействия на них.

На основе анализа исходных данных, а также результатов оценки возможных целей реализации нарушителями угроз безопасности информации определен перечень рассматриваемых нарушителей, актуальных для систем и сетей. Перечень нарушителей перечислен в таблице 3.

Таблица 3 – Перечень нарушителей

№ п/п	Вид нарушителя	Возможные цели реализации угроз безопасности информации	Предположения об отнесении к числу возможных нарушителей
1.	Террористические, экстремистские группировки	Совершение террористических актов, угроза жизни граждан. Нанесение ущерба отдельным сферам деятельности или секторам экономики государства. Дестабилизация общества. Дестабилизация деятельности органов государственной власти, организаций.	Не имеют достаточной мотивации для реализации угроз, однако рассматриваются, т.к. могут вступить в сговор с внутренними нарушителями
2.	Преступные группы	Получение финансовой или иной материальной выгоды.	Не имеют достаточной мотивации для реализации угроз, однако рассматриваются, т.к. могут вступить в сговор с внутренними нарушителями
3.	Конкурирующие организации	Получение конкурентных преимуществ. Получение финансовой или иной материальной выгоды.	Не имеют достаточной мотивации для реализации целей
4.	Разработчики программных, программно-аппаратных средств	Получение финансовой или иной материальной выгоды. Непреднамеренные, неосторожные или неквалифицированные действия.	Не имеют достаточной мотивации для реализации целей
5.	Лица, обеспечивающие поставку программных, программно-аппаратных средств,	Получение финансовой или иной материальной выгоды. Непреднамеренные, неосторожные или	Не имеют достаточной мотивации для реализации целей

	обеспечивающих систем	неквалифицированные действия.	
6.	Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора (администрация, охрана, уборщики и т. д.)	Получение финансовой или иной материальной выгоды. Непреднамеренные, неосторожные или неквалифицированные действия	Не имеют достаточной мотивации для реализации целей
7.	Авторизованные пользователи систем и сетей	Любопытство или желание самореализации (подтверждение статуса). Месть за ранее совершенные действия. Непреднамеренные, неосторожные или неквалифицированные действия.	Является возможным нарушителем, исходя из целей реализации угроз
8.	Системные администраторы и администраторы безопасности	Получение финансовой или иной материальной выгоды. Месть за ранее совершенные действия. Непреднамеренные, неосторожные или неквалифицированные действия	Является возможным нарушителем, исходя из целей реализации угроз
9.	Бывшие работники (пользователи)	Получение финансовой или иной материальной выгоды. Месть за ранее совершенные действия	Является возможным нарушителем, исходя из целей реализации угроз

На основе анализа этих исходных данных и результатов оценки возможных целей нарушителей формируется перечень актуальных нарушителей. В таблице 4 представлены возможные нарушители и их цели для реализации угроз безопасности информации нарушителями.

Таблица 4 – Возможные нарушители и их цели для 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. Является возможным нарушителем, исходя из целей реализации угроз
2	Хакеры	Внешний	Уничтожение данных в системе, в том числе ИС предприятия. Выкладывание в сеть различные ПДн сотрудников и партнеров предприятия. Кража конфиденциальной информации Не имеют достаточной мотивации для реализации угроз, однако рассматриваются, т.к. могут вступить в сговор с внутренними нарушителями
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 Не имеют достаточной мотивации для реализации целей
4	Бывшие(уволенные) сотрудники ПАО Роснефть	Внешний	Получение финансовой выгоды. Месть за прошлый опыт. Финансовые и репутационные убытки для компании Не имеют достаточной мотивации для реализации целей
5	Рэнсомвареры	Внешний	Получение финансовой выгоды
6	Шпионы и конкуренты	Внешний	Получение финансовой выгоды. Финансовые и репутационные убытки для компании Является возможным нарушителем, исходя из целей реализации угроз
7	Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем	Внутренний/Внешний	Получение финансовой или иной материальной выгоды. Непреднамеренные. Не имеют достаточной мотивации для реализации целей
8	Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора (охрана, уборщица)	Внутренний	Получение финансовой или иной материальной выгоды. Непреднамеренные, неосторожные или неквалифицированные действия Не имеют достаточной мотивации для реализации целей

Нарушители обладают различными уровнями компетентности, ресурсной оснащенности и мотивации для осуществления угроз безопасности информации. Эти характеристики в совокупности определяют уровень возможностей нарушителей по реализации угроз в области информационной безопасности. В данном контексте выделяются следующие уровни возможностей нарушителей:

− Нарушитель с базовыми возможностями (УН1);

− Нарушитель с базово-повышенными возможностями (УН2);

− Нарушитель с средним уровнем возможностей (УН3);

− Нарушитель с высокими возможностями (УН4).

Однако при сопоставлении банка данных угроз безопасности информации (https://bdu.fstec.ru/) с методическим документом "Методика оценки угроз безопасности информации" выявляется несоответствие уровней возможностей нарушителей.

Таблица 5 демонстрирует расхождение потенциала нарушителей согласно банку данных угроз ФСТЭК. Это может указывать на необходимость пересмотра или согласования методологии оценки угроз безопасности информации для более точного отражения реальных возможностей нарушителей.

Таблица 5 − Соотношение потенциала нарушителей, в соответствии с банком данных угроз ФСТЭК

Банк данных угроз, сформированный ФСТЭК России	**Методика оценки угроз безопасности информации**
Нарушитель с низким потенциалом	Нарушитель с базовыми возможностями по осуществлению угроз безопасности информации.
	Нарушитель с базовыми, но усиленными возможностями по реализации угроз безопасности информации
Нарушитель со средним потенциалом	Нарушитель с средним уровнем возможностей по реализации угроз безопасности информации
Нарушитель с высоким потенциалом	Нарушитель с высоким уровнем возможностей по реализации угроз безопасности информации

В зависимости от имеющихся прав и условий доступа к системам и сетям, которые обусловлены архитектурой и функционированием данных систем, а также от возможностей нарушителей, выделяются две основные категории:

− Внешние нарушители, которые лишены прав доступа к контролируемой (охраняемой) зоне (территории) и/или авторизации на доступ к информационным ресурсам и компонентам систем и сетей;

− Внутренние нарушители, обладающие соответствующими правами доступа к контролируемой (охраняемой) зоне (территории) и/или полномочиями для автоматизированного доступа к информационным ресурсам и компонентам систем и сетей.

Подробное описание уровней возможностей нарушителей при осуществлении угроз безопасности информации представлено в таблице 6. Это обеспечивает систематизацию и понимание различий в подходах к защите от внешних и внутренних угроз, а также позволяет эффективно анализировать и противостоять различным видам потенциальных нарушений безопасности информации.

Таблица 6 – Описание уровней возможностей нарушителей при осуществлении угроз безопасности информации

№	Уровень возможностей нарушителей	Возможности нарушителей по реализации угроз безопасности
УН1	Нарушитель, обладающий базовыми возможностями	Возможность осуществления угроз безопасности информации заключается в способности использовать лишь известные уязвимости, скрипты и инструменты. Также, нарушитель способен использовать средства для реализации угроз, которые свободно распространены в сети "Интернет" и разработаны третьими лицами. Его знания о механизмах функционирования, доставке и выполнении вредоносного программного обеспечения, эксплойтов ограничены минимальными знаниями. Нарушитель обладает базовыми компьютерными навыками, соответствующими уровню пользователя. В дополнение, у него имеется возможность реализации угроз путем физического воздействия на технические средства обработки и хранения информации, линии связи, а также обеспечивающие системы при наличии физического доступа к ним.

УН2	Нарушитель, обладающий базовыми повышенными возможностями	Располагает всеми базовыми возможностями, характерными для нарушителей с базовыми умениями. Владеет средствами реализации угроз, которые свободно распространяются в сети "Интернет" и разработаны другими лицами, однако обладает глубоким пониманием и отличным владением этими инструментами, способен вносить изменения в их функционирование для повышения эффективности реализации угроз. Оборудован фреймворками и комплектами инструментов для осуществления угроз безопасности информации и эксплуатации уязвимостей. Проявляет навыки самостоятельного планирования и воплощения сценариев угроз безопасности информации. Обладает практическими знаниями о работе систем и сетей, операционных системах, а также обладает экспертными знаниями в области защитных механизмов, используемых в программном обеспечении и аппаратных средствах.
УН3	Нарушитель, обладающий средними возможностями	Обладает всеми характеристиками нарушителей, обладающих базово-повышенными возможностями. Способен получать информацию о уязвимостях, предоставляемую на платных специализированных ресурсах, таких как биржи уязвимостей. Есть возможность приобретения дорогостоящих средств и инструментов для реализации угроз, также доступных на платных специализированных ресурсах. Способен самостоятельно разрабатывать средства (инструменты), необходимые для осуществления угроз, и использовать их для проведения атак. Есть возможность получения доступа к встраиваемому программному обеспечению аппаратных платформ, системному и прикладному программному обеспечению, телекоммуникационному оборудованию и другим программно-аппаратным средствам для их анализа.Обладает знаниями и практическими навыками анализа программного кода для выявления уязвимостей. Перемещается в области высоких знаний и практических навыков в функционировании систем и сетей, операционных систем, а также обладает глубоким пониманием защитных механизмов, применяемых в программном обеспечении и аппаратных средствах. Способен реализовывать угрозы безопасности информации в рамках группы лиц.
УН4	Нарушитель, обладающий высокими возможностями	Обладает всеми характеристиками нарушителей, обладающих средними возможностями. Способен получать доступ к исходному коду встраиваемого программного обеспечения аппаратных платформ, системного и прикладного программного обеспечения, телекоммуникационного оборудования и других программно-аппаратных средств с целью выявления сведений о "нулевых днях". Обладает способностью внедрять программные или программно-аппаратные закладки на различных этапах поставки программного обеспечения или программно-аппаратных средств.Может создавать методы и средства реализации угроз, привлекая специализированные научные организации, а также реализовывать угрозы с использованием специально разработанных средств, включая те, которые обеспечивают скрытое проникновение. Обладает способностью реализации угроз с привлечением специалистов, обладающих базовыми повышенными, средними и высокими возможностями.Может создавать и использовать специальные технические средства для извлечения информации или воздействия на информацию и технические средства, распространяющиеся в виде физических полей или явлений. Обладает способностью долговременной и незаметной реализации угроз безопасности информации для операторов систем и сетей. Обладает выдающимися знаниями и практическими навыками в области функционирования систем и сетей, операционных систем, аппаратного обеспечения, а также обладает экспертными знаниями о конкретных защитных механизмах, применяемых в программном обеспечении и программно-аппаратных средствах целевых систем и сетей.

На основании сопоставления выявляются актуальные нарушители согласно следующему принципу: нарушитель считается актуальным, если осуществление им угроз безопасности информации может иметь определенные негативные последствия для АИСПДН ПАО “Роснефть”.

Этот процесс анализа направлен на выявление потенциальных угроз и оценку их воздействия на информационные ресурсы и компоненты системы университета, что позволяет более эффективно противостоять возможным инцидентам безопасности. Полученные результаты сопоставления позволяют выявить конкретные угрозы, требующие приоритетного внимания и мер по защите. Актуальные нарушителя для АИСПДН ПАО “Роснефть” показаны в таблице 7.

Таблица 7 − Актуальные нарушителя для АИСПДН ПАО “Роснефть”

Возможные негативные последствия*	**Виды нарушителя**	**Категория нарушителя**	**Уровень возможностей нарушителя**
Нанесение ущерба физическому лицу	Отдельные физические лица (хакеры)	Внешний	УН2
	Авторизованные пользователи систем и сетей	Внутренний	УН1
	Системные администраторы и администраторы безопасности	Внутренний	УН2
	Бывшие работники (пользователи)	Внешний	УН1
	Шпионы и конкуренты	Внутренний/ Внешний	УН2
Нанесение ущерба юридическому лицу, индивидуальному предпринимателю	Отдельные физические лица (хакеры)	Внешний	УН2
	Системные администраторы и администраторы безопасности	Внутренний	УН2
	Рэнсомвареры	Внешний	УН1
	Шпионы и конкуренты	Внешний	УН2

Также в таблице 8 показана оценка целей реализации нарушителями угроз безопасности информации в зависимости от возможных негативных последствий и видов ущерба от их реализации

Таблица 8 – 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

В ходе процесса оценки угроз безопасности информации выявляются потенциальные методы, которые могут быть задействованы актуальными нарушителями для осуществления угроз безопасности информации в АИСПДН ПАО “Роснефть”.

В таблице 9 представлены конкретные способы реализации угроз безопасности информации, а также соответствующие им типы нарушителей и их возможности. Полученные данные предоставляют важные сведения для разработки эффективных стратегий по обеспечению безопасности в информационной системе, что способствует предотвращению и минимизации возможных рисков.

Таблица 9 – 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.

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 Y_1, а именно:

0 – для высокой степени исходной защищенности;

5 – для средней степени исходной защищенности;

10 – для низкой степени исходной защищенности

Таблица 10 – 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 11 – 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.

В ходе оценки угроз безопасности информации проводится анализ возможных угроз безопасности информации и производится их оценка на актуальность для АИСПДН ПАО Роснефть. В ходе анализа возможных угроз безопасности информации, применимых к объекту оценки, была сформирована таблица применимых угроз, которая представлена в таблице 12.

Таблица 12 – Применимые к объекту оценки угрозы безопасности информации с возможными последствиями реализации

№	Идентификатор угрозы	Угроза	Последствия реализации угрозы
1.	УБИ.004	Угроза аппаратного сброса пароля BIOS	Нарушение целостности
2.	УБИ.006	Угроза внедрения кода или данных	Нарушение конфиденциальности, целостности, доступности

3.	УБИ.009	Угроза восстановления предыдущей уязвимой версии BIOS	Нарушение конфиденциальности, целостности, доступности
4.	УБИ.012	Угроза деструктивного изменения конфигурации/среды окружения программ	Нарушение конфиденциальности, целостности, доступности
5.	УБИ.013	Угроза деструктивного использования декларированного функционала BIOS	Нарушение целостности
6.	УБИ.014	Угроза длительного удержания вычислительных ресурсов пользователями	Нарушение доступности
7.	УБИ.015	Угроза доступа к защищаемым файлам с использованием обходного пути	Нарушение конфиденциальности
8.	УБИ.018	Угроза загрузки нештатной операционной системы	Нарушение конфиденциальности, целостности, доступности
9.	УБИ.019	Угроза заражения DNS-кеша	Нарушение конфиденциальности
10.	УБИ.022	Угроза избыточного выделения оперативной памяти	Нарушение доступности
11.	УБИ.023	Угроза изменения компонентов системы	Нарушение конфиденциальности, целостности, доступности
12.	УБИ.027	Угроза искажения вводимой и выводимой на периферийные устройства информации	Нарушение целостности
13.	УБИ.028	Угроза использования альтернативных путей доступа к ресурсам	Нарушение конфиденциальности
14.	УБИ.030	Угроза использования информации идентификации/аутентификации, заданной по умолчанию	Нарушение конфиденциальности, целостности, доступности
15.	УБИ.031	Угроза использования механизмов авторизации для повышения привилегий	Нарушение конфиденциальности
16.	УБИ.034	Угроза использования слабостей протоколов сетевого/локального обмена данными	Нарушение конфиденциальности, целостности, доступности
17.	УБИ.041	Угроза межсайтового скриптинга	Нарушение конфиденциальности, целостности, доступности
18.	УБИ.042	Угроза межсайтовой подделки запроса	Нарушение конфиденциальности, целостности, доступности

19.	УБИ.045	Угроза нарушения изоляции среды исполнения BIOS	Нарушение конфиденциальности, целостности, доступности
20.	УБИ.046	Угроза нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия	Нарушение конфиденциальности, целостности, доступности
21.	УБИ.049	Угроза нарушения целостности данных кеша	Нарушение целостности, доступности
22.	УБИ.051	Угроза невозможности восстановления сессии работы на ПЭВМ при выводе из промежуточных состояний питания	Нарушение целостности, доступности
23.	УБИ.052	Угроза невозможности миграции образов виртуальных машин из-за несовместимости аппаратного и программного обеспечения	Нарушение целостности, доступности
24.	УБИ.053	Угроза невозможности управления правами пользователей BIOS	Нарушение конфиденциальности, целостности, доступности
25.	УБИ.062	Угроза некорректного использования прозрачного прокси-сервера за счёт плагинов браузера	Нарушение конфиденциальности, целостности, доступности
26.	УБИ.067	Угроза неправомерного ознакомления с защищаемой информацией	Нарушение конфиденциальности, целостности, доступности
27.	УБИ.069	Угроза неправомерных действий в каналах связи	Нарушение конфиденциальности, целостности, доступности
28.	УБИ.071	Угроза несанкционированного восстановления удалённой защищаемой информации	Нарушение конфиденциальности, целостности, доступности
29.	УБИ.072	Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS	Нарушение конфиденциальности, целостности, доступности
30.	УБИ.074	Угроза несанкционированного доступа к аутентификационной информации	Нарушение конфиденциальности, целостности, доступности
31.	УБИ.078	Угроза несанкционированного доступа к защищаемым виртуальным машинам из виртуальной и (или) физической сети	Нарушение конфиденциальности, целостности, доступности
32.	УБИ.079	Угроза несанкционированного доступа к защищаемым виртуальным машинам со стороны других	Нарушение конфиденциальности, целостности, доступности

		виртуальных машин	
33.	УБИ.084	Угроза несанкционированного доступа к системе хранения данных из виртуальной и (или) физической сети	Нарушение конфиденциальности, целостности, доступности
34.	УБИ.086	Угроза несанкционированного изменения аутентификационной информации	Нарушение конфиденциальности, целостности, доступности
35.	УБИ.087	Угроза несанкционированного использования привилегированных функций BIOS	Нарушение конфиденциальности, целостности, доступности
36.	УБИ.088	Угроза несанкционированного копирования защищаемой информации	Нарушение конфиденциальности, целостности, доступности
37.	УБИ.089	Угроза несанкционированного редактирования реестра	Нарушение конфиденциальности, целостности, доступности
38.	УБИ.090	Угроза несанкционированного создания учётной записи пользователя	Нарушение конфиденциальности, целостности, доступности
39.	УБИ.091	Угроза несанкционированного удаления защищаемой информации	Нарушение конфиденциальности, целостности, доступности
40.	УБИ.093	Угроза несанкционированного управления буфером	Нарушение конфиденциальности, целостности, доступности
41.	УБИ.098	Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб	Нарушение конфиденциальности, целостности, доступности
42.	УБИ.099	Угроза обнаружения хостов	Нарушение конфиденциальности, целостности, доступности
43.	УБИ.100	Угроза обхода некорректно настроенных механизмов аутентификации	Нарушение конфиденциальности, целостности, доступности
44.	УБИ.103	Угроза определения типов объектов защиты	Нарушение конфиденциальности, целостности, доступности
45.	УБИ.104	Угроза определения топологии вычислительной сети	Нарушение конфиденциальности, целостности, доступности
46.	УБИ.111	Угроза передачи данных по скрытым каналам	Нарушение конфиденциальности, целостности, доступности
47.	УБИ.113	Угроза перезагрузки аппаратных и	Нарушение

		программно-аппаратных средств вычислительной техники	конфиденциальности, целостности, доступности
48.	УБИ.115	Угроза перехвата вводимой и выводимой на периферийные устройства информации	Нарушение конфиденциальности, целостности, доступности
49.	УБИ.116	Угроза перехвата данных, передаваемых по вычислительной сети	Нарушение конфиденциальности, целостности, доступности
50.	УБИ.121	Угроза повреждения системного реестра	Нарушение конфиденциальности, целостности, доступности
51.	УБИ.123	Угроза подбора пароля BIOS	Нарушение конфиденциальности, целостности, доступности
52.	УБИ.124	Угроза подделки записей журнала регистрации событий	Нарушение конфиденциальности, целостности, доступности
53.	УБИ.128	Угроза подмены доверенного пользователя	Нарушение конфиденциальности, целостности, доступности
54.	УБИ.129	Угроза подмены резервной копии программного обеспечения BIOS	Нарушение конфиденциальности, целостности, доступности
55.	УБИ.130	Угроза подмены содержимого сетевых ресурсов	Нарушение конфиденциальности, целостности, доступности
56.	УБИ.140	Угроза приведения системы в состояние «отказ в обслуживании»	Нарушение конфиденциальности, целостности, доступности
57.	УБИ.143	Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	Нарушение конфиденциальности, целостности, доступности
58.	УБИ.144	Угроза программного сброса пароля BIOS	Нарушение конфиденциальности, целостности, доступности
59.	УБИ.145	Угроза пропуска проверки целостности программного обеспечения	Нарушение конфиденциальности, целостности, доступности
60.	УБИ.152	Угроза удаления аутентификационной информации	Нарушение конфиденциальности, целостности, доступности
61.	УБИ.153	Угроза усиления воздействия на вычислительные ресурсы	Нарушение конфиденциальности,

		пользователей при помощи сторонних серверов	целостности, доступности
62.	УБИ.155	Угроза утраты вычислительных ресурсов	Нарушение конфиденциальности, целостности, доступности
63.	УБИ.156	Угроза утраты носителей информации	Нарушение конфиденциальности, целостности, доступности
64.	УБИ.157	Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	Нарушение конфиденциальности, целостности, доступности
65.	УБИ.158	Угроза форматирования носителей информации	Нарушение конфиденциальности, целостности, доступности
66.	УБИ.159	Угроза «форсированного веб-браузинга»	Нарушение конфиденциальности, целостности, доступности
67.	УБИ.160	Угроза хищения средств хранения, обработки и (или) ввода/ вывода/ передачи информации	Нарушение конфиденциальности, целостности, доступности
68.	УБИ.162	Угроза эксплуатации цифровой подписи программного кода	Нарушение конфиденциальности, целостности, доступности
69.	УБИ.167	Угроза заражения компьютера при посещении неблагонадёжных сайтов	Нарушение конфиденциальности, целостности, доступности
70.	УБИ.168	Угроза «кражи» учётной записи доступа к сетевым сервисам	Нарушение конфиденциальности, целостности, доступности
71.	УБИ.171	Угроза скрытного включения вычислительного устройства в состав бот-сети	Нарушение конфиденциальности, целостности, доступности
72.	УБИ.172	Угроза распространения «почтовых червей»	Нарушение конфиденциальности, целостности, доступности
73.	УБИ.173	Угроза «спама» веб-сервера	Нарушение доступности
74.	УБИ.174	Угроза «фарминга»	Нарушение конфиденциальности, целостности, доступности
75.	УБИ.175	Угроза «фишинга»	Нарушение конфиденциальности,

			целостности, доступности
76.	УБИ.176	Угроза нарушения технологического/производственного процесса из-за временных задержек, вносимых средством защиты	Нарушение конфиденциальности, целостности, доступности
77.	УБИ.177	Угроза неподтверждённого ввода данных оператором в систему, связанную с безопасностью	Нарушение конфиденциальности, целостности, доступности
78.	УБИ.178	Угроза несанкционированного использования системных и сетевых утилит	Нарушение конфиденциальности, целостности, доступности
79.	УБИ.179	Угроза несанкционированной модификации защищаемой информации	Нарушение конфиденциальности, целостности, доступности
80.	УБИ.182	Угроза физического устаревания аппаратных компонентов	Нарушение конфиденциальности, целостности, доступности
81.	УБИ.185	Угроза несанкционированного изменения параметров настройки средств защиты информации	Нарушение конфиденциальности, целостности, доступности
82.	УБИ.186	Угроза внедрения вредоносного кода через рекламу, сервисы и контент	Нарушение конфиденциальности, целостности, доступности
83.	УБИ.191	Угроза внедрения вредоносного кода в дистрибутив программного обеспечения	Нарушение конфиденциальности, целостности, доступности
84.	УБИ.192	Угроза использования уязвимых версий программного обеспечения	Нарушение конфиденциальности, целостности, доступности
85.	УБИ.203	Угроза утечки информации с неподключенных к сети Интернет компьютеров	Нарушение конфиденциальности, целостности, доступности
86.	УБИ.205	Угроза нарушения работы компьютера и блокирования доступа к его данным из-за некорректной работы установленных на нем средств защиты	Нарушение конфиденциальности, целостности, доступности
87.	УБИ.208	Угроза нецелевого использования вычислительных ресурсов средства вычислительной техники	Нарушение конфиденциальности, целостности, доступности
88.	УБИ.211	Угроза использования непроверенных пользовательских данных при формировании конфигурационного файла, используемого программным обеспечением администрирования	Нарушение конфиденциальности, целостности, доступности

		информационных систем	
89.	УБИ.217	Угроза использования скомпрометированного доверенного источника обновлений программного обеспечения	Нарушение конфиденциальности, целостности, доступности