ПРАВИТЕЛЬСТВО КУРГАНСКОЙ ОБЛАСТИ

ДЕПАРТАМЕНТ ЗДРАВООХРАНЕНИЯ КУРГАНСКОЙ ОБЛАСТИ

ПРИКАЗ

от 30 мая 2018 года № 632

г. Курган

Об утверждении перечня угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных в Департаменте здравоохранения Курганской области и подведомственных ему учреждениях, организациях

В соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказом Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 года № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» ПРИКАЗЫВАЮ:

1. Утвердить перечень угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных в Департаменте здравоохранения Курганской области и подведомственных ему учреждениях, организациях согласно приложению к настоящему приказу.

2. Опубликовать настоящий приказ в установленном порядке.

3. Контроль за выполнением настоящего приказа возложить заместителя директора Департамента здравоохранения Курганской области – начальника управления финансового и материально-технического обеспечения Департамента здравоохранения Курганской области.

Директор Департамента здравоохранения Курганской области Л.И. Кокорина

Петровская Е.В.
(3522) 49-84-85

Приложение к приказу
Департамента здравоохранения
Курганской области
от 30 мая 2018 года № 632
«Об утверждении перечня угроз
безопасности персональных данных,
актуальных при обработке
персональных данных в
информационных системах
персональных данных в Департаменте
здравоохранения Курганской области и
подведомственных ему учреждениях,
организациях»

Перечень угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных в Департаменте здравоохранения Курганской области и подведомственных ему учреждениях, организациях

1. Общие положения

1.1. Перечень угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных (далее – ИСПДн) в Департаменте здравоохранения Курганской области (далее соответственно – Департамент, Перечень актуальных угроз безопасности персональных данных) и подведомственных ему учреждениях, организациях разработан в соответствии с частью 5 статьи 19 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» (далее – Федеральный закон «О персональных данных»).

Перечень актуальных угроз безопасности персональных данных необходимо учитывать при разработке частной модели угроз безопасности персональных данных (далее соответственно – частная модель угроз, ПДн) и других документов Департамента и подведомственных ему учреждений, организаций.

1.2. В частной модели угроз указываются:

описание ИСПДн и их структурно-функциональных характеристик;

описание угроз безопасности информации, включающее описание возможностей нарушителя (модель нарушителя), возможных уязвимостей информационной системы, способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации.

Типовая форма частной модели угроз для Департамента разрабатывается специалистом по защите информации с учетом Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 года № 17.

1.3. Актуальные угрозы безопасности персональных данных, обрабатываемых в ИСПДн, содержащиеся в Перечне актуальных угроз безопасности персональных данных, уточняются и дополняются по мере выявления новых источников угроз, развития способов и средств реализации угроз безопасности персональных данных в ИСПДн. Указанные изменения согласовываются с Федеральной службой по

техническому и экспортному контролю (далее – ФСТЭК России) и Федеральной службой безопасности Российской Федерации (далее – ФСБ) в установленном порядке.

1.4. В Департаменте создаются и эксплуатируются однотипные и разноплановые информационные системы (далее – ИС), в которых могут обрабатываться ПДн. В зависимости от предназначения ИСПДн подразделяются на:

1.4.1. ИСПДн обеспечения типовой деятельности Департамента, предназначенные для автоматизации обеспечивающей деятельности Департамента в рамках исполнения им типовых полномочий, предусмотренных нормативными правовыми актами.

К ИСПДн обеспечения типовой деятельности Департамента относятся:

– ИСПДн управления персоналом (учет кадров);

– ИСПДн управления финансами (расчет заработной платы);

1.4.2. ИСПДн обеспечения специальной деятельности Департамента, предназначенные для автоматизации или информационной поддержки предоставления услуг, предусмотренных правовыми актами в Департаменте в качестве полномочий конкретного органа исполнительной власти.

К ИСПДн обеспечения специальной деятельности относятся:

– «Системы мониторинга реализации государственного задания по оказанию высокотехнологичной медицинской помощи за счет средств федерального бюджета»;

– «Подсистемы мониторинга проведения диспансеризации детей-сирот, находящихся в трудной жизненной ситуации»;

– «Подсистемы мониторинга санаторно-курортного лечения»;

– ИСПДн по направлениям Департамента, предназначенные для предоставления государственных услуг, исполнения государственных функций (например: для оказания высокотехнологичной медицинской помощи, а также информирование о порядке и условиях оказания высокотехнологичной медицинской помощи).

2. ИСПДн обеспечения типовой деятельности Департамента

2.1. ИСПДн обеспечения типовой деятельности Департамента характеризуются тем, что в качестве объектов информатизации выступают локальные автоматизированные рабочие места (далее – АРМ) или АРМ, подключенные к локальным вычислительным сетям, объединенные в объектовые ИСПДн, имеющие или не имеющие подключения к сетям общего пользования и (или) сетям международного информационного обмена. Ввод ПДн в ИСПДн осуществляется с бумажных носителей. ПДн могут выводиться из ИСПДн в электронном виде или на бумажных носителях.

2.2. Операторами ИСПДн обеспечения типовой деятельности Департамента являются подведомственные ему учреждения, организации. Количество субъектов ПДн не превышает 100 тысяч. ПДн хранятся на учтенных машинных носителях информации (далее – МНИ), в качестве которых используются средства электронно-вычислительной техники.

2.3. ИСПДн управления персоналом в Департаменте предназначены для кадрового учета служащих и работников, управления кадровым резервом и других функций, связанных с управлением персоналом в Департаменте. В ИСПДн управления персоналом обрабатываются ПДн сотрудников Департамента, претендентов на замещение должности государственной гражданской службы Курганской области по конкурсу или включение в кадровый резерв Департамента, претендентов на замещение должности руководителя подведомственного Департаменту учреждения, организации.

2.4. ИСПДн управления финансами в Департаменте предназначены для обработки ПДн, необходимых для бухгалтерского и финансового учета, представления информации в пенсионные фонды, налоговые органы, фонды обязательного социального страхования. В ИСПДн управления финансами в Департаменте

обрабатываются следующие ПДн сотрудников Департамента: фамилия, имя, отчество; дата и место рождения; паспортные данные; адрес места жительства; номер телефона, идентификационный номер налогоплательщика, страховой номер индивидуального лицевого счета, табельный номер, наименование должности, номер приказа и дата приема на работу (увольнения), номер лицевого счета для перечисления денежного содержания и иных выплат работнику.

2.5. В ИСПДн обеспечения типовой деятельности Департамента применяются следующие меры по защите ПДн и средств криптографической защиты информации (далее – СКЗИ):

– утверждение правил доступа в помещения, где располагаются АРМ, на которых осуществляется обработка ПДн, СКЗИ, в рабочее и нерабочее время, а также в нештатных ситуациях;

– утверждение перечня лиц, имеющих право доступа в помещения, где располагаются АРМ, СКЗИ;

– обеспечение доступа в контролируемую зону (далее – КЗ), где располагается АРМ, СКЗИ, в соответствии с контрольно-пропускным режимом;

– при работе в помещениях, где расположены АРМ, СКЗИ, нахождение в этих помещениях представителей технических, обслуживающих и других вспомогательных служб, а также сотрудников, не являющихся пользователями СКЗИ, только в присутствии уполномоченных сотрудников Департамента;

– информирование сотрудников, являющихся пользователями ИСПДн, но не являющихся пользователями СКЗИ, о правилах работы в ИСПДн и ответственности за несоблюдение правил обеспечения безопасности информации;

– информирование пользователей СКЗИ о правилах работы в ИСПДн, правилах работы с СКЗИ и ответственности за несоблюдение правил обеспечения безопасности информации;

– оснащение помещений, в которых располагаются СКЗИ, входными дверьми с замками, обеспечение постоянного закрытия дверей помещений на замок и их открытия только для санкционированного прохода;

– осуществление разграничения и контроля доступа пользователей к защищаемым ресурсам;

– осуществление регистрации и учета действий пользователей с ПДн;

– осуществление контроля целостности средств защиты;

– использование на АРМ и серверах, на которых установлены сертифицированные СКЗИ, сертифицированных средств защиты информации от несанкционированного доступа, сертифицированных средств антивирусной защиты.

2.6. ИСПДн управления персоналом в Департаменте могут взаимодействовать с ИСПДн управления финансами в Департаменте.

3. ИСПДн обеспечения специальной деятельности

3.1. ИСПДн обеспечения специальной деятельности Департамента характеризуются тем, что в качестве объектов информатизации выступают локальные или распределенные ИС регионального масштаба, подключенные к сетям общего пользования и (или) сетям международного информационного обмена. Ввод ПДн в ИСПДн осуществляется с бумажных носителей или с электронных носителей информации. ПДн субъектов ПДн обрабатываются с целью предоставления государственных услуг, исполнения функций Департамента и могут выводиться из ИСПДн в электронном виде или на бумажных носителях.

3.2. Операторами ИСПДн обеспечения специальной деятельности Департамента являются подведомственные Департаменту учреждения, организации. Количество субъектов ПДн не превышает 100 тысяч. ПДн хранятся на учтенных МНИ, в качестве

которых используются средства электронно-вычислительной техники.

3.3. В ИСПДн обеспечения специальной деятельности Департамента обрабатываются ПДн, представляемые заявителями при обращении за получением государственных услуг, сведения, получаемые из ИС Департамента, используемые для подготовки ответов на запросы в соответствии с административными регламентами предоставления государственных услуг, утвержденными нормативными правовыми актами Департамента и Правительства Курганской области.

3.4. ИСПДн по направлениям деятельности Департамента предназначены для обеспечения деятельности Департамента и исполнения функций, не отраженных в пункте 3.3. настоящего Перечня актуальных угроз. В ИСПДн обрабатываются ПДн субъектов ПДн, необходимые для исполнения функций, определенных в правовых актах Департамента.

3.5. ИСПДн электронного документооборота предназначены для автоматизации делопроизводства, служебной переписки, архивной деятельности, учета корреспонденции, обращений граждан, обеспечения доступа работников Департамента к электронным документам в ИСПДн. В ИСПДн обрабатываются: фамилия, имя, отчество, наименование должности работников, информация о ПДн граждан, имеющаяся в документах.

3.6. Информационный обмен по сетям связи общего пользования и (или) сетям международного информационного обмена осуществляется с использованием сертифицированных ФСТЭК России СКЗИ. Контролируемой зоной ИСПДн являются служебные здания Департамента или отдельные помещения в этих зданиях. В пределах КЗ находятся АРМ пользователей, серверы ИСПДн, телекоммуникационное оборудование и аппаратные средства защиты информации. Вне КЗ находятся линии передачи данных и телекоммуникационное оборудование операторов связи, используемое для информационного обмена по сетям связи общего пользования и (или) сетям международного информационного обмена.

3.7. В ИСПДн обеспечения специальной деятельности применяются следующие меры по защите ПДн и СКЗИ:

– утверждение правил доступа в помещения, где располагаются АРМ, на которых осуществляется обработка ПДн, СКЗИ, в рабочее и нерабочее время, а также в нештатных ситуациях;

– утверждение перечня лиц, имеющих право доступа в помещения, где располагаются АРМ, СКЗИ;

– обеспечение доступа в КЗ, где располагается АРМ, СКЗИ, в соответствии с контрольно-пропускным режимом;

– при работе в помещениях, где расположены АРМ, СКЗИ, нахождение в этих помещениях представителей технических, обслуживающих и других вспомогательных служб, а также сотрудников, не являющихся пользователями СКЗИ, только в присутствии уполномоченных сотрудников органа исполнительной власти;

– информирование сотрудников, являющихся пользователями ИСПДн, но не являющихся пользователями СКЗИ, о правилах работы в ИСПДн и ответственности за несоблюдение правил обеспечения безопасности информации;

– информирование пользователей СКЗИ о правилах работы в ИСПДн, правилах работы с СКЗИ и ответственности за несоблюдение правил обеспечения безопасности информации;

– оснащение помещений, в которых располагаются СКЗИ, входными дверьми с замками, обеспечение постоянного закрытия дверей помещений на замок и их открытия только для санкционированного прохода;

– осуществление разграничения и контроля доступа пользователей к защищаемым ресурсам;

– осуществление регистрации и учета действий пользователей с ПДн;

– осуществление контроля целостности средств защиты;

– использование на АРМ и серверах, на которых установлены сертифицированные СКЗИ, сертифицированных средств защиты информации от несанкционированного доступа, сертифицированных средств антивирусной защиты.

3.8. Осуществляется информационное взаимодействие между ИСПДн и подсистемами: «Подсистемы мониторинга санаторно-курортного лечения», «Подсистемы мониторинга проведения диспансеризации детей-сирот, находящихся в трудной жизненной ситуации», «Системы мониторинга реализации государственного задания по оказанию высокотехнологичной медицинской помощи за счет средств федерального бюджета» и ИСПДн по направлениям деятельности Департамента, предназначенные для предоставления государственных услуг, исполнения государственных функций.

4. Объекты защиты ИСПДн, классификация и характеристики нарушителей

4.1. В системе защиты информации ИСПДн к объектам защиты относятся:

Объект 1 - персональные данные;

Объект 2 - СКЗИ;

Объект 3 - среда функционирования СКЗИ (далее – СФ);

Объект 4 - информация, относящаяся к криптографической защите ПДн, включая ключевую, парольную и аутентифицирующую информацию СКЗИ;

Объект 5 - документы, дела, журналы, картотеки, издания, технические документы, видео-, кино- и фотоматериалы, рабочие материалы и т.п., в которых отражена защищаемая информация, относящаяся к ИСПДн;

Объект 6 - носители защищаемой информации, используемые в ИС в процессе криптографической защиты ПДн, носители ключевой, парольной и аутентифицирующей информации СКЗИ и порядок доступа к ним;

Объект 7 - используемые информационной системой каналы (линии) связи, включая кабельные системы;

Объект 8 - помещения, в которых находятся ресурсы ИС, имеющие отношение к криптографической защите ПДн.

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

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

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

4.3. Внешними нарушителями могут быть разведывательные службы государств; криминальные структуры; физические лица.

4.4. Внешний нарушитель имеет возможность осуществлять: несанкционированный доступ к каналам связи, выходящим за пределы служебных помещений;

– несанкционированный доступ через АРМ, подключенные к сетям связи общего пользования и (или) сетям международного информационного обмена;

– несанкционированный доступ к информации с использованием специальных программных воздействий посредством программных вирусов, вредоносных программ, алгоритмических или программных закладок;

– несанкционированный доступ через элементы информационной инфраструктуры ИСПДн, которые в процессе своего жизненного цикла (модернизации, ремонта) оказываются за пределами контролируемой зоны;

– несанкционированный доступ через ИС взаимодействующих ведомств,

подведомственных Департаменту учреждений, организаций при их подключении к ИСПДн.

4.5. Внутренние потенциальные нарушители подразделяются на восемь категорий в зависимости от способа доступа и полномочий доступа к ПДн.

4.5.1. К первой категории относятся лица, имеющие санкционированный доступ к ИСПДн, но не имеющие доступа к ПДн. К этому типу нарушителей относятся должностные лица, обеспечивающие нормальное функционирование ИСПДн.

Лицо этой категории может:

– иметь доступ к фрагментам информации, содержащей ПДн и распространяющейся по внутренним каналам связи ИСПДн;

располагать фрагментами информации о топологии ИСПДн 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.

4.5.2. Ко второй категории относятся зарегистрированные пользователи ИСПДн, осуществляющие ограниченный доступ к ресурсам ИСПДн с рабочего места.

Лицо этой категории:

– обладает всеми возможностями лиц первой категории;

– знает, по меньшей мере, одно легальное имя доступа;

– обладает всеми необходимыми атрибутами, обеспечивающими доступ к некоторому подмножеству ПДн;

– располагает конфиденциальными данными, к которым имеет доступ.

4.5.3. К третьей категории относятся зарегистрированные пользователи ИСПДн, осуществляющие удаленный доступ к ПДн по локальным и (или) распределенным ИС.

Лицо этой категории:

– обладает всеми возможностями лиц первой и второй категорий;

– располагает информацией о топологии ИСПДн на базе локальной и (или) распределенной ИС, через которую осуществляется доступ, и о составе технических средств защиты ИСПДн;

– имеет возможность физического доступа к фрагментам технических средств защиты ИСПДн.

4.5.4. К четвертой категории относятся зарегистрированные пользователи ИСПДн с полномочиями администратора безопасности сегмента ИСПДн.

Лицо этой категории:

– обладает всеми возможностями лиц предыдущих категорий;

– обладает полной информацией о системном и прикладном программном обеспечении, используемом в сегменте 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 ИСПДн;

– имеет доступ ко всем техническим средствам сегмента ИСПДн;

– обладает правами конфигурирования и административной настройки некоторого подмножества технических средств сегмента ИСПДн.

4.5.5. К пятой категории относятся зарегистрированные пользователи с полномочиями системного администратора ИСПДн.

Лицо этой категории:

– 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.

4.5.6. К шестой категории относятся зарегистрированные пользователи с полномочиями администратора безопасности ИСПДн.

Лицо этой категории:

– 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).

4.5.7. К седьмой категории относятся программисты-разработчики прикладного программного обеспечения и лица, обеспечивающие его сопровождение на защищаемом объекте.

Лицо этой категории:

– обладает информацией об алгоритмах и программах обработки информации на ИСПДн;

– обладает возможностями внесения ошибок, недекларированных возможностей, программных закладок, вредоносных программ в программное обеспечение (далее – ПО) 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.

4.5.8. К восьмой категории относятся разработчики и лица, обеспечивающие поставку, сопровождение и ремонт технических средств на ИСПДн.

Лицо этой категории:

– 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.

4.6. Актуальность каждой категории нарушителей и возможность или невозможность доступа к объектам защиты определяется в соответствии с таблицей 1.

Таблица 1

	I категория нарушителей	II категория нарушителей	III категория нарушителей	IV категория нарушителей	V категория нарушителей	VI категория нарушителей	VII категория нарушителей	VIII категория нарушителей
Объект 1	нет доступа	есть доступ	есть доступ	есть доступ	есть доступ	нет доступа	нет доступа	нет доступа
Объект 2	есть доступ	есть доступ	есть доступ	есть доступ	есть доступ	есть доступ	нет доступа	есть доступ
Объект 3	есть доступ	есть доступ	есть доступ	есть доступ	есть доступ	есть доступ	нет доступа	есть доступ
Объект 4	есть доступ	есть доступ	есть доступ	есть доступ	есть доступ	есть доступ	нет доступа	нет доступа

	I категория наруши-телей	II категория наруши-телей	III катего-рия нару-ши-телей	IV катего-рия наруши-телей	V катего-рия наруши-телей	VI катего-рия наруши-телей	VII катего-рия наруши-телей	VIII катего-рия наруши-телей
Объект 5	есть доступ	нет доступа	нет доступа	нет доступа	нет доступа	есть доступ	нет доступа	нет доступа
Объект 6	есть доступ	нет доступа	нет доступа	есть доступ	есть доступ	есть доступ	нет доступа	нет доступа
Объект 7	есть доступ	нет доступа	есть доступ	есть доступ	есть доступ	есть доступ	нет доступа	нет доступа
Объект 8	есть доступ	есть доступ	есть доступ	есть доступ	есть доступ	есть доступ	нет доступа	есть доступ

4.7. Источники атак на объекты ИСПДн располагают обобщенными возможностями в соответствии с таблицей 2.

Таблица 2

№ п/п	Обобщенные возможности источников атак	Да/Нет
1.	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак только за пределами КЗ	Да
2.	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах КЗ, но без физического доступа к аппаратным средствам (далее – АС), на которых реализованы СКЗИ и среда их функционирования	Да
3.	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах КЗ, с физическим доступом к АС, на которых реализованы СКЗИ и среда их функционирования	Нет
4.	Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области анализа сигналов линейной передачи и сигналов побочного электромагнитного излучения и наводок СКЗИ)	Нет
5.	Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области использования для реализации атак недокументированных возможностей ПО)	Нет
6.	Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области использования для реализации атак недокументированных возможностей аппаратного и программного компонентов среды функционирования СКЗИ)	Нет

4.8. Обоснование угроз обобщенной возможности пункта 2 из таблицы 2 в соответствии с таблицей 3.

Таблица 3

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
1.1	проведение атаки при нахождении в пределах контролируемой зоны.	актуально	
1.2	проведение атак на этапе эксплуатации СКЗИ на следующие объекты: - документацию на СКЗИ и компоненты СФ; - помещения, в которых находится совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем (далее – СВТ), на которых реализованы СКЗИ и СФ	не актуально	проводятся работы по подбору персонала; доступ в контролируемую зону, где располагается СКЗИ, обеспечивается в соответствии с контрольно-пропускным режимом; документация на СКЗИ хранится у ответственного за СКЗИ в металлическом сейфе; помещение, в которых располагаются документация на СКЗИ, СКЗИ и компоненты СФ, оснащены входными дверьми с замками, обеспечение постоянного закрытия дверей помещений на замок и их открытия только для санкционированного прохода; утвержден перечень лиц, имеющих право доступа в помещения
1.3	получение в рамках предоставленных полномочий, а также в результате наблюдений следующей информации: - сведений о физических мерах защиты объектов, в которых размещены ресурсы информационной системы; - сведений о мерах по обеспечению контролируемой зоны объектов, в которых размещены ресурсы информационной системы; - сведений о мерах по разграничению доступа в Помещения, в которых находятся СВТ, на которых реализованы СКЗИ и СФ	не актуально	проводятся работы по подбору персонала; доступ в контролируемую зону и помещения, где располагается ресурсы ИСПДн, обеспечивается в соответствии с контрольно-пропускным режимом; сведения о физических мерах защиты объектов, в которых размещены ИСПДн, доступны ограниченному кругу сотрудников; сотрудники проинформированы об ответственности за несоблюдение правил обеспечения безопасности информации
1.4	использование штатных средств ИСПДн, ограниченное	не актуально	проводятся работы по подбору персонала;

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий		помещения, в которых располагаются СВТ, на которых располагаются СКЗИ и СФ, оснащены входными дверьми с замками, обеспечивается постоянное закрытие дверей помещений на замок и их открытие только для санкционированного прохода; сотрудники проинформированы об ответственности за несоблюдение правил обеспечения безопасности информации; осуществляется разграничение и контроль доступа пользователей к защищаемым ресурсам; осуществляется регистрация и учет действий пользователей; в ИСПДн используются: сертифицированные средства защиты информации от несанкционированного доступа; сертифицированные средства антивирусной защиты
2.1	физический доступ к СВТ, на которых реализованы СКЗИ и СФ	не актуально	проводятся работы по подбору персонала; доступ в контролируемую зону и помещения, где располагается СВТ, на которых реализованы СКЗИ и СФ, обеспечивается в соответствии с контрольно-пропускным режимом; помещения, в которых располагаются СВТ, на которых располагаются СКЗИ и СФ, оснащены входными дверьми с замками, обеспечивается постоянное закрытие дверей помещений на замок и их открытие только

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
			для санкционированного прохода
2.2	возможность воздействовать на аппаратные компоненты СКЗИ и СФ, ограниченная мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий	не актуально	проводятся работы по подбору персонала; доступ в контролируемую зону и помещения, где располагается СВТ, на которых реализованы СКЗИ и СФ, обеспечивается в соответствии с контрольно-пропускным режимом; помещения, в которых располагаются СКЗИ и СФ, оснащены входными дверьми с замками, обеспечивается постоянное закрытие дверей помещений на замок и их открытие только для санкционированного прохода; представители технических, обслуживающих и других вспомогательных служб при работе в помещениях (стойках), где расположены компоненты СКЗИ и СФ, и сотрудники, не являющиеся пользователями СКЗИ, находятся в этих помещениях только в присутствии сотрудников по эксплуатации
3.1	создание способов, подготовка и проведение атак с привлечением специалистов в области анализа сигналов, сопровождающих функционирование СКЗИ и СФ, и в области использования для реализации атак недокументированных (недекларированных) возможностей прикладного ПО	не актуально	не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности; высокая стоимость и сложность подготовки реализации возможности; проводятся работы по подбору персонала; доступ в контролируемую зону и помещения, где располагается СВТ, на которых реализованы СКЗИ и СФ, обеспечивается в

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
			соответствии с контрольно-пропускным режимом; помещения, в которых располагаются СКЗИ и СФ, оснащены входными дверьми с замками, обеспечивается постоянное закрытие дверей помещений на замок и их открытие только для санкционированного прохода; представители технических, обслуживающих и других вспомогательных служб при работе в помещениях (стойках), где расположены компоненты СКЗИ и СФ, и сотрудники, не являющиеся пользователями СКЗИ, находятся в этих помещениях только в присутствии сотрудников по эксплуатации; осуществляется разграничение и контроль доступа пользователей к защищаемым ресурсам; осуществляется регистрация и учет действий пользователей; на АРМ и серверах, на которых установлены СКЗИ, используются: сертифицированные средства защиты информации от несанкционированного доступа; используются сертифицированные средства антивирусной защиты
3.2	проведение лабораторных исследований СКЗИ, используемых вне контролируемой зоны, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на	не актуально	не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности; высокая стоимость и сложность подготовки реализации возможности

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	предотвращение и пресечение несанкционированных действий		
3.3	проведение работ по созданию способов и средств атак в научно-исследовательских центрах, специализирующихся в области разработки и анализа СКЗИ и СФ, в том числе с использованием исходных текстов входящего в СФ прикладного ПО, непосредственно использующего вызовы программных функций СКЗИ	не актуально	не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности; высокая стоимость и сложность подготовки реализации возможности
4.1	создание способов, подготовка и проведение атак с привлечением специалистов в области использования для реализации атак недокументированных (недекларированных) возможностей системного ПО	не актуально	не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности; высокая стоимость и сложность подготовки реализации возможности; проводятся работы по подбору персонала; доступ в контролируемую зону и помещения, где располагается СВТ, на которых реализованы СКЗИ и СФ, обеспечивается в соответствии с контрольно-пропускным режимом; помещения, в которых располагаются СКЗИ и СФ, оснащены входными дверьми с замками, обеспечивается постоянное закрытие дверей помещений на замок и их открытие только для

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
			санкционированного прохода; представители технических, обслуживающих и других вспомогательных служб при работе в помещениях (стойках), где расположены компоненты СКЗИ и СФ, и сотрудники, не являющиеся пользователями СКЗИ, находятся в этих помещениях только в присутствии сотрудников по эксплуатации; осуществляется разграничение и контроль доступа пользователей к защищаемым ресурсам; осуществляется регистрация и учет действий пользователей; на АРМ и серверах, на которых установлены СКЗИ: используются сертифицированные средства защиты информации от несанкционированного доступа; используются сертифицированные средства антивирусной защиты
4.2	возможность располагать сведениями, содержащимися в конструкторской документации на аппаратные и программные компоненты СФ	не актуально	не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности
4.3	возможность воздействовать на любые компоненты СКЗИ и СФ	не актуально	не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности

5. Актуальные угрозы безопасности

5.1. Учитывая особенности обработки ПДн в Департаменте, а также категорию и объем обрабатываемых в ИСПДн ПДн, основными характеристиками безопасности являются конфиденциальность, целостность и доступность.

Конфиденциальность – обязательное для соблюдения оператором или иным получившим доступ к ПДн лицом требование не допускать их распространение без согласия субъекта ПДн или наличия иного законного основания.

Целостность – состояние защищенности информации, характеризуемое способностью автоматизированной системы обеспечивать сохранность и неизменность информации при попытках несанкционированных воздействий на нее в процессе обработки или хранения.

Доступность – состояние информации, при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно.

5.2. Под актуальными угрозами безопасности ПДн понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного доступа к ПДн при их обработке в ИС, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение ПДн, а также иные неправомерные действия.

5.3. Основной целью применения СКЗИ в ИСПДн Департамента является защита ПДн при информационном обмене по сетям связи общего пользования и (или) сетям международного информационного обмена, не защищенным от перехвата нарушителем передаваемой по ним информации или от несанкционированных воздействий на эту информацию.

5.4. В ИСПДн обеспечения типовой и специальной деятельности Департамента не используются отчуждаемые носители защищаемой информации, для которых несанкционированный доступ к хранимой на них информации не может быть исключен без использования криптографических методов и способов.

5.5. Основными видами угроз безопасности ПДн в ИСПДн являются:

а) угрозы, связанные с преднамеренными или непреднамеренными действиями лиц, имеющих доступ к ИСПДн, включая пользователей ИСПДн, реализующих угрозы непосредственно в ИСПДн (внутренний нарушитель);

б) угрозы, связанные с преднамеренными или непреднамеренными действиями лиц, не имеющих доступа к ИСПДн, реализующих угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена (внешний нарушитель);

в) угрозы, возникновение которых напрямую зависит от свойств техники и ПО, используемого в ИСПДн;

г) угрозы, возникающие в результате внедрения аппаратных закладок и вредоносных программ;

д) угрозы, направленные на нарушение нормальной работы технических средств, используемых в ИСПДн;

5.6. Перечень актуальных и неактуальных угроз безопасности приведен в таблице 4.

Таблица 4

№ п/п	Наименование угрозы безопасности	Актуальность	Обоснования отсутствия актуальности угроз безопасности
1.	Угроза с использованием уязвимости, вызванной недостатками организации технической защиты информации (далее – ТЗИ) от несанкционированного доступа (далее – НСД)		
1.1.	Угроза определения типов объектов защиты	Не актуально	Проведение еженедельных проверок систем защиты в соответствии с Порядком контроля защиты информации в ИСПДн и приостановки предоставления ПДн в случае обнаружения нарушений порядка их предоставления, утвержденным приказом Департамента здравоохранения Курганской области от 15 октября 2017 года № 1067 «Об утверждении Положения об организации и проведении работ в Департаменте здравоохранения Курганской области по обеспечению безопасности персональных данных при их автоматизированной обработке в информационных системах персональных данных (далее соответственно – Порядок контроля защиты информации в ИСПДн, приказ Департамента № 1067)
1.2.	Угроза определения топологии вычислительной сети	Не актуально	Доступ к сети есть только у сотрудников Департамента в соответствии с Матрицей доступа пользователей к персональным данным, обрабатываемым в информационной системе персональных данных «Департамент здравоохранения», утвержденной приказом Департамента № 1067 (далее – Матрица доступа пользователей к персональным данным)
1.3.	Угроза отключения контрольных датчиков	Не актуально	Доступ к созданию учетных записей имеет только администратор сети в соответствии с Порядком управления учетными записями, утвержденным приказом Департамента № 1067
1.4.	Угроза переполнения целочисленных переменных	Не актуально	Нет беспроводных каналов связи

№ п/п	Наименование угрозы безопасности	Актуальность	Обоснования отсутствия актуальности угроз безопасности
1.5.	Угроза доступа к защищаемым файлам с использованием обходного пути	Не актуально	Присутствует проверка пользователя в соответствии с Порядком контроля защиты информации в ИСПДн
1.6.	Угроза несанкционированного использования системных и сетевых утилит	Не актуально	Возможности пользователей ограничены в соответствии с Порядком контроля защиты информации в ИСПДн
1.7.	Угроза несанкционированного воздействия на средство защиты информации	Не актуально	Средства защиты настраиваются на сервере, доступ к которому ограничен в соответствии с Порядком контроля защиты информации в ИСПДн
1.8.	Угроза изменения компонентов системы	Не актуально	Возможности пользователей ограничены в соответствии с Порядком контроля защиты информации в ИСПДн
1.9.	Угроза использования альтернативных путей доступа к ресурсам	Не актуально	Возможности пользователей ограничены в соответствии с Порядком контроля защиты информации в ИСПДн
1.10.	Угроза использования информации идентификации/аутентификации, заданной по умолчанию	Не актуально	Доступ к объекту защиты ограничен
1.11.	Угроза использования механизмов авторизации для повышения привилегий	Не актуально	Возможности пользователей ограничены в соответствии с Порядком контроля защиты информации в ИСПДн
1.12.	Угроза нарушения технологии обработки информации путем несанкционированного внесения изменений в образы виртуальных машин	Не актуально	Отсутствуют виртуальные машины
1.13.	Угроза неконтролируемого роста числа виртуальных машин	Не актуально	Отсутствуют виртуальные машины
1.14.	Угроза неконтролируемого роста числа зарезервированных вычислительных ресурсов	Не актуально	Отсутствуют виртуальные машины
1.15.	Угроза некорректного использования функционала программного обеспечения	Актуально	

№ п/п	Наименование угрозы безопасности	Актуальность	Обоснования отсутствия актуальности угроз безопасности
1.16.	Угроза некорректной реализации политики лицензирования в облаке	Не актуально	Нет облачной инфраструктуры
1.17.	Угроза неопределенности ответственности за обеспечение безопасности облака	Не актуально	Нет облачной инфраструктуры
1.18.	Угроза неправомерного ознакомления с защищаемой информацией	Актуально	
1.19.	Угроза несанкционированного восстановления удаленной защищаемой информации	Актуально	
1.20.	Угроза несанкционированного доступа к аутентификационной информации	Не актуально	Проверка безопасности проводится каждый месяц в соответствии с Порядком контроля защиты информации в ИСПДн
1.21.	Угроза несанкционированного доступа к защищаемым виртуальным машинам из виртуальной и (или) физической сети	Не актуально	Отсутствуют виртуальные машины
1.22.	Угроза несанкционированного доступа к защищаемым виртуальным машинам со стороны других виртуальных машин	Не актуально	Нет виртуальных машин
1.23.	Угроза несанкционированного доступа к защищаемым виртуальным устройствам из виртуальной и (или) физической сети	Не актуально	Нет гипервизора
1.24.	Угроза несанкционированного доступа к сегментам вычислительного поля	Не актуально	Нет суперкомпьютера
1.25.	Угроза несанкционированного доступа к хранимой в виртуальном пространстве защищаемой информации	Актуально	
1.26.	Угроза несанкционированного изменения аутентификационной информации	Не актуально	Проводятся проверки на наличие уязвимостей в соответствии с планом графиком, разработанным на основании Правил осуществления внутреннего контроля соответствия обработки персональных данных, утвержденных приказом Департамента № 1067

№ п/п	Наименование угрозы безопасности	Актуальность	Обоснования отсутствия актуальности угроз безопасности
1.27.	Угроза несанкционированного редактирования реестра	Не актуально	Проводятся проверки контроля доступа в соответствии с Порядком контроля защиты информации в ИСПДн
1.28.	Угроза несанкционированного создания учетной записи пользователя	Не актуально	Учетные записи создает только администратор сети, пользовательские учетные записи ограничены в соответствии с Порядком управления учетными записями, утвержденным приказом Департамента № 1067
1.29.	Угроза несанкционированного удаления защищаемой информации	Не актуально	Доступ в помещения ограничен в соответствии с Матрицей доступа пользователей к персональным данным
1.30.	Угроза несанкционированного удаленного внеполосного доступа к аппаратным средствам	Актуально	
1.31.	Угроза несанкционированного управления буфером	Не актуально	Возможности пользователей ограничены в соответствии с Порядком контроля защиты информации в ИСПДн
1.32.	Угроза несанкционированного управления синхронизацией и состоянием	Актуально	
1.33.	Угроза несанкционированного управления указателями	Не актуально	Проводятся проверки контроля доступа в соответствии с Порядком контроля защиты информации в ИСПДн
1.34.	Угроза несогласованности политик безопасности элементов облачной инфраструктуры	Не актуально	Нет облачной инфраструктуры
1.35.	Угроза несогласованности правил доступа к большим данным	Не актуально	Проводятся проверки контроля доступа в соответствии с Порядком контроля защиты информации в ИСПДн
2.	Угрозы с использованием уязвимости программного обеспечения		
2.1.	Угроза привязки к поставщику облачных услуг	Не актуально	Нет облачной инфраструктуры
2.2.	Угроза наличия механизмов разработчика	Не актуально	Возможности пользователей ограничены в соответствии с Порядком контроля защиты информации в ИСПДн

№ п/п	Наименование угрозы безопасности	Актуальность	Обоснования отсутствия актуальности угроз безопасности
2.3.	Угроза агрегирования данных, обрабатываемых с помощью мобильного устройства	Не актуально	Нет мобильных устройств
2.4.	Угроза использования уязвимых версий программного обеспечения	Актуально	
2.5.	Угроза несанкционированного использования привилегированных функций мобильного устройства	Не актуально	Нет мобильных устройств
3.	Угрозы с использованием уязвимости протоколов сетевого взаимодействия и каналов передачи данных		
3.1.	Угроза обхода некорректно настроенных механизмов аутентификации	Актуально	
3.2.	Угроза общедоступности облачной инфраструктуры	Не актуально	Нет облачной инфраструктуры
3.3.	Угроза деавторизации санкционированного клиента беспроводной сети	Не актуально	Нет беспроводных сетей
3.4.	Угроза перехвата данных, передаваемых по вычислительной сети	Не актуально	Нет грид-системы
3.5.	Угроза перехвата привилегированного потока	Не актуально	Возможности пользователей ограничены в соответствии с Порядком контроля защиты информации в ИСПДн
3.6.	Угроза перехвата привилегированного процесса	Не актуально	Возможности пользователей ограничены в соответствии с Порядком контроля защиты информации в ИСПДн
3.7.	Угроза перехвата управления гипервизором	Не актуально	Нет гипервизора
3.8.	Угроза перехвата управления средой виртуализации	Не актуально	Нет гипервизора
3.9.	Угроза сканирования веб-сервисов, разработанных на основе языка описания WSDL	Не актуально	Нет веб-сервисов, разработанных на основе языка описания WSDL
3.10.	Угроза доступа к локальным файлам сервера при помощи URL	Не актуально	Нет доступа к серверу по URL

№ п/п	Наименование угрозы безопасности	Актуальность	Обоснования отсутствия актуальности угроз безопасности
3.11.	Угроза доступа/перехвата/изменения HTTP cookies	Актуально	
3.12.	Угроза заражения DNS-кэша	Не актуально	Запросы к DNS серверу имеет только администратор, пользовательские учетные записи ограничены в соответствии с Порядком управления учетными записями, утвержденным приказом Департамента № 1067
3.13.	Угроза злоупотребления доверием потребителей облачных услуг	Не актуально	Нет облачной инфраструктуры
3.14.	Угроза искажения XML-схемы	Не актуально	Отсутствует XML-схема
3.15.	Угроза использования слабостей протоколов сетевого/локального обмена данными	Актуально	
3.16.	Угроза конфликта юрисдикций различных стран	Не актуально	Не обрабатываются данные иностранных граждан
3.17.	Угроза межсайтового скриптинга	Не актуально	Установлен антивирус Kaspersky endpoint security 10 с настройками сетевой защиты
3.18.	Угроза межсайтовой подделки запроса	Актуально	
3.19.	Угроза нарушения доступности облачного сервера	Не актуально	Нет облачной инфраструктуры
3.20.	Угроза нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия	Не актуально	Отсутствуют виртуальные машины
3.21.	Угроза незащищенного администрирования облачных услуг	Не актуально	Нет облачной инфраструктуры
3.22.	Угроза некорректного задания структуры данных транзакции	Не актуально	Передача проходит по защищенным каналам. Организована защищенная сеть на основе ПО VipNet.
3.23.	Угроза некорректного использования прозрачного прокси-сервера за счет плагинов браузера	Не актуально	Администратором сети в браузерах пользователей разрешены только сертифицированные расширения и плагины

№ п/п	Наименование угрозы безопасности	Актуальность	Обоснования отсутствия актуальности угроз безопасности
3.24.	Угроза неправомерных действий в каналах связи	Не актуально	Проверки целостности проводятся еженедельно в соответствии с Порядком контроля защиты информации в ИСПДн
3.25.	Угроза несанкционированного доступа к виртуальным каналам передачи	Не актуально	Возможности пользователей ограничены в соответствии с Порядком контроля защиты информации в ИСПДн
3.26.	Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб	Не актуально	Установлено СЗИ в соответствии с Федеральным законом «О персональных данных»
3.27.	Угроза обнаружения хостов	Актуально	
4.	Угрозы с использованием уязвимости ПО		
4.1.	Угроза ошибки обновления гипервизора	Не актуально	Нет гипервизора
4.2.	Угроза перебора всех настроек и параметров приложения	Не актуально	Возможности пользователей ограничены в соответствии с Порядком контроля защиты информации в ИСПДн
4.3.	Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники	Не актуально	Доступ в помещения ограничен в соответствии с Матрицей доступа пользователей к персональным данным
4.4.	Угроза повреждения системного реестра	Не актуально	Нет гипервизора
4.5.	Угроза повышения привилегий	Актуально	
4.6.	Угроза подбора пароля BIOS	Не актуально	Доступ в помещения ограничен в соответствии с Матрицей доступа пользователей к персональным данным
4.7.	Угроза длительного удержания вычислительных ресурсов пользователями	Актуально	
4.8.	Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети	Актуально	
5.	Угрозы целостности (утраты, уничтожения, модификации информации)		

№ п/п	Наименование угрозы безопасности	Актуальность	Обоснования отсутствия актуальности угроз безопасности
5.1.	Угроза опосредованного управления группой программ через совместно используемые данные	Не актуально	Возможности пользователей ограничены в соответствии с Порядком контроля защиты информации в ИСПДн
5.2.	Угроза отказа в загрузке входных данных неизвестного формата хранилищем больших данных	Не актуально	Установлено антивирусное ПО Kaspersky endpoint security 10
5.3.	Угроза подделки записей журнала регистрации событий	Не актуально	Возможности пользователей ограничены в соответствии с Порядком контроля защиты информации в ИСПДн
5.4.	Угроза подмены беспроводного клиента или точки доступа	Не актуально	Нет беспроводных каналов связи
5.5.	Угроза подмены действия пользователя путем обмана	Не актуально	Нет облачной инфраструктуры
5.6.	Угроза подмены доверенного пользователя	Актуально	
5.7.	Угроза подмены резервной копии программного обеспечения BIOS	Не актуально	Возможности пользователей ограничены в соответствии с Порядком контроля защиты информации в ИСПДн
5.8.	Угроза подмены содержимого сетевых ресурсов	Не актуально	Установлено антивирусное ПО Kaspersky endpoint security 10
5.9.	Угроза подмены субъекта сетевого доступа	Актуально	
5.10.	Угроза получения предварительной информации об объекте защиты	Актуально	
5.11.	Угроза получения сведений о владельце беспроводного устройства	Не актуально	Нет беспроводной сети
5.12.	Угроза потери доверия к поставщику облачных услуг	Не актуально	Нет облачной инфраструктуры
5.13.	Угроза потери и утечки данных, обрабатываемых в облаке	Не актуально	Нет облачной инфраструктуры
5.14.	Угроза потери информации вследствие несогласованности работы узлов хранилища больших данных	Актуально	
5.15.	Угроза потери управления облачными ресурсами	Не актуально	Нет облачной инфраструктуры

№ п/п	Наименование угрозы безопасности	Актуальность	Обоснования отсутствия актуальности угроз безопасности
5.16.	Угроза потери управления собственной инфраструктурой при переносе ее в облако	Не актуально	Нет облачной инфраструктуры
5.17.	Угроза преодоления физической защиты	Не актуально	На входе размещен пост охраны, а также установлена система видеонаблюдения по всему периметру
5.18.	Угроза приведения системы в состояние «отказ в обслуживании»	Актуально	
5.19.	Угроза приостановки оказания облачных услуг вследствие технических сбоев	Не актуально	Нет облачной инфраструктуры
5.20.	Угроза пропуска проверки целостности программного обеспечения	Не актуально	Возможности пользователей ограничены в соответствии с Порядком контроля защиты информации в ИСПДн
5.21.	Угроза прямого обращения к памяти вычислительного поля суперкомпьютера	Не актуально	Нет суперкомпьютера
5.22.	Угроза распространения несанкционированно повышенных прав на всю грид-систему	Не актуально	Нет грид-системы
5.23.	Угроза сбоя автоматического управления системой разграничения доступа хранилища больших данных	Не актуально	Проводятся регулярные проверки в соответствии с Порядком контроля защиты информации в ИСПДн
5.24.	Угроза сбоя обработки специальным образом измененных файлов	Не актуально	Возможности пользователей ограничены в соответствии с Порядком контроля защиты информации в ИСПДн
5.25.	Угроза удаления аутентификационной информации	Не актуально	Управление аутентификацией имеет только администратор, пользовательские учетные записи ограничены в соответствии с Порядком управления учетными записями, утвержденным приказом Департамента № 1067
5.26.	Угроза утраты вычислительных ресурсов	Актуально	
5.27.	Угроза утраты носителей информации	Актуально	

№ п/п	Наименование угрозы безопасности	Актуальность	Обоснования отсутствия актуальности угроз безопасности
5.28.	Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	Не актуально	Доступ в помещения ограничен в соответствии с Матрицей доступа пользователей к персональным данным
5.29.	Угроза форматирования носителей информации	Актуально	
5.30.	Угроза «форсированного веб-браузинга»	Не актуально	Доступ к компьютерам есть только у пользователей в соответствии с Матрицей доступа пользователей к персональным данным
5.31.	Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации	Не актуально	Доступ в помещения ограничен в соответствии с Матрицей доступа пользователей к персональным данным
5.32.	Угроза чрезмерного использования вычислительных ресурсов суперкомпьютера в ходе интенсивного обмена межпроцессорными сообщениями	Не актуально	Нет суперкомпьютера
5.33.	Угроза эксплуатации цифровой подписи программного кода	Не актуально	Доступ в помещения ограничен в соответствии с Матрицей доступа пользователей к персональным данным
5.34.	Угроза перехвата исключения/сигнала из привилегированного блока функций	Не актуально	Доступ в помещения ограничен в соответствии с Матрицей доступа пользователей к персональным данным
5.35.	Угроза распространения состояния «отказ в обслуживании» в облачной инфраструктуре	Не актуально	Нет облачной инфраструктуры
5.36.	Угроза включения в проект не достоверно испытанных компонентов	Не актуально	Приобретение оборудования для защиты информации производятся у фирм, имеющих сертификаты ФСТЭК и ФСБ
5.37.	Угроза внедрения системной избыточности	Актуально	
5.38.	Угроза «кражи» учетной записи доступа к сетевым сервисам	Актуально	

№ п/п	Наименование угрозы безопасности	Актуальность	Обоснования отсутствия актуальности угроз безопасности
5.39.	Угроза неправомерного шифрования информации	Не актуально	Установкой программ занимается только системный администратор, пользовательские учетные записи ограничены в соответствии с Порядком управления учетными записями, утвержденным приказом Департамента № 1067
5.40.	Угроза нарушения технологического/производственного процесса из-за временных задержек, вносимых средством защиты	Актуально	
5.41.	Угроза неподтвержденного ввода данных оператором в систему, связанную с безопасностью	Актуально	
5.42.	Угроза несанкционированной модификации защищаемой информации	Не актуально	Возможности пользователей ограничены в соответствии с Порядком контроля защиты информации в ИСПДн
5.43.	Угроза отказа подсистемы обеспечения температурного режима	Актуально	
5.44.	Угроза перехвата одноразовых паролей в режиме реального времени	Не актуально	Данные логин/пароль хранятся у администратора, в соответствии с Порядком управления учетными записями, утвержденным приказом Департамента № 1067
5.45.	Угроза перехвата управления автоматизированной системой управления технологическими процессами	Не актуально	Доступ к автоматизированной системе ограничен в соответствии с Матрицей доступа пользователей к персональным данным
5.46.	Угроза несанкционированного изменения параметров настройки средств защиты информации	Не актуально	Средства защиты настраиваются на сервере, доступ к которому ограничен в соответствии с Матрицей доступа пользователей к персональным данным
5.47.	Угроза агрегирования данных, передаваемых в грид-системе	Не актуально	Нет грид-системы
5.48.	Угроза исчерпания вычислительных ресурсов хранилища больших данных	Актуально	
5.49.	Угроза нарушения целостности данных кэша	Актуально	

№ п/п	Наименование угрозы безопасности	Актуальность	Обоснования отсутствия актуальности угроз безопасности
5.50.	Угроза неверного определения формата входных данных, поступающих в хранилище больших данных	Актуально	
5.51.	Угроза невозможности восстановления сессии работы на ПЭВМ при выводе из промежуточных состояний питания	Актуально	
5.52.	Угроза невозможности миграции образов виртуальных машин из-за несовместимости аппаратного и программного обеспечения	Не актуально	Отсутствуют виртуальные машины
5.53.	Угроза недобросовестного исполнения обязательств поставщиками облачных услуг	Не актуально	Нет облачной инфраструктуры
5.54.	Угроза некачественного переноса инфраструктуры в облако	Не актуально	Нет облачной инфраструктуры
5.55.	Угроза неконтролируемого копирования данных внутри хранилища больших данных	Актуально	
5.56.	Угроза неконтролируемого уничтожения информации хранилищем больших данных	Актуально	
5.57.	Угроза неопределенности в распределении ответственности между ролями в облаке	Не актуально	Нет облачной инфраструктуры
5.58.	Угроза непрерывной модернизации облачной инфраструктуры	Не актуально	Нет облачной инфраструктуры
6.	Угрозы, реализуемые с использованием уязвимостей СКЗИ		
6.1.	Угроза несанкционированного копирования защищаемой информации	Не актуально	Установлены средства СКЗИ
7.	Угрозы, реализуемые с применением вредоносных программ		
7.1.	Угроза автоматического распространения вредоносного кода в грид-системе	Не актуально	Нет грид-системы

№ п/п	Наименование угрозы безопасности	Актуальность	Обоснования отсутствия актуальности угроз безопасности
7.2.	Угроза выхода процесса за пределы виртуальной машины	Не актуально	Нет виртуальной системы
7.3.	Угроза перегрузки грид-системы вычислительными заданиями	Не актуально	Нет грид-системы
7.4.	Угроза перехвата вводимой и выводимой на периферийные устройства информации	Не актуально	Возможности пользователей ограничены в соответствии с Порядком контроля защиты информации в ИСПДн
7.5.	Угроза подключения к беспроводной сети в обход процедуры аутентификации	Не актуально	Нет беспроводной сети
7.6.	Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	Не актуально	Возможности пользователей ограничены в соответствии с Порядком контроля защиты информации в ИСПДн
7.7.	Угроза усиления воздействия на вычислительные ресурсы пользователей при помощи сторонних серверов	Не актуально	Установлены средства СЗИ
7.8.	Угроза заражения компьютера при посещении неблагонадежных сайтов	Не актуально	Установлено антивирусное ПО Kaspersky endpoint security 10
7.9.	Угроза скрытного включения вычислительного устройства в состав бот-сети	Не актуально	Антивирусное ПО Kaspersky endpoint security 10 регулярно обновляется
7.10.	Угроза распространения «почтовых червей»	Не актуально	Установлено антивирусное ПО Kaspersky endpoint security 10
7.11.	Угроза «спама» веб-сервера	Не актуально	Установлено антивирусное ПО Kaspersky endpoint security 10
7.12.	Угроза «фарминга»	Не актуально	Установлено антивирусное ПО Kaspersky endpoint security 10
7.13.	Угроза «фишинга»	Не актуально	Установлено антивирусное ПО Kaspersky endpoint security 10
7.14.	Угроза внедрения вредоносного кода через рекламу, сервисы и контент	Не актуально	Установлено антивирусное ПО Kaspersky endpoint security 10
7.15.	Угроза подмены программного обеспечения	Не актуально	Установлено антивирусное ПО Kaspersky endpoint security 10

№ п/п	Наименование угрозы безопасности	Актуальность	Обоснования отсутствия актуальности угроз безопасности
7.16.	Угроза маскирования действий вредоносного кода	Не актуально	Средства защиты постоянно обновляются
7.17.	Угроза внедрения вредоносного кода за счет посещения зараженных сайтов в сети Интернет	Не актуально	Установлено антивирусное ПО Kaspersky endpoint security 10
7.18.	Угроза внедрения вредоносного кода в дистрибутив программного обеспечения	Не актуально	Установлено антивирусное ПО Kaspersky endpoint security 10
7.19.	Угроза утечки информации за счет применения вредоносным программным обеспечением алгоритмов шифрования графика	Не актуально	Установлено антивирусное ПО Kaspersky endpoint security 10
7.20.	Угроза злоупотребления возможностями, предоставленными потребителям облачных услуг	Не актуально	Нет облачной инфраструктуры
7.21.	Угроза избыточного выделения оперативной памяти	Не актуально	Возможности пользователей ограничены в соответствии с Порядком контроля защиты информации в ИСПДн
7.22.	Угроза искажения вводимой и выводимой на периферийные устройства информации	Не актуально	Проводятся ежемесячные проверки по требованиям безопасности в соответствии с Порядком контроля защиты информации в ИСПДн
7.23.	Угроза использования вычислительных ресурсов суперкомпьютера «паразитными» процессами	Не актуально	Нет суперкомпьютера
7.24.	Угроза нарушения изоляции пользовательских данных внутри виртуальной машины	Не актуально	Отсутствует виртуальная машина
7.25.	Угроза внедрения кода или данных	Не актуально	Антивирусное ПО Kaspersky endpoint security 10 регулярно обновляется
7.26.	Угроза несанкционированного доступа к данным за пределами зарезервированного адресного пространства, в том числе выделенного под виртуальное аппаратное обеспечение	Не актуально	Нет гипервизора

№ п/п	Наименование угрозы безопасности	Актуальность	Обоснования отсутствия актуальности угроз безопасности
7.27.	Угроза несанкционированного доступа к локальному компьютеру через клиента грид-системы	Не актуально	Нет грид-системы
7.28.	Угроза анализа криптографических алгоритмов и их реализации	Не актуально	Данные хранятся на сервере, доступ к которому ограничен, в соответствии с Порядком контроля защиты информации в ИСПДн
8.	Угрозы, реализуемые с применением специально разработанного ПО		
8.1.	Угроза отказа в обслуживании системой хранения данных суперкомпьютера	Не актуально	Нет суперкомпьютера
8.2.	Угроза передачи данных по скрытым каналам	Не актуально	Доступ в серверное помещение ограничен в соответствии с Матрицей доступа пользователей к персональным данным
8.3.	Угроза деструктивного изменения конфигурации/среды окружения программ	Не актуально	Возможности пользователей ограничены в соответствии с Порядком контроля защиты информации в ИСПДн
8.4.	Угроза деструктивного использования декларированного функционала BIOS	Не актуально	Возможности пользователей ограничены в соответствии с Порядком контроля защиты информации в ИСПДн
8.5.	Угроза загрузки нештатной операционной системы	Не актуально	Установкой операционных систем занимается системный администратор, пользовательские учетные записи ограничены, установлен пароль на вход в BIOS в соответствии с Порядком управления учетными записями, утвержденным приказом Департамента № 1067
8.6.	Угроза изменения режимов работы аппаратных элементов компьютера	Не актуально	Возможности пользователей ограничены в соответствии с Порядком контроля защиты информации в ИСПДн
8.7.	Угроза изменения системных и глобальных переменных	Актуально	
8.8.	Угроза использования поддельных цифровых подписей BIOS	Не актуально	Доступ к установке ПО есть только у администратора, пользовательские учетные записи ограничены, в соответствии с Порядком управления учетными записями, утвержденным приказом Департамента

№ п/п	Наименование угрозы безопасности	Актуальность	Обоснования отсутствия актуальности угроз безопасности
			№ 1067
8.9.	Угроза использования слабостей кодирования входных данных	Не актуально	Возможности пользователей ограничены в соответствии с Порядком контроля защиты информации в ИСПДн
8.10.	Угроза использования слабых криптографических алгоритмов BIOS	Не актуально	Возможности пользователей ограничены в соответствии с Порядком контроля защиты информации в ИСПДн
8.11.	Угроза исчерпания запаса ключей, необходимых для обновления BIOS	Не актуально	Возможности пользователей ограничены в соответствии с Порядком контроля защиты информации в ИСПДн
8.12.	Угроза аппаратного сброса пароля BIOS	Не актуально	Доступ в помещения есть только у сотрудников в соответствии с Матрицей доступа пользователей к персональным данным
8.13.	Угроза нарушения изоляции среды исполнения BIOS	Не актуально	Возможности пользователей ограничены в соответствии с Порядком контроля защиты информации в ИСПДн
8.14.	Угроза внедрения вредоносного кода в BIOS	Не актуально	Возможности пользователей ограничены в соответствии с Порядком контроля защиты информации в ИСПДн
8.15.	Угроза невозможности управления правами пользователей BIOS	Не актуально	Доступ в помещения ограничен в соответствии с Матрицей доступа пользователей к персональным данным
8.16.	Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением	Не актуально	Возможности пользователей ограничены в соответствии с Порядком контроля защиты информации в ИСПДн
8.17.	Угроза воздействия на программы с высокими привилегиями	Не актуально	Возможности пользователей ограничены в соответствии с Порядком контроля защиты информации в ИСПДн
8.18.	Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS	Не актуально	Возможности пользователей ограничены в соответствии с Порядком контроля защиты информации в ИСПДн
8.19.	Угроза несанкционированного доступа к гипервизору из виртуальной машины и (или) физической сети	Не актуально	Нет гипервизора
8.20.	Угроза восстановления аутентификационной информации	Актуально	
8.21.	Угроза несанкционированного доступа к системе по беспроводным каналам	Не актуально	Нет беспроводных каналов связи

№ п/п	Наименование угрозы безопасности	Актуальность	Обоснования отсутствия актуальности угроз безопасности
8.22.	Угроза несанкционированного доступа к системе хранения данных из виртуальной и (или) физической сети	Актуально	
8.23.	Угроза несанкционированного использования привилегированных функций BIOS	Не актуально	Возможности пользователей ограничены в соответствии с Порядком контроля защиты информации в ИСПДн
8.24.	Угроза восстановления предыдущей уязвимой версии BIOS	Актуально	
9.	Угрозы, с использованием уязвимостей системного ПО		
9.1.	Угроза передачи запрещенных команд на оборудование с числовым программным управлением	Не актуально	Возможности пользователей ограничены в соответствии с Порядком контроля защиты информации в ИСПДн
9.2.	Угроза программного сброса пароля BIOS	Не актуально	Возможности пользователей ограничены в соответствии с Порядком контроля защиты информации в ИСПДн
9.3.	Угроза сбоя процесса обновления BIOS	Актуально	
9.4.	Угроза установки уязвимых версий обновления программного обеспечения BIOS	Не актуально	Возможности пользователей ограничены в соответствии с Порядком контроля защиты информации в ИСПДн
9.5.	Угроза исследования механизмов работы программы	Не актуально	Доступ к исходным файлам программ хранятся у администратора, в соответствии с Порядком управления учетными записями, утвержденным приказом Департамента № 1067
9.6.	Угроза исследования приложения через отчеты об ошибках	Не актуально	Информация об ошибках отправляется на сервер, доступ к которому ограничен в соответствии с Порядком управления учетными записями, утвержденным приказом Департамента № 1067
9.7.	Угроза нарушения работоспособности грид-системы при нетипичной сетевой нагрузке	Не актуально	Нет грид-системы
9.8.	Угроза физического устаревания аппаратных компонентов	Актуально	

5.7. Актуальные угрозы безопасности ИСПДн обеспечения типовой деятельности.

5.7.1. ИСПДн обеспечения типовой деятельности отличаются следующими особенностями:

– использованием стандартных (унифицированных) технических средств обработки информации;

– использованием типового ПО;

– наличием незначительного количества АРМ, участвующих в обработке ПДн;

– дублированием информации, содержащей ПДн, на бумажных носителях и МНИ;

– незначительными негативными последствиями для субъектов ПДн при реализации угроз безопасности ИСПДн;

– эксплуатацией ИСПДн, как правило, сотрудниками Департамента без привлечения на постоянной основе сторонних организаций;

– жесткой регламентацией процедуры взаимодействия со сторонними организациями (банки, пенсионные, страховые и налоговые органы, органы статистики).

5.7.2. Актуальными угрозами безопасности ПДн в ИСПДн обеспечения типовой деятельности в Департаменте являются:

– угроза неправомерного ознакомления с защищаемой информацией;

– угроза несанкционированного восстановления удаленной защищаемой информации;

– угроза несанкционированного доступа к хранимой в виртуальном пространстве защищаемой информации;

– угроза использования слабостей протоколов сетевого/локального обмена данными;

– угроза обнаружения хостов;

– угроза подмены доверенного пользователя;

– угроза получения предварительной информации об объекте защиты;

– угроза неконтролируемого копирования данных внутри хранилища больших данных;

– угроза восстановления аутентификационной информации.

5.8. Актуальные угрозы безопасности ПДн в ИСПДн обеспечения специальной деятельности.

5.8.1. ИСПДн обеспечения специальной деятельности отличаются следующими особенностями:

– использованием широкой номенклатуры технических средств получения, отображения и обработки информации;

– использованием специального ПО;

– наличием значительного количества АРМ, участвующих в обработке ПДн;

– построением ИСПДн на базе распределенной по территории области вычислительной сети со сложной архитектурой;

– наличием подключений к сетям связи общего пользования и (или) международного информационного обмена;

– использованием разнообразной телекоммуникационной инфраструктуры, принадлежащей различным операторам связи;

– широким применением средств защиты информации, включая сертифицированные СКЗИ;

– использованием аутсорсинга при создании и эксплуатации ИСПДн и ее элементов;

– сложностью с дублированием больших массивов информации, содержащей ПДн, на бумажных носителях и МНИ;

– значительными негативными последствиями при реализации угроз безопасности ИСПДн;

– недостаточной квалификацией пользователей и обслуживающего ИСПДн и средства защиты информации персонала;

– проблемами взаимодействия различных ИСПДн, вызванных несовершенством действующего законодательства и ведомственных инструкций.

5.8.2. Актуальными угрозами безопасности ПДн в ИСПДн обеспечения специальной деятельности в Департаменте являются:

– угроза некорректного использования функционала программного обеспечения;

– угроза несанкционированного удаленного внеполосного доступа к аппаратным средствам;

– угроза несанкционированного управления синхронизацией и состоянием;

– угроза использования уязвимых версий программного обеспечения;

– угроза обхода некорректно настроенных механизмов аутентификации;

– угроза доступа/перехвата/изменения HTTP cookies;

– угроза межсайтовой подделки запроса;

– угроза повышения привилегий;

– угроза длительного удержания вычислительных ресурсов пользователями;

– угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети;

– угроза подмены субъекта сетевого доступа;

– угроза потери информации вследствие несогласованности работы узлов хранилища больших данных;

– угроза приведения системы в состояние «отказ в обслуживании»;

– угроза утраты вычислительных ресурсов;

– угроза утраты носителей информации;

– угроза форматирования носителей информации;

– угроза внедрения системной избыточности;

– угроза «кражи» учетной записи доступа к сетевым сервисам;

– угроза нарушения технологического/производственного процесса из-за временных задержек, вносимых средством защиты;

– угроза неподтвержденного ввода данных оператором в систему, связанную с безопасностью;

– угроза отказа подсистемы обеспечения температурного режима;

– угроза исчерпания вычислительных ресурсов хранилища больших данных;

– угроза нарушения целостности данных кэша;

– угроза неверного определения формата входных данных, поступающих в хранилище больших данных;

– угроза невозможности восстановления сессии работы на ПЭВМ при выводе из промежуточных состояний питания;

– угроза неконтролируемого уничтожения информации хранилищем больших данных;

– угроза изменения системных и глобальных переменных;

– угроза несанкционированного доступа к системе хранения данных из виртуальной и (или) физической сети;

– угроза восстановления предыдущей уязвимой версии BIOS;

– угроза физического устаревания аппаратных компонентов.