Приложение № 7 к приказу № 104 от « 07 » 02 2020 г.

ПОЛОЖЕНИЕ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

СОДЕРЖАНИЕ

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники.

Безопасность персональных данных – состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

Блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

Вирус (компьютерный, программный) - исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

Доступ к информации – возможность получения информации и ее использования.

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Источник угрозы безопасности информации – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

Нарушитель безопасности персональных данных – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

Носитель информации - физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение,

использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Оператор (персональных данных) – государственный орган, муниципальный орган, юридическое или физическое лицо, организующее и (или) осуществляющее обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Побочные электромагнитные излучения и наводки - электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

Пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц

Программная закладка - скрытно внесенный в программное обеспечение функциональный объект, который при определенных условиях способен обеспечить несанкционированное программное воздействие. Программная закладка может быть реализована в виде вредоносной программы или программного кода.

Программное (программно-математическое) воздействие - несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

Распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц

Угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

Уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

Утечка (защищаемой) информации по техническим каналам – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

Уязвимость ИСПДн – недостаток или слабое место в системном или прикладном программном (программно-аппаратном) обеспечении автоматизированной информационной системы, которое может быть использовано для реализации угрозы безопасности ПДн.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

АРМ – автоматизированное рабочее место;
ИСПДн – информационная система персональных данных;
НСД – несанкционированный доступ;
ОБПДн – обеспечение безопасности персональных данных;
ОС– операционная система;
ПДн – персональные данные;
ПЭМИН – побочные электромагнитные излучения и наводки;

1. ПЕРЕЧЕНЬ ИСПД В МП КАЛИНИНГРАДТЕПЛОСЕТЬ

№ п/п	Наименование ИСПДн	Категории, обрабатываемых данных	Типы угроз, актуальных для ИС	Объем обрабатываемых данных	Необходимый уровень защищенности
1.	1С: Зарплата и управление персоналом	специальные	3	менее 100 000	3
2.	1С: Управление производственным предприятием	иные	3	менее 100 000	4
3.	1С: Управление сбытом тепловой энергии	иные	3	менее 100 000	4
4.	Расчетно-информационный комплекс РИВЦ Симплекс	иные	3	более 100 000	3
5.	База обращений населения с помощью сайта	иные	3	менее 100 000	3
6.	СЭД «Дело»	иные	3	более 100 000	3

2. МОДЕЛИ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИСПДН

2.1 ОБЩИЕ ПОЛОЖЕНИЯ

В модели угроз представлено описание структуры ИСПДн, состава и режима обработки ПДн, классификация потенциальных нарушителей, оценка исходного уровня защищенности, анализ угроз безопасности персональных данных.

Анализ УБПДн включает:

- Описание угроз;
- Оценку вероятности возникновения угроз;
- Оценку реализуемости угроз;
- Оценку опасности угроз;
- Определение актуальности угроз.

Модель угроз разработана на основании следующих документов:

- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной 15.02.2008 Заместителем директора ФСТЭК России;
- Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной 14.02.2008 заместителем директора ФСТЭК России.
- Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации, утверждённые ФСБ РФ 21.02.2008 № 149/54-144.

2.2. ОБЩЕЕ ОПИСАНИЕ ИНФОРМАЦИОННЫХ СИСТЕМ

2.2.1. ОПИСАНИЕ ИСПДН 1С: ЗАРПЛАТА И УПРАВЛЕНИЕ ПЕРСОНАЛОМ

Цель обработки ПДн

ИСПДн 1С: Зарплата и управление персоналом предназначена для ведения кадрового учета и расчета заработной платы. Персональные данные обрабатываются в рамках трудовых отношений, в целях соблюдения законов и иных нормативных правовых актов в области трудового законодательства, законодательства о налогах и сборах и т. д.

В ИСПДн обрабатываются следующие ПДн:

- фамилия, имя, отчество;
- дата рождения и место рождения;
- данные документа, удостоверяющего личность (серия, номер, когда и кем выдан, код подразделения);
- адрес постоянной регистрации и проживания;
- гражданство;
- пол;
- адрес электронной почты;
- номер контактного телефона;
- семейное положение;
- сведения из свидетельства о постановке на налоговый учет (ИНН);
- сведения из свидетельства о государственном пенсионном страховании (СНИЛС);
- сведения о воинском учёте;
- сведения об образовании, о повышении квалификации, о профессиональной переподготовке;
- сведения об исполнительных производствах;
- сведения об ученой степени, ученых званиях;
- информация о владении иностранными языками, степень владения;
- сведения по начисленной заработной плате;
- должность;
- данные о трудовом стаже, включая предыдущие места работы;
- состав семьи: степень родства, ФИО, дата рождения;
- сведения из медицинского полиса;
- сведения о состоянии здоровья;
- сведения о социальных льготах.

Необходимый уровень защищенности персональных данных:

- категория, обрабатываемых данных: специальные;
- типы угроз, актуальных для ИСПДн: 3;
- объем обрабатываемых данных: менее 100 000;
- необходимый уровень защищенности: 3.

Субъекты персональных данных:

Работники предприятия (в том числе близкие родственники работников).

Действия, осуществляемые с данными в ходе их обработки:

В ИСПДн 1С: Зарплата и управление персоналом оператором ПДн осуществляются следующие операции с персональными данными: запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление.

2.2.2. ОПИСАНИЕ ИСПДН 1С: УПРАВЛЕНИЕ ПРОИЗВОДСТВЕННЫМ ПРЕДПРИЯТИЕМ

Цель обработки ПДн

ИСПДн 1С: Управление производственным предприятием предназначена для комплексной автоматизации учета на предприятии. Персональные данные обрабатываются в рамках исполнения обязательств по гражданско-правовым договорам, в рамках трудового законодательства

В ИСПДн обрабатываются следующие ПДн:

- фамилия, имя, отчество;
- паспортные данные;
- адрес проживания;
- ИНН;
- банковские реквизиты;
- сведения о заработной плате к выплате.

Необходимый уровень защищенности персональных данных:

- категория, обрабатываемых данных: иные;
- типы угроз, актуальных для ИСПДн: 3;
- объем обрабатываемых данных: менее 100 000;
- необходимый уровень защищенности: 4.

Субъекты персональных данных:

Работники предприятия, контрагенты (физические лица).

Действия, осуществляемые с данными в ходе их обработки:

В ИСПДн Управление производственным предприятием оператором ПДн осуществляются следующие операции с персональными данными: запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление.

2.2.3. ОПИСАНИЕ ИСПДН 1С: УПРАВЛЕНИЕ СБЫТОМ ТЕПЛОВОЙ ЭНЕРГИИ

Цель обработки ПДн

ИСПДн 1С: Управление сбытом тепловой энергии предназначена для автоматизации расчетов за услуги горячего водоснабжения и отопления. Персональные данные обрабатываются в рамках исполнения обязательств по гражданско-правовым договорам.

В ИСПДн обрабатываются следующие ПДн:

- фамилия, имя, отчество;
- паспортные данные;
- адрес проживания;
- ИНН;

- банковские реквизиты

Необходимый уровень защищенности персональных данных:

- категория, обрабатываемых данных: иные;
- типы угроз, актуальных для ИСПДн: 3;
- объем обрабатываемых данных: менее 100 000;
- необходимый уровень защищенности: 4.

Субъекты персональных данных:

Потребители (контрагенты).

Действия, осуществляемые с данными в ходе их обработки:

В ИСПДн Управление сбытом тепловой энергии оператором ПДн осуществляются следующие операции с персональными данными: запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление.

2.2.4. ОПИСАНИЕ ИСПДН РАСЧЕТНО-ИНФОРМАЦИОННЫЙ КОМПЛЕКС РИВЦ СИМПЛЕКС

Данный комплекс предоставляется ООО «РИВЦ «Симплекс». Состоит из двух программных модулей: Симплекс. Город, Симплекс. Иски.

Цель обработки ПДн

ИСПДн расчетно-информационный комплекс РИВЦ Симплекс содержит сведения о состоянии расчетов контрагентов (физических лиц) за услуги ЖКХ. Персональные данные обрабатываются в рамках исполнения обязательств по гражданско-правовым договорам.

В ИСПДн обрабатываются следующие ПДн:

- фамилия, имя, отчество;
- паспортные данные;
- адрес проживания;
- ИНН;
- банковские реквизиты

Необходимый уровень защищенности персональных данных:

- категория, обрабатываемых данных: иные;
- типы угроз, актуальных для ИСПДн: 3;
- объем обрабатываемых данных: более 100 000;
- необходимый уровень защищенности: 3.

Субъекты персональных данных:

Контрагенты (физические лица).

Действия, осуществляемые с данными в ходе их обработки:

В ИСПДн расчетно-информационный комплекс РИВЦ Симплекс оператором ПДн осуществляются следующие операции с персональными данными: запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление.

2.2.5. ОПИСАНИЕ ИСПДН БАЗА ОБРАЩЕНИЙ НАСЕЛЕНИЯ С ПОМОЩЬЮ САЙТА

Данная база находится на серверах хостинг-провайдера nic.ru

Цель обработки ПДн

В базу обращений населения с помощью сайта сведения, данные записываются из формы «Задать вопрос», размещенной на сайте предприятия. Данная форма предусмотрена для обращения населения, персональные данные обрабатывают в рамках гражданских правоотношений.

В ИСПДн обрабатываются следующие ПДн:

- фамилия, имя, отчество;
- адрес проживания;
- телефон;
- электронная почта;
- при описании вопроса, контрагентом может быть указана иная информация, не предусмотренная в списке.

Необходимый уровень защищенности персональных данных:

- категория, обрабатываемых данных: иные;
- типы угроз, актуальных для ИСПДн: 3;
- объем обрабатываемых данных: более 100 000;
- необходимый уровень защищенности: 3.

Субъекты персональных данных:

Контрагенты (физические лица).

Действия, осуществляемые с данными в ходе их обработки:

В ИСПДн База обращений населения с помощью сайта оператором ПДн осуществляются следующие операции с персональными данными: запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление.

2.2.6. СЭД «ДЕЛО»

Цель обработки ПДн

ИСПДн СЭД «ДЕЛО» предназначена для автоматизации документооборота на предприятии. Персональные данные обрабатываются в целях учета документов (обращений, писем, заявлений).

В ИСПДн обрабатываются следующие ПДн:

- фамилия, имя, отчество;
- адрес проживания;
- телефон;
- электронная почта;
- сведения об образовании, о повышении квалификации, о профессиональной переподготовке;
- сведения об исполнительных производствах;
- сведения о задолженности по услугам, оказываемым МП «Калининградтеплосеть».

Необходимый уровень защищенности персональных данных:

- категория, обрабатываемых данных: иные;
- типы угроз, актуальных для ИСПДн: 3;

- объем обрабатываемых данных: более 100 000;
- необходимый уровень защищенности: 3.

Субъекты персональных данных:

Работники предприятия, контрагенты (физические лица).

Действия, осуществляемые с данными в ходе их обработки:

В ИСПДн База обращений населения с помощью сайта оператором ПДн осуществляются следующие операции с персональными данными: запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление.

2.3. ОПРЕДЕЛЕНИЕ АКТУАЛЬНЫХ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИСПДН

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

Актуальность угрозы определяется следующими параметрами:

- уровень исходной защищенности ИСПДн;
- частота (вероятность) реализации рассматриваемой угрозы.

Под уровнем исходной защищенности ИСПДн понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПДн.

Таблица 1 – Характеристики ИСПДн 1 С: Зарплата и управление персоналом

№	Параметр	Значение	Уровень защищенности
1	Территориальное размещение	локальная ИСПДн, развернутая в пределах одного здания	высокий
2	Наличие соединений с сетями общего пользования	ИСПДн, имеющая одноточечный выход в сеть общего пользования	средний
3	Встроенные (легальные) операции с записями баз персональных данных	запись, удаление, сортировка	средний
4	Разграничение доступа к персональным данным	ИСПДн, к которой имеют доступ определенные перечнем сотрудники организации, являющейся владельцем ИСПДн, либо субъект ПДн	средний
5	Наличие соединений с другими базами ПДн иных ИСПДн	ИСПДн, в которой используется одна база ПДн, принадлежащая организации – владельцу данной ИСПДн	высокий
6	Уровень обобщения (обезличивания) ПДн	ИСПДн, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта ПДн)	низкий
7	Объем ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки	ИСПДн, предоставляющая часть ПДн	средний

Таблица 2 – Характеристики ИСПДн 1 С: Управление производственным предприятием

№	Параметр	Значение	Уровень защищенности
1	Территориальное размещение	локальная ИСПДн, развернутая в пределах одного здания	высокий
2	Наличие соединений с сетями общего пользования	ИСПДн, имеющая одноточечный выход в сеть общего пользования	средний
3	Встроенные (легальные) операции с записями баз персональных данных	запись, удаление, сортировка	средний
4	Разграничение доступа к персональным данным	ИСПДн, к которой имеют доступ определенные перечнем сотрудники организации, являющейся владельцем ИСПДн, либо субъект ПДн	средний
5	Наличие соединений с другими базами ПДн иных ИСПДн	ИСПДн, в которой используется одна база ПДн, принадлежащая организации – владельцу данной ИСПДн	высокий
6	Уровень обобщения (обезличивания) ПДн	ИСПДн, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта ПДн)	низкий
7	Объем ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки	ИСПДн, предоставляющая часть ПДн	средний

Таблица 3 – Характеристики ИСПДн 1 С: Управление сбытом тепловой энергии

№	Параметр	Значение	Уровень защищенности
1	Территориальное размещение	локальная ИСПДн, развернутая в пределах одного здания	высокий
2	Наличие соединений с сетями общего пользования	ИСПДн, имеющая одноточечный выход в сеть общего пользования	средний
3	Встроенные (легальные) операции с записями баз персональных данных	запись, удаление, сортировка	средний
4	Разграничение доступа к персональным данным	ИСПДн, к которой имеют доступ определенные перечнем сотрудники	средний

		организации, являющейся владельцем ИСПДн, либо субъект ПДн	
5	Наличие соединений с другими базами ПДн иных ИСПДн	ИСПДн, в которой используется одна база ПДн, принадлежащая организации – владельцу данной ИСПДн	высокий
6	Уровень обобщения (обезличивания) ПДн	ИСПДн, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта ПДн)	низкий
7	Объем ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки	ИСПДн, предоставляющая часть ПДн	средний

Таблица 4 – Характеристики ИСПДн Расчетно-информационный комплекс РИВЦ Симплекс

№	Параметр	Значение	Уровень защищенности
1	Территориальное размещение	городская ИСПДн, охватывающая не более одного населенного пункта (города, поселка)	низкий
2	Наличие соединений с сетями общего пользования	ИСПДн, имеющая одноточечный выход в сеть общего пользования	средний
3	Встроенные (легальные) операции с записями баз персональных данных	запись, удаление, сортировка	средний
4	Разграничение доступа к персональным данным	ИСПДн, к которой имеют доступ определенные перечнем сотрудники организации, являющейся владельцем ИСПДн, либо субъект ПДн	средний
5	Наличие соединений с другими базами ПДн иных ИСПДн	ИСПДн, в которой используется одна база ПДн, принадлежащая организации – владельцу данной ИСПДн	высокий
6	Уровень обобщения (обезличивания) ПДн	ИСПДн, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта ПДн)	низкий
7	Объем ПДн, которые предоставляются сторонним пользователям ИСПДн без	ИСПДн, предоставляющая часть ПДн	средний

	предварительной обработки		

Таблица 5 – Характеристики ИСПДн База обращений населения с помощью сайта

№	Параметр	Значение	Уровень защищенности
1	Территориальное размещение	распределенная ИСПДн, которая охватывает несколько областей, краев, округов или государство в целом	низкий
2	Наличие соединений с сетями общего пользования	ИСПДн, имеющая одноточечный выход в сеть общего пользования	средний
3	Встроенные (легальные) операции с записями баз персональных данных	чтение, поиск	высокий
4	Разграничение доступа к персональным данным	ИСПДн, к которой имеют доступ определенные перечнем сотрудники организации, являющейся владельцем ИСПДн, либо субъект ПДн	средний
5	Наличие соединений с другими базами ПДн иных ИСПДн	ИСПДн, в которой используется одна база ПДн, принадлежащая организации – владельцу данной ИСПДн	высокий
6	Уровень обобщения (обезличивания) ПДн	ИСПДн, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта ПДн)	низкий
7	Объем ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки	ИСПДн, не предоставляющая никакой информации.	высокий

Таблица 6 – Характеристики ИСПДн СЭД «Дело»

№	Параметр	Значение	Уровень защищенности
1	Территориальное размещение	локальная ИСПДн, развернутая в пределах одного здания	высокий
2	Наличие соединений с сетями общего пользования	ИСПДн, имеющая одноточечный выход в сеть общего пользования	средний
3	Встроенные (легальные) операции с записями баз	модификация, передача	низкий

	персональных данных		
4	Разграничение доступа к персональным данным	ИСПДн, к которой имеют доступ определенные перечнем сотрудники организации, являющейся владельцем ИСПДн, либо субъект ПДн	средний
5	Наличие соединений с другими базами ПДн иных ИСПДн	ИСПДн, в которой используется одна база ПДн, принадлежащая организации – владельцу данной ИСПДн	высокий
6	Уровень обобщения (обезличивания) ПДн	ИСПДн, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта ПДн)	низкий
7	Объем ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки	ИСПДн, предоставляющая часть ПДн	средний

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

0 - для высокой степени исходной защищенности;

5 - для средней степени исходной защищенности;

10 - для низкой степени исходной защищенности.

Таблица 7 – Значения уровня защищенности

№ п/п	Наименование ИСПДн	Уровни защищенности			Коэффициент
		Высокий	Средний	Низкий	
1	1С: Зарплата и управление персоналом	2	4	1	5
2	1С: Управление производственным предприятием	2	4	1	5
3	Управление сбытом тепловой энергии	2	4	1	5
4	Расчетно-информационный комплекс РИВЦ Симплекс	1	4	2	5
5	База обращений населения через сайт	3	2	2	5
6	СЭД «Дело»	2	3	2	5

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 Y_2, а именно:

- 0 для маловероятной угрозы;
- 2 для низкой вероятности угрозы;
- 5 для средней вероятности угрозы;
- 10 для высокой вероятности угрозы.

По итогам оценки уровня защищенности (Y_1) и вероятности реализации угрозы (Y_2), рассчитывается коэффициент реализуемости угрозы (Y)

$$Y = \frac{Y_1 + Y_2}{20}$$

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

- 0 <Y <0,3 - возможность реализации угрозы признается низкой
- 0,3 <Y <0,6 - возможность реализации угрозы признается средней
- 0,6 <Y <0,8 - возможность реализации угрозы признается высокой
- Y >0,8 - 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.

Затем осуществляется выбор из общего (предварительного) перечня угроз безопасности те, которые относятся к актуальным для данной ИСПДн, в соответствии с правилами, приведенными в Таблице 2.

Таблица 8 - Правила отнесения угрозы безопасности ПДн к актуальной

Возможность реализации угрозы	Показатель опасности угрозы		
	низкая	средняя	высокая
Низкая	неактуальная	неактуальная	актуальная
Средняя	неактуальная	актуальная	актуальная
Высокая	актуальная	актуальная	актуальная
Очень высокая	актуальная	актуальная	актуальная

Таблица 9 - Угрозы и их характеристики для информационных систем на базе 1С: зарплата и управление кадров, Управление производственным предприятием, Управление сбытом тепловой энергии, а также СЭД «Дело»

Наименование угрозы	Вероятность (Y2)	Реализуемость (Y)	Опасность	Актуальность	Принимаемые меры
УГРОЗЫ УТЕЧКИ ИНФОРМАЦИИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ					
Угрозы утечки акустической (речевой) информации	маловероятно (0)	низкая (0.25)	низкая	неактуальная	-
Угрозы утечки видовой информации	низкая вероятность (2)	средняя (0.35)	средняя	актуальная	Установка средств воспроизведения таким образом, чтобы исключить возможность просмотра информации посторонними лицами
Угрозы утечки информации по каналу ПЭМИН	маловероятно (0)	низкая (0.25)	низкая	неактуальная	-
УГРОЗЫ НСД К ПДн, ОБРАБАТЫВАЕМЫМ НА АВТОМАТИЗИРОВАННОМ РАБОЧЕМ МЕСТЕ					
Угрозы, реализуемые в ходе загрузки операционной системы и направленные на перехват паролей или идентификаторов, модификацию базовой системы ввода/вывода (BIOS), перехват управления загрузкой	маловероятно (0)	низкая (0.25)	низкая	неактуальная	-
Угрозы, реализуемые после загрузки операционной системы и направленные на выполнение несанкционированного доступа с применением стандартных функций (уничтожение, копирование, перемещение, форматирование и т.п.) операционной системы или какой-либо прикладной программы, с	низкая вероятность (2)	средняя (0.35)	средняя	актуальная	Реализация разрешительной системы допуска пользователей; разграничение доступа пользователей и обслуживающего персонала к

применением специально созданных для выполнения НСД программ					информационным ресурсам, программным средствам обработки и защиты информации. Регистрация действий пользователей. Реализация подсистемы антивирусной защиты. Реализация подсистемы идентификации и аутентификации, централизованного управления учетными записями. Учет и хранение машинных носителей, и их обращение, исключающее хищение, подмену и уничтожение.
					Резервирование технических средств, дублирование массивов информации и носителей.
Угрозы внедрения вредоносных	низкая вероятность	средняя	средняя	актуальная	Реализация

программ	(2)	(0.35)			разрешительной системы допуска пользователей; разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки и защиты информации. Регистрация действий пользователей. Реализация подсистемы антивирусной защиты. Реализация подсистемы идентификации и аутентификации, централизованного управления учетными записями. Учет и хранение машинных носителей, и их обращение, исключающее хищение, подмену и уничтожение.

					Резервирование технических средств, дублирование массивов информации и носителей.
СЕТЕВЫЕ УГРОЗЫ					
Угрозы "Анализа сетевого трафика" с перехватом передаваемой по сети информации	низкая вероятность (2)	средняя (0.35)	низкая	неактуальная	-
Угрозы выявления паролей	низкая вероятность (2)	средняя (0.35)	низкая	неактуальная	-
Угрозы удаленного запуска приложений	низкая вероятность (2)	средняя (0.35)	средняя	актуальная	Разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки и защиты информации. Регистрация действия пользователя и обслуживающего персонала. Реализация подсистемы антивирусной защиты. Реализация подсистемы

					идентификации и аутентификации, централизованного управления учетными записями. Реализация подсистемы межсетевого взаимодействия.
Угрозы внедрения по сети вредоносных программ	низкая вероятность (2)	средняя (0.35)	средняя	актуальная	Реализация разрешительной системы доступа. Разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки и защиты информации. Регистрация действия пользователя и
					обслуживающего персонала. Реализация подсистемы антивирусной защиты. Реализация подсистемы идентификации и

					аутентификации, централизованного управления учетными записями. Реализация подсистемы межсетевого взаимодействия.
УГРОЗЫ ИЗ ВНЕШНИХ СЕТЕЙ					
Угрозы "Анализа сетевого трафика" с перехватом передаваемой во внешние сети и принимаемой из внешних сетей информации	маловероятно (0)	низкая (0.25)	низкая	неактуальная	-
Угрозы сканирования, направленные на выявление типа операционной системы АРМ, открытых портов и служб, открытых соединений и др.	маловероятно (0)	низкая (0.25)	низкая	неактуальная	-
Угрозы выявления паролей	низкая вероятность (2)	средняя (0.35)	средняя	актуальная	Реализация разрешительной системы доступа. Разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки и защиты информации. Регистрация действия пользователя и

					обслуживающего персонала. Реализация подсистемы антивирусной защиты. Реализация подсистемы идентификации и аутентификации, централизованного управления учетными записями. Реализация подсистемы межсетевого взаимодействия
Угрозы получения НСД путем подмены доверенного объекта	маловероятно (0)	низкая (0.25)	низкая	неактуальная	-
Угрозы типа "Отказ в обслуживании"	маловероятно (0)	низкая (0.25)	низкая	неактуальная	-
Угрозы удаленного запуска приложений	маловероятно (0)	низкая (0.25)	низкая	неактуальная	-
Угрозы внедрения по сети вредоносных программ	маловероятно (0)	низкая (0.25)	низкая	неактуальная	-

Таблица 10 - Угрозы и их характеристики ИСПДн Расчетно-информационный комплекс РИВЦ Симплекс

Наименование угрозы	Вероятность (Y2)	Реализуемость (Y)	Опасность	Актуальность	Принимаемые меры
УГРОЗЫ УТЕЧКИ ИНФОРМАЦИИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ					
Угрозы утечки акустической (речевой) информации	маловероятно (0)	низкая (0.25)	низкая	неактуальная	-
Угрозы утечки видовой информации	низкая вероятность (2)	средняя (0.35)	средняя	актуальная	Установка средств воспроизведения таким образом,

					чтобы исключить возможность просмотра информации посторонними лицами
Угрозы утечки информации по каналу ПЭМИН	маловероятно (0)	низкая (0.25)	низкая	неактуальная	-
УГРОЗЫ НСД К ПДн, ОБРАБАТЫВАЕМЫМ НА АВТОМАТИЗИРОВАННОМ РАБОЧЕМ МЕСТЕ					
Угрозы, реализуемые в ходе загрузки операционной системы и направленные на перехват паролей или идентификаторов, модификацию базовой системы ввода/вывода (BIOS), перехват управления загрузкой	маловероятно (0)	низкая (0.25)	низкая	неактуальная	-
Угрозы, реализуемые после загрузки операционной системы и направленные на выполнение несанкционированного доступа с применением стандартных функций (уничтожение, копирование, перемещение, форматирование и т.п.) операционной системы или какой-либо прикладной программы, с применением специально созданных для выполнения НСД программ	низкая вероятность (2)	средняя (0.35)	средняя	актуальная	Реализация разрешительной системы допуска пользователей; разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам,
					программным средствам обработки и защиты информации. Регистрация действий пользователей. Реализация

					подсистемы антивирусной защиты. Реализация подсистемы идентификации и аутентификации, централизованного управления учетными записями. Учет и хранение машинных носителей, и их обращение, исключающее хищение, подмену и уничтожение. Резервирование технических средств, дублирование массивов информации и носителей.
Угрозы внедрения вредоносных программ	низкая вероятность (2)	средняя (0.35)	средняя	актуальная	Реализация разрешительной системы допуска пользователей; разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам,

					программным средствам обработки и защиты информации. Регистрация действий пользователей. Реализация подсистемы антивирусной защиты. Реализация подсистемы идентификации и аутентификации, централизованного управления учетными записями. Учет и хранение машинных носителей, и их обращение, исключающее хищение, подмену и уничтожение. Резервирование технических средств, дублирование массивов информации и носителей.
СЕТЕВЫЕ УГРОЗЫ					
Угрозы "Анализа сетевого трафика" с перехватом передаваемой по сети	низкая вероятность (2)	средняя (0.35)	низкая	неактуальная	-

информации					
Угрозы выявления паролей	низкая вероятность (2)	средняя (0.35)	низкая	неактуальная	-
Угрозы удаленного запуска приложений	маловероятно (0)	низкая (0.25)	средняя	неактуальная	-
Угрозы внедрения по сети вредоносных программ	низкая вероятность (2)	средняя (0.35)	средняя	актуальная	Реализация разрешительной системы доступа. Разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки и защиты информации. Регистрация действия пользователя и обслуживающего персонала. Реализация подсистемы антивирусной защиты. Реализация подсистемы идентификации и аутентификации, централизованного управления учетными записями.

					Реализация подсистемы межсетевого взаимодействия.
УГРОЗЫ ИЗ ВНЕШНИХ СЕТЕЙ					
Угрозы "Анализа сетевого трафика" с перехватом передаваемой во внешние сети и принимаемой из внешних сетей информации	средняя вероятность (2)	средняя (0.35)	низкая	неактуальная	-
Угрозы сканирования, направленные на выявление типа операционной системы АРМ, открытых портов и служб, открытых соединений и др.	маловероятно (0)	низкая (0.25)	низкая	неактуальная	-
Угрозы выявления паролей	низкая вероятность (2)	средняя (0.35)	низкая	неактуальная	-
Угрозы получения НСД путем подмены доверенного объекта	маловероятно (0)	низкая (0.25)	низкая	неактуальная	-
Угрозы типа "Отказ в обслуживании"	низкая вероятность (2)	средняя (0.35)	низкая	неактуальная	-
Угрозы удаленного запуска приложений	низкая вероятность (2)	средняя (0.35)	низкая	неактуальная	-
Угрозы внедрения по сети вредоносных программ	низкая вероятность (2)	средняя (0.35)	низкая	неактуальная	-

Таблица 11 - База обращений населения с помощью сайта

Наименование угрозы	Вероятность (Y2)	Реализуемость (Y)	Опасность	Актуальность	Принимаемые меры
УГРОЗЫ УТЕЧКИ ИНФОРМАЦИИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ					
Угрозы утечки акустической (речевой) информации	маловероятно (0)	низкая (0.25)	низкая	неактуальная	-
Угрозы утечки видовой информации	низкая вероятность (2)	средняя (0.35)	средняя	актуальная	Установка средств воспроизведения таким образом,

					чтобы исключить возможность просмотра информации посторонними лицами
Угрозы утечки информации по каналу ПЭМИН	маловероятно (0)	низкая (0.25)	низкая	неактуальная	-
УГРОЗЫ НСД К ПДн, ОБРАБАТЫВАЕМЫМ НА АВТОМАТИЗИРОВАННОМ РАБОЧЕМ МЕСТЕ					
Угрозы, реализуемые в ходе загрузки операционной системы и направленные на перехват паролей или идентификаторов, модификацию базовой системы ввода/вывода (BIOS), перехват управления загрузкой	маловероятно (0)	низкая (0.25)	низкая	неактуальная	-
Угрозы, реализуемые после загрузки операционной системы и направленные на выполнение несанкционированного доступа с применением стандартных функций (уничтожение, копирование, перемещение, форматирование и т.п.) операционной системы или какой-либо прикладной программы, с применением специально созданных для выполнения НСД программ	низкая вероятность (2)	средняя (0.35)	средняя	актуальная	Реализация разрешительной системы допуска пользователей; разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки и защиты информации. Регистрация действий пользователей. Реализация

					подсистемы антивирусной защиты. Реализация подсистемы идентификации и аутентификации, централизованного управления учетными записями. Учет и хранение машинных носителей, и их обращение, исключающее хищение, подмену и уничтожение. Резервирование технических средств, дублирование массивов информации и носителей.
Угрозы внедрения вредоносных программ	низкая вероятность (2)	средняя (0.35)	средняя	актуальная	Реализация разрешительной системы допуска пользователей; разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам,

					программным средствам обработки и защиты информации. Регистрация действий пользователей. Реализация подсистемы антивирусной защиты. Реализация подсистемы идентификации и аутентификации, централизованного управления учетными записями. Учет и хранение машинных носителей, и их обращение, исключающее хищение, подмену и уничтожение. Резервирование технических средств, дублирование массивов информации и носителей.
СЕТЕВЫЕ УГРОЗЫ					
Угрозы "Анализа сетевого трафика" с перехватом передаваемой по сети	низкая вероятность (2)	средняя (0.35)	низкая	неактуальная	-

информации					
Угрозы выявления паролей	низкая вероятность (2)	средняя (0.35)	низкая	неактуальная	-
Угрозы удаленного запуска приложений	маловероятно (0)	низкая (0.25)	средняя	неактуальная	-
Угрозы внедрения по сети вредоносных программ	низкая вероятность (2)	средняя (0.35)	средняя	актуальная	Реализация разрешительной системы доступа. Разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки и защиты информации. Регистрация действия пользователя и обслуживающего персонала. Реализация подсистемы антивирусной защиты. Реализация подсистемы идентификации и аутентификации, централизованного управления учетными записями.

					Реализация подсистемы межсетевого взаимодействия.
УГРОЗЫ ИЗ ВНЕШНИХ СЕТЕЙ					
Угрозы "Анализа сетевого трафика" с перехватом передаваемой во внешние сети и принимаемой из внешних сетей информации	средняя вероятность (5)	средняя (0.5)	средняя	актуальная	Реализация разрешительной системы доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки и защиты информации. Регистрация действия пользователя и обслуживающего персонала. Реализация подсистемы антивирусной защиты. Реализация подсистемы идентификации и аутентификации, централизованного управления учетными записями. Реализация подсистемы

					межсетевого взаимодействия.
Угрозы сканирования, направленные на выявление типа операционной системы АРМ, открытых портов и служб, открытых соединений и др.	маловероятно (0)	низкая (0.25)	низкая	неактуальная	-
Угрозы выявления паролей	низкая вероятность (2)	средняя (0.35)	низкая	неактуальная	-
Угрозы получения НСД путем подмены доверенного объекта	маловероятно (0)	низкая (0.25)	низкая	неактуальная	-
Угрозы типа "Отказ в обслуживании"	низкая вероятность (2)	средняя (0.35)	низкая	неактуальная	-
Угрозы удаленного запуска приложений	низкая вероятность (2)	средняя (0.35)	низкая	неактуальная	-
Угрозы внедрения по сети вредоносных программ	низкая вероятность (2)	средняя (0.35)	низкая	неактуальная	-

2.4. МОДЕЛЬ ВЕРОЯТНОГО НАРУШИТЕЛЯ

По наличию права постоянного или разового доступа в контролируемую зону ИСПДн нарушители подразделяются на два типа:

внешние нарушители - нарушители, не имеющие доступа к ИСПДн, реализующие угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена;

внутренние нарушители - нарушители, имеющие доступ к ИСПДн, включая пользователей ИСПДн, реализующие угрозы непосредственно в ИСПДн

Внешними нарушителями могут быть:

- криминальные структуры;
- недобросовестные партнеры;
- внешние субъекты (физические лица).

Внешний нарушитель имеет следующие возможности:

- осуществлять несанкционированный доступ к каналам связи, выходящим за пределы служебных помещений;
- осуществлять несанкционированный доступ через автоматизированные рабочие места, подключенные к сетям связи общего пользования и (или) сетям международного информационного обмена;
- осуществлять несанкционированный доступ к информации с использованием специальных программных воздействий посредством программных вирусов, вредоносных программ, алгоритмических или программных закладок;
- осуществлять несанкционированный доступ через элементы информационной инфраструктуры ИСПДн, которые в процессе своего жизненного цикла (модернизации, сопровождения, ремонта, утилизации) оказываются за пределами контролируемой зоны;
- осуществлять несанкционированный доступ через информационные системы взаимодействующих ведомств, организаций и учреждений при их подключении к ИСПДн.

Внутренние потенциальные нарушители подразделяются на восемь категорий в зависимости от способа доступа и полномочий доступа к ПДн (Таблица 12).

Таблица 12 - Категории нарушителей

№	Описание	Нарушитель может	Возможный нарушитель
1	Лица, имеющие санкционированный доступ к ИСПДн, но не имеющие доступа к ПДн. К этому типу нарушителей относятся должностные лица, обеспечивающие нормальное функционирование ИСПДн.	- иметь доступ к фрагментам информации, содержащей ПДн и распространяющейся по внутренним каналам связи ИСПДн; - располагать фрагментами информации о топологии ИСПДн (коммуникационной части подсети) и об используемых коммуникационных протоколах и их сервисах; - располагать именами и вести выявление паролей зарегистрированных пользователей; - изменять конфигурацию технических средств ИСПДн, вносить в нее программно-аппаратные закладки и обеспечивать съем информации, используя непосредственное подключение к техническим средствам ИСПДн.	Сотрудники отдела АСУ
2	Зарегистрированные пользователи ИСПДн, осуществляющие ограниченный доступ к ресурсам ИСПДн с рабочего места.	- обладает всеми возможностями лиц первой категории; - знает по меньшей мере одно легальное имя доступа; - обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству ПДн; - располагает конфиденциальными данными, к которым имеет доступ.	Сотрудники, обрабатывающие ПДн
3	Зарегистрированные пользователи ИСПДн, осуществляющие удаленный доступ к ПДн по локальным и (или) распределенным информационным системам	- обладает всеми возможностями лиц первой и второй категорий; - располагает информацией о топологии ИСПДн на базе локальной и (или) распределенной информационной системам, через которую он осуществляет доступ, и составе технических средств ИСПДн; - имеет возможность прямого (физического) доступа к фрагментам технических средств ИСПДн.	Отсутствует
4	Зарегистрированные пользователи ИСПДн с полномочиями администратора безопасности сегмента (фрагмента) ИСПДн.	- обладает всеми возможностями лиц предыдущих категорий; - обладает полной информацией о системном и прикладном программном обеспечении, используемом в сегменте (фрагменте) ИСПДн; - обладает полной информацией о технических средствах и конфигурации сегмента (фрагмента) ИСПДн; - имеет доступ к средствам защиты информации и протоколирования, а также к отдельным элементам, используемым в сегменте (фрагменте) ИСПДн; - имеет доступ ко всем техническим средствам сегмента (фрагмента) ИСПДн; - обладает правами конфигурирования и административной настройки	Отсутствует

		некоторого подмножества технических средств сегмента (фрагмента) ИСПДн.	
5	Зарегистрированные пользователи с полномочиями системного администратора ИСПДн	- обладает всеми возможностями лиц предыдущих категорий; - обладает полной информацией о системном и прикладном программном обеспечении ИСПДн; - обладает полной информацией о технических средствах и конфигурации ИСПДн; - имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн; - обладает правами конфигурирования и административной настройки технических средств ИСПДн.	Сотрудники отдела АСУ
6	Зарегистрированные пользователи с полномочиями администратора безопасности ИСПДн	- обладает всеми возможностями лиц предыдущих категорий; - обладает полной информацией об ИСПДн; - имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн; - не имеет прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных).	Отсутствует
7	Программисты-разработчики (поставщики) прикладного программного обеспечения и лица, обеспечивающие его сопровождение на защищаемом объекте	- обладает информацией об алгоритмах и программах обработки информации на ИСПДн; - обладает возможностями внесения ошибок, недекларированных возможностей, программных закладок, вредоносных программ в программное обеспечение ИСПДн на стадии ее разработки, внедрения и сопровождения; - может располагать любыми фрагментами информации о топологии ИСПДн и технических средствах обработки и защиты ПДн, обрабатываемых в ИСПДн.	Отсутствует
8	Разработчики и лица, обеспечивающие поставку, сопровождение и ремонт технических средств на ИСПДн	- обладает возможностями внесения закладок в технические средства ИСПДн на стадии их разработки, внедрения и сопровождения; - может располагать любыми фрагментами информации о топологии ИСПДн и технических средствах обработки и защиты информации в ИСПДн.	Сотрудники отдела АСУ

3. МЕРЫ ПО ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИСПД

3.1. СОСТАВ И СОДЕРЖАНИЕ МЕР ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ДЛЯ ИНФОРМАЦИОННЫХ СИСТЕМ 3 УРОВНЯ ЗАЩИЩЕННОСТИ

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных
I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)	
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов
ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации
ИАФ.5	Защита обратной связи при вводе аутентификационной информации
ИАФ.6	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)
II. Управление доступом субъектов доступа к объектам доступа (УПД)	
УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей
УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа
УПД.3	Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами
УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы
УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы
УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)

УПД.10	Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу
УПД.11	Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации
УПД.13	Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети
УПД.14	Регламентация и контроль использования в информационной системе технологий беспроводного доступа
УПД.15	Регламентация и контроль использования в информационной системе мобильных технических средств
УПД.16	Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)
IV. Защита машинных носителей персональных данных (ЗНИ)	
ЗНИ.8	Уничтожение (стирание) или обезличивание персональных данных на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) или обезличивания
V. Регистрация событий безопасности (РСБ)	
РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения
РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации
РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения
РСБ.7	Защита информации о событиях безопасности
VI. Антивирусная защита (АВЗ)	
АВЗ.1	Реализация антивирусной защиты
АВЗ.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)
VIII. Контроль (анализ) защищенности персональных данных (АНЗ)	
АНЗ.1	Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей
АНЗ.2	Контроль установки обновлений программного обеспечения, включая

	обновление программного обеспечения средств защиты информации
АНЗ.3	Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации
АНЗ.4	Контроль состава технических средств, программного обеспечения и средств защиты информации
XI. Защита среды виртуализации (ЗСВ)	
ЗСВ.1	Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации
ЗСВ.2	Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин
ЗСВ.3	Регистрация событий безопасности в виртуальной инфраструктуре
ЗСВ.9	Реализация и управление антивирусной защитой в виртуальной инфраструктуре
ЗСВ.10	Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки персональных данных отдельным пользователем и (или) группой пользователей
XII. Защита технических средств (ЗТС)	
ЗТС.3	Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр
XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)	
ЗИС.3	Обеспечение защиты персональных данных от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи
ЗИС.20	Защита беспроводных соединений, применяемых в информационной системе
XV. Управление конфигурацией информационной системы и системы защиты	

персональных данных (УКФ)	
УКФ.1	Определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и системы защиты персональных данных
УКФ.2	Управление изменениями конфигурации информационной системы и системы защиты персональных данных
УКФ.3	Анализ потенциального воздействия планируемых изменений в конфигурации информационной системы и системы защиты персональных данных на обеспечение защиты персональных данных и согласование изменений в конфигурации информационной системы с должностным лицом (работником), ответственным за обеспечение безопасности персональных данных
УКФ.4	Документирование информации (данных) об изменениях в конфигурации информационной системы и системы защиты персональных данных

3.2. СОСТАВ И СОДЕРЖАНИЕ МЕР ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ДЛЯ ИНФОРМАЦИОННЫХ СИСТЕМ 4 УРОВНЯ ЗАЩИЩЕННОСТИ

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных
I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)	
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов
ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации
ИАФ.5	Защита обратной связи при вводе аутентификационной информации
ИАФ.6	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)
II. Управление доступом субъектов доступа к объектам доступа (УПД)	
УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей
УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа
УПД.3	Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами
УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы

УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы
УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)
УПД.13	Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети
УПД.14	Регламентация и контроль использования в информационной системе технологий беспроводного доступа
УПД.15	Регламентация и контроль использования в информационной системе мобильных технических средств
УПД.16	Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)
V. Регистрация событий безопасности (РСБ)	
РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения
РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации
РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения
РСБ.7	Защита информации о событиях безопасности
VI. Антивирусная защита (АВЗ)	
АВЗ.1	Реализация антивирусной защиты
АВЗ.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)
VIII. Контроль (анализ) защищенности персональных данных (АНЗ)	
АНЗ.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации
XI. Защита среды виртуализации (ЗСВ)	
ЗСВ.1	Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации
ЗСВ.2	Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин

XII. Защита технических средств (ЗТС)		
	ЗТС.3	Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены
	ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр
XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)		
	ЗИС.3	Обеспечение защиты персональных данных от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи