УТВЕРЖДЕНО
приказом директора
ГБУ КЦСОН Дубровского района
от 03.09.2018 г. № 72

МОДЕЛЬ
угроз безопасности персональных данных при их обработке в информационных системах персональных данных «Бухгалтерия», «Зарплата и кадры» и «Обращение граждан» в Государственном бюджетном учреждении Брянской области «Комплексный центр социального обслуживания населения Дубровского района»

1. Общие положения

1.1. Модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных «Бухгалтерия», «Зарплата и кадры» и «Обращение граждан» (далее – ИСПДн) в Государственном бюджетном учреждении Брянской области «Комплексный центр социального обслуживания населения Дубровского района» (далее — ГБУ КЦСОН Дубровского района, Модель угроз) разработана в соответствии со следующими действующими нормативно-методическими документами по защите персональных данных:

1.1.1. Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных».

1.1.2. Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

1.1.3. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденная Федеральной службой по техническому и экспортному контролю14 февраля 2008 года (далее - Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных).

1.1.4. Базовая модель угроз безопасности персональных данных при их обработке, в информационных системах персональных данных, утвержденная Федеральной службой по техническому и экспортному контролю15 февраля 2008 года).

1.1.5. Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденные Федеральной службой безопасности Российской Федерации 21 февраля 2008 года № 149/6/6-622.

1.1.6. Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации, утвержденные Федеральной службой безопасности Российской Федерации 21 февраля 2008 года № 149/54-144.

1.1.7. Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности, утвержденные Федеральной службой безопасности Российской Федерации 31 марта 2015 года № 149/7/2/6-432.

1.2. Настоящая Модель угроз содержит систематизированный перечень угроз безопасности персональных данных при их обработке в ИСПДн.

1.3. Модель угроз содержит данные по угрозам безопасности персональных данных, обрабатываемых в ИСПДн, связанным:

1.3.1. С перехватом (съемом) персональных данных (далее – ПДн) по техническим каналам с целью их копирования или неправомерного распространения.

1.3.2. С несанкционированным, в том числе случайным, доступом в ИСПДн с целью изменения, копирования, неправомерного распространения ПДн или деструктивных воздействий на элементы ИСПДн и обрабатываемых в них ПДн.

1.3.3. С использованием программных и программно-аппаратных средств с целью уничтожения или блокирования ПДн.

1.4. Модель угроз является методическим документом и предназначена для должностных и ответственных лиц ГБУ КЦСОН Дубровского района как Оператора персональных данных (далее - Оператор), администраторов ИСПДн.

1.5. Модель угроз разработана для ИСПДн с учетом их назначения, условий и особенностей функционирования.

1.6. Модель угроз предназначена для решения следующих задач:

1.6.1. Анализ защищенности ИСПДн от угроз безопасности ПДн в ходе организации и выполнения работ по обеспечению безопасности ПДн.

1.6.2. Разработка системы защиты ПДн, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты ПДн, предусмотренных для соответствующего уровня защищенности ИСПДн.

1.6.3. Проведение мероприятий, направленных на предотвращение несанкционированного доступа к ПДн и (или) передачи их лицам, не имеющим права доступа к такой информации.

1.6.4. Недопущение воздействия на технические средства ИСПДн, в результате которого может быть нарушено их функционирование.

1.6.5. Контроль обеспечения уровня защищенности персональных данных.

1.7. В Модели угроз дано обобщенное описание ИСПДн как объекта защиты, возможных источников угроз безопасности персональных данных

(далее - УБПДн), основных классов уязвимостей ИСПДн, возможных видов неправомерных действий и деструктивных воздействий на ПДн, а также основных способов их реализации.

1.8. Угрозы безопасности ПДн, обрабатываемых в ИСПДн, содержащиеся в настоящей Модели угроз, могут уточняться и дополняться по мере выявления новых источников угроз, развития способов и средств реализации УБПДн в ИСПДн.

1.9. Модель угроз может быть пересмотрена по решению Оператора на основе периодически проводимых им анализа и оценки угроз безопасности ПДн с учетом особенностей и (или) изменений ИСПДн, а также по результатам мероприятий по контролю выполнения требований к обеспечению безопасности ПДн при их обработке в информационной системе.

2. Описание информационной системы ПДн

2.1. Наименование ИСПДн: «Бухгалтерия», «Зарплата и кадры» и «Обращение граждан».

2.2. ИСПДн является собственностью оператора.

2.3. Местонахождение ИСПДн: Брянская область, Дубровский район, рп. Дубровка, 1-й микрорайон, д. 1.

2.4. Осуществляется физическая охрана помещений.

2.5. Перечень технических средств, входящих в состав ИСПДн, указан в «Техническом паспорте информационных систем ПДн Государственного бюджетного учреждения Брянской области «Комплексный центр социального обслуживания населения Дубровского района» (далее – Технический паспорт»).

2.6. Состав программного обеспечения, с использованием которого ведется обработка ПДн в ИСПДн, приведен в «Техническом паспорте».

2.7. В ИСПДн реализован многопользовательский режим обработки ПДн с разграничением прав доступа пользователей.

2.8. ИСПДн «1С: Бухгалтерия», «1С: Зарплата и кадры» имеют подключение к сетям связи общего пользования.

3. Возможные последствия нарушения безопасности ПДн

3.1. Возможными последствиями нарушения безопасности ПДн, обрабатываемых в ИСПДн, являются:

3.1.1. Разглашение персональных данных, несанкционированное изменение ПДн субъектов ПДн и причинение им физического, материального, финансового или морального ущерба.

3.1.2. Причинение материального ущерба Оператору.

3.1.3. Вред репутации Оператора в обществе.

3.2. Разглашение ПДн субъектов ПДн и причинение им физического, материального, финансового или морального ущерба может проявляться в виде:

3.2.1. Незапланированных и (или) непроизводительных финансовых или материальных затрат субъекта.

3.2.2. Потери субъектом свободы действий вследствие шантажа и угроз, осуществляемых с использованием ПДн.

3.2.3. Нарушения конституционных прав субъекта вследствие вмешательства в его личную жизнь.

4. Объекты угроз

4.1. Объектами угроз в ИСПДн, подлежащими защите, являются информационные ресурсы, содержащие ПДн, информационные технологии, технические и программные средства, используемые для обработки ПДн, программные средства защиты.

5. Основные ресурсы, содержащие персональные данные

5.1. Основными информационными ресурсами, содержащими ПДн, в ИСПДн, являются ресурсы:

5.1.1. АИС «1С: Предприятие – Зарплата и кадры бюджетного учреждения».

5.1.2. АИС «1С: — Бухгалтерия для бюджетных организаций».

5.1.3. Электронные документы и таблицы, содержащие ПДн сотрудников и клиентов Оператора.

6. Информация, формируемая в процессе создания и обработки ПДн, но не содержащая ПДн

6.1. В процессе обработки ПДн в ИСПДн осуществляется формирование информации, не являющейся к ПДн, но получение которой злоумышленником способствует получению им доступа к персональным данным. По этой причине к объектам угроз относится:

- ключевая, аутентифицирующая и парольная информация;
- криптографически опасная информация;
- конфигурационная и управляющая информация;
- информация в электронных журналах регистрации;
- остаточная информация на носителях информации;
- информация, подверженная съему по побочному электромагнитному излучению и наводкам.

7. Характеристики безопасности персональных данных

7.1. Для ПДн и объектов, которые могут выступать в качестве объектов угроз и требуют защиты, необходимо обеспечить выполнение следующих характеристик безопасности:

- конфиденциальность;
- целостность;
- доступность.

7.2. Обеспечение других характеристик безопасности в ИСПДн не требуется, так как их нарушение не может привести к негативным последствиям для субъектов Пдн.

8. Модель нарушителя безопасности персональных данных

8.1. Описание нарушителей:

8.1.1. В качестве нарушителя безопасности ПДн могут выступать физические лица или организации, которые преднамеренно или случайно совершают действия, в результате которых нарушаются заданные характеристики безопасности ПДн.

8.1.2. В зависимости от прав доступа к ресурсам ИСПДн, нарушители подразделяются на два типа:

- внешние;
- внутренние.

8.1.3. Внешними нарушителями могут являться:

- организованные преступные группы, сообщества;
- бывшие сотрудники оператора;
- недобросовестные партнеры.

8.1.4. Внутренними (потенциальными) нарушителями являются сотрудники оператора, находящиеся в пределах контролируемой зоны.

8.1.5. Привилегированные пользователи ИСПДн (администраторы), которые осуществляют техническое управление и обслуживание аппаратных и программных средств ИСПДн, в том числе и средств защиты, включая их настройку, конфигурирование и распределение ключевой и парольной документации, относятся к особо доверенным лицам и исключаются из числа потенциальных нарушителей.

8.1.6. Предполагается, что потенциальные нарушители:

8.1.6.1. Не могут организовывать или заказывать работы по созданию способов и средств атак в научно-исследовательских центрах, специализирующихся в области разработки и анализа криптосредств и среды их функционирования.

8.1.6.1. Являются, в силу специфики информации ИСПДн, одиночками, самостоятельно осуществляющими освоение способов, подготовку и проведение атак.

8.2. Основными объектами атак являются:

8.2.1. Документация, технические и программные компоненты.

8.2.2. Ресурсы персональных данных.

8.2.3. Ключевая, аутентифицирующая и парольная информация.

8.2.4. Криптографически опасная информация.

8.2.5. Аппаратные и программные средства защиты.

8.2.6. Технические и программные компоненты среды функционирования криптосредств.

8.2.7. Помещения, в которых размещены ресурсы ИСПДн.

8.3. Целью атаки является неправомерный доступ к информации или к вычислительным ресурсам ИСПДн как с умыслом нанесения ущерба оператору, так и без такого умысла.

9. Предположения об имеющейся у нарушителя информации об объектах атак

9.1. Предполагается, что потенциальный нарушитель не располагает исходными текстами прикладного программного обеспечения.

9.2. Разработчики прикладного программного обеспечения относятся к особо доверенным лицам и исключаются из числа потенциальных нарушителей.

9.3. Основными каналами атак являются:

9.3.1. Визуальный канал, который может позволить получить персональные данные путем просматривания документированной и отображаемой на технических средствах информации.

9.3.2. Физический доступ к документации и в помещения, в которых расположены ресурсы ИСПДн.

9.3.3. Каналы связи, не защищенные от несанкционированного доступа к информации организационно-техническими мерами;

9.3.4. Средства обработки информации.

9.3.5. Машинные носители информации.

10. Основные угрозы безопасности персональных данных

10.1.Формирование Модели угроз осуществлено на основе определенных ранее угроз безопасности ПДн при их обработке.

10.2.Проведен анализ Перечня угроз безопасности персональных данных с учетом оперативной обстановки, складывающейся вокруг оператора, имеющихся доступных материалов о реально зафиксированных угрозах безопасности персональных ПДн с учетом опыта Оператора, а также имеющихся на общедоступном рынке средств защиты и средств технической разведки в информационной сфере.

10.3.При этом были выполнены требования нормативных правовых актов и учтены положения методических документов Федеральной службы безопасности Российской Федерации и Федеральной службы по техническому и экспортному контролю.

10.4.Перечень и актуальность угроз безопасности персональных данных сформирован исходя из анализа непреднамеренных (ошибочных, случайных) действий персонала Оператора, учета условий жизнеобеспечения и системы энергоснабжения ИСПДн, а также влияния иных техногенных и природных факторов (стихийные бедствия и т .п.).

11. Оценка уровня исходной защищенности ИСПДн

11.1.В соответствии с табл.1 Методики определения актуальных угроз безопасности персональных данных при их обработке в ИСПДн, утвержденной ФСТЭК России от 14.02.2008 г., ИСПДн «Бухгалтерия» имеет следующие технические, эксплуатационные характеристики и показатели исходного уровня защищенности:

Характеристика ИСПД	**Значение характеристики**	**Уровень защищенности**
1. Территориальное размещение	Локальная ИСПД, развернутая в пределах одного здания	высокий
2. Наличие соединения с сетями общего пользования *(интернет)*	ИСПД, физически отделенная от сети общего пользования	высокий
3. Встроенные операции с записями баз персональных данных	Модификация, передача	низкий
4. Разграничение доступа к персональным данным	ИСПД, к которой имеют доступ определенные перечнем сотрудники	высокий

Характеристика ИСПД	Значение характеристики	Уровень защищенности
5. Наличие соединений с другими базами ПД иных ИСПД	ИСПД, в которой используется одна база ПД	высокий
6. Обобщение (обезличивание) ПД	ИСПД, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта ПД)	низкий
7. Объем ПД, которые предоставляются сторонним пользователям ИСПД без предварительной обработки	ИСПД, не предоставляющая никакой информации сторонним пользователям	высокий
Исходный уровень защищенности		5

Поскольку более 70% показателей исходной защищенности ИСПД имеют значение «высокий» уровень исходной защищенности, то согласно раздела 2 «Методики определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» ИСПДн относится к информационным системам со средней степенью исходной защищенности и соответствующий числовой коэффициент (Yi) равен 5.

11.2.В соответствии с табл.1 Методики определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной ФСТЭК России от 14.02.2008 г., ИСПД имеет следующие технические, эксплуатационные характеристики и показатели исходного уровня защищенности:

Характеристика ИСПД	Значение характеристики	Уровень защищенности
1. Территориальное размещение	Локальная ИСПД, развернутая в пределах одного здания	высокий
2. Наличие соединения с сетями общего пользования *(интернет)*	ИСПД, физически отделенная от сети общего пользования	высокий
3. Встроенные операции с записями баз персональных данных	Модификация, передача	низкий
4. Разграничение доступа к персональным данным	ИСПД, к которой имеют доступ определенные перечнем сотрудники	высокий
5. Наличие соединений с другими базами ПД иных ИСПД	ИСПД, в которой используется одна база ПД	высокий
6. Обобщение (обезличивание) ПД	ИСПД, в которой предоставляемые пользователю данные не являются обезличенными (т.е.	низкий

Характеристика ИСПД	Значение характеристики	Уровень защищенности
	присутствует информация, позволяющая идентифицировать субъекта ПД)	
7. Объем ПД, которые предоставляются сторонним пользователям ИСПД без предварительной обработки	ИСПД, не предоставляющая никакой информации сторонним пользователям	высокий

Поскольку более 70% показателей исходной защищенности ИСПД имеют значение «высокий» уровень исходной защищенности, то согласно раздела 2 «Методики определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» ИСПДн относится к информационным системам со средней степенью исходной защищенности и соответствующий числовой коэффициент (Yi) равен 5.

11.3. В соответствии с табл.1 Методики определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной ФСТЭК России от 14.02.2008 г., ИСПД «Обращение граждан» имеет следующие технические, эксплуатационные характеристики и показатели исходного уровня защищенности:

Характеристика ИСПД	Значение характеристики	Уровень защищенности
1. Территориальное размещение	локальная ИСПД, развернутая в пределах одного здания	высокий
2. Наличие соединения с сетями общего пользования (интернет)	ИСПД, физически отделенная от сети общего пользования	высокий
3. Встроенные операции с записями баз персональных данных	запись, удаление, сортировка	средний
4. Разграничение доступа к персональным данным	ИСПД, к которой имеют доступ определенные перечнем сотрудники	средний
5. Наличие соединений с другими базами ПД иных ИСПД	ИСПД, в которой используется одна база ПД	высокий
6. Обобщение (обезличивание) ПД	ИСПД, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта ПД)	низкий
7. Объем ПД, которые предоставляются сторонним пользователям ИСПД без предварительной обработки	ИСПД, не предоставляющая никакой информации сторонним пользователям	высокий

Поскольку менее 70% показателей исходной защищенности ИСПД имеют значение «высокий» уровень исходной защищенности, то согласно раздела 2 «Методики определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» ИСПДн относится к информационным системам со средней степенью исходной защищенности и соответствующий числовой коэффициент (Yi) равен 4.

12. Определение вероятности реализации угроз безопасности ПДн

12.1.Вероятность реализации угроз безопасности ПДн определена экспертным методом в соответствии с Методикой и на основании результатов обследования ИСПДн.

13. Угрозы утечки по техническим каналам

13.1.Утечка акустической информации: речевое воспроизведение защищаемой информации в ИСПДн не производится. Вероятность реализации угрозы – маловероятно.

13.2.Утечка видовой информации со средств отображения индивидуального пользования.

Мониторы рабочих станций пользователей расположены таким образом, что исключен несанкционированный просмотр отображаемой на них информации посторонними лицами.

Окна помещений оборудованы жалюзи.

Вероятность реализации угрозы – маловероятно.

13.3.С печатных документов.

Принтеры рабочих станций расположены таким образом, что исключен несанкционированный просмотр информации, выводимой на печать, документы, содержащие защищаемую информацию, хранятся на рабочих столах.

Окна помещений оборудованы жалюзи.

Вероятность реализации угрозы – маловероятно.

13.4.Утечка информации за счет побочных электромагнитных излучений информативных сигналов от технических средств.

В ИСПДн используются технические средства, удовлетворяющие требованиям национальных стандартов по электромагнитной совместимости, по безопасности и эргономическим требованиям к средствам отображения информации, по санитарным нормам, предъявляемым к видеодисплейным терминалам средств вычислительной техники.

Вероятность реализации угрозы – маловероятно.

13.5.Утечка информации за счет наводок информативного сигнала, обрабатываемого техническими средствами, на цепи электропитания и линии связи, выходящие за пределы контролируемой зоны.

В ИСПДн используются технические средства, удовлетворяющие требованиям национальных стандартов по электромагнитной совместимости, по безопасности и эргономическим требованиям к средствам отображения информации, по санитарным нормам, предъявляемым к видеодисплейным терминалам средств вычислительной техники. Вероятность реализации угрозы – маловероятно.

13.6.Утечка информации за счет радиоизлучений или электрических сигналов от электронных устройств перехвата информации, подключенных к каналам связи или техническим средствам обработки информации.

Меры по защите информации, передаваемой по каналам связи, выходящим за пределы контролируемой зоны, не удовлетворяют требованиям нормативных документов Федеральной службы по техническому и экспортному контролю и Федеральной службы безопасности Российской Федерации.

Несанкционированный доступ посторонних лиц к техническим средствам, входящим в состав ИСПДн, исключен. Вероятность реализации угрозы – средняя.

14. Несанкционированный доступ к информации

14.1.Угрозы уничтожения, хищения, модификации технических средств ИСПДн, носителей информации путем физического доступа к элементам ИСПДн. Кража ПЭВМ.

14.1.1.1. Охрана здания осуществляется.

14.1.1.2. Территория учреждения огорожена по всему периметру металлическим забором (сетка), средняя высота ограждения от 1 до 1,5

м.

14.1.1.3. Тревожная кнопка и система противопожарной защиты (АПС).

14.1.1.4. Видеонаблюдение – 8 камер наблюдения: 6 - по периметру здания на улице, 1 – на первом этаже Отделения помощи семье, женщинам и детям со стационаром, 1 – на втором этаже.

14.1.1.5. Осуществляется пропускной режим.

14.1.1.6. В ночное время и в выходные дни - физическая защита - 3 сторожа.

14.1.1.7. Кабинеты закрываются на ключ.

14.1.1.8. На первом этаже на окнах есть решетки.

14.2.Вероятность реализации угрозы – маловероятно.

14.3.Кража носителей информации. В ИСПДн используются съемные носители информации. Учет съемных носителей информации не ведется. Вероятность реализации угрозы – средняя.

14.4.Кража ключей и атрибутов доступа. Аппаратные идентификаторы и ключи доступа не используются. Вероятность реализации угрозы – маловероятно.

14.5.Внедрение аппаратных закладок в технические средства ИСПДн. Системные блоки технических средств, входящих в состав ИСПДн, не опечатаны, что делает возможным незамеченное внедрение аппаратных закладок в данные технические средства. Вероятность реализации угрозы – средняя.

14.6.Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) технических средств ИСПДн. Обслуживание технических средств производится без присутствия администратора безопасности. Вероятность реализации угрозы – средняя.

14.7.Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий). Воздействие вредоносных программ.

На серверах и автоматизированных рабочих местах (далее — АРМ) пользователей установлено средство антивирусной защиты Kaspersky Endpoint Security

14.8.Производится регулярное обновление антивирусных баз. Вероятность реализации угрозы – маловероятно.

14.9.Недекларированные возможности общесистемного и прикладного программного обеспечения.

В ИСПДн используется нелицензионное программное обеспечение. В ИСПДн отсутствуют средства модификации объектного кода программного обеспечения. Вероятность реализации угрозы – средняя.

14.10. Ошибки в общесистемном и прикладном программном обеспечении.

В ИСПДн используется нелицензионное программное обеспечение. Средства модификации объектного кода программного обеспечения отсутствуют. Ведется резервное копирование баз данных защищаемой информации. Вероятность реализации угрозы – средняя.

14.11. Установка программного обеспечения, не связанного с исполнением служебных обязанностей.

У пользователей ИСПДн имеются учетные записи без прав администрирования, что исключает возможность установки пользователями программного обеспечения, не связанного с выполнением должностных обязанностей, в том числе для поиска уязвимостей в ИСПДн и анализа информации, циркулирующей в ИСПДн. Вероятность реализации угрозы – маловероятно.

14.12. Неумышленные деструктивные действия персонала:

14.12.1. Утрата ключей и атрибутов доступа. Аппаратные идентификаторы и ключи доступа не используются. Вероятность реализации угрозы – маловероятно.

14.12.2. Непреднамеренная модификация (уничтожение) информации сотрудниками. У пользователей ИСПДн имеются учетные записи без прав администрирования. Вероятность реализации угрозы – маловероятно.

14.12.3. Непреднамеренное отключение средств защиты. У пользователей ИСПДн имеются учетные записи без прав администрирования. Вероятность реализации угрозы – маловероятно.

14.12.4. Вывод из строя аппаратно-программных средств вследствие ошибочных действий. Отсутствуют инструкции пользователей по работе с защищаемой информацией и техническими средствами. Вероятность реализации угрозы – средняя.

14.12.5. Умышленные деструктивные действия персонала. Копирование баз данных администратором. У пользователей ИСПДн имеются учетные записи без прав администрирования. Аудит действий пользователей не ведется. Вероятность реализации угрозы – маловероятно.

14.12.6. Накопление данных пользователем информационной системы. У пользователей ИСПДн имеются учетные записи без прав администрирования. Аудит действий пользователей не ведется. Вероятность реализации угрозы – маловероятно.

14.12.7. Злонамеренное разрушение (искажение) информации. У пользователей ИСПДн имеются учетные записи без прав администрирования. Аудит действий пользователей не ведется. Ведется резервное копирование баз данных защищаемой информации администратором. Вероятность реализации угрозы – маловероятная.

14.12.8. Злонамеренное блокирование данных. У пользователей ИСПДн имеются учетные записи без прав администрирования. Ведется резервное копирование баз данных защищаемой информации. Вероятность реализации угрозы – низкая.

14.12.9. Фальсификация данных. У пользователей ИСПДн имеются учетные записи без прав администрирования. Аудит действий пользователей не ведется. Ведется резервное копирование баз данных защищаемой информации. Вероятность реализации угрозы – маловероятно.

14.12.10. Несанкционированный доступ персонала информационной системы к ресурсам. У пользователей ИСПДн имеются учетные записи без прав администрирования. Аудит действий пользователей не ведется. Матрица доступа пользователей к защищаемым информационным ресурсам формализована. Вероятность реализации угрозы – маловероятно.

14.12.11. Компрометация аутентификатора. Есть правила хранения парольной информации. Вероятность реализации угрозы – средняя.

14.12.12. Компрометация ключа средства криптографической защиты информации (далее – СКЗИ). Назначен Ответственный пользователь криптосредств. Журнал учета криптографических ключей не ведется. Вероятность реализации угрозы – средняя.

14.12.13. Нарушение функционирования средства защиты. У пользователей ИСПДн имеются учетные записи без прав администрирования. Вероятность реализации угрозы – маловероятно.

14.12.14. Произвольное создание точек входа в систему за счет неправомерных действий. Все коммутационное оборудование ИСПДн находится в серверном помещении, доступ в которое ограничен. Линии связи внутри здания проложены в кабель-каналах. Вероятность реализации угрозы – маловероятно.

14.12.15. Угрозы несанкционированного доступа по каналам связи. Перехват передаваемой информации за пределами контролируемой зоны. В ИСПДн производится передача защищаемой информации через линии связи, выходящие за границы контролируемой зоны. Вероятность реализации угрозы – высокая.

14.12.16. Перехват в пределах контролируемой зоны внешними нарушителями. Внутри здания исключено неконтролируемое пребывание посторонних лиц. Вероятность реализации угрозы – маловероятно.

14.12.17. Перехват в пределах контролируемой зоны внутренними нарушителями. У пользователей ИСПДн имеются учетные записи без прав администрирования, не дающие возможность установки программ-снифферов. Вероятность реализации угрозы – маловероятно.

14.12.18. Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др. ИСПДн имеет подключение к сетям связи общего пользования. Средства межсетевого экранирования, удовлетворяющие требованиям нормативных документов Федеральной службы по техническому и экспортному контролю, в наличии. У пользователей ИСПДн имеются учетные записи с административными правами. Вероятность реализации угрозы – средняя.

14.12.19. Угрозы выявления паролей по сети. ИСПДн имеет подключение к сетям связи общего пользования. Средства межсетевого экранирования, удовлетворяющие требованиям нормативных документов Федеральной службы по техническому и экспортному контролю, в наличии. У пользователей ИСПДн не имеется учетных записей с административными правами, не предоставляющими возможность установки программ-сниферов. Вероятность реализации угрозы – маловероятно.

14.12.20. Угрозы навязывания ложного маршрута сети. ИСПДн имеет подключение к сетям связи общего пользования. Средства межсетевого экранирования, удовлетворяющие требованиям нормативных документов Федеральной службы по техническому и экспортному контролю, в наличии. У пользователей ИСПДн отсутствуют учетные записи с административными правами. Вероятность реализации угрозы – маловероятно.

14.12.21. Угрозы подмены доверенного объекта в сети. ИСПДн имеет подключение к сетям связи общего пользования. Средства межсетевого экранирования, удовлетворяющие требованиям нормативных документов Федеральной службы по техническому и экспортному контролю, в наличии. У пользователей ИСПДн имеются учетные записи без прав администрирования. Вероятность реализации угрозы – маловероятно.

14.12.22. Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях. ИСПДн имеет подключение к сетям связи общего пользования. Средства межсетевого экранирования, удовлетворяющие требованиям нормативных документов Федеральной службы по техническому и экспортному контролю, в наличии. У пользователей ИСПДн имеются учетные записи без прав администрирования. Вероятность реализации угрозы – маловероятно.

14.12.23. Угрозы типа «Отказ в обслуживании». ИСПДн имеет подключение к сетям связи общего пользования. Средства межсетевого экранирования, удовлетворяющие требованиям нормативных документов Федеральной службы по техническому и экспортному контролю, в наличии. У пользователей ИСПДн имеются учетные записи без прав администрирования. Вероятность реализации угрозы – маловероятно.

14.12.24. Угрозы удаленного запуска приложений. ИСПДн не имеет подключение к сетям связи общего пользования. Средства межсетевого экранирования, удовлетворяющие требованиям нормативных документов Федеральной службы по техническому и экспортному контролю, в наличии. У пользователей ИСПДн имеются учетные записи без прав администрирования. Вероятность реализации угрозы – маловероятно.

14.12.25. Угрозы внедрения по сети вредоносных программ. На серверах и АРМ пользователей установлено средство антивирусной защиты Kaspersky Endpoint Security. Производится регулярное обновление антивирусных баз. Вероятность реализации угрозы – маловероятно.

14.12.26. Вторжение в ИСПДн по информационно-телекоммуникационным сетям. ИСПДн имеет подключение к сетям связи общего поль-

зования. Средства межсетевого экранирования, удовлетворяющие требованиям нормативных документов Федеральной службы по техническому и экспортному контролю, отсутствуют. Вероятность реализации угрозы – средняя.

14.12.27. Искажение в каналах передачи. Передача данных производится по оптико-волоконным линиям связи, при передаче используется избыточное кодирование информации. Вероятность реализации угрозы – маловероятно.

15. Угрозы стихийного характера

15.1.Нарушение электроснабжения

15.1.1. Внешнего. Серверное и коммутационное оборудование ИСПДн подключено к системе источников бесперебойного питания. Производится регулярное резервное копирование защищаемой информации. Вероятность реализации угрозы – маловероятно.

15.1.2. Объектового. Серверное и коммутационное оборудование ИСПДн подключено к системе источников бесперебойного питания. Производится регулярное резервное копирование защищаемой информации. Вероятность реализации угрозы – маловероятно.

15.2.Стихийное бедствие, катастрофа

В связи с географическим расположением оператора, отсутствуют объективные предпосылки для осуществления угрозы. Вероятность реализации угрозы – маловероятно.

№ п/п	**Угроза**	**Вероятность реализации угрозы (Y2)**	**Коэффициент реализуемости угрозы Y. Возможность реализации угрозы**	
1.	**Утечки по техническим каналам**			
1.1.	Утечка акустической информации	маловероятно (0)	низкая	0,25
1.2.	Утечка видовой информации			
1.2.1.	со средств отображения индивидуального пользователя	маловероятно (0)	низкая	0,25
1.2.2.	со средств коллективного отображения	маловероятно (0)	низкая	0,25
1.2.3.	с печатных документов	маловероятно (0)	низкая	0,25
1.3.	Утечка информации за счет побочных электромагнитных излучений информативных сигналов от технических средств	маловероятно (0)	низкая	0,25
1.4.	Утечка информации за счет наводок информативного сигнала, обрабатываемого техническими средствами, на цепи элек-	маловероятно (0)	низкая	0,25

	тропитания и линии связи, выходящие за пределы контролируемой зоны			
1.5.	Утечка информации за счет радиоизлучений или электрических сигналов от электронных устройств перехвата информации, подключенных к каналам связи или техническим средствам обработки информации	средняя (5)	средняя	0,5
2.	**Несанкционированный доступ к информации**			
2.1.	Угрозы уничтожения, хищения, модификации технических средств ИСПДн, носителей информации путем физического доступа к элементам ИСПДн:			
2.1.1.	кража персональных электронно-вычислительных машин (далее ПЭВМ)	маловероятно (0)	низкая	0,25
2.1.2.	кража носителей информации	средняя (5)	средняя	0,5
2.1.3.	кража ключей и атрибутов доступа	маловероятно (0)	низкая	0,25
2.1.4.	нарушение функционирования телекоммуникационных каналов, технических средств ИСПДн	маловероятно (0)	низкая	0,25
2.1.5.	внедрение аппаратных закладок в технические средства ИСПДн	средняя (5)	средняя	0,5
2.1.6.	несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) технических средств ИСПДн	маловероятно (0)	низкая	0,25
2.2.	Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий):			
2.2.1.	воздействие вредоносных программ	маловероятно (0)	низкая	0,25
2.2.2.	недекларированные возможности общесистемного и прикладного програмного обеспечения (далее - ПО)	маловероятно (0)	низкая	0,25
2.2.3.	ошибки в общесистемном и прикладном ПО	маловероятно (0)	низкая	0,25

2.2.4.	установка ПО не связанного с исполнением служебных обязанностей	маловероятно (0)	низкая	0,25
2.3.	Неумышленные деструктивные действия персонала:			
2.3.1.	утрата ключей и атрибутов доступа	маловероятно (0)	низкая	0,25
2.3.2.	непреднамеренная модификация (уничтожение) информации сотрудниками	средняя (5)	средняя	0,5
2.3.3.	непреднамеренное отключение средств защиты	высокая (10)	высокая	0,75
2.3.4.	вывод из строя аппаратно-программных средств вследствие ошибочных действий	средняя (5)	средняя	0,5
2.4.	Умышленные деструктивные действия персонала:			
2.4.1.	произвольное копирование баз данных	средняя (5)	средняя	0,5
2.4.2.	накопление данных пользователем информационной системы	средняя (5)	средняя	0,5
2.4.3.	злонамеренное разрушение (искажение) информации	средняя (5)	средняя	0,5
2.4.4.	злонамеренное блокирование данных	низкая (2)	средняя	0,35
2.4.5.	фальсификация данных	низкая (2)	средняя	0,35
2.4.6.	несанкционированный доступ персонала информационной системы к ресурсам	средняя (5)	средняя	0,5
2.4.7.	компрометация аутентификатора	высокая (10)	высокая	0,75
2.4.8.	компрометация ключа СКЗИ	средняя (5)	средняя	0,5
2.4.9.	нарушение функционирования средства защиты	высокая (10)	низкая	
2.4.10.	произвольное создание точек входа в систему за счет неправомерных действий	маловероятно (0)	низкая	0,25
2.5.	Угрозы несанкционированного доступа по каналам связи:			
2.5.1.	перехват передаваемой информации за переделами контролируемой зоны	маловероятно (0)	низкая	0,25
2.5.2.	перехват в пределах контролируемой зоны внешними нарушителями	маловероятно (0)	низкая	0,25
2.5.3.	перехват в пределах контролируемой	средняя (5)	средняя	0,5

	зоны внутренними нарушителями			
2.5.4.	угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.	низкая (2)	средняя	0,35
2.5.5.	угрозы выявления паролей по сети	маловероятно (0)	низкая	0,25
2.5.6.	угрозы навязывание ложного маршрута сети	маловероятно (0)	низкая	0,25
2.5.7.	угрозы подмены доверенного объекта в сети	маловероятно (0)	низкая	0,25
2.5.8.	угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях	средняя (5)	средняя	0,5
2.5.9.	угрозы типа «Отказ в обслуживании»	средняя (5)	средняя	0,5
2.5.10.	угрозы удаленного запуска приложений	средняя (5)	средняя	0,5
2.5.11.	угрозы внедрения по сети вредоносных программ	маловероятно (0)	низкая	0,25
2.5.12.	вторжение в ИСПДн по информационно-телекоммуникационным сетям	средняя (5)	средняя	0,5
2.5.13.	искажение в каналах передачи	маловероятно (0)	низкая	0,25
3.	Угрозы стихийного характера			
3.1.1.	Нарушение электроснабжения:			
3.1.2.	внешнего	маловероятно (0)	низкая	0,25
3.1.3.	объектового	маловероятно (0)	низкая	0,25
3.2.	Стихийное, бедствие, катастрофа	маловероятно (0)	низкая	0,25

16. Определение опасности угроз безопасности персональных данных

Определение опасности угроз безопасности ПДн проведено экспертным методом на основе опроса экспертов (специалистов в области защиты информации) с учетом результатов обследования ИСПДн. Результаты определения опасности угроз с мнениями экспертов приведены ниже:

№ п/п	**Угроза**	**Показатель опасности угрозы**

1.	**Утечки по техническим каналам**	
1.1.	Утечка акустической информации	средняя
1.2.	Утечка видовой информации:	
1.2.1.	со средств отображения индивидуального пользователя	средняя
1.2.2.	со средств коллективного отображения	средняя
1.2.3.	с печатных документов	средняя
1.3.	Утечка информации за счет побочных электромагнитных излучений информативных сигналов от технических средств	средняя
1.4.	Утечка информации за счет наводок информативного сигнала, обрабатываемого техническими средствами, на цепи электропитания и линии связи, выходящие за пределы контролируемой зоны	средняя
1.5.	Утечка информации за счет радиоизлучений или электрических сигналов от электронных устройств перехвата информации, подключенных к каналам связи или техническим средствам обработки информации	средняя
2.	**Несанкционированный доступ к информации**	
2.1.	Угрозы уничтожения, хищения, модификации технических средств ИСПДн, носителей информации путем физического доступа к элементам ИСПДн:	
2.1.1.	кража персональных электронно-вычислительных машин (далее ПЭВМ)	средняя
2.1.2.	кража носителей информации	высокая
2.1.3.	кража ключей и атрибутов доступа	средняя
2.1.4.	нарушение функционирования телекоммуникационных каналов, технических средств ИСПДн	низкая
2.1.5.	внедрение аппаратных закладок в технические средства ИСПДн	средняя
2.1.6.	несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) технических средств ИСПДн	средняя
2.2.	Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий):	
2.2.1.	воздействие вредоносных программ	средняя
2.2.2.	недекларированные возможности общесистемного и прикладного програмного обеспечения (далее - ПО)	средняя
2.2.3.	ошибки в общесистемном и прикладном ПО	средняя
2.2.4.	установка ПО не связанного с исполнением служебных обязанностей	средняя
2.3.	Неумышленные деструктивные действия персонала:	

2.3.1.	утрата ключей и атрибутов доступа	средняя
2.3.2.	непреднамеренная модификация (уничтожение) информации сотрудниками	средняя
2.3.3.	непреднамеренное отключение средств защиты	средняя
2.3.4.	вывод из строя аппаратно-программных средств вследствие ошибочных действий	средняя
2.4.	Умышленные деструктивные действия персонала:	
2.4.1.	произвольное копирование баз данных	низкая
2.4.2.	накопление данных пользователем информационной системы	высокая
2.4.3.	злонамеренное разрушение (искажение) информации	средняя
2.4.4.	злонамеренное блокирование данных	средняя
2.4.5.	фальсификация данных	средняя
2.4.6.	несанкционированный доступ персонала информационной системы к ресурсам	средняя
2.4.7.	компрометация аутентификатора	средняя
2.4.8.	компрометация ключа СКЗИ	высокая
2.4.9.	нарушение функционирования средства защиты	средняя
2.4.10.	произвольное создание точек входа в систему за счет неправомерных действий	средняя
2.5.	Угрозы несанкционированного доступа по каналам связи:	
2.5.1.	перехват передаваемой информации за переделами контролируемой зоны	низкая
2.5.2.	перехват в пределах контролируемой зоны внешними нарушителями	средняя
2.5.3.	перехват в пределах контролируемой зоны внутренними нарушителями	высокая
2.5.4.	угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.	средняя
2.5.5.	угрозы выявления паролей по сети	средняя
2.5.6.	угрозы навязывание ложного маршрута сети	средняя
2.5.7.	угрозы подмены доверенного объекта в сети	средняя
2.5.8.	угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях	средняя
2.5.9.	угрозы типа «Отказ в обслуживании»	средняя
2.5.10.	угрозы удаленного запуска приложений	средняя
2.5.11.	угрозы внедрения по сети вредоносных программ	средняя

2.5.12.	вторжение в ИСПДн по информационно-телекоммуникационным сетям	высокая
2.5.13.	искажение в каналах передачи	средняя
3.	**Угрозы стихийного характера**	
3.1.	Нарушение электроснабжения:	
3.1.1.	внешнего	средняя
3.1.2.	объектового	средняя
3.2.	Стихийное, бедствие, катастрофа	средняя

17. Определение актуальности угроз безопасности ПДн

Актуальность угрозы в соответствии с Методикой определения актуальных угроз безопасности ПДн при их обработке в информационных системах ПДн определяется с учетом оценок вероятности ее реализации и опасности. Результаты приведены ниже.

№ п/п	Форма реализации угрозы	Интерпретация реализуемости угрозы	Опасность угрозы	Актуальность угрозы
1.	**Утечки по техническим каналам**			
1.1.	Утечка акустической информации	низкая	средняя	неактуальная
1.2.	Утечка видовой информации:			
1	со средств отображения индивидуального пользователя	низкая	средняя	неактуальная
1	со средств коллективного отображения	низкая	средняя	неактуальная
1	с печатных документов	низкая	средняя	неактуальная
1.3.	Утечка информации за счет побочных электромагнитных излучений информативных сигналов от технических средств	низкая	средняя	неактуальная
1.4.	Утечка информации за счет наводок информативного сигнала, обрабатываемого техническими средствами, на цепи электропитания и линии связи, выходящие за пределы контролируемой зоны	низкая	средняя	неактуальная

1.5.	Утечка информации за счет радиоизлучений или электрических сигналов от электронных устройств перехвата информации, подключенных к каналам связи или техническим средствам обработки информации	низкая	средняя	актуальная
2.	**Несанкционированный доступ к информации**			
2.1.	Угрозы уничтожения, хищения, модификации технических средств ИСПДн, носителей информации путем физического доступа к элементам ИСПДн:			
2.1.1.	кража персональных электронно-вычислительных машин (далее ПЭВМ)	низкая	средняя	неактуальная
2.1.2	кража носителей информации	средняя	средняя	актуальная
2.1.3.	кража ключей и атрибутов доступа	низкая	средняя	неактуальная
2.1.4.	нарушение функционирования телекоммуникационных каналов, технических средств ИСПДн	низкая	средняя	неактуальная
2.1.5.	внедрение аппаратных закладок в технические средства ИСПДн	средняя	средняя	неактуальная
2.1.6.	несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) технических средств ИСПДн	низкая	средняя	неактуальная
2.2.	Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий):			
2.2.1.	воздействие вредоносных программ	низкая	средняя	неактуальная
2.2.2.	недекларированные возможности общесистем-	низкая	средняя	неактуальная

	ного и прикладного программного обеспечения (далее - ПО)			
2.2.3.	ошибки в общесистемном и прикладном ПО	низкая	средняя	неактуальная
2.2.4.	установка ПО не связанного с исполнением служебных обязанностей	средняя	высокая	актуальная
2.3.	Неумышленные деструктивные действия персонала:			
2.3.1.	утрата ключей и атрибутов доступа	низкая	средняя	неактуальная
2.3.2.	непреднамеренная модификация (уничтожение) информации сотрудниками	средняя	средняя	актуальная
2.3.3.	непреднамеренное отключение средств защиты	средняя	средняя	актуальная
2.3.4.	вывод из строя аппаратно-программных средств вследствие ошибочных действий	средняя	средняя	актуальная
2.4.	Умышленные деструктивные действия персонала:			
2.4.1.	произвольное копирование баз данных	низкая	высокая	актуальная
2.4.2.	накопление данных пользователем информационной системы	средняя	высокая	актуальная
2.4.3.	злонамеренное разрушение (искажение) информации	средняя	высокая	актуальная
2.4.4.	злонамеренное блокирование данных	низкая	средняя	актуальная
2.4.5.	фальсификация данных	средняя	высокая	актуальная
2.4.6.	несанкционированный доступ персонала информационной системы к ресурсам	средняя	средняя	актуальная
2.4.7.	компрометация аутентификатора	высокая	средняя	актуальная
2.4.8.	компрометация ключа СКЗИ	средняя	высокая	актуальная
2.4.9.	нарушение функционирования	низкая	средняя	актуальная

	средства защиты			
2.4.10.	произвольное создание точек входа в систему за счет неправомерных действий	низкая	средняя	неактуальная
2.5.	Угрозы несанкционированного доступа по каналам связи:			
2.5.1.	перехват передаваемой информации за пределами контролируемой зоны	низкая	низкая	неактуальная
2.5.2.	перехват в пределах контролируемой зоны внешними нарушителями	низкая	средняя	неактуальная
2.5.3.	перехват в пределах контролируемой зоны внутренними нарушителями	средняя	высокая	актуальная
2.5.4.	угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.	средняя	средняя	актуальная
2.5.5.	угрозы выявления паролей по сети	средняя	средняя	актуальная
2.5.6.	угрозы навязывание ложного маршрута сети	средняя	средняя	актуальная
2.5.7.	угрозы подмены доверенного объекта в сети	средняя	средняя	актуальная
2.5.8.	угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях	средняя	средняя	актуальная
2.5.9.	угрозы типа «Отказ в обслуживании»	средняя	средняя	актуальная
2.5.10.	угрозы удаленного запуска приложений	средняя	средняя	актуальная

2.5.11.	угрозы внедрения по сети вредоносных программ	низкая	средняя	актуальная
2.5.12.	вторжение в ИСПДн по информационно-телекоммуникационным сетям	средняя	высокая	актуальная
2.5.13.	искажение в каналах передачи	низкая	средняя	неактуальная
3.	**Угрозы стихийного характера**			
3.1.	Нарушение электроснабжения:			
3.1.1.	внешнего	низкая	средняя	неактуальная
3.1.2.	объектового	низкая	средняя	неактуальная
3.2.	Стихийное, бедствие, катастрофа	низкая	средняя	неактуальная

18. Заключительные положения

18.1. В отношении персональных данных, обрабатываемых в ИСПДн, актуальными являются следующие угрозы безопасности:

- утечка информации за счет радиоизлучений или электрических сигналов от электронных устройств перехвата информации, подключенных к каналам связи или техническим средствам обработки информации;
- кража носителей информации;
- внедрение аппаратных закладок в технические средства ИСПДн;
-непреднамеренная модификация (уничтожение) информации сотрудниками;
-непреднамеренное отключение средств защиты;
-вывод из строя аппаратно-программных средств вследствие ошибочных действий;
-накопление данных пользователем информационной системы;
-злонамеренное блокирование данных;
-фальсификация данных;
-несанкционированный доступ персонала ИС к ресурсам;
-компрометация аутентификатора;
-компрометация ключа СКЗИ;
-нарушение функционирования средства защиты;
-перехват в пределах контролируемой зоны внутренними нарушителями;
-угрозы сканирования, направленные на выявление типа или типов используемых, операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.;
-угрозы выявления паролей по сети;
-угрозы навязывание ложного маршрута сети;
-угрозы подмены доверенного объекта в сети;

-угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях;

-угрозы типа «Отказ в обслуживании»;

-угрозы удаленного запуска приложений;

-вторжение в ИСПДн по информационно-телекоммуникационным сетям.