У К А З

ГУБЕРНАТОРА ПЕРМСКОГО КРАЯ

22.02.2018 № 13

Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных в Аппарате Правительства Пермского края, Администрации губернатора Пермского края, исполнительных органах государственной власти Пермского края

В соответствии с частью 5 статьи 19 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», с целью обеспечения единого подхода к определению угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных в Аппарате Правительства Пермского края, Администрации губернатора Пермского края, исполнительных органах государственной власти Пермского края,

ПОСТАНОВЛЯЮ:

1. Утвердить Положение об угрозах безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных в Аппарате Правительства Пермского края, Администрации губернатора Пермского края, исполнительных органах государственной власти Пермского края.

2. Рекомендовать органам местного самоуправления муниципальных образований Пермского края руководствоваться настоящим указом при обработке персональных данных в информационных системах персональных данных, используемых в органах местного самоуправления муниципальных образований Пермского края.

3. Настоящий указ вступает в силу через 10 дней после дня его официального опубликования.

4. Контроль за исполнением указа оставляю за собой.

М.Г. Решетников

Приложение
к указу
губернатора Пермского края
от 22.02.2018 № 13

ПОЛОЖЕНИЕ

об угрозах безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных в Аппарате Правительства Пермского края, Администрации губернатора Пермского края, исполнительных органах государственной власти Пермского края

I. Общие положения

1.1. Настоящее Положение об угрозах безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных в Аппарате Правительства Пермского края, Администрации губернатора Пермского края, исполнительных органах государственной власти Пермского края, определяет угрозы безопасности персональных данных (далее – ПДн), актуальные при обработке ПДн в информационных системах персональных данных (далее – ИСПДн), эксплуатируемых Аппаратом Правительства Пермского края, Администрацией губернатора Пермского края, исполнительными органами государственной власти Пермского края (далее – ОГВ).

1.2. Настоящее Положение предназначено для руководства ОГВ при решении следующих задач:

определение угроз безопасности ПДн, актуальных при обработке ПДн в ИСПДн;

проведение анализа защищенности ИСПДн от актуальных угроз безопасности ПДн;

проведение мероприятий по минимизации и (или) нейтрализации угроз безопасности ПДн;

модернизация системы защиты ИСПДн;

предотвращение несанкционированного воздействия на технические средства ИСПДн;

контроль за обеспечением уровня защищенности ИСПДн.

1.3. При определении угроз безопасности ПДн использованы следующие правовые акты, методические документы:

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

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

постановление Правительства Российской Федерации от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» (далее – Постановление № 1119);

приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденная заместителем директора ФСТЭК России 15 февраля 2008 г.;

Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденная заместителем директора ФСТЭК России 14 февраля 2008 г.;

Методические рекомендации по составлению Частной модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных учреждений здравоохранения, социальной сферы, труда и занятости, разработанные Министерством здравоохранения и социального развития Российской Федерации, 2009 г.;

Модель угроз и нарушителя безопасности персональных данных, обрабатываемых в типовых информационных системах персональных данных отрасли, согласованная с ФСТЭК России, ФСБ России и одобренная решением секции № 1 Научно-технического совета Минкомсвязи России «Научно-техническое и стратегическое развитие отрасли» от 21 апреля 2010 г. № 2;

Банк данных угроз безопасности информации, размещенный в информационно-телекоммуникационной сети «Интернет» (далее – сеть «Интернет») по адресу: http://bdu.fstec.ru.

II. Основные термины и определения

Понятия, используемые в настоящем Положении, применяются в значениях, определенных Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных». В настоящем Положении применяются следующие сокращения:

АРМ – автоматизированное рабочее место;

ИС – информационная система;
КЗ – контролируемая зона;
СВТ – средства вычислительной техники;
СПО – системное программное обеспечение;
ППО – прикладное программное обеспечение;
СЗИ – средства защиты информации;
СКЗИ – средства криптографической защиты информации.

III. Определение актуальных угроз безопасности ПДн при разработке частной модели угроз ПДн

3.1. Под угрозами безопасности ПДн понимается совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к ПДн при их обработке в ИСПДн, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение ПДн, а также иные неправомерные действия.

3.2. Угрозы безопасности ПДн в ИСПДн, приведенные в настоящем Положении, подлежат адаптации в ходе разработки частных моделей угроз безопасности ПДн при их обработке в ИСПДн.

3.3. В целях настоящего Положения под частной моделью угроз безопасности ПДн при их обработке в ИСПДн понимается модель угроз безопасности ПДн при их обработке в ИСПДн, учитывающая особенности обработки персональных данных в отдельном ОГВ.

3.4. В целях создания частной модели угроз безопасности ПДн определяется тип ИСПДн и группы угроз безопасности ПДн, актуальные для данного типа ИСПДн.

3.5. Тип ИСПДн определяется по результатам анализа структурно-функциональных характеристик ИСПДн, применяемых в ней информационных технологий и особенностей ее функционирования, согласно разделу IV настоящего Положения.

3.6. Группы угроз безопасности ПДн в ИСПДн определяются в соответствии с типом ИСПДн согласно разделу VII настоящего Положения.

3.7. Расширенный перечень угроз безопасности ПДн в ИСПДн (по группам) представлен в приложении к настоящему Положению.

3.8. В частной модели угроз безопасности ПДн описываются ИСПДн и ее структурно-функциональные характеристики, угрозы безопасности ПДн, включающие описание возможностей нарушителя (модель нарушителя), возможных уязвимостей ИСПДн, способов реализации угроз безопасности ПДн и их последствия.

IV. Типы ИСПДн

Операторы ИСПДн создают и эксплуатируют ИСПДн в целях обработки ПДн. Ввод ПДн осуществляется как с бумажных носителей, так и с электронных носителей информации. ПДн субъектов могут выводиться из ИСПДн с целью передачи ПДн третьим лицам как в электронном, так и в бумажном виде.

Информационный обмен по сетям связи общего пользования и (или) сетям международного информационного обмена осуществляется с использованием сертифицированных средств криптографической защиты.

КЗ ИСПДн являются здания или отдельные помещения. В пределах КЗ находятся рабочие места пользователей, серверы, сетевое и телекоммуникационное оборудование ИСПДн. Вне КЗ находятся линии передачи данных и телекоммуникационное оборудование, используемое для информационного обмена по сетям связи общего пользования и (или) сетям международного информационного обмена.

В зависимости от структурно-функциональных характеристик такие ИСПДн подразделяются на:

ИСПДн обеспечения типовой деятельности;

ИСПДн обеспечения специальной деятельности.

4.1. ИСПДн обеспечения типовой деятельности.

К ИСПДн обеспечения типовой деятельности относятся ИСПДн, используемые для управления персоналом, управления финансами, информационного обеспечения деятельности ОГВ.

ИСПДн управления персоналом предназначены для персонального кадрового учета, анализа кадрового состава, сопровождения кадровых процедур и для иных целей, связанных с управлением персоналом. Обработке подлежит информация, являющаяся ПДн, и иная информация, имеющая характер ПДн, сотрудников оператора ИСПДн, кандидатов на замещение должностей и (или) граждан, подавших сведения для участия в конкурсе на замещение вакантных должностей, конкурсе на включение в кадровый резерв.

ИСПДн управления финансами предназначены для обработки ПДн, необходимых для бухгалтерского и управленческого финансового учета, предоставления информации в пенсионные и налоговые органы, систему обязательного медицинского страхования. В ИСПДн обрабатываются: фамилия, имя, отчество; дата и место рождения; паспортные данные; адрес; номер телефона; идентификационный номер налогоплательщика; страховой номер индивидуального лицевого счета (СНИЛС); табельный номер;

должность; номер приказа и дата приема на работу (увольнения); номер лицевого счета для перечисления денежного содержания и иных выплат.

ИСПДн информационного обеспечения предназначены для официального доведения любой информации до определенного или неопределенного круга лиц, при этом факт доведения такой информации не порождает правовых последствий, однако может являться обязательным в силу действующего законодательства. ИСПДн информационного обеспечения является общедоступным источником ПДн, где с письменного согласия субъекта ПДн обрабатываются: фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные ПДн.

К ИСПДн информационного обеспечения относятся:

официальные сайты (порталы) ОГВ в сети «Интернет»;

информационные сайты (порталы) ОГВ в сети «Интернет», посвященные определенному проекту или мероприятию, проводимому на территории Пермского края.

4.2. ИСПДн обеспечения специальной деятельности.

К ИСПДн обеспечения специальной деятельности можно отнести ведомственные ИСПДн, краевые ИСПДн, сегментные (распределенные) ИСПДн, подключенные к сетям общего пользования и (или) сетям международного информационного обмена. ИСПДн обеспечения специальной деятельности предназначены для исполнения функций (полномочий) ОГВ, технологического обеспечения предоставления государственных услуг в электронной форме.

В ИСПДн обеспечения специальной деятельности обрабатываются ПДн заявителей, необходимые для предоставления государственных услуг и получаемые в рамках межведомственного информационного взаимодействия, в том числе из базовых государственных информационных ресурсов, а также для осуществления ОГВ иных функций в соответствии с действующим законодательством.

Ведомственные ИСПДн создаются (эксплуатируются) по решению одного ОГВ в его интересах и предназначены для исполнения функций (полномочий) ОГВ.

Краевые ИСПДн создаются и эксплуатируются по решению ОГВ в интересах нескольких ОГВ, при этом цели и задачи создания и эксплуатации данных ИСПДн, а также требования к ним определяются на уровне Пермского края.

Сегментные (распределенные) ИСПДн представляют собой сегменты федеральных ИС, созданные и эксплуатируемые на уровне Пермского края на основании решения федеральных органов власти. ИСПДн используются

для обработки данных на уровне Пермского края и передачи их на федеральный уровень и наоборот, при этом цели и задачи создания и эксплуатации данных ИСПДн определяются на федеральном уровне. Данные ИСПДн предназначены для реализации функций (полномочий) федеральных органов власти и исполнения функций (полномочий) ОГВ.

V. Источники угроз безопасности ПДн в ИСПДн

Источниками угроз безопасности ПДн в ИСПДн выступают:

носитель вредоносной программы;

аппаратная закладка;

нарушитель.

5.1. Носителем вредоносной программы может быть аппаратный элемент компьютера или программный контейнер. В качестве носителя вредоносной программы рассматриваются:

отчуждаемый носитель (дискета), оптический диск (CD-R, CD-RW и т.п.), флеш-память, отчуждаемый винчестер и т.п.;

встроенные носители информации (винчестеры, микросхемы оперативной памяти, процессор, микросхемы системной платы, микросхемы устройств, видеоадаптеры, сетевые платы, звуковые платы, модемы, устройства ввода/вывода магнитных жестких и оптических дисков, блоки питания и т.п.);

микросхемы внешних устройств (монитора, клавиатуры, принтера, модема, сканера и т.п.);

пакеты, передаваемые по сетям связи общего пользования и (или) сетям международного информационного обмена;

файлы (текстовые, графические, исполняемые и т.д.).

5.2. Аппаратная закладка может применяться в аппаратных средствах, предназначенных для ввода информации (ПДн) в ИСПДн с клавиатуры АРМ, например:

аппаратная закладка внутри клавиатуры;

считывание данных с кабеля клавиатуры бесконтактным методом;

включение устройства в разрыв кабеля;

аппаратная закладка внутри системного блока и др.

5.3. Под нарушителем безопасности информации понимается физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности ПДн при обработке ПДн в ИСПДн.

По наличию права постоянного или разового доступа в ИСПДн нарушители подразделяются на три типа.

5.3.1. Внешний нарушитель. Данный тип нарушителя не имеет права постоянного доступа в КЗ или имеет право разового (контролируемого) доступа в КЗ, а также не имеет доступа к СВТ ИСПДн, расположенным в пределах КЗ, или он ограничен и контролируется. Данный тип нарушителя может реализовывать угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена.

5.3.2. Внутренний нарушитель, имеющий доступ к ИСПДн. Данный тип нарушителя имеет право постоянного (периодического) доступа на территорию КЗ, а также доступ к СВТ ИСПДн, расположенным в пределах КЗ. Данный тип нарушителя может проводить атаки с использованием внутренней (локальной) сети передачи данных и непосредственно в ИСПДн.

5.3.3. Внутренний нарушитель, не имеющий доступ к ИСПДн. Данный тип нарушителя имеет право постоянного (периодического) доступа на территорию КЗ, но не имеет доступ к СВТ ИСПДн, расположенным в пределах КЗ. Данный тип нарушителя может проводить атаки с использованием внутренней (локальной) сети передачи данных.

VI. Группы угроз безопасности ПДн в ИСПДн

6.1. Основными группами угроз безопасности ПДн в ИСПДн являются:

угрозы нарушения функционирования аппаратного обеспечения;

угрозы инженерной инфраструктуры;

угрозы, обеспечивающие предоставление доступа к хранилищу данных;

угрозы ошибок/внесения уязвимостей при проектировании, внедрении ИСПДн/системы информационной безопасности ИСПДн;

угрозы, предоставляющие доступ к грид-системам и позволяющие их модифицировать;

угрозы физического доступа к компонентам ИСПДн;

угрозы эксплуатации уязвимостей в аппаратных компонентах ИСПДн и микропрограммном обеспечении;

угрозы эксплуатации уязвимостей в ППО;

угрозы эксплуатации уязвимостей в СПО;

угрозы эксплуатации уязвимостей СЗИ;

угрозы, обеспечивающие доступ к мобильным устройствам;

угрозы, позволяющие внести изменения в состав программных или аппаратных средств ИСПДн;

угрозы, связанные с использованием облачных услуг;

угрозы, связанные с использованием сетевых технологий;

угрозы, связанные с использованием суперкомпьютерных технологий;

угрозы, связанные с использованием технологий виртуализации;

угрозы, связанные с нарушением правил эксплуатации машинных носителей;

угрозы, связанные с предоставлением доступа к беспроводным каналам передачи данных.

6.2. При рассмотрении групп угроз эксплуатации уязвимостей в ППО и угроз эксплуатации уязвимостей в СПО согласно пункту 6 Постановления № 1119 определяются угрозы 1-го, 2-го или 3-го типа, актуальные для каждой ИСПДн, независимо от типа ИСПДн. Определение типа угроз безопасности ПДн, актуальных для ИСПДн, производится оператором с учетом оценки возможного вреда, который может быть причинен субъектам ПДн.

6.3. Группы угроз безопасности ПДн в ИСПДн уточняются по мере выявления новых угроз безопасности ПДн и их источников, развития способов и средств их реализации.

VII. Группы угроз безопасности ПДн, актуальные при обработке ПДн по типам ИСПДн

В настоящем разделе представлены группы угроз безопасности ПДн, актуальные для каждого типа ИСПДн, в соответствии с разделом IV настоящего Положения.

7.1. ИСПДн обеспечения типовой деятельности.

7.1.1. Группы угроз безопасности ПДн, актуальные в ИСПДн управления персоналом:

угрозы нарушения функционирования аппаратного обеспечения;

угрозы, обеспечивающие предоставление доступа к хранилищу данных;

угрозы ошибок/внесения уязвимостей при проектировании, внедрении ИСПДн/системы информационной безопасности ИСПДн;

угрозы физического доступа к компонентам ИСПДн;

угрозы эксплуатации уязвимостей в аппаратных компонентах ИСПДн и микропрограммном обеспечении;

угрозы эксплуатации уязвимостей в ППО;

угрозы эксплуатации уязвимостей в СПО;

угрозы эксплуатации уязвимостей СЗИ;

угрозы, позволяющие внести изменения в состав программных или аппаратных средств ИСПДн;

угрозы, связанные с использованием сетевых технологий;

угрозы, связанные с использованием технологий виртуализации;

угрозы, связанные с нарушением правил эксплуатации машинных носителей.

7.1.2. Группы угроз безопасности ПДн, актуальные в ИСПДн управления финансами:

угрозы нарушения функционирования аппаратного обеспечения;

угрозы, обеспечивающие предоставление доступа к хранилищу данных;

угрозы ошибок/внесения уязвимостей при проектировании, внедрении ИСПДн/системы информационной безопасности ИСПДн;

угрозы физического доступа к компонентам ИСПДн;

угрозы эксплуатации уязвимостей в аппаратных компонентах ИСПДн и микропрограммном обеспечении;

угрозы эксплуатации уязвимостей в ППО;

угрозы эксплуатации уязвимостей в СПО;

угрозы эксплуатации уязвимостей СЗИ;

угрозы, позволяющие внести изменения в состав программных или аппаратных средств ИСПДн;

угрозы, связанные с использованием сетевых технологий;

угрозы, связанные с использованием технологий виртуализации;

угрозы, связанные с нарушением правил эксплуатации машинных носителей.

7.1.3. Группы угроз безопасности ПДн, актуальные в ИСПДн информационного обеспечения:

угрозы нарушения функционирования аппаратного обеспечения;

угрозы, обеспечивающие предоставление доступа к хранилищу данных;

угрозы ошибок/внесения уязвимостей при проектировании, внедрении ИСПДн/системы информационной безопасности ИСПДн;

угрозы физического доступа к компонентам ИСПДн;

угрозы эксплуатации уязвимостей в аппаратных компонентах ИСПДн и микропрограммном обеспечении;

угрозы эксплуатации уязвимостей в ППО;

угрозы эксплуатации уязвимостей в СПО;

угрозы эксплуатации уязвимостей СЗИ;

угрозы, обеспечивающие доступ к мобильным устройствам;

угрозы, позволяющие внести изменения в состав программных или аппаратных средств ИСПДн;

угрозы, связанные с использованием облачных услуг;

угрозы, связанные с использованием сетевых технологий;

угрозы, связанные с использованием технологий виртуализации;

угрозы, связанные с нарушением правил эксплуатации машинных носителей.

7.2. ИСПДн обеспечения специальной деятельности.

7.2.1. Группы угроз безопасности ПДн, актуальные в ведомственных ИСПДн:

угрозы нарушения функционирования аппаратного обеспечения;

угрозы инженерной инфраструктуры;

угрозы, обеспечивающие предоставление доступа к хранилищу данных;

угрозы ошибок/внесения уязвимостей при проектировании, внедрении ИСПДн/системы информационной безопасности ИСПДн;

угрозы физического доступа к компонентам ИСПДн;

угрозы эксплуатации уязвимостей в аппаратных компонентах ИСПДн и микропрограммном обеспечении;

угрозы эксплуатации уязвимостей в ППО;

угрозы эксплуатации уязвимостей в СПО;

угрозы эксплуатации уязвимостей СЗИ;

угрозы, обеспечивающие доступ к мобильным устройствам;

угрозы, позволяющие внести изменения в состав программных или аппаратных средств ИСПДн;

угрозы, связанные с использованием облачных услуг;

угрозы, связанные с использованием сетевых технологий;

угрозы, связанные с использованием технологий виртуализации;

угрозы, связанные с нарушением правил эксплуатации машинных носителей;

угрозы, связанные с предоставлением доступа к беспроводным каналам передачи данных.

7.2.2. Группы угроз безопасности ПДн, актуальные в краевых ИСПДн:

угрозы нарушения функционирования аппаратного обеспечения;

угрозы инженерной инфраструктуры;

угрозы, обеспечивающие предоставление доступа к хранилищу данных;

угрозы ошибок/внесения уязвимостей при проектировании, внедрении ИСПДн/системы информационной безопасности ИСПДн;

угрозы физического доступа к компонентам ИСПДн;

угрозы эксплуатации уязвимостей в аппаратных компонентах ИСПДн и микропрограммном обеспечении;

угрозы эксплуатации уязвимостей в ППО;

угрозы эксплуатации уязвимостей в СПО;

угрозы эксплуатации уязвимостей СЗИ;

угрозы, обеспечивающие доступ к мобильным устройствам;

угрозы, позволяющие внести изменения в состав программных или аппаратных средств ИСПДн;

угрозы, связанные с использованием облачных услуг;

угрозы, связанные с использованием сетевых технологий;

угрозы, связанные с использованием технологий виртуализации;

угрозы, связанные с нарушением правил эксплуатации машинных носителей;

угрозы, связанные с предоставлением доступа к беспроводным каналам передачи данных.

7.2.3. Группы угроз безопасности ПДн, актуальные в сегментных (распределенных) ИСПДн:

угрозы нарушения функционирования аппаратного обеспечения;

угрозы инженерной инфраструктуры;

угрозы, обеспечивающие предоставление доступа к хранилищу данных;

угрозы ошибок/внесения уязвимостей при проектировании, внедрении ИСПДн/системы информационной безопасности ИСПДн;

угрозы физического доступа к компонентам ИСПДн;

угрозы эксплуатации уязвимостей в аппаратных компонентах ИСПДн и микропрограммном обеспечении;

угрозы эксплуатации уязвимостей в ППО;

угрозы эксплуатации уязвимостей в СПО;

угрозы эксплуатации уязвимостей СЗИ;

угрозы, обеспечивающие доступ к мобильным устройствам;

угрозы, позволяющие внести изменения в состав программных или аппаратных средств ИСПДн;

угрозы, связанные с использованием облачных услуг;

угрозы, связанные с использованием сетевых технологий;

угрозы, связанные с использованием технологий виртуализации;

угрозы, связанные с нарушением правил эксплуатации машинных носителей;

угрозы, связанные с предоставлением доступа к беспроводным каналам передачи данных.

Приложение
к Положению об угрозах
безопасности персональных
данных, актуальных
при обработке персональных
данных в информационных
системах персональных данных
в Аппарате Правительства
Пермского края,
Администрации губернатора
Пермского края,
исполнительных органах
государственной власти
Пермского края

РАСШИРЕННЫЙ ПЕРЕЧЕНЬ

угроз безопасности персональных данных в информационных системах персональных данных (по группам)

№	Наименование угрозы безопасности персональных данных (далее – ПДн) в информационных системах персональных данных (далее – ИСПДн)	Источники угрозы безопасности ПДн
1	2	3
1	**Угрозы нарушения функционирования аппаратного обеспечения**	
1.1	Угроза избыточного выделения оперативной памяти	Внешний нарушитель, внутренний нарушитель, носитель вредоносной программы
1.2	Угроза неправомерного ознакомления с защищаемой информацией	Внутренний нарушитель
1.3	Угроза несанкционированного использования привилегированных функций BIOS	Внешний нарушитель, внутренний нарушитель
1.4	Угроза физического устаревания аппаратных компонентов	Внутренний нарушитель
2	**Угрозы инженерной инфраструктуры**	
2.1	Угроза отказа подсистемы обеспечения температурного режима	Внешний нарушитель, внутренний нарушитель, носитель вредоносной программы
2.2	Угрозы сбоев в сети электропитания	Внешний нарушитель, внутренний нарушитель
2.3	Угроза выхода из строя ТС в результате нарушения климатических параметров работы	Внешний нарушитель, внутренний нарушитель
2.4	Угрозы нарушения схем электропитания	Внешний нарушитель, внутренний нарушитель
2.5	Угрозы, связанные с отсутствием заземления/неправильным заземлением	Внешний нарушитель, внутренний нарушитель
3	**Угрозы, обеспечивающие предоставление доступа к хранилищу данных**	
3.1	Угроза неверного определения формата входных данных, поступающих в хранилище больших данных	Внутренний нарушитель
3.2	Угроза неконтролируемого копирования данных внутри хранилища больших данных	Внутренний нарушитель, носитель вредоносной программы

1	2	3
3.3	Угроза неконтролируемого уничтожения информации хранилищем больших данных	Внутренний нарушитель, носитель вредоносной программы
3.4	Угроза несанкционированного восстановления удаленной защищаемой информации	Внешний нарушитель, внутренний нарушитель
3.5	Угроза несанкционированного удаления защищаемой информации	Внешний нарушитель, внутренний нарушитель, носитель вредоносной программы
3.6	Угроза несогласованности правил доступа к большим данным	Внутренний нарушитель
3.7	Угроза отказа в загрузке входных данных неизвестного формата хранилищем больших данных	Внутренний нарушитель
3.8	Угроза сбоя обработки специальным образом измененных файлов	Внешний нарушитель, внутренний нарушитель, носитель вредоносной программы
4	**Угрозы ошибок/внесения уязвимостей при проектировании, внедрении ИСПДн/системы информационной безопасности ИСПДн**	
4.1	Угроза включения в проект недостоверно испытанных компонентов	Внутренний нарушитель
4.2	Угроза внедрения системной избыточности	Внутренний нарушитель
4.3	Угроза наличия механизмов разработчика	Внутренний нарушитель
4.4	Угроза перехвата управления автоматизированной системой управления технологическими процессами	Внешний нарушитель, внутренний нарушитель, носитель вредоносной программы
5	**Угрозы, предоставляющие доступ к грид-системам и позволяющие их модифицировать**	
5.1	Угроза автоматического распространения вредоносного кода в грид-системе	Внешний нарушитель, внутренний нарушитель, носитель вредоносной программы
5.2	Угроза агрегирования данных, передаваемых в грид-системе	Внешний нарушитель
5.3	Угроза нарушения работоспособности грид-системы при нетипичной сетевой нагрузке	Внешний нарушитель, внутренний нарушитель, носитель вредоносной программы
5.4	Угроза несанкционированного доступа к локальному компьютеру через клиента грид-системы	Внешний нарушитель, носитель вредоносной программы
5.5	Угроза перегрузки грид-системы вычислительными заданиями	Внутренний нарушитель, носитель вредоносной программы
5.6	Угроза распространения несанкционированно повышенных прав на всю грид-систему	Внутренний нарушитель
6	**Угрозы физического доступа к компонентам ИСПДн**	
6.1	Угроза преодоления физической защиты	Внешний нарушитель
6.2	Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/ передачи информации	Внешний нарушитель
6.3	Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации	Внешний нарушитель
7	**Угрозы эксплуатации уязвимостей в аппаратных компонентах ИСПДн и микропрограммном обеспечении**	
7.1	Угроза аппаратного сброса пароля BIOS	Внутренний нарушитель

1	2	3
7.2	Угроза внедрения вредоносного кода в BIOS	Внутренний нарушитель
7.3	Угроза восстановления предыдущей уязвимой версии BIOS	Внутренний нарушитель
7.4	Угроза деструктивного использования декларированного функционала BIOS	Внутренний нарушитель
7.5	Угроза загрузки нештатной операционной системы	Внутренний нарушитель
7.6	Угроза изменения режимов работы аппаратных элементов компьютера	Внутренний нарушитель
7.7	Угроза использования поддельных цифровых подписей BIOS	Внешний нарушитель
7.8	Угроза использования слабых криптографических алгоритмов BIOS	Внешний нарушитель
7.9	Угроза исчерпания запаса ключей, необходимых для обновления BIOS	Внешний нарушитель
7.10	Угроза нарушения изоляции среды исполнения BIOS	Внутренний нарушитель
7.11	Угроза невозможности управления правами пользователей BIOS	Внутренний нарушитель
7.12	Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS	Внутренний нарушитель
7.13	Угроза подбора пароля BIOS	Внутренний нарушитель
7.14	Угроза подмены резервной копии программного обеспечения BIOS	Внутренний нарушитель
7.15	Угроза программного сброса пароля BIOS	Внутренний нарушитель
7.16	Угроза сбоя процесса обновления BIOS	Внутренний нарушитель
7.17	Угроза установки уязвимых версий обновления программного обеспечения BIOS	Внешний нарушитель, внутренний нарушитель
8	**Угрозы эксплуатации уязвимостей в прикладном программном обеспечении**	
8.1	Угроза доступа/перехвата/изменения HTTP cookies	Внешний нарушитель, носитель вредоносной программы
8.2	Угроза подмены действия пользователя путем обмана	Внешний нарушитель, носитель вредоносной программы
8.3	Угроза подмены содержимого сетевых ресурсов	Внешний нарушитель, носитель вредоносной программы
8.4	Угроза подмены субъекта сетевого доступа	Внешний нарушитель
8.5	Угроза подмены программного обеспечения	Внутренний нарушитель
8.6	Угроза внедрения вредоносного кода в дистрибутив программного обеспечения	Внешний нарушитель, внутренний нарушитель
8.7	Угроза использования уязвимых версий программного обеспечения	Внешний нарушитель, внутренний нарушитель
9	**Угрозы эксплуатации уязвимостей в системном программном обеспечении**	
9.1	Угроза внедрения кода или данных	Внешний нарушитель, носитель вредоносной программы
9.2	Угроза невозможности восстановления сессии работы на ПЭВМ при выводе из промежуточных состояний питания	Внутренний нарушитель

1	2	3
9.3	Угроза восстановления аутентификационной информации	Внешний нарушитель, внутренний нарушитель
9.4	Угроза повреждения системного реестра	Внешний нарушитель, внутренний нарушитель
9.5	Угроза деструктивного изменения конфигурации/среды окружения программ	Внутренний нарушитель, носитель вредоносной программы
9.6	Угроза изменения системных и глобальных переменных	Внутренний нарушитель
9.7	Угроза искажения вводимой и выводимой на периферийные устройства информации	Внешний нарушитель, внутренний нарушитель
9.8	Угроза использования механизмов авторизации для повышения привилегий	Внешний нарушитель, внутренний нарушитель
9.9	Угроза использования слабостей кодирования входных данных	Внешний нарушитель, внутренний нарушитель
9.10	Угроза использования слабостей протоколов сетевого/локального обмена данными	Внешний нарушитель, внутренний нарушитель
9.11	Угроза исследования механизмов работы программы	Внешний нарушитель, внутренний нарушитель
9.12	Угроза исследования приложения через отчеты об ошибках	Внешний нарушитель, внутренний нарушитель
9.13	Угроза некорректного использования функционала программного обеспечения	Внешний нарушитель, внутренний нарушитель
9.14	Угроза некорректной реализации политики лицензирования в облаке	Внешний нарушитель, внутренний нарушитель
9.15	Угроза неопределенности в распределении ответственности между ролями в облаке	Внешний нарушитель, внутренний нарушитель
9.16	Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением	Внешний нарушитель, внутренний нарушитель
9.17	Угроза несанкционированного доступа к аутентификационной информации	Внешний нарушитель, внутренний нарушитель
9.18	Угроза несанкционированного изменения аутентификационной информации	Внешний нарушитель, внутренний нарушитель, носитель вредоносной программы
9.19	Угроза несанкционированного редактирования реестра	Внешний нарушитель, внутренний нарушитель, носитель вредоносной программы
9.10	Угроза несанкционированного создания учетной записи пользователя	Внешний нарушитель, внутренний нарушитель
9.21	Угроза несанкционированного управления буфером	Внешний нарушитель, внутренний нарушитель, носитель вредоносной программы
9.22	Угроза несанкционированного управления синхронизацией и состоянием	Внешний нарушитель, внутренний нарушитель
9.23	Угроза несанкционированного управления указателями	Внешний нарушитель, внутренний нарушитель
9.24	Угроза обхода некорректно настроенных механизмов аутентификации	Внешний нарушитель, внутренний нарушитель
9.25	Угроза опосредованного управления группой программ через совместно используемые данные	Внешний нарушитель, внутренний нарушитель

1	2	3
9.26	Угроза отключения контрольных датчиков	Внешний нарушитель, внутренний нарушитель, носитель вредоносной программы
9.27	Угроза ошибки обновления гипервизора	Внутренний нарушитель
9.28	Угроза перебора всех настроек и параметров приложения	Внешний нарушитель, внутренний нарушитель
9.29	Угроза передачи запрещенных команд на оборудование с числовым программным управлением	Внутренний нарушитель, носитель вредоносной программы
9.30	Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники	Внешний нарушитель, внутренний нарушитель, носитель вредоносной программы
9.31	Угроза переполнения целочисленных переменных	Внешний нарушитель, внутренний нарушитель
9.32	Угроза перехвата вводимой и выводимой на периферийные устройства информации	Внешний нарушитель, внутренний нарушитель
9.33	Угроза перехвата привилегированного потока	Внешний нарушитель, внутренний нарушитель
9.34	Угроза перехвата привилегированного процесса	Внешний нарушитель, внутренний нарушитель, носитель вредоносной программы
9.35	Угроза повышения привилегий	Внешний нарушитель, внутренний нарушитель
9.36	Угроза подделки записей журнала регистрации событий	Внешний нарушитель, внутренний нарушитель
9.37	Угроза потери и утечки данных, обрабатываемых в облаке	Внутренний нарушитель
9.38	Угроза приостановки оказания облачных услуг вследствие технических сбоев	Носитель вредоносной программы
9.39	Угроза пропуска проверки целостности программного обеспечения	Внешний нарушитель, внутренний нарушитель
9.10	Угроза удаления аутентификационной информации	Внешний нарушитель, внутренний нарушитель
9.41	Угроза эксплуатации цифровой подписи программного кода	Внешний нарушитель, внутренний нарушитель
9.42	Угроза перехвата исключения/сигнала из привилегированного блока функций	Внешний нарушитель, внутренний нарушитель, носитель вредоносной программы
9.43	Угроза неподтвержденного ввода данных оператором в систему, связанную с безопасностью	Внутренний нарушитель
9.44	Угроза несанкционированного использования системных и сетевых утилит	Внешний нарушитель, внутренний нарушитель
9.45	Угроза маскирования действий вредоносного кода	Внешний нарушитель, носитель вредоносной программы
10	**Угрозы эксплуатации уязвимостей средств защиты информации**	
10.1	Угроза анализа криптографических алгоритмов и их реализации	Внешний нарушитель
10.2	Угроза использования информации идентификации/аутентификации, заданной по умолчанию	Внешний нарушитель, внутренний нарушитель

1	2	3
10.3	Угроза нарушения технологического/ производственного процесса из-за временных задержек, вносимых средством защиты	Внешний нарушитель
10.4	Угроза несанкционированного изменения параметров настройки средств защиты информации	Внешний нарушитель, внутренний нарушитель
10.5	Угроза несанкционированного воздействия на средство защиты информации	Внешний нарушитель, внутренний нарушитель
11	**Угрозы, обеспечивающие доступ к мобильным устройствам**	
11.1	Угроза агрегирования данных, обрабатываемых с помощью мобильного устройства	Внутренний нарушитель
11.2	Угроза несанкционированного использования привилегированных функций мобильного устройства	Внешний нарушитель
12	**Угрозы, позволяющие внести изменения в состав программных или аппаратных средств ИСПДн**	
12.1	Угроза воздействия на программы с высокими привилегиями	Внешний нарушитель, внутренний нарушитель, носитель вредоносной программы
12.2	Угроза выхода процесса за пределы виртуальной машины	Внешний нарушитель, внутренний нарушитель, носитель вредоносной программы
12.3	Угроза длительного удержания вычислительных ресурсов пользователями	Внешний нарушитель, внутренний нарушитель
12.4	Угроза изменения компонентов системы	Внутренний нарушитель
12.5	Угроза исчерпания вычислительных ресурсов хранилища больших данных	Внутренний нарушитель
12.6	Угроза неконтролируемого роста числа зарезервированных вычислительных ресурсов	Внешний нарушитель, внутренний нарушитель
12.7	Угроза несанкционированного удаленного внеполосного доступа к аппаратным средствам	Внешний нарушитель, носитель вредоносной программы
12.8	Угроза потери информации вследствие несогласованности работы узлов хранилища больших данных	Внутренний нарушитель
12.9	Угроза приведения системы в состояние «отказ в обслуживании»	Внешний нарушитель, внутренний нарушитель
12.10	Угроза сбоя автоматического управления системой разграничения доступа хранилища больших данных	Носитель вредоносной программы
12.11	Угроза усиления воздействия на вычислительные ресурсы пользователей при помощи сторонних серверов	Внешний нарушитель, внутренний нарушитель
12.12	Угроза утраты вычислительных ресурсов	Внешний нарушитель, внутренний нарушитель
12.13	Угроза утечки информации за счет применения вредоносным программным обеспечением алгоритмов шифрования графика	Внешний нарушитель, носитель вредоносной программы
13	**Угрозы, связанные с использованием облачных услуг**	
13.1	Угроза злоупотребления возможностями, предоставленными потребителям облачных услуг	Внутренний нарушитель

1	2	3
13.2	Угроза несогласованности политик безопасности элементов облачной инфраструктуры	Внешний нарушитель, внутренний нарушитель
13.3	Угроза потери управления собственной инфраструктурой при переносе ее в облако	Внутренний нарушитель
13.4	Угроза привязки к поставщику облачных услуг	Внутренний нарушитель
13.5	Угроза недобросовестного исполнения обязательств поставщиками облачных услуг	Внешний нарушитель
13.6	Угроза злоупотребления доверием потребителей облачных услуг	Внешний нарушитель
13.7	Угроза некачественного переноса инфраструктуры в облако	Внешний нарушитель
13.8	Угроза конфликта юрисдикций различных стран	Внешний нарушитель
13.9	Угроза нарушения доступности облачного сервера	Внешний нарушитель, внутренний нарушитель
13.10	Угроза невозможности миграции образов виртуальных машин из-за несовместимости аппаратного и программного обеспечения	Внешний нарушитель
13.11	Угроза незащищенного администрирования облачных услуг	Внешний нарушитель, внутренний нарушитель
13.12	Угроза неопределенности ответственности за обеспечение безопасности облака	Внешний нарушитель
13.13	Угроза непрерывной модернизации облачной инфраструктуры	Внутренний нарушитель
13.14	Угроза общедоступности облачной инфраструктуры	Внешний нарушитель
13.15	Угроза потери доверия к поставщику облачных услуг	Внутренний нарушитель
13.16	Угроза потери управления облачными ресурсами	Внешний нарушитель
13.17	Угроза распространения состояния «отказ в обслуживании» в облачной инфраструктуре	Внешний нарушитель, внутренний нарушитель
14	**Угрозы, связанные с использованием сетевых технологий**	
14.1	Угроза доступа к локальным файлам сервера при помощи URL	Внешний нарушитель
14.2	Угроза заражения DNS-кеша	Внешний нарушитель, носитель вредоносной программы
14.3	Угроза искажения XML-схемы	Внешний нарушитель, внутренний нарушитель
14.4	Угроза использования альтернативных путей доступа к ресурсам	Внешний нарушитель, внутренний нарушитель
14.5	Угроза межсайтового скриптинга	Внешний нарушитель
14.6	Угроза межсайтовой подделки запроса	Внешний нарушитель, носитель вредоносной программы
14.7	Угроза нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия	Внешний нарушитель, внутренний нарушитель
14.8	Угроза нарушения целостности данных кеша	Внешний нарушитель, внутренний нарушитель

1	2	3
14.9	Угроза некорректного задания структуры данных транзакции	Внутренний нарушитель
14.10	Угроза некорректного использования прозрачного прокси-сервера за счет плагинов браузера	Внешний нарушитель
14.11	Угроза неправомерных действий в каналах связи	Внешний нарушитель, носитель вредоносной программы
14.12	Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети	Внешний нарушитель, внутренний нарушитель
14.13	Угроза несанкционированного доступа к виртуальным каналам передачи	Внешний нарушитель, внутренний нарушитель
14.14	Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб	Внешний нарушитель
14.15	Угроза обнаружения хостов	Внешний нарушитель
14.16	Угроза определения типов объектов защиты	Внешний нарушитель
14.17	Угроза определения топологии вычислительной сети	Внешний нарушитель
14.18	Угроза передачи данных по скрытым каналам	Внешний нарушитель, внутренний нарушитель
14.19	Угроза перехвата данных, передаваемых по вычислительной сети	Внешний нарушитель
14.20	Угроза подмены доверенного пользователя	Внешний нарушитель, носитель вредоносной программы
14.21	Угроза получения предварительной информации об объекте защиты	Внешний нарушитель
14.22	Угроза сканирования веб-сервисов, разработанных на основе языка описания WSDL	Внешний нарушитель, носитель вредоносной программы
14.23	Угроза форсированного веб-браузинга	Внешний нарушитель
14.24	Угроза заражения компьютера при посещении неблагонадежных сайтов	Внутренний нарушитель, носитель вредоносной программы
14.25	Угроза «кражи» учетной записи доступа к сетевым сервисам	Внешний нарушитель
14.26	Угроза скрытного включения вычислительного устройства в состав бот-сети	Внешний нарушитель, носитель вредоносной программы
14.27	Угроза распространения «почтовых червей»	Внешний нарушитель, носитель вредоносной программы
14.28	Угроза спама веб-сервера	Внешний нарушитель, носитель вредоносной программы
14.29	Угроза фарминга	Внешний нарушитель
14.30	Угроза фишинга	Внешний нарушитель, носитель вредоносной программы
14.31	Угроза перехвата одноразовых паролей в режиме реального времени	Внешний нарушитель, носитель вредоносной программы
14.32	Угроза внедрения вредоносного кода через рекламу, сервисы и контент	Внутренний нарушитель, носитель вредоносной программы
14.33	Угроза внедрения вредоносного кода за счет посещения зараженных сайтов в сети «Интернет»	Внешний нарушитель, носитель вредоносной программы

1	2	3
15	**Угрозы, связанные с использованием технологий виртуализации**	
15.1	Угроза нарушения изоляции пользовательских данных внутри виртуальной машины	Внешний нарушитель, внутренний нарушитель
15.2	Угроза нарушения технологии обработки информации путем несанкционированного внесения изменений в образы виртуальных машин	Внешний нарушитель, внутренний нарушитель
15.3	Угроза несанкционированного доступа к хранимой в виртуальном пространстве защищаемой информации	Внешний нарушитель, внутренний нарушитель
15.4	Угроза неконтролируемого роста числа виртуальных машин	Внешний нарушитель, внутренний нарушитель
15.5	Угроза перехвата управления средой виртуализации	Внешний нарушитель, внутренний нарушитель
15.6	Угроза перехвата управления гипервизором	Внешний нарушитель, внутренний нарушитель
15.7	Угроза несанкционированного доступа к гипервизору из виртуальной машины и (или) физической сети	Внешний нарушитель, внутренний нарушитель
15.8	Угроза несанкционированного доступа к данным за пределами зарезервированного адресного пространства, в том числе выделенного под виртуальное аппаратное обеспечение	Внешний нарушитель, внутренний нарушитель
15.9	Угроза несанкционированного доступа к защищаемым виртуальным машинам из виртуальной и (или) физической сети	Внешний нарушитель, внутренний нарушитель
15.10	Угроза несанкционированного доступа к защищаемым виртуальным машинам со стороны других виртуальных машин	Внешний нарушитель, внутренний нарушитель
15.11	Угроза несанкционированного доступа к защищаемым виртуальным устройствам из виртуальной и (или) физической сети	Внешний нарушитель, внутренний нарушитель
15.12	Угроза несанкционированного доступа к системе хранения данных из виртуальной и (или) физической сети	Внешний нарушитель, внутренний нарушитель
16	**Угрозы, связанные с нарушением правил эксплуатации машинных носителей**	
16.1	Угроза доступа к защищаемым файлам с использованием обходного пути	Внешний нарушитель, внутренний нарушитель
16.2	Угроза несанкционированного копирования защищаемой информации	Внешний нарушитель, внутренний нарушитель
16.3	Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	Внешний нарушитель, внутренний нарушитель
16.4	Угроза утраты носителей информации	Внутренний нарушитель
16.5	Угроза форматирования носителей информации	Внешний нарушитель, внутренний нарушитель
16.6	Угроза неправомерного шифрования информации	Внешний нарушитель, носитель вредоносной программы

1	2	3
16.7	Угроза несанкционированной модификации защищаемой информации	Внешний нарушитель, внутренний нарушитель, носитель вредоносной программы
17	**Угрозы, связанные с предоставлением доступа к беспроводным каналам передачи данных**	
17.1	Угроза деавторизации санкционированного клиента беспроводной сети	Внешний нарушитель, внутренний нарушитель
17.2	Угроза несанкционированного доступа к системе по беспроводным каналам	Внешний нарушитель
17.3	Угроза подключения к беспроводной сети в обход процедуры аутентификации	Внешний нарушитель
17.4	Угроза подмены беспроводного клиента или точки доступа	Внешний нарушитель
17.5	Угроза получения сведений о владельце беспроводного устройства	Внешний нарушитель