ЧĂВАШ РЕСПУБЛИКИН МИНИСТРСЕН КАБИНЕЧĔ

ЙЫШĂНУ

27.12.2017 543 №

Шупашкар хули

КАБИНЕТ МИНИСТРОВ ЧУВАШСКОЙ РЕСПУБЛИКИ

ПОСТАНОВЛЕНИЕ

27.12.2017 № 543

г. Чебоксары

Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых в органах исполнительной власти Чувашской Республики и подведомственных им организациях

В соответствии с частью 5 статьи 19 Федерального закона «О персональных данных» в целях обеспечения единого подхода к определению угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, Кабинет Министров Чувашской Республики п о с т а н о в л я е т:

1. Определить угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых в органах исполнительной власти Чувашской Республики и подведомственных им организациях (далее – угрозы), согласно приложению к настоящему постановлению.

2. Органам исполнительной власти Чувашской Республики:

определить угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых ими при осуществлении соответствующих видов деятельности, в соответствии с угрозами;

обеспечить определение подведомственными им организациями угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых ими при осуществлении соответствующих видов деятельности, в соответствии с угрозами.

3. Настоящее постановление вступает в силу через десять дней после дня его официального опубликования.

Председатель Кабинета Министров
Чувашской Республики – И.Моторин

Общий отдел № 1

Приложение
к постановлению Кабинета Министров
Чувашской Республики
от 27.12.2017 № 543

У Г Р О З Ы
безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых в органах исполнительной власти Чувашской Республики и подведомственных им организациях

I. Общие положения

1.1. Настоящий документ определяет перечень угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных (далее также – актуальная угроза безопасности персональных данных), эксплуатируемых в органах исполнительной власти Чувашской Республики (далее – орган исполнительной власти) и организациях, находящихся в их ведении (далее также соответственно – информационная система персональных данных, подведомственная организация), при осуществлении ими соответствующих видов деятельности, с учетом содержания персональных данных, характера и способов их обработки.

1.2. В настоящем документе не рассматриваются вопросы обеспечения безопасности персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну.

1.3. Настоящий документ предназначен для органов исполнительной власти и подведомственных организаций при решении ими следующих задач:

определение актуальных угроз безопасности персональных данных;

проведение анализа защищенности информационных систем персональных данных;

реализация мер по обеспечению безопасности персональных данных, направленных на нейтрализацию актуальных угроз безопасности персональных данных;

осуществление контроля за обеспечением уровня защищенности персональных данных.

1.4. При определении актуальных угроз безопасности персональных данных органы исполнительной власти и подведомственные организации разрабатывают модели угроз безопасности персональных данных для эксплуатируемых ими информационных систем персональных данных с учетом содержания персональных данных, характера и способов их обработки, условий и особенностей функционирования информационных систем персональных данных и совокупности условий и факторов, создающих актуальную опасность несанкционированного доступа к персональным данным, и применяют:

группы актуальных угроз безопасности персональных данных в информационных системах персональных данных, эксплуатируемых в органах исполнительной власти и подведомственных организациях, приведенные в разделе VI настоящего документа;

расширенный перечень угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых в органах исполнительной власти Чувашской Республики и подведомственных им организациях, приведенный в приложении № 1 к настоящему документу;

типовые возможности нарушителей безопасности информации и направления атак, приведенные в приложении № 2 к настоящему документу.

1.5. В настоящем документе дано описание:

категорий информационных систем персональных данных как объектов защиты;

объектов, защищаемых при определении актуальных угроз безопасности персональных данных в информационных системах персональных данных;

возможных источников угроз безопасности персональных данных, обрабатываемых в информационных системах персональных данных;

возможных видов неправомерных действий и деструктивных воздействий на персональные данные в информационных системах персональных данных;

основных способов реализации угроз безопасности персональных данных.

1.6. В настоящем документе используются термины и понятия, установленные федеральными законами «О связи», «Об информации, информационных технологиях и о защите информации», «О персональных данных», требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119.

II. Объекты защиты и технологии обработки персональных данных в информационных системах персональных данных

2.1. При обработке персональных данных в информационных системах персональных данных, эксплуатируемых в органах исполнительной власти и подведомственных организациях, объектами защиты являются:

персональные данные, обрабатываемые в информационных системах персональных данных;

информационные ресурсы информационных систем персональных данных;

технические средства информационных систем персональных данных и средства вычислительной техники, используемые для обработки персональных данных;

средства защиты информации;

средства криптографической защиты информации (далее – СКЗИ);

среда функционирования СКЗИ;

информация, относящаяся к криптографической защите персональных данных, включая ключевую, парольную и аутентифицирующую информацию СКЗИ;

документы, дела, журналы, картотеки, издания, технические документы, видео-, кино- и фотоматериалы, рабочие материалы и т.п., в которых отражена защищаемая информация, относящаяся к информационным системам персональных данных и их криптографической защите, включая документацию на СКЗИ и на технические и программные компоненты среды функционирования СКЗИ;

машинные носители информации, используемые в информационных системах персональных данных, в том числе носители защищаемой информации, используемые в процессе криптографической защиты персональных данных, носители ключевой, парольной и аутентифицирующей информации СКЗИ и порядок доступа к ним;

средства и системы связи и передачи данных, используемые для передачи персональных данных и иной информации при ее обработке в информационных системах персональных данных, в том числе каналы (линии) связи, включая кабельные системы, находящиеся в пределах контролируемой зоны органов исполнительной власти или подведомственных организаций;

помещения, в которых осуществляется обработка персональных данных или располагаются технические средства, используемые для обработки персональных данных;

помещения, в которых находятся ресурсы информационных систем персональных данных, имеющие отношение к криптографической защите персональных данных.

2.2. Технические средства информационных систем персональных данных размещаются в пределах контролируемой зоны органов исполнительной власти или подведомственных организаций, в которой исключено неконтролируемое пребывание лиц, а также использование посторонних технических средств.

Границы контролируемой зоны органа исполнительной власти или подведомственной организации устанавливаются соответствующим органом исполнительной власти или подведомственной организацией в зависимости от размещения используемых ими технических средств информационных систем персональных данных.

2.3. Информационно-телекоммуникационные сети органов исполнительной власти или подведомственных организаций или отдельные сегменты данных сетей (далее соответственно – локальная вычислительная сеть органа исполнительной власти, локальная вычислительная сеть подведомственной организации), к которым подключены технические средства информационных систем персональных данных, функционируют без подключения к иным информационно-телекоммуникационным сетям или имеют подключение к одной или нескольким информационно-телекоммуникационным сетям:

информационно-телекоммуникационным сетям операторов связи, в том числе информационно-телекоммуникационной сети «Интернет» (далее – сеть «Интернет»);

корпоративной сети передачи данных органов исполнительной власти;

иным информационно-телекоммуникационным сетям организаций, расположенных на территории Российской Федерации.

2.4. В зависимости от используемых технологий и характеристик среды передачи данных подключение к информационно-телекоммуникационным сетям осуществляется с использованием проводных или беспроводных каналов связи.

2.5. Подключение к корпоративной сети передачи данных органов исполнительной власти иных информационно-телекоммуникационных сетей, отдельных их сегментов или средств вычислительной техники, участвующих в обработке персональных данных и взаимодействующих с сетью «Интернет», осуществляется по защищенным каналам связи с использованием сертифицированных по требованиям безопасности информации средств защиты информации и

СКЗИ, обеспечивающих защиту локальных вычислительных сетей органов исполнительной власти и локальных вычислительных сетей подведомственных организаций от несанкционированного доступа и криптографическую защиту информации при ее передаче по информационно-телекоммуникационным сетям, в том числе сети «Интернет».

2.6. Подключение локальных вычислительных сетей органов исполнительной власти и локальных вычислительных сетей подведомственных организаций к сети «Интернет» осуществляется органами исполнительной власти и подведомственными организациями при условии соблюдения ими мер по обеспечению безопасности персональных данных, в том числе мер по защите информационных систем персональных данных, средств и систем связи и передачи данных.

2.7. Технические средства информационных систем персональных данных и средства вычислительной техники, используемые для обработки персональных данных, состоят из одного или нескольких нижеперечисленных элементов:

2.7.1. Автоматизированное рабочее место, представляющее собой программно-аппаратный комплекс, позволяющий производить локальную обработку информации, в том числе персональных данных, без подключения данного комплекса к информационно-телекоммуникационным сетям или с использованием подключения к информационным ресурсам информационных систем персональных данных по информационно-телекоммуникационным сетям.

2.7.2. Терминальная станция, представляющая собой программно-аппаратный комплекс, позволяющий производить обработку информации, в том числе персональных данных, с использованием технологий удаленного доступа к информационным ресурсам информационных систем персональных данных по информационно-телекоммуникационным сетям и не предназначенный для локального хранения обрабатываемых персональных данных.

2.7.3. Технические средства, обеспечивающие функционирование серверов и входящего в их состав системного и прикладного программного обеспечения, систем управления базами данных и предназначенные для обработки и хранения персональных данных и иной информации (далее – серверное оборудование).

2.7.4. Средства и системы связи и передачи данных, используемые для передачи персональных данных и иной информации по информационно-телекоммуникационным сетям между серверным оборудованием, автоматизированными рабочими местами и терминальными станциями (далее – сетевое и телекоммуникационное оборудование).

2.7.5. Программное обеспечение, входящее в состав автоматизированных рабочих мест, терминальных станций, серверного оборудования, сетевого и телекоммуникационного оборудования и обеспечивающее их функционирование.

2.8. Ввод персональных данных в информационные системы персональных данных осуществляется как с бумажных носителей, так и с электронных носителей информации. Персональные данные выводятся из информационных систем персональных данных как в электронном, так и в бумажном виде с целью их использования, хранения и (или) передачи третьим лицам.

2.9. С целью осуществления своих полномочий органами исполнительной власти и подведомственными организациями, являющимися операторами в соответствии с Федеральным законом «О персональных данных» (далее – оператор), обрабатываются следующие категории персональных данных:

специальные категории персональных данных;

общедоступные персональные данные;

иные категории персональных данных, не относящихся к общедоступным, биометрическим или специальным категориям персональных данных (далее – иные категории персональных данных).

2.10. Для всех категорий персональных данных, обрабатываемых в информационных системах персональных данных, за исключением общедоступных персональных данных, требуется обеспечить следующие характеристики безопасности: конфиденциальность, целостность, доступность и подлинность информации. При обработке общедоступных персональных данных требуется обеспечить следующие характеристики безопасности: целостность, доступность и подлинность информации.

III. Общее описание информационных систем персональных данных, эксплуатируемых в органах исполнительной власти и подведомственных организациях при осуществлении ими соответствующих видов деятельности

3.1. Информационные системы персональных данных, эксплуатируемые в органах исполнительной власти и подведомственных организациях при осуществлении ими соответствующих видов деятельности, в зависимости от технологии обработки персональных данных, состава персональных данных и целей их обработки подразделяются на:

информационно-справочные информационные системы персональных данных;

сегментные информационные системы персональных данных;

республиканские информационные системы персональных данных;

ведомственные информационные системы персональных данных;

служебные информационные системы персональных данных.

3.2. В зависимости от технологии обработки персональных данных и используемого программного обеспечения информационные системы персональных данных подразделяются на:

информационные системы персональных данных, построенные на основе технологий использования «толстого клиента»;

информационные системы персональных данных, построенные на основе технологий использования «тонкого клиента» и веб-технологий;

информационные системы персональных данных, построенные на основе технологий удаленного доступа.

3.2.1. Информационные системы персональных данных, построенные на основе технологий использования «толстого клиента», характеризуются тем, что для обработки персональных данных в указанных информационных системах персональных данных используется установленное на автоматизированные рабочие места специальное прикладное программное обеспечение (далее – клиентское прикладное программное обеспечение), взаимодействующее с прикладным программным обеспечением, установленным на серверные компоненты информационной системы персональных данных (далее – серверное прикладное программное обеспечение), обеспечивающее прием персональных данных, обраба-

тываемых на автоматизированных рабочих местах, их обработку и хранение в базах данных информационной системы персональных данных.

В зависимости от технологий, реализованных в клиентском прикладном программном обеспечении, обработка персональных данных на автоматизированных рабочих местах может выполняться как с возможностью записи отдельных персональных данных или части базы данных на машинные носители информации, используемые на автоматизированных рабочих местах, так и без наличия такой возможности.

Доступ к базам данных информационной системы персональных данных или ее отдельным частям обеспечивается в соответствии с правами доступа, установленными в информационной системе персональных данных. Доступ к персональным данным, обрабатываемым локально с использованием клиентского прикладного программного обеспечения, обеспечивается в соответствии с правами доступа, установленными на автоматизированных рабочих местах.

3.2.2. Информационные системы персональных данных, построенные на основе использования «тонкого клиента» и веб-технологий, характеризуются тем, что для обработки персональных данных в указанных информационных системах персональных данных используется установленное на автоматизированные рабочие места прикладное программное обеспечение, позволяющее выполнять поиск и просмотр информации, размещенной на сайтах в информационно-телекоммуникационной сети, в том числе сети «Интернет» (далее – веб-браузер), и размещенных на сайте в информационно-телекоммуникационной сети сервисов информационной системы персональных данных, позволяющих с использованием веб-браузера и экранных форм сайта (далее – веб-интерфейс) выполнять обработку персональных данных и иной информации.

В зависимости от функциональных возможностей веб-интерфейса информационной системы персональных данных обработка персональных данных может выполняться как с возможностью выгрузки из информационной системы персональных данных отдельных персональных данных или части обрабатываемой базы данных на машинные носители информации, используемые на автоматизированных рабочих местах, так и без наличия такой возможности.

Доступ к веб-интерфейсу информационной системы персональных данных, базам данных информационной системы персональных данных или ее отдельным частям обеспечивается в соответствии с правами доступа, установленными в информационной системе персональных данных. Доступ к персональным данным, обрабатываемым локально на автоматизированных рабочих местах, обеспечивается в соответствии с правами доступа, установленными на автоматизированных рабочих местах.

3.2.3. Информационные системы персональных данных, построенные на основе технологий удаленного доступа, характеризуются тем, что для обработки персональных данных в указанных информационных системах персональных данных используются терминальные станции или автоматизированные рабочие места, подключенные к серверным компонентам информационной системы персональных данных по защищенным каналам связи с использованием технологии удаленного (терминального) доступа. Непосредственная обработка персональных данных выполняется с использованием серверного прикладного программного обеспечения. На терминальные станции и автоматизированные рабочие места передается только графическая информация. Базы данных, содержащие пер-

сональные данные, хранятся и обрабатываются на сервере, без их непосредственного хранения на терминальных станциях и автоматизированных рабочих местах. Доступ к базам данных информационной системы персональных данных или ее отдельным частям обеспечивается в соответствии с правами доступа, установленными в информационной системе персональных данных.

3.3. По архитектуре построения информационные системы персональных данных подразделяются на:

сегментированные информационные системы персональных данных;

централизованные информационные системы персональных данных;

смешанные информационные системы персональных данных;

одноуровневые информационные системы персональных данных.

3.3.1. Сегментированные информационные системы персональных данных состоят из центрального сегмента и взаимодействующих с ним периферийных сегментов информационной системы персональных данных.

Технические средства центрального сегмента информационной системы персональных данных включают в себя телекоммуникационное и серверное оборудование, с использованием которого обеспечиваются взаимодействие с периферийными сегментами, а также централизованный сбор и обработка персональных данных и иной информации, получаемой от периферийных сегментов.

Технические средства периферийных сегментов информационной системы персональных данных включают в себя телекоммуникационное и серверное оборудование, с использованием которого обеспечивается централизованный сбор персональных данных и иной информации, обрабатываемой на автоматизированных рабочих местах или терминальных станциях.

3.3.2. Централизованные информационные системы персональных данных состоят из центрального сегмента и непосредственно взаимодействующих с ним автоматизированных рабочих мест или терминальных станций.

Технические средства центрального сегмента информационной системы персональных данных включают в себя телекоммуникационное и серверное оборудование, с использованием которого обеспечивается централизованный сбор персональных данных и иной информации, обрабатываемой на автоматизированных рабочих местах или терминальных станциях.

3.3.3. Смешанные информационные системы персональных данных построены на основе архитектуры сегментированных информационных систем персональных данных. В данном случае центральный сегмент информационной системы персональных данных взаимодействует как с периферийными сегментами, так и с автоматизированными рабочими местами или терминальными станциями.

3.3.4. Одноуровневые информационные системы персональных данных характеризуются тем, что не имеют центральных и периферийных сегментов и персональные данные обрабатываются непосредственно на автоматизированных рабочих местах.

3.4. По структуре информационные системы персональных данных в зависимости от их территориального размещения подразделяются на локальные информационные системы персональных данных и распределенные информационные системы персональных данных.

3.4.1. Распределенные информационные системы персональных данных характеризуются тем, что технические средства информационных систем персо-

нальных данных размещаются в пределах нескольких зданий, расположенных в одном или нескольких населенных пунктах.

3.4.2. Локальные информационные системы персональных данных характеризуются тем, что технические средства информационных систем персональных данных размещаются в пределах одного здания.

IV. Информационные системы персональных данных

4.1. Информационно-справочные информационные системы персональных данных.

4.1.1. Информационно-справочные информационные системы персональных данных предназначены для обработки общедоступных персональных данных и иной информации, в том числе подлежащей размещению в сети «Интернет» в соответствии с законодательством Российской Федерации и законодательством Чувашской Республики.

4.1.2. К информационно-справочным информационным системам персональных данных относятся порталы, сайты или страницы сайтов в сети «Интернет» органов исполнительной власти или подведомственных организаций, содержащие общедоступные персональные данные.

4.1.3. Режим обработки персональных данных в информационно-справочных информационных системах персональных данных – многопользовательский с разграничением прав доступа.

В целях обеспечения поиска и получения общедоступных персональных данных и иной информации, размещенной в информационно-справочных информационных системах персональных данных, доступ к указанной информации и общедоступным персональным данным предоставляется неограниченному кругу лиц.

4.1.4. Информационно-справочные информационные системы персональных данных построены на основе технологий использования «тонкого клиента» и веб-технологий. Для обработки и размещения в сети «Интернет» общедоступных персональных данных и иной информации применяются веб-браузеры и веб-интерфейс сайта в сети «Интернет».

Доступ к веб-интерфейсу сайта в сети «Интернет» осуществляется в соответствии с правами доступа, установленными в информационной системе персональных данных.

4.1.5. По архитектуре построения информационно-справочные информационные системы персональных данных являются централизованными информационными системами персональных данных.

4.1.6. В информационно-справочных информационных системах персональных данных обрабатываются персональные данные сотрудников оператора и (или) субъектов персональных данных, не являющихся сотрудниками оператора.

4.1.7. Информационно-справочные информационные системы персональных данных по структуре являются локальными информационными системами персональных данных.

4.1.8. Автоматизированные рабочие места органов исполнительной власти или подведомственных организаций, с использованием которых осуществляется обработка персональных данных в информационно-справочных информа-

ционных системах персональных данных, размещаются в контролируемой зоне органов исполнительной власти или подведомственных организаций. Серверное, сетевое и телекоммуникационное оборудование размещается в контролируемой зоне органов исполнительной власти или подведомственных организаций и (или) в контролируемой зоне иных государственных органов и организаций, операторов связи, провайдеров хостинга или поставщиков «облачных» услуг, оказывающих услуги по предоставлению вычислительной мощности для размещения информации.

4.1.9. Информационно-справочные информационные системы персональных данных подключены к сетям связи общего пользования (сети «Интернет»). По типу подключения к сетям связи общего пользования (сети «Интернет») информационно-справочные информационные системы персональных данных подразделяются на:

подключенные с использованием корпоративной сети передачи данных органов исполнительной власти;

подключенные с использованием информационно-телекоммуникационных сетей операторов связи.

4.1.10. Технические средства информационно-справочных информационных систем персональных данных и средства вычислительной техники, используемые для обработки персональных данных:

автоматизированные рабочие места;

серверное оборудование;

сетевое и телекоммуникационное оборудование.

4.2. Сегментные информационные системы персональных данных.

4.2.1. Сегментные информационные системы персональных данных представляют собой сегменты федеральных информационных систем, создаваемые и эксплуатируемые органами исполнительной власти и используемые в органах исполнительной власти и (или) подведомственных организациях для обработки персональных данных и информационного взаимодействия с федеральными органами исполнительной власти или иными государственными органами.

Сегментные информационные системы персональных данных предназначены для исполнения функций органов исполнительной власти и (или) подведомственных организаций.

4.2.2. В сегментных информационных системах персональных данных обрабатываются специальные, общедоступные или иные категории персональных данных сотрудников оператора и (или) субъектов персональных данных, не являющихся сотрудниками оператора.

4.2.3. Режим обработки персональных данных в сегментных информационных системах персональных данных – многопользовательский с разграничением прав доступа.

4.2.4. В сегментных информационных системах персональных данных для обработки персональных данных применяются следующие технологии:

технологии на основе использования «толстого клиента»;

технологии на основе использования «тонкого клиента» и веб-технологий;

технологии использования удаленного доступа.

4.2.5. По архитектуре построения сегментные информационные системы персональных данных являются сегментированными информационными систе-

мами персональных данных или централизованными информационными системами персональных данных.

4.2.6. Сегментные информационные системы персональных данных по структуре являются локальными информационными системами персональных данных или распределенными информационными системами персональных данных.

4.2.7. Автоматизированные рабочие места органов исполнительной власти или подведомственных организаций, с использованием которых осуществляется обработка персональных данных в сегментных информационных системах персональных данных, размещаются в контролируемой зоне органов исполнительной власти или подведомственных организаций. При наличии регионального сегмента информационной системы персональных данных, взаимодействующего с центральным сегментом вышеуказанной информационной системы персональных данных, серверное оборудование, обеспечивающее функционирование регионального сегмента информационной системы персональных данных, размещается в контролируемой зоне органов исполнительной власти или подведомственных организаций, эксплуатирующих данное оборудование, и (или) в контролируемой зоне поставщика «облачных» услуг или юридического лица, определенного в соответствии с Федеральным законом «Об информации, информационных технологиях и о защите информации» оператором информационной системы.

Технические средства, обеспечивающие функционирование центральных сегментов данных информационных систем персональных данных, размещаются вне контролируемой зоны органов исполнительной власти или подведомственных организаций.

4.2.8. В зависимости от наличия подключения к сетям связи общего пользования (сети «Интернет») сегментные информационные системы персональных данных подразделяются на:

подключенные к сетям связи общего пользования (сети «Интернет»);

не имеющие подключений к сетям связи общего пользования (сети «Интернет»). В данном случае передача персональных данных осуществляется с использованием машинных носителей информации.

По типу подключения к сетям связи общего пользования (сети «Интернет») сегментные информационные системы персональных данных подразделяются на:

подключенные с использованием корпоративной сети передачи данных органов исполнительной власти;

подключенные с использованием информационно-телекоммуникационных сетей операторов связи.

4.2.9. Информационный обмен между автоматизированными рабочими местами и региональным сегментом информационной системы персональных данных (при наличии) может осуществляться с использованием:

локальных вычислительных сетей органов исполнительной власти или локальных вычислительных сетей подведомственных организаций;

корпоративной сети передачи данных органов исполнительной власти;

сети связи общего пользования (сети «Интернет») и СКЗИ, обеспечивающих защиту информации при ее передаче по открытым каналам связи.

4.2.10. Информационный обмен между автоматизированными рабочими местами, региональным сегментом информационной системы персональных данных (при наличии) и ее центральным сегментом осуществляется с использованием сети связи общего пользования (сети «Интернет») и СКЗИ, обеспечивающих защиту информации при ее передаче по открытым каналам связи.

4.2.11. Технические средства сегментных информационных систем персональных данных и средства вычислительной техники, используемые для обработки персональных данных:

автоматизированные рабочие места;

терминальные станции;

серверное оборудование;

сетевое и телекоммуникационное оборудование.

4.3. Республиканские информационные системы персональных данных.

4.3.1. Республиканские информационные системы персональных данных представляют собой информационные системы персональных данных, создаваемые на основании законов Чувашской Республики, правовых актов органов исполнительной власти Чувашской Республики и эксплуатируемые с целью реализации полномочий и функций нескольких органов исполнительной власти и (или) подведомственных организаций.

4.3.2. По выполняемым функциям республиканские информационные системы персональных данных подразделяются на:

интеграционные республиканские информационные системы персональных данных;

многопрофильные республиканские информационные системы персональных данных;

специальные республиканские информационные системы персональных данных.

4.3.3. Интеграционные республиканские информационные системы персональных данных.

4.3.3.1. Интеграционные республиканские информационные системы персональных данных обеспечивают интеграцию и взаимодействие иных информационных систем персональных данных и функционируют исключительно в целях передачи данных между ними, в том числе персональных данных. Интеграционные республиканские информационные системы персональных данных характеризуются отсутствием пользователей, осуществляющих обработку персональных данных непосредственно в указанных информационных системах персональных данных, за исключением привилегированных пользователей, осуществляющих функции по администрированию данных информационных систем персональных данных.

4.3.3.2. В процессе передачи данных между иными информационными системами персональных данных в интеграционных республиканских информационных системах персональных данных обрабатываются специальные, общедоступные или иные категории персональных данных сотрудников оператора и (или) субъектов персональных данных, не являющихся сотрудниками оператора.

4.3.3.3. Непосредственная обработка персональных данных, передаваемых через интеграционные республиканские информационные системы персональных данных, осуществляется в иных информационных системах персональных данных, взаимодействующих с интеграционными республиканскими информа-

ционными системами персональных данных. Режим обработки персональных данных в интеграционных республиканских информационных системах персональных данных – многопользовательский с разграничением прав доступа.

4.3.3.4. В интеграционных республиканских информационных системах персональных данных для обработки персональных данных применяются технологии на основе использования «тонкого клиента» и веб-технологий.

4.3.3.5. По архитектуре построения интеграционные республиканские информационные системы персональных данных являются сегментированными информационными системами персональных данных или централизованными информационными системами персональных данных.

4.3.3.6. Интеграционные республиканские информационные системы персональных данных по структуре являются локальными информационными системами персональных данных или распределенными информационными системами персональных данных, функционирующими в контролируемой зоне органов исполнительной власти и (или) подведомственных организаций.

4.3.3.7. Интеграционные республиканские информационные системы персональных данных подключены к сетям связи общего пользования (сети «Интернет») с использованием защищенных каналов связи.

По типу подключения к сетям связи общего пользования (сети «Интернет») интеграционные республиканские информационные системы персональных данных подразделяются на:

подключенные с использованием корпоративной сети передачи данных органов исполнительной власти;

подключенные с использованием информационно-телекоммуникационных сетей операторов связи.

4.3.3.8. Интеграционные республиканские информационные системы персональных данных взаимодействуют с иными информационными системами персональных данных с использованием:

локальных вычислительных сетей органов исполнительной власти или локальных вычислительных сетей подведомственных организаций;

корпоративной сети передачи данных органов исполнительной власти;

сети связи общего пользования (сети «Интернет») и СКЗИ, обеспечивающих защиту информации при ее передаче по открытым каналам связи.

4.3.3.9. Технические средства интеграционных республиканских информационных систем персональных данных и средства вычислительной техники, используемые для обработки персональных данных:

автоматизированные рабочие места;

серверное оборудование;

сетевое и телекоммуникационное оборудование.

4.3.4. Многопрофильные республиканские информационные системы персональных данных.

4.3.4.1. Многопрофильные республиканские информационные системы персональных данных предназначены для централизованной автоматизации деятельности органов исполнительной власти, в том числе деятельности, связанной с ведением электронного делопроизводства и документооборота, учета корреспонденции, обращений граждан, обеспечения доступа к электронным документам в органах исполнительной власти.

4.3.4.2. В многопрофильных информационных системах персональных данных обрабатываются специальные, общедоступные или иные категории персональных данных сотрудников оператора и (или) субъектов персональных данных, не являющихся сотрудниками оператора.

4.3.4.3. Режим обработки персональных данных в многопрофильных республиканских информационных системах персональных данных – многопользовательский с разграничением прав доступа.

4.3.4.4. В многопрофильных республиканских информационных системах персональных данных для обработки персональных данных применяются следующие технологии:

технологии на основе использования «толстого клиента»;

технологии на основе использования «тонкого клиента» и веб-технологий.

4.3.4.5. По архитектуре построения многопрофильные республиканские информационные системы персональных данных являются централизованными информационными системами персональных данных или смешанными информационными системами персональных данных.

4.3.4.6. Многопрофильные республиканские информационные системы персональных данных по структуре являются локальными информационными системами персональных данных или распределенными информационными системами персональных данных, функционирующими в контролируемой зоне органов исполнительной власти.

4.3.4.7. В зависимости от наличия подключения к сетям связи общего пользования (сети «Интернет») многопрофильные республиканские информационные системы персональных данных подразделяются на:

подключенные к сетям связи общего пользования (сети «Интернет»);

не имеющие подключений к сетям связи общего пользования (сети «Интернет»). В данном случае передача персональных данных осуществляется с использованием машинных носителей информации.

По типу подключения к сетям связи общего пользования (сети «Интернет») многопрофильные республиканские информационные системы персональных данных подразделяются на:

подключенные с использованием корпоративной сети передачи данных органов исполнительной власти;

подключенные с использованием информационно-телекоммуникационных сетей операторов связи.

4.3.4.8. Многопрофильные республиканские информационные системы персональных данных взаимодействуют с иными информационными системами персональных данных с использованием:

локальных вычислительных сетей органов исполнительной власти;

корпоративной сети передачи данных органов исполнительной власти;

сети связи общего пользования (сети «Интернет») и СКЗИ, обеспечивающих защиту информации при ее передаче по открытым каналам связи.

4.3.4.9. Технические средства многопрофильных республиканских информационных систем персональных данных и средства вычислительной техники, используемые для обработки персональных данных:

автоматизированные рабочие места;

серверное оборудование;

сетевое и телекоммуникационное оборудование.

4.3.5. Специальные республиканские информационные системы персональных данных.

4.3.5.1. Специальные республиканские информационные системы персональных данных предназначены для автоматизации совместной деятельности органов исполнительной власти и (или) подведомственных организаций.

4.3.5.2. В специальных республиканских информационных системах персональных данных обрабатываются общедоступные или иные категории персональных данных сотрудников оператора и (или) субъектов персональных данных, не являющихся сотрудниками оператора.

4.3.5.3. Режим обработки персональных данных в специальных республиканских информационных системах персональных данных многопользовательский с разграничением прав доступа.

4.3.5.4. В специальных республиканских информационных системах персональных данных для обработки персональных данных применяются технологии на основе использования «тонкого клиента» и веб-технологий.

4.3.5.5. По архитектуре построения специальные республиканские информационные системы персональных данных являются централизованными информационными системами персональных данных.

4.3.5.6. Специальные республиканские информационные системы персональных данных по структуре являются локальными информационными системами персональных данных, функционирующими в контролируемой зоне органов исполнительной власти и (или) подведомственных организаций.

4.3.5.7. Специальные республиканские информационные системы персональных данных подключены к сетям связи общего пользования (сети «Интернет»).

По типу подключения к сетям связи общего пользования (сети «Интернет») специальные республиканские информационные системы персональных данных подразделяются на:

подключенные с использованием корпоративной сети передачи данных органов исполнительной власти;

подключенные с использованием информационно-телекоммуникационных сетей операторов связи.

4.3.5.8. Специальные республиканские информационные системы персональных данных взаимодействуют с иными информационными системами персональных данных с использованием:

локальных вычислительных сетей органов исполнительной власти или локальных вычислительных сетей подведомственных организаций;

корпоративной сети передачи данных органов исполнительной власти;

сети связи общего пользования (сети «Интернет») и СКЗИ, обеспечивающих защиту информации при ее передаче по открытым каналам связи.

4.3.5.9. Технические средства специальных республиканских информационных систем персональных данных и средства вычислительной техники, используемые для обработки персональных данных:

автоматизированные рабочие места;

серверное оборудование;

сетевое и телекоммуникационное оборудование.

4.4. Ведомственные информационные системы персональных данных.

4.4.1. Ведомственные информационные системы персональных данных представляют собой информационные системы персональных данных, создавае-

мые и эксплуатируемые на основании решения органа исполнительной власти в целях реализации его полномочий и исполнения функций органа исполнительной власти и (или) подведомственных организаций в определенной отраслевой сфере деятельности.

4.4.2. В ведомственных информационных системах персональных данных обрабатываются специальные, общедоступные или иные категории персональных данных сотрудников оператора и (или) субъектов персональных данных, не являющихся сотрудниками оператора.

4.4.3. Режим обработки персональных данных в ведомственных информационных системах персональных данных – многопользовательский с разграничением прав доступа.

4.4.4. В ведомственных информационных системах персональных данных для обработки персональных данных применяются следующие технологии:

технологии на основе использования «толстого клиента»;

технологии на основе использования «тонкого клиента» и веб-технологий.

4.4.5. По архитектуре построения ведомственные информационные системы персональных данных являются сегментированными информационными системами персональных данных, централизованными информационными системами персональных данных или смешанными информационными системами персональных данных.

4.4.6. Ведомственные информационные системы персональных данных по структуре являются локальными информационными системами персональных данных или распределенными информационными системами персональных данных, функционирующими в контролируемой зоне органов исполнительной власти и (или) подведомственных организаций.

4.4.7. В зависимости от наличия подключения к сетям связи общего пользования (сети «Интернет») ведомственные информационные системы персональных данных подразделяются на:

подключенные к сетям связи общего пользования (сети «Интернет»);

не имеющие подключений к сетям связи общего пользования (сети «Интернет»). В данном случае передача персональных данных осуществляется с использованием машинных носителей информации.

По типу подключения к сетям связи общего пользования (сети «Интернет») ведомственные информационные системы персональных данных подразделяются на:

подключенные с использованием корпоративной сети передачи данных органов исполнительной власти;

подключенные с использованием информационно-телекоммуникационных сетей операторов связи.

4.4.8. Ведомственные информационные системы персональных данных взаимодействуют с иными информационными системами персональных данных с использованием:

локальных вычислительных сетей органов исполнительной власти или локальных вычислительных сетей подведомственных организаций;

корпоративной сети передачи данных органов исполнительной власти;

сети связи общего пользования (сети «Интернет») и СКЗИ, обеспечивающих защиту информации при ее передаче по открытым каналам связи.

4.4.9. Технические средства ведомственных информационных систем персональных данных и средства вычислительной техники, используемые для обработки персональных данных:

автоматизированные рабочие места;

серверное оборудование;

сетевое и телекоммуникационное оборудование.

4.5. Служебные информационные системы персональных данных.

4.5.1. Служебные информационные системы персональных данных представляют собой информационные системы персональных данных, создаваемые и эксплуатируемые в органе исполнительной власти и (или) подведомственной организации в целях автоматизации типовых видов деятельности.

4.5.2. К основным служебным информационным системам персональных данных относятся:

информационные системы персональных данных бухгалтерского учета и управления финансами;

информационные системы персональных данных кадрового учета и управления персоналом;

информационные системы персональных данных документооборота и делопроизводства;

информационные системы персональных данных информационного обеспечения.

4.5.3. Информационные системы персональных данных бухгалтерского учета и управления финансами.

4.5.3.1. Информационные системы персональных данных бухгалтерского учета и управления финансами предназначены для автоматизации деятельности, связанной с ведением бухгалтерского учета и управлением финансами, представлением информации в налоговые органы и органы управления государственными внебюджетными фондами Российской Федерации.

4.5.3.2. В информационных системах персональных данных бухгалтерского учета и управления финансами обрабатываются иные категории персональных данных сотрудников оператора и (или) субъектов персональных данных, не являющихся сотрудниками оператора.

4.5.3.3. Режим обработки персональных данных в информационных системах персональных данных бухгалтерского учета и управления финансами – многопользовательский с разграничением прав доступа.

4.5.3.4. В информационных системах персональных данных бухгалтерского учета и управления финансами для обработки персональных данных используются следующие технологии:

технологии на основе использования «толстого клиента»;

технологии на основе использования «тонкого клиента» и веб-технологий.

4.5.3.5. По архитектуре построения информационные системы персональных данных бухгалтерского учета и управления финансами являются централизованными информационными системами персональных данных или одноуровневыми информационными системами персональных данных.

4.5.3.6. Информационные системы персональных данных бухгалтерского учета и управления финансами по структуре являются локальными информационными системами персональных данных, функционирующими в контролируемой зоне органов исполнительной власти или подведомственных организаций.

4.5.3.7. В зависимости от наличия подключения к сетям связи общего пользования (сети «Интернет») информационные системы персональных данных бухгалтерского учета и управления финансами подразделяются на:

подключенные к сетям связи общего пользования (сети «Интернет»);

не имеющие подключений к сетям связи общего пользования (сети «Интернет»). В данном случае передача персональных данных осуществляется с использованием машинных носителей информации.

По типу подключения к сетям связи общего пользования (сети «Интернет») информационные системы персональных данных бухгалтерского учета и управления финансами подразделяются на:

подключенные с использованием корпоративной сети передачи данных органов исполнительной власти;

подключенные с использованием информационно-телекоммуникационных сетей операторов связи.

4.5.3.8. Информационные системы персональных данных бухгалтерского учета и управления финансами взаимодействуют с иными информационными системами персональных данных с использованием:

локальных вычислительных сетей органов исполнительной власти или локальных вычислительных сетей подведомственных организаций;

корпоративной сети передачи данных органов исполнительной власти;

сети связи общего пользования (сети «Интернет») и СКЗИ, обеспечивающих защиту информации при ее передаче по открытым каналам связи.

4.5.3.9. Технические средства информационных систем персональных данных бухгалтерского учета и управления финансами и средства вычислительной техники, используемые для обработки персональных данных:

автоматизированные рабочие места;

серверное оборудование;

сетевое и телекоммуникационное оборудование.

4.5.4. Информационные системы персональных данных кадрового учета и управления персоналом.

4.5.4.1. Информационные системы персональных данных кадрового учета и управления персоналом предназначены для автоматизации деятельности, связанной с ведением кадрового делопроизводства, учета и управления персоналом.

4.5.4.2. В информационных системах персональных данных кадрового учета и управления персоналом обрабатываются специальные, общедоступные или иные категории персональных данных сотрудников оператора и (или) субъектов персональных данных, не являющихся сотрудниками оператора.

4.5.4.3. Режим обработки персональных данных в информационных системах персональных данных кадрового учета и управления персоналом многопользовательский с разграничением прав доступа.

4.5.4.4. В информационных системах персональных данных кадрового учета и управления персоналом для обработки персональных данных используются следующие технологии:

технологии на основе использования «толстого клиента»;

технологии на основе использования «тонкого клиента» и веб-технологий;

технологии на основе использования удаленного доступа.

4.5.4.5. По архитектуре построения информационные системы персональных данных кадрового учета и управления персоналом являются централизован-

ными информационными системами персональных данных или одноуровневыми информационными системами персональных данных.

4.5.4.6. Информационные системы персональных данных кадрового учета и управления персоналом по структуре являются локальными информационными системами персональных данных, функционирующими в контролируемой зоне органов исполнительной власти или подведомственных организаций.

4.5.4.7. В зависимости от наличия подключения к сетям связи общего пользования (сети «Интернет») информационные системы персональных данных кадрового учета и управления персоналом подразделяются на:

подключенные к сетям связи общего пользования (сети «Интернет»);

не имеющие подключений к сетям связи общего пользования (сети «Интернет»). В данном случае передача персональных данных осуществляется с использованием машинных носителей информации.

По типу подключения к сетям связи общего пользования (сети «Интернет») информационные системы персональных данных кадрового учета и управления персоналом подразделяются на:

подключенные с использованием корпоративной сети передачи данных органов исполнительной власти;

подключенные с использованием информационно-телекоммуникационных сетей операторов связи.

4.5.4.8. Информационные системы персональных данных кадрового учета и управления персоналом взаимодействуют с иными информационными системами персональных данных с использованием:

локальных вычислительных сетей органов исполнительной власти или локальных вычислительных сетей подведомственных организаций;

корпоративной сети передачи данных органов исполнительной власти;

сети связи общего пользования (сети «Интернет») и СКЗИ, обеспечивающих защиту информации при ее передаче по открытым каналам связи.

4.5.4.9. Технические средства информационных систем персональных данных кадрового учета и управления персоналом и средства вычислительной техники, используемые для обработки персональных данных:

автоматизированные рабочие места;

серверное оборудование;

сетевое и телекоммуникационное оборудование.

4.5.5. Информационные системы персональных данных документооборота и делопроизводства.

4.5.5.1. Информационные системы персональных данных документооборота и делопроизводства предназначены для автоматизации деятельности, связанной с ведением электронного документооборота и делопроизводства, учета обращений граждан в подведомственных организациях.

4.5.5.2. В информационных системах персональных данных документооборота и делопроизводства обрабатываются общедоступные или иные категории персональных данных сотрудников оператора и (или) субъектов персональных данных, не являющихся сотрудниками оператора.

4.5.5.3. Режим обработки персональных данных в информационных системах персональных данных документооборота и делопроизводства – многопользовательский с разграничением прав доступа.

4.5.5.4. В информационных системах персональных данных документооборота и делопроизводства для обработки персональных данных применяются технологии на основе использования «толстого клиента».

4.5.5.5. По архитектуре построения информационные системы персональных данных документооборота и делопроизводства являются централизованными информационными системами персональных данных или одноуровневыми информационными системами персональных данных.

4.5.5.6. Информационные системы персональных данных документооборота и делопроизводства по структуре являются локальными информационными системами персональных данных, функционирующими в контролируемой зоне подведомственной организации.

4.5.5.7. В зависимости от наличия подключения к сетям связи общего пользования (сети «Интернет») информационные системы персональных данных документооборота и делопроизводства подразделяются на:

подключенные к сетям связи общего пользования (сети «Интернет»);

не имеющие подключений к сетям связи общего пользования (сети «Интернет»). В данном случае передача персональных данных осуществляется с использованием машинных носителей информации.

По типу подключения к сетям связи общего пользования (сети «Интернет») информационные системы персональных данных документооборота и делопроизводства подразделяются на:

подключенные с использованием корпоративной сети передачи данных органов исполнительной власти;

подключенные с использованием информационно-телекоммуникационных сетей операторов связи.

4.5.5.8. Информационные системы персональных данных документооборота и делопроизводства взаимодействуют с иными информационными системами персональных данных с использованием:

локальных вычислительных сетей органов исполнительной власти или локальных вычислительных сетей подведомственных организаций;

корпоративной сети передачи данных органов исполнительной власти;

сети связи общего пользования (сети «Интернет») и СКЗИ, обеспечивающих защиту информации при ее передаче по открытым каналам связи.

4.5.5.9. Технические средства информационных систем персональных данных документооборота и делопроизводства и средства вычислительной техники, используемые для обработки персональных данных:

автоматизированные рабочие места;

серверное оборудование;

сетевое и телекоммуникационное оборудование.

4.5.6. Информационные системы персональных данных информационного обеспечения.

4.5.6.1. Информационные системы персональных данных информационного обеспечения предназначены для автоматизации деятельности, связанной с осуществлением сотрудниками органа исполнительной власти и (или) подведомственной организации своих функций и задач.

4.5.6.2. В информационных системах персональных данных информационного обеспечения обрабатываются общедоступные или иные категории пер-

сональных данных сотрудников оператора и (или) субъектов персональных данных, не являющихся сотрудниками оператора.

4.5.6.3. Режим обработки персональных данных в информационных системах персональных данных информационного обеспечения – многопользовательский с разграничением прав доступа.

4.5.6.4. В информационных системах персональных данных информационного обеспечения персональные данные обрабатываются на автоматизированных рабочих местах с использованием прикладного программного обеспечения общего пользования (текстовые или графические редакторы) или с применением технологии на основе использования «толстого клиента». В данном случае клиентское и серверное программное обеспечение устанавливается на автоматизированных рабочих местах.

4.5.6.5. По архитектуре построения информационные системы персональных данных информационного обеспечения являются одноуровневыми информационными системами персональных данных.

4.5.6.6. Информационные системы персональных данных информационного обеспечения по структуре являются локальными информационными системами персональных данных, функционирующими в контролируемой зоне органов исполнительной власти или подведомственных организаций.

4.5.6.7. В зависимости от наличия подключения к сетям связи общего пользования (сети «Интернет») информационные системы персональных данных информационного обеспечения подразделяются на:

подключенные к сетям связи общего пользования (сети «Интернет»);

не имеющие подключений к сетям связи общего пользования (сети «Интернет»). В данном случае передача персональных данных осуществляется с использованием машинных носителей информации.

По типу подключения к сетям связи общего пользования (сети «Интернет») информационные системы персональных данных информационного обеспечения подразделяются на:

подключенные с использованием корпоративной сети передачи данных органов исполнительной власти;

подключенные с использованием информационно-телекоммуникационных сетей операторов связи.

4.5.6.8. Информационные системы персональных данных информационного обеспечения не взаимодействуют с иными информационными системами персональных данных.

4.5.6.9. Технические средства информационных систем персональных данных информационного обеспечения и средства вычислительной техники, используемые для обработки персональных данных:

автоматизированные рабочие места;

сетевое и телекоммуникационное оборудование.

V. Угрозы безопасности персональных данных, выявленные при функционировании информационных систем персональных данных

5.1. Источники угроз безопасности персональных данных.

5.1.1. Источниками угроз безопасности персональных данных в информационных системах персональных данных выступают:

носитель вредоносной программы;

аппаратная закладка;

нарушитель безопасности информации.

5.1.2. Носитель вредоносной программы.

Носителем вредоносной программы может быть аппаратный элемент компьютера или программный контейнер. Если вредоносная программа не ассоциируется с какой-либо прикладной программой, то в качестве ее носителя рассматриваются:

отчуждаемый носитель (дискета, оптический диск, флэш-память, отчуждаемый винчестер и т.п.);

встроенные носители информации (винчестеры, микросхемы оперативной памяти, процессор, микросхемы системной платы, микросхемы устройств, встраиваемых в системный блок, – видеоадаптера, сетевой платы, звуковой платы, модема, устройств ввода/вывода магнитных жестких и оптических дисков, блока питания и т.п., микросхемы прямого доступа к памяти, шин передачи данных, портов ввода/вывода);

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

Если вредоносная программа ассоциируется с какой-либо прикладной программой, с файлами, имеющими определенные расширения или иные атрибуты, с сообщениями, передаваемыми по сети, то ее носителем являются:

пакеты передаваемых по компьютерной сети сообщений;

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

5.1.3. Аппаратная закладка.

Потенциально может рассматриваться возможность применения нарушителем безопасности информации аппаратных средств, предназначенных для скрытого съема информации, в том числе вводимой с клавиатуры (аппаратная закладка внутри клавиатуры, считывание данных с кабеля клавиатуры бесконтактным методом, включение устройства в разрыв кабеля, аппаратная закладка внутри системного блока и т.п.).

Технические средства информационных систем персональных данных размещаются в пределах контролируемой зоны органов исполнительной власти или подведомственных организаций в соответствии с пунктом 2.2 настоящего документа. Операторами обеспечивается режим безопасности, исключающий возможность неконтролируемого проникновения и пребывания посторонних лиц в помещениях, в которых осуществляется обработка персональных данных или располагаются технические средства информационных систем персональных данных, а также обеспечивается сохранность указанных технических средств и носителей защищаемой информации, в связи с чем отсутствуют объективные предпосылки для возможности применения нарушителем безопасности информации аппаратных средств, предназначенных для скрытого съема информации, и угрозы установки аппаратных закладок являются неактуальными и исключаются из числа рассматриваемых угроз безопасности персональных данных.

5.1.4. Нарушитель безопасности информации.

5.1.4.1. Под нарушителем безопасности информации (далее также – нарушитель) понимается физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персо-

нальных данных при их обработке в информационных системах персональных данных.

5.1.4.2. По наличию права постоянного или разового доступа в информационные системы персональных данных нарушители подразделяются на три типа:

внешний нарушитель, под которым понимается нарушитель, не имеющий права постоянного доступа в контролируемую зону органа исполнительной власти или подведомственной организации или имеющий право разового (контролируемого) доступа в указанную контролируемую зону, а также не имеющий доступа к техническим средствам и ресурсам информационных систем персональных данных, расположенным в пределах указанной контролируемой зоны, или имеющий ограниченный и контролируемый доступ к таким средствам и ресурсам. Внешний нарушитель может реализовывать угрозы безопасности персональных данных из внешних информационно-телекоммуникационных сетей, взаимодействующих с локальной вычислительной сетью органа исполнительной власти или локальной вычислительной сетью подведомственной организации, в которой функционирует информационная система персональных данных;

внутренний нарушитель, имеющий доступ к информационной системе персональных данных, под которым понимается нарушитель, имеющий право постоянного (периодического) доступа в контролируемую зону органа исполнительной власти или подведомственной организации, а также доступ к техническим средствам и ресурсам информационной системы персональных данных, расположенным в пределах указанной контролируемой зоны. Внутренний нарушитель, имеющий доступ к информационной системе персональных данных, может реализовывать угрозы безопасности персональных данных с использованием локальной вычислительной сети органа исполнительной власти или локальной вычислительной сети подведомственной организации и проводить атаки непосредственно на информационную систему персональных данных;

внутренний нарушитель, не имеющий доступа к информационной системе персональных данных, под которым понимается нарушитель, имеющий право постоянного (периодического) доступа в контролируемую зону органа исполнительной власти или подведомственной организации, но не имеющий доступа к техническим средствам и информационным ресурсам информационной системы персональных данных, расположенным в пределах указанной контролируемой зоны. Внутренний нарушитель, не имеющий доступа к информационной системе персональных данных, может реализовывать угрозы безопасности персональных данных с использованием локальной вычислительной сети органа исполнительной власти или локальной вычислительной сети подведомственной организации.

5.1.4.3. В зависимости от меры усилий, затрачиваемых нарушителем при реализации угроз безопасности персональных данных, различают низкий, средний и высокий потенциалы нарушителя.

Низкий потенциал нарушителя подразумевает наличие возможностей уровня физического лица по использованию специальных средств эксплуатации уязвимостей.

Средний потенциал нарушителя подразумевает наличие возможностей уровня группы физических лиц или организации по разработке и использованию специальных средств эксплуатации уязвимостей.

Высокий потенциал нарушителя подразумевает наличие возможностей уровня группы организаций по разработке и использованию специальных средств эксплуатации уязвимостей.

5.1.4.4. Типовые возможности нарушителей безопасности информации и направления атак приведены в приложении № 2 к настоящему документу.

5.2. Основные группы угроз безопасности персональных данных в информационных системах персональных данных.

5.2.1. Основными группами угроз безопасности персональных данных в информационных системах персональных данных являются:

угрозы утечки информации по техническим каналам;

угрозы использования штатных средств информационных систем персональных данных с целью совершения несанкционированного доступа к информации;

угрозы нарушения доступности информации;

угрозы нарушения целостности информации;

угрозы нарушения конфиденциальности информации;

угрозы недекларированных возможностей в системном или прикладном программном обеспечении;

угрозы, не являющиеся атаками;

угрозы несанкционированного доступа, создающие предпосылки для реализации несанкционированного доступа в результате нарушения процедуры авторизации и аутентификации;

угрозы несанкционированного доступа к информации в результате слабости процедур разграничения ролей и полномочий, правил управления доступом;

угрозы ошибок или внесения уязвимостей при проектировании, внедрении информационной системы персональных данных или системы защиты информационной системы персональных данных;

угрозы ошибочных или деструктивных действий лиц;

угрозы программно-математических воздействий;

угрозы, связанные с использованием «облачных» услуг;

угрозы, связанные с использованием технологий виртуализации;

угрозы, связанные с нарушением правил эксплуатации машинных носителей информации;

угрозы, связанные с нарушением процедур установки или обновления программного обеспечения и оборудования;

угрозы физического доступа к компонентам информационной системы персональных данных;

угрозы эксплуатации уязвимостей системного или прикладного программного обеспечения, средств защиты информации, СКЗИ, аппаратных компонентов информационной системы персональных данных, микропрограммного обеспечения;

угрозы, связанные с использованием сетевых технологий;

угрозы инженерной инфраструктуры;

угрозы, связанные с отсутствием системы регистрации событий информационной безопасности;

угрозы, связанные с контролем защищенности информационной системы персональных данных;

угрозы, связанные с перехватом защищаемой информации при ее передаче по каналам связи;

угрозы, связанные с использованием мобильных устройств.

5.2.2. Угрозы утечки информации по техническим каналам, в том числе угрозы утечки информации по каналам побочных электромагнитных излучений и наводок, угрозы утечки видовой информации и угрозы утечки акустической (речевой) информации, исключаются из числа рассматриваемых актуальных угроз безопасности персональных данных в связи со следующими факторами, отрицательно влияющими на вероятность реализации данных угроз:

органами исполнительной власти и подведомственными организациями принимаются организационные и технические меры по защите своей контролируемой зоны и обеспечению режима безопасности, исключающие возможность неконтролируемого проникновения и пребывания посторонних лиц в помещениях, в которых осуществляется обработка персональных данных или располагаются технические средства соответствующих информационных систем персональных данных, эксплуатируемых в органе исполнительной власти и подведомственной организации;

отсутствует необходимая мотивация нарушителя: техническая сложность реализации угроз безопасности персональных данных, связанных с утечками информации по техническим каналам, а также стоимость технических средств, необходимых для реализации данных угроз, не сопоставимы с результатом, полученным от их реализации, с учетом объема и содержания персональных данных, доступ к которым может получить нарушитель.

VI. Актуальные угрозы безопасности персональных данных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых в органах исполнительной власти и подведомственных организациях

6.1. В настоящем разделе документа приведены группы актуальных угроз безопасности персональных данных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых в органах исполнительной власти и подведомственных организациях, в соответствии с основными группами угроз безопасности персональных данных в информационных системах персональных данных, указанными в пункте 5.2 настоящего документа, с учетом содержания персональных данных, характера и способов их обработки в информационных системах персональных данных, приведенных в разделе IV настоящего документа.

6.2. В информационно-справочных информационных системах персональных данных актуальными угрозами безопасности персональных данных являются угрозы, включенные в следующие группы:

угрозы использования штатных средств информационных систем персональных данных с целью совершения несанкционированного доступа к информации;

угрозы нарушения доступности информации;

угрозы нарушения целостности информации;

угрозы нарушения конфиденциальности информации;

угрозы недекларированных возможностей в системном или прикладном программном обеспечении;

угрозы, не являющиеся атаками;

угрозы несанкционированного доступа, создающие предпосылки для реализации несанкционированного доступа в результате нарушения процедуры авторизации и аутентификации;

угрозы несанкционированного доступа к информации в результате слабости процедур разграничения ролей и полномочий, правил управления доступом;

угрозы ошибок или внесения уязвимостей при проектировании, внедрении информационной системы персональных данных или системы защиты информационной системы персональных данных;

угрозы ошибочных или деструктивных действий лиц;

угрозы программно-математических воздействий;

угрозы, связанные с использованием «облачных» услуг;

угрозы, связанные с использованием технологий виртуализации;

угрозы, связанные с нарушением процедур установки или обновления программного обеспечения и оборудования;

угрозы физического доступа к компонентам информационной системы персональных данных;

угрозы эксплуатации уязвимостей системного или прикладного программного обеспечения, средств защиты информации, СКЗИ, аппаратных компонентов информационной системы персональных данных, микропрограммного обеспечения;

угрозы, связанные с использованием сетевых технологий;

угрозы инженерной инфраструктуры;

угрозы, связанные с отсутствием системы регистрации событий информационной безопасности;

угрозы, связанные с контролем защищенности информационной системы персональных данных;

угрозы, связанные с перехватом защищаемой информации при ее передаче по каналам связи;

угрозы, связанные с использованием мобильных устройств.

6.3. В сегментных информационных системах персональных данных актуальными угрозами безопасности персональных данных являются угрозы, включенные в следующие группы:

угрозы использования штатных средств информационных систем персональных данных с целью совершения несанкционированного доступа к информации;

угрозы нарушения доступности информации;

угрозы нарушения целостности информации;

угрозы нарушения конфиденциальности информации;

угрозы недекларированных возможностей в системном или прикладном программном обеспечении;

угрозы, не являющиеся атаками;

угрозы несанкционированного доступа, создающие предпосылки для реализации несанкционированного доступа в результате нарушения процедуры авторизации и аутентификации;

угрозы несанкционированного доступа к информации в результате слабости процедур разграничения ролей и полномочий, правил управления доступом;

угрозы ошибок или внесения уязвимостей при проектировании, внедрении информационной системы персональных данных или системы защиты информационной системы персональных данных;

угрозы ошибочных или деструктивных действий лиц;

угрозы программно-математических воздействий;

угрозы, связанные с использованием технологий виртуализации;

угрозы, связанные с нарушением правил эксплуатации машинных носителей информации;

угрозы, связанные с нарушением процедур установки или обновления программного обеспечения и оборудования;

угрозы физического доступа к компонентам информационной системы персональных данных;

угрозы эксплуатации уязвимостей системного или прикладного программного обеспечения, средств защиты информации, СКЗИ, аппаратных компонентов информационной системы персональных данных, микропрограммного обеспечения;

угрозы, связанные с использованием сетевых технологий;

угрозы инженерной инфраструктуры;

угрозы, связанные с отсутствием системы регистрации событий информационной безопасности;

угрозы, связанные с контролем защищенности информационной системы персональных данных;

угрозы, связанные с перехватом защищаемой информации при ее передаче по каналам связи.

6.4. Республиканские информационные системы персональных данных.

6.4.1. В интеграционных республиканских информационных системах персональных данных актуальными угрозами безопасности персональных данных являются угрозы, включенные в следующие группы:

угрозы использования штатных средств информационных систем персональных данных с целью совершения несанкционированного доступа к информации;

угрозы нарушения доступности информации;

угрозы нарушения целостности информации;

угрозы нарушения конфиденциальности информации;

угрозы недекларированных возможностей в системном или прикладном программном обеспечении;

угрозы, не являющиеся атаками;

угрозы несанкционированного доступа, создающие предпосылки для реализации несанкционированного доступа в результате нарушения процедуры авторизации и аутентификации;

угрозы несанкционированного доступа к информации в результате слабости процедур разграничения ролей и полномочий, правил управления доступом;

угрозы ошибок или внесения уязвимостей при проектировании, внедрении информационной системы персональных данных или системы защиты информационной системы персональных данных;

угрозы ошибочных или деструктивных действий лиц;

угрозы программно-математических воздействий;

угрозы, связанные с использованием технологий виртуализации;

угрозы, связанные с нарушением процедур установки или обновления программного обеспечения и оборудования;

угрозы физического доступа к компонентам информационной системы персональных данных;

угрозы эксплуатации уязвимостей системного или прикладного программного обеспечения, средств защиты информации, СКЗИ, аппаратных компонентов информационной системы персональных данных, микропрограммного обеспечения;

угрозы, связанные с использованием сетевых технологий;

угрозы инженерной инфраструктуры;

угрозы, связанные с отсутствием системы регистрации событий информационной безопасности;

угрозы, связанные с контролем защищенности информационной системы персональных данных;

угрозы, связанные с перехватом защищаемой информации при ее передаче по каналам связи.

6.4.2. В многопрофильных республиканских информационных системах персональных данных актуальными угрозами безопасности персональных данных являются угрозы, включенные в следующие группы:

угрозы использования штатных средств информационных систем персональных данных с целью совершения несанкционированного доступа к информации;

угрозы нарушения доступности информации;

угрозы нарушения целостности информации;

угрозы нарушения конфиденциальности информации;

угрозы недекларированных возможностей в системном или прикладном программном обеспечении;

угрозы, не являющиеся атаками;

угрозы несанкционированного доступа, создающие предпосылки для реализации несанкционированного доступа в результате нарушения процедуры авторизации и аутентификации;

угрозы несанкционированного доступа к информации в результате слабости процедур разграничения ролей и полномочий, правил управления доступом;

угрозы ошибок или внесения уязвимостей при проектировании, внедрении информационной системы персональных данных или системы защиты информационной системы персональных данных;

угрозы ошибочных или деструктивных действий лиц;

угрозы программно-математических воздействий;

угрозы, связанные с использованием технологий виртуализации;

угрозы, связанные с нарушением правил эксплуатации машинных носителей информации;

угрозы, связанные с нарушением процедур установки или обновления программного обеспечения и оборудования;

угрозы физического доступа к компонентам информационной системы персональных данных;

угрозы эксплуатации уязвимостей системного или прикладного программного обеспечения, средств защиты информации, СКЗИ, аппаратных ком-

понентов информационной системы персональных данных, микропрограммного обеспечения;

угрозы, связанные с использованием сетевых технологий;

угрозы инженерной инфраструктуры;

угрозы, связанные с отсутствием системы регистрации событий информационной безопасности;

угрозы, связанные с контролем защищенности информационной системы персональных данных;

угрозы, связанные с перехватом защищаемой информации при ее передаче по каналам связи;

угрозы, связанные с использованием мобильных устройств.

6.4.3. В специальных республиканских информационных системах персональных данных актуальными угрозами безопасности персональных данных являются угрозы, включенные в следующие группы:

угрозы использования штатных средств информационных систем персональных данных с целью совершения несанкционированного доступа к информации;

угрозы нарушения доступности информации;

угрозы нарушения целостности информации;

угрозы нарушения конфиденциальности информации;

угрозы недекларированных возможностей в системном или прикладном программном обеспечении;

угрозы, не являющиеся атаками;

угрозы несанкционированного доступа, создающие предпосылки для реализации несанкционированного доступа в результате нарушения процедуры авторизации и аутентификации;

угрозы несанкционированного доступа к информации в результате слабости процедур разграничения ролей и полномочий, правил управления доступом;

угрозы ошибок или внесения уязвимостей при проектировании, внедрении информационной системы персональных данных или системы защиты информационной системы персональных данных;

угрозы ошибочных или деструктивных действий лиц;

угрозы программно-математических воздействий;

угрозы, связанные с использованием технологий виртуализации;

угрозы, связанные с нарушением правил эксплуатации машинных носителей информации;

угрозы, связанные с нарушением процедур установки или обновления программного обеспечения и оборудования;

угрозы физического доступа к компонентам информационной системы персональных данных;

угрозы эксплуатации уязвимостей системного или прикладного программного обеспечения, средств защиты информации, СКЗИ, аппаратных компонентов информационной системы персональных данных, микропрограммного обеспечения;

угрозы, связанные с использованием сетевых технологий;

угрозы инженерной инфраструктуры;

угрозы, связанные с отсутствием системы регистрации событий информационной безопасности;

угрозы, связанные с контролем защищенности информационной системы персональных данных;

угрозы, связанные с перехватом защищаемой информации при ее передаче по каналам связи.

6.5. В ведомственных информационных системах персональных данных актуальными угрозами безопасности персональных данных являются угрозы, включенные в следующие группы:

угрозы использования штатных средств информационных систем персональных данных с целью совершения несанкционированного доступа к информации;

угрозы нарушения доступности информации;

угрозы нарушения целостности информации;

угрозы нарушения конфиденциальности информации;

угрозы недекларированных возможностей в системном или прикладном программном обеспечении;

угрозы, не являющиеся атаками;

угрозы несанкционированного доступа, создающие предпосылки для реализации несанкционированного доступа в результате нарушения процедуры авторизации и аутентификации;

угрозы несанкционированного доступа к информации в результате слабости процедур разграничения ролей и полномочий, правил управления доступом;

угрозы ошибок или внесения уязвимостей при проектировании, внедрении информационной системы персональных данных или системы защиты информационной системы персональных данных;

угрозы ошибочных или деструктивных действий лиц;

угрозы программно-математических воздействий;

угрозы, связанные с использованием технологий виртуализации;

угрозы, связанные с нарушением правил эксплуатации машинных носителей информации;

угрозы, связанные с нарушением процедур установки или обновления программного обеспечения и оборудования;

угрозы физического доступа к компонентам информационной системы персональных данных;

угрозы эксплуатации уязвимостей системного или прикладного программного обеспечения, средств защиты информации, СКЗИ, аппаратных компонентов информационной системы персональных данных, микропрограммного обеспечения;

угрозы, связанные с использованием сетевых технологий;

угрозы инженерной инфраструктуры;

угрозы, связанные с отсутствием системы регистрации событий информационной безопасности;

угрозы, связанные с контролем защищенности информационной системы персональных данных;

угрозы, связанные с перехватом защищаемой информации при ее передаче по каналам связи.

6.6. Служебные информационные системы персональных данных.

6.6.1. В информационных системах персональных данных бухгалтерского учета и управления финансами актуальными угрозами безопасности персональных данных являются угрозы, включенные в следующие группы:

угрозы использования штатных средств информационных систем персональных данных с целью совершения несанкционированного доступа к информации;

угрозы нарушения доступности информации;

угрозы нарушения целостности информации;

угрозы нарушения конфиденциальности информации;

угрозы недекларированных возможностей в системном или прикладном программном обеспечении;

угрозы, не являющиеся атаками;

угрозы несанкционированного доступа, создающие предпосылки для реализации несанкционированного доступа в результате нарушения процедуры авторизации и аутентификации;

угрозы несанкционированного доступа к информации в результате слабости процедур разграничения ролей и полномочий, правил управления доступом;

угрозы ошибок или внесения уязвимостей при проектировании, внедрении информационной системы персональных данных или системы защиты информационной системы персональных данных;

угрозы ошибочных или деструктивных действий лиц;

угрозы программно-математических воздействий;

угрозы, связанные с использованием технологий виртуализации;

угрозы, связанные с нарушением правил эксплуатации машинных носителей информации;

угрозы, связанные с нарушением процедур установки или обновления программного обеспечения и оборудования;

угрозы физического доступа к компонентам информационной системы персональных данных;

угрозы эксплуатации уязвимостей системного или прикладного программного обеспечения, средств защиты информации, СКЗИ, аппаратных компонентов информационной системы персональных данных, микропрограммного обеспечения;

угрозы, связанные с использованием сетевых технологий;

угрозы инженерной инфраструктуры;

угрозы, связанные с отсутствием системы регистрации событий информационной безопасности;

угрозы, связанные с контролем защищенности информационной системы персональных данных;

угрозы, связанные с перехватом защищаемой информации при ее передаче по каналам связи.

6.6.2. В информационных системах персональных данных кадрового учета и управления персоналом актуальными угрозами безопасности персональных данных являются угрозы, включенные в следующие группы:

угрозы использования штатных средств информационных систем персональных данных с целью совершения несанкционированного доступа к информации;

угрозы нарушения доступности информации;

угрозы нарушения целостности информации;

угрозы нарушения конфиденциальности информации;

угрозы недекларированных возможностей в системном или прикладном программном обеспечении;

угрозы, не являющиеся атаками;

угрозы несанкционированного доступа, создающие предпосылки для реализации несанкционированного доступа в результате нарушения процедуры авторизации и аутентификации;

угрозы несанкционированного доступа к информации в результате слабости процедур разграничения ролей и полномочий, правил управления доступом;

угрозы ошибок или внесения уязвимостей при проектировании, внедрении информационной системы персональных данных или системы защиты информационной системы персональных данных;

угрозы ошибочных или деструктивных действий лиц;

угрозы программно-математических воздействий;

угрозы, связанные с использованием технологий виртуализации;

угрозы, связанные с нарушением правил эксплуатации машинных носителей информации;

угрозы, связанные с нарушением процедур установки или обновления программного обеспечения и оборудования;

угрозы физического доступа к компонентам информационной системы персональных данных;

угрозы эксплуатации уязвимостей системного или прикладного программного обеспечения, средств защиты информации, СКЗИ, аппаратных компонентов информационной системы персональных данных, микропрограммного обеспечения;

угрозы, связанные с использованием сетевых технологий;

угрозы инженерной инфраструктуры;

угрозы, связанные с отсутствием системы регистрации событий информационной безопасности;

угрозы, связанные с контролем защищенности информационной системы персональных данных;

угрозы, связанные с перехватом защищаемой информации при ее передаче по каналам связи.

6.6.3. В информационных системах персональных данных документооборота и делопроизводства актуальными угрозами безопасности персональных данных являются угрозы, включенные в следующие группы:

угрозы использования штатных средств информационных систем персональных данных с целью совершения несанкционированного доступа к информации;

угрозы нарушения доступности информации;

угрозы нарушения целостности информации;

угрозы нарушения конфиденциальности информации;

угрозы недекларированных возможностей в системном или прикладном программном обеспечении;

угрозы, не являющиеся атаками;

угрозы несанкционированного доступа, создающие предпосылки для реализации несанкционированного доступа в результате нарушения процедуры авторизации и аутентификации;

угрозы несанкционированного доступа к информации в результате слабости процедур разграничения ролей и полномочий, правил управления доступом;

угрозы ошибок или внесения уязвимостей при проектировании, внедрении информационной системы персональных данных или системы защиты информационной системы персональных данных;

угрозы ошибочных или деструктивных действий лиц;

угрозы программно-математических воздействий;

угрозы, связанные с нарушением правил эксплуатации машинных носителей информации;

угрозы, связанные с нарушением процедур установки или обновления программного обеспечения и оборудования;

угрозы физического доступа к компонентам информационной системы персональных данных;

угрозы эксплуатации уязвимостей системного или прикладного программного обеспечения, средств защиты информации, СКЗИ, аппаратных компонентов информационной системы персональных данных, микропрограммного обеспечения;

угрозы, связанные с использованием сетевых технологий;

угрозы инженерной инфраструктуры;

угрозы, связанные с отсутствием системы регистрации событий информационной безопасности;

угрозы, связанные с контролем защищенности информационной системы персональных данных;

угрозы, связанные с перехватом защищаемой информации при ее передаче по каналам связи.

6.6.4. В информационных системах персональных данных информационного обеспечения актуальными угрозами безопасности персональных данных являются угрозы, включенные в следующие группы:

угрозы использования штатных средств информационных систем персональных данных с целью совершения несанкционированного доступа к информации;

угрозы нарушения доступности информации;

угрозы нарушения целостности информации;

угрозы нарушения конфиденциальности информации;

угрозы недекларированных возможностей в системном или прикладном программном обеспечении;

угрозы, не являющиеся атаками;

угрозы несанкционированного доступа, создающие предпосылки для реализации несанкционированного доступа в результате нарушения процедуры авторизации и аутентификации;

угрозы несанкционированного доступа к информации в результате слабости процедур разграничения ролей и полномочий, правил управления доступом;

угрозы ошибок или внесения уязвимостей при проектировании, внедрении информационной системы персональных данных или системы защиты информационной системы персональных данных;

угрозы ошибочных или деструктивных действий лиц;

угрозы программно-математических воздействий;

угрозы, связанные с нарушением правил эксплуатации машинных носителей информации;

угрозы, связанные с нарушением процедур установки или обновления программного обеспечения и оборудования;

угрозы физического доступа к компонентам информационной системы персональных данных;

угрозы эксплуатации уязвимостей системного или прикладного программного обеспечения, средств защиты информации, СКЗИ, аппаратных компонентов информационной системы персональных данных, микропрограммного обеспечения;

угрозы, связанные с использованием сетевых технологий;

угрозы инженерной инфраструктуры;

угрозы, связанные с отсутствием системы регистрации событий информационной безопасности;

угрозы, связанные с контролем защищенности информационной системы персональных данных;

угрозы, связанные с перехватом защищаемой информации при ее передаче по каналам связи.

Приложение № 1
к угрозам безопасности персональных данных, актуальным при обработке персональных данных в информационных системах персональных данных, эксплуатируемых в органах исполнительной власти Чувашской Республики и подведомственных им организациях

РАСШИРЕННЫЙ ПЕРЕЧЕНЬ
угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых в органах исполнительной власти Чувашской Республики и подведомственных им организациях

№ пп	Идентификатор угрозы безопасности персональных данных*	Наименование угрозы безопасности персональных данных	Источник угрозы безопасности персональных данных**	Объект воздействия**	Последствия реализации угрозы безопасности персональных данных**
1	2	3	4	5	6
1.	Угрозы использования штатных средств информационных систем персональных данных с целью совершения несанкционированного доступа к информации				
1.1.	УБИ.63	Угроза некорректного использования функционала программного обеспечения	внешний нарушитель безопасности информации (далее – нарушитель) со средним потенциалом, внутренний нарушитель со средним потенциалом	системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение, микропрограммное обеспечение, аппаратное обеспечение	нарушение конфиденциальности информации, целостности информации, доступности информации (далее также соответственно – конфиденциальность, целостность, доступность)

1	2	3	4	5	6
1.2.	УБИ.68	Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением	внешний нарушитель со средним потенциалом, внутренний нарушитель со средним потенциалом	системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение, микропрограммное обеспечение, реестр	нарушение конфиденциальности, целостности, доступности
1.3.	УБИ.86	Угроза несанкционированного изменения аутентификационной информации	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	системное программное обеспечение, объекты файловой системы, учетные данные пользователя, реестр	нарушение целостности, доступности
1.4.	УБИ.87	Угроза несанкционированного использования привилегированных функций базовой системы ввода-вывода (далее – BIOS)	внешний нарушитель с высоким потенциалом, внутренний нарушитель с низким потенциалом	аппаратное обеспечение, микропрограммное обеспечение BIOS или единого расширяемого микропрограммного интерфейса (далее – UEFI)	нарушение конфиденциальности, целостности, доступности
1.5.	УБИ.178	Угроза несанкционированного использования системных и сетевых утилит	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	системное программное обеспечение	нарушение конфиденциальности, целостности, доступности
1.6.		Доступ в среду функционирования локальной операционной системы с возможностью выполнения несанкционированного доступа путем вызова штатных процедур или запуска специально разработанных программ***			
2.	Угрозы нарушения доступности информации				
2.1.	УБИ.14	Угроза длительного удержания вычислительных ресурсов пользователями	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	информационная система персональных данных (далее также – информационная система), сетевой узел, машинный носитель информации (далее также – машинный носитель, носи-	нарушение доступности

1	2	3	4	5	6
				тель информации), системное программное обеспечение, сетевое программное обеспечение, сетевой трафик	
2.2.	УБИ.76	Угроза несанкционированного доступа к гипервизору из виртуальной машины и (или) физической сети	внешний нарушитель со средним потенциалом, внутренний нарушитель со средним потенциалом	гипервизор	нарушение доступности
2.3.	УБИ.105	Угроза отказа в загрузке входных данных неизвестного формата хранилищем больших данных	внутренний нарушитель с низким потенциалом	хранилище больших данных, метаданные	нарушение целостности, доступности
2.4.	УБИ.121	Угроза повреждения системного реестра	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	объекты файловой системы, реестр	нарушение целостности, доступности
2.5.	УБИ.140	Угроза приведения информационной системы в состояние «отказ в обслуживании»	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	информационная система, сетевой узел, системное программное обеспечение, сетевое программное обеспечение, сетевой трафик	нарушение доступности
2.6.	УБИ.153	Угроза усиления воздействия на вычислительные ресурсы пользователей при помощи сторонних серверов	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	информационная система, сетевой узел, системное программное обеспечение, сетевое программное обеспечение	нарушение доступности
2.7.	УБИ.155	Угроза утраты вычислительных ресурсов	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	информационная система, сетевой узел, носитель информации, системное программное обеспечение, сетевое программное обеспечение, сетевой трафик	нарушение доступности
2.8.	УБИ.180	Угроза отказа подсистемы обеспечения температурного режима	внешний нарушитель со средним потенциалом,	технические средства воздушного кондиционирова-	нарушение доступности

1	2	3	4	5	6
			внутренний нарушитель с низким потенциалом	ния, включая трубопроводные системы для циркуляции охлажденного воздуха в центре обработки данных, программируемые логические контроллеры, распределенные системы контроля, управленческие системы и другие программные средства контроля	
2.9.		Угроза вывода из строя или выхода из строя отдельных технических средств***			
2.10.		Угроза вывода из строя незарезервированных технических средств, программных средств или каналов связи			
2.11.		Угроза отсутствия актуальных резервных копий информации***			
2.12.		Угроза потери информации в процессе ее обработки техническими и (или) программными средствами и при передаче по каналам связи***			
2.13.		Угроза переполнения канала связи вследствие множества параллельных попыток авторизации***			
2.14.		Угроза нехватки ресурсов информационной системы для выполнения штатных задач в результате обработки множества параллельных задач, выполняемых одной учетной записью***			
2.15.		Угроза вывода из строя информационных систем при подаче на интерфейсы информационного обмена «неожидаемой» информации***			
3.	Угрозы нарушения целостности информации				
3.1.	УБИ.49	Угроза нарушения целостности данных кеша	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенци-	сетевое программное обеспечение	нарушение целостности, доступности

1	2	3	4	5	6
			алом		
3.2.	УБИ.61	Угроза некорректного задания структуры данных транзакции	внутренний нарушитель со средним потенциалом	сетевой трафик, база данных, сетевое программное обеспечение	нарушение целостности, доступности
3.3.	УБИ.114	Угроза переполнения целочисленных переменных	внешний нарушитель со средним потенциалом, внутренний нарушитель со средним потенциалом	системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение	нарушение конфиденциальности, целостности, доступности
3.4.	УБИ.130	Угроза подмены содержимого сетевых ресурсов	внешний нарушитель с низким потенциалом	прикладное программное обеспечение, сетевое программное обеспечение, сетевой трафик	нарушение конфиденциальности
3.5.	УБИ.136	Угроза потери информации вследствие несогласованности работы узлов хранилища больших данных	внутренний нарушитель с низким потенциалом	информационная система, узлы хранилища больших данных	нарушение целостности, доступности
3.6.	УБИ.149	Угроза сбоя обработки специальным образом измененных файлов	внешний нарушитель со средним потенциалом, внутренний нарушитель со средним потенциалом	метаданные, объекты файловой системы, системное программное обеспечение	нарушение конфиденциальности, целостности, доступности
3.7.	УБИ.179	Угроза несанкционированной модификации защищаемой информации	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	объекты файловой системы	нарушение целостности
3.8.		Угроза отсутствия контроля целостности обрабатываемой в информационной системе информации, применяемого программного обеспечения, в том числе средств защиты информации***			
3.9.		Угроза отсутствия целостных резервных копий информации, программного обеспечения, средств защиты информации в случае реализации угроз информационной безопасности***			
3.10.		Угроза отсутствия контроля за поступающими в информационную систему данными, в том числе			

1	2	3	4	5	6
		незапрашиваемыми***			
3.11.		Отсутствие средств централизованного управления за поступающими в информационную систему данными, в том числе незапрашиваемыми			
3.12.		Отсутствие автоматизированных фильтров, осуществляющих обработку поступающей в информационную систему информации			
3.13.		Угроза доступа в информационную систему информации от неаутентифицированных серверов или пользователей			
3.14.		Угроза отсутствия контроля за данными, передаваемыми из информационной системы***			
3.15.		Отсутствие резервного копирования информации, передаваемой из информационной системы			
3.16.		Угроза передачи из информационной системы недопустимой информации			
3.17.		Угроза отсутствия контроля за данными, вводимыми в информационную систему пользователями***			
3.18.		Угроза ввода или передачи недостоверных или ошибочных данных***			
3.19.		Угроза подмены используемых информационной системой файлов***			
3.20.		Угроза модификации или удаления файлов журналов системного, прикладного программного обеспечения, средств защиты информации***			
3.21.		Угроза установки или запуска модифицированного программного обеспечения и (или) модифицированных обновлений программного обеспечения			
3.22.		Угроза модификации, стирания или удаления данных системы регистрации событий информационной безопасности			
3.23.		Отсутствие регламента или графика проведения контроля целостности применяемых программных средств, в том числе средств защиты информации			

1	2	3	4	5	6
3.24.		Угроза отсутствия контроля целостности информации, обрабатываемой в информационной системе, и ее структуры			
4.	Угрозы нарушения конфиденциальности информации				
4.1.	УБИ.36	Угроза исследования механизмов работы программы	внешний нарушитель со средним потенциалом, внутренний нарушитель со средним потенциалом	системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение, микропрограммное обеспечение	нарушение конфиденциальности, доступности
4.2.	УБИ.37	Угроза исследования приложения через отчеты об ошибках	внешний нарушитель со средним потенциалом, внутренний нарушитель со средним потенциалом	системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение, микропрограммное обеспечение	нарушение конфиденциальности
4.3.	УБИ.98	Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб	внешний нарушитель с низким потенциалом	сетевой узел, сетевое программное обеспечение, сетевой трафик	нарушение конфиденциальности
4.4.	УБИ.99	Угроза обнаружения хостов	внешний нарушитель с низким потенциалом	сетевой узел, сетевое программное обеспечение, сетевой трафик	нарушение конфиденциальности
4.5.	УБИ.103	Угроза определения типов объектов защиты	внешний нарушитель с низким потенциалом	сетевой узел, сетевое программное обеспечение, сетевой трафик	нарушение конфиденциальности
4.6.	УБИ.104	Угроза определения топологии вычислительной сети	внешний нарушитель с низким потенциалом	сетевой узел, сетевое программное обеспечение, сетевой трафик	нарушение конфиденциальности
4.7.	УБИ.132	Угроза получения предварительной информации об объекте защиты	внешний нарушитель со средним потенциалом	сетевой узел, сетевое программное обеспечение, сетевой трафик, прикладное программное обеспечение	нарушение конфиденциальности
4.8.	УБИ.133	Угроза получения сведений о владельце беспроводного устройства	внешний нарушитель с низким потенциалом	сетевой узел, метаданные	нарушение конфиденциальности
4.9.	УБИ.151	Угроза сканирования веб-сервисов, разработан-	внешний нарушитель с	сетевое программное обес-	нарушение конфиден-

1	2	3	4	5	6
		ных на основе языка описания WSDL	низким потенциалом	печение, сетевой узел	циальности
4.10.		Сканирование сети для изучения логики работы информационной системы, выявления протоколов, портов***			
4.11.		Анализ сетевого трафика для изучения логики работы информационной системы, выявления протоколов, портов, перехвата служебных данных (в том числе идентификаторов и паролей), их подмены***			
4.12.		Применение специальных программ для выявления пароля (IP-спуффинг, разные виды перебора)***			
4.13.		Угроза получения нарушителем сведений о структуре, конфигурации и настройках информационной системы и системы защиты			
4.14.		Угроза получения нарушителем конфиденциальных сведений, обрабатываемых в информационной системе			
4.15.		Угроза получения нарушителем идентификационных данных легальных пользователей информационной системы			
4.16.		Разглашение сведений конфиденциального характера			
5.	Угрозы недекларированных возможностей в системном или прикладном программном обеспечении				
5.1.	УБИ.109	Угроза перебора всех настроек и параметров приложения	внешний нарушитель со средним потенциалом, внутренний нарушитель со средним потенциалом	системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение, микропрограммное обеспечение, реестр	нарушение целостности, доступности
5.2.		Угроза возникновения ошибок функционирования системного программного обеспечения, реализация недекларированных возможностей системного программного обеспечения			
5.3.		Угроза использования встроенных недекларированных возможностей для получения несанкционированного доступа в информационную систему			

1	2	3	4	5	6
6.	Угрозы, не являющиеся атаками				
6.1.	УБИ.38	Угроза исчерпания вычислительных ресурсов хранилища больших данных	внутренний нарушитель с низким потенциалом	информационная система	нарушение доступности
6.2.	УБИ.50	Угроза неверного определения формата входных данных, поступающих в хранилище больших данных	внутренний нарушитель с низким потенциалом	хранилище больших данных, метаданные	нарушение целостности
6.3.	УБИ.51	Угроза невозможности восстановления сессии работы на ПЭВМ при выводе из промежуточных состояний питания	внутренний нарушитель с низким потенциалом	рабочая станция, носитель информации, системное программное обеспечение, метаданные, объекты файловой системы, реестр	нарушение целостности, доступности
6.4.	УБИ.57	Угроза неконтролируемого копирования данных внутри хранилища больших данных	внутренний нарушитель с низким потенциалом	хранилище больших данных, метаданные, защищаемые данные	нарушение конфиденциальности
6.5.	УБИ.60	Угроза неконтролируемого уничтожения информации хранилищем больших данных	внутренний нарушитель с низким потенциалом	хранилище больших данных, метаданные, защищаемые данные	нарушение целостности, доступности
6.6.	УБИ.176	Угроза нарушения технологического/производственного процесса из-за временных задержек, вносимых средством защиты	внешний нарушитель с низким потенциалом	средство защиты информации	нарушение доступности
6.7.	УБИ.182	Угроза физического устаревания аппаратных компонентов	внутренний нарушитель с низким потенциалом	аппаратное средство	нарушение доступности
6.8.		Угроза выхода из строя или отказа отдельных технических средств, программных средств, каналов связи			
7.	Угрозы несанкционированного доступа, создающие предпосылки для реализации несанкционированного доступа в результате нарушения процедуры авторизации и аутентификации				
7.1.	УБИ.4	Угроза аппаратного сброса пароля BIOS	внутренний нарушитель с низким потенциалом	микропрограммное и аппаратное обеспечение BIOS/UEFI	нарушение целостности
7.2.	УБИ.46	Угроза нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия	внешний нарушитель с низким потенциалом, внутренний наруши-	сетевой узел, сетевое программное обеспечение, метаданные, учетные данные	нарушение конфиденциальности, доступности

1	2	3	4	5	6
			тель с низким потенциалом	пользователя	
7.3.	УБИ.100	Угроза обхода некорректно настроенных механизмов аутентификации	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	системное программное обеспечение, сетевое программное обеспечение	нарушение конфиденциальности, целостности, доступности
7.4.	УБИ.144	Угроза программного сброса пароля BIOS	внутренний нарушитель с низким потенциалом	микропрограммное обеспечение BIOS/UEFI, системное программное обеспечение	нарушение конфиденциальности, целостности
7.5.	УБИ.168	Угроза «кражи» учетной записи доступа к сетевым сервисам	внешний нарушитель с низким потенциалом	сетевое программное обеспечение	нарушение конфиденциальности, доступности
7.6.	УБИ.181	Угроза перехвата одноразовых паролей в режиме реального времени	внешний нарушитель со средним потенциалом	сетевое программное обеспечение	нарушение целостности
7.7.		Угроза получения доступа к информационной системе, компонентам информационной системы, информации, обрабатываемой в информационной системе без прохождения процедуры идентификации и аутентификации***			
7.8.		Угроза получения доступа к информационной системе вследствие ошибок подсистемы идентификации и аутентификации***			
7.9.		Угроза получения несанкционированного доступа в результате сбоев или ошибок подсистемы идентификации и аутентификации***			
7.10.		Угроза получения несанкционированного доступа сторонними лицами, устройствами***			
7.11.		Угроза отсутствия или слабости процедур аутентификации при доступе пользователей или устройств к ресурсам информационной системы			
7.12.		Угроза авторизации с использованием устаревших, но не отключенных учетных записей***			
7.13.		Угроза использования «слабых» методов иденти-			

1	2	3	4	5	6
		фикации и аутентификации пользователей, в том числе при использовании удаленного доступа			
7.14.		Угроза применения только программных методов двухфакторной аутентификации			
7.15.		Угроза использования долговременных паролей для подключения к информационной системе посредством удаленного доступа			
7.16.		Угроза передачи аутентифицирующей информации по открытым каналам связи без использования криптографических средств защиты информации			
7.17.		Угроза доступа к информационной системе неаутентифицированных устройств и пользователей			
7.18.		Угроза повторного использования идентификаторов в течение как минимум одного года			
7.19.		Угроза использования идентификаторов, не используемых более 45 дней			
7.20.		Угроза раскрытия используемых идентификаторов пользователя в публичном доступе			
7.21.		Отсутствие управления идентификаторами внешних пользователей			
7.22.		Угроза использования «слабых» или предсказуемых паролей			
7.23.		Отсутствие отказоустойчивой централизованной системы идентификации и аутентификации			
7.24.		Угроза использования пользователями идентичных идентификаторов в разных информационных системах			
7.25.		Угроза использования неподписанных программных средств			
7.26.		Угроза запуска несанкционированных процессов и служб от имени системных пользователей			
7.27.		Угроза отсутствия регламента работы с персональными идентификаторами			
7.28.		Отсутствие в централизованной системе иденти-			

1	2	3	4	5	6
		фикации и аутентификации атрибутов, позволяющих однозначно определить внешних и внутренних пользователей			
7.29.		Угроза бесконтрольного доступа пользователей к процессу загрузки			
7.30.		Угроза подмены или модификации базовой системы ввода-вывода, программного обеспечения телекоммуникационного оборудования			
8.	Угрозы несанкционированного доступа к информации в результате слабости процедур разграничения ролей и полномочий, правил управления доступом				
8.1.	УБИ.7	Угроза воздействия на программы с высокими привилегиями	внешний нарушитель со средним потенциалом, внутренний нарушитель со средним потенциалом	информационная система, виртуальная машина, сетевое программное обеспечение, сетевой трафик	нарушение конфиденциальности, целостности
8.2.	УБИ.15	Угроза доступа к защищаемым файлам с использованием обходного пути	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	объекты файловой системы	нарушение конфиденциальности
8.3.	УБИ.16	Угроза доступа к локальным файлам сервера при помощи единообразного локатора ресурса (URL)	внешний нарушитель со средним потенциалом	сетевое программное обеспечение	нарушение конфиденциальности
8.4.	УБИ.18	Угроза загрузки нештатной операционной системы	внутренний нарушитель с низким потенциалом	микропрограммное обеспечение BIOS/UEFI	нарушение конфиденциальности, целостности, доступности
8.5.	УБИ.24	Угроза изменения режимов работы аппаратных элементов компьютера	внутренний нарушитель с высоким потенциалом	микропрограммное и аппаратное обеспечение BIOS/UEFI	нарушение целостности, доступности
8.6.	УБИ.25	Угроза изменения системных и глобальных переменных	внутренний нарушитель со средним потенциалом	системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение	нарушение конфиденциальности, целостности, доступности
8.7.	УБИ.28	Угроза использования альтернативных путей доступа к ресурсам	внешний нарушитель с низким потенциалом, внутренний наруши-	сетевой узел, объекты файловой системы, прикладное программное обеспечение,	нарушение конфиденциальности

1	2	3	4	5	6
			тель с низким потенциалом	системное программное обеспечение	
8.8.	УБИ.30	Угроза использования информации идентификации/аутентификации, заданной по умолчанию	внешний нарушитель со средним потенциалом, внутренний нарушитель с низким потенциалом	средства защиты информации, системное программное обеспечение, сетевое программное обеспечение, микропрограммное обеспечение, программно-аппаратные средства со встроенными функциями защиты	нарушение конфиденциальности, целостности, доступности
8.9.	УБИ.31	Угроза использования механизмов авторизации для повышения привилегий	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение	нарушение конфиденциальности
8.10.	УБИ.45	Угроза нарушения изоляции среды исполнения BIOS	внутренний нарушитель с низким потенциалом	микропрограммное и аппаратное обеспечение BIOS/UEFI	нарушение конфиденциальности, целостности, доступности
8.11.	УБИ.53	Угроза невозможности управления правами пользователей BIOS	внутренний нарушитель с низким потенциалом	микропрограммное обеспечение BIOS/UEFI	нарушение конфиденциальности, целостности, доступности
8.12.	УБИ.62	Угроза некорректного использования прозрачного прокси-сервера за счет плагинов браузера	внешний нарушитель с низким потенциалом	сетевое программное обеспечение	нарушение конфиденциальности
8.13.	УБИ.67	Угроза неправомерного ознакомления с защищаемой информацией	внутренний нарушитель с низким потенциалом	аппаратное обеспечение, носители информации, объекты файловой системы	нарушение конфиденциальности
8.14.	УБИ.74	Угроза несанкционированного доступа к аутентификационной информации	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	системное программное обеспечение, объекты файловой системы, учетные данные пользователя, реестр, машинные носители информации	нарушение конфиденциальности
8.15.	УБИ.83	Угроза несанкционированного доступа к системе по беспроводным каналам	внешний нарушитель с низким потенциалом	сетевой узел, учетные данные пользователя, сетевой трафик, аппаратное обес-	нарушение конфиденциальности

1	2	3	4	5	6
				печение	
8.16.	УБИ.97	Угроза несогласованности правил доступа к большим данным	внутренний нарушитель с низким потенциалом	хранилище больших данных	нарушение конфиденциальности, доступности
8.17.	УБИ.88	Угроза несанкционированного копирования защищаемой информации	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	объекты файловой системы, машинный носитель информации	нарушение конфиденциальности
8.18.	УБИ.89	Угроза несанкционированного редактирования реестра	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	системное программное обеспечение, использующее реестр, реестр	нарушение конфиденциальности, целостности, доступности
8.19.	УБИ.90	Угроза несанкционированного создания учетной записи пользователя	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	системное программное обеспечение	нарушение конфиденциальности, целостности, доступности
8.20.	УБИ.93	Угроза несанкционированного управления буфером	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение	нарушение конфиденциальности, целостности, доступности
8.21.	УБИ.94	Угроза несанкционированного управления синхронизацией и состоянием	внешний нарушитель со средним потенциалом, внутренний нарушитель со средним потенциалом	системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение, микропрограммное обеспечение	нарушение целостности, доступности
8.22.	УБИ.95	Угроза несанкционированного управления указателями	внешний нарушитель со средним потенциалом, внутренний нарушитель со средним потенциалом	системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение	нарушение конфиденциальности, целостности, доступности

1	2	3	4	5	6
8.23.	УБИ.112	Угроза передачи запрещенных команд на оборудование с числовым программным управлением	внутренний нарушитель с низким потенциалом	системное программное обеспечение, прикладное программное обеспечение	нарушение целостности
8.24.	УБИ.113	Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	системное программное обеспечение, аппаратное обеспечение	нарушение целостности, доступности
8.25.	УБИ.117	Угроза перехвата привилегированного потока	внешний нарушитель со средним потенциалом, внутренний нарушитель со средним потенциалом	системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение	нарушение конфиденциальности, целостности, доступности
8.26.	УБИ.118	Угроза перехвата привилегированного процесса	внешний нарушитель со средним потенциалом, внутренний нарушитель со средним потенциалом	системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение	нарушение конфиденциальности, целостности, доступности
8.27.	УБИ.122	Угроза повышения привилегий	внешний нарушитель со средним потенциалом, внутренний нарушитель со средним потенциалом	системное программное обеспечение, сетевое программное обеспечение, информационная система	нарушение конфиденциальности, целостности, доступности
8.28.	УБИ.123	Угроза подбора пароля BIOS	внутренний нарушитель с низким потенциалом	микропрограммное обеспечение BIOS/UEFI	нарушение конфиденциальности, доступности
8.29.	УБИ.124	Угроза подделки записей журнала регистрации событий	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	системное программное обеспечение	нарушение целостности
8.30.	УБИ.148	Угроза сбоя автоматического управления системой разграничения доступа хранилища больших данных		информационная система, система разграничения доступа хранилища больших данных	нарушение конфиденциальности, доступности

1	2	3	4	5	6
8.31.	УБИ.152	Угроза удаления аутентификационной информации	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	системное программное обеспечение, микропрограммное обеспечение, учетные данные пользователя	нарушение конфиденциальности, целостности, доступности
8.32.	УБИ.159	Угроза «форсированного веб-браузинга»	внешний нарушитель с низким потенциалом	сетевой узел, сетевое программное обеспечение	нарушение конфиденциальности
8.33.	УБИ.162	Угроза эксплуатации цифровой подписи программного кода	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	системное программное обеспечение, прикладное программное обеспечение	нарушение конфиденциальности, целостности, доступности
8.34.	УБИ.185	Угроза несанкционированного изменения параметров настройки средств защиты информации	внутренний нарушитель с низким потенциалом, внешний нарушитель с низким потенциалом	средство защиты информации	нарушение целостности
8.35.	УБИ.187	Угроза несанкционированного воздействия на средство защиты информации	внутренний нарушитель со средним потенциалом, внешний нарушитель со средним потенциалом	средство защиты информации	нарушение конфиденциальности, целостности, доступности
8.36.		Угроза доступа к информации и командам, хранящимся в BIOS, с возможностью перехвата управления загрузкой операционной системы и получения прав доверенного пользователя***			
8.37.		Угроза получения несанкционированного доступа к средствам управления персональными идентификаторами или учетными записями, в том числе с повышенными правами доступа***			
8.38.		Угроза получения доступа к данным в обход механизмов разграничения доступа, в том числе с повышенными правами доступа***			
8.39.		Угроза бесконтрольной передачи данных как внутри информационной системы, так и между			

1	2	3	4	5	6
		информационными системами***			
8.40.		Угроза получения дополнительных данных, не предусмотренных технологией обработки***			
8.41.		Угроза получения разными пользователями, лицами, обеспечивающими функционирование информационной системы, доступа к данным и полномочиям, не предназначенным для данных лиц в соответствии с их должностными обязанностями***			
8.42.		Угроза предоставления прав доступа, которые не являются необходимыми для исполнения должностных обязанностей и функционирования информационной системы***			
8.43.		Отсутствие ограничения на количество неудачных попыток входа в информационную систему***			
8.44.		Угроза использования или подключения к открытому (незаблокированному) сеансу пользователя***			
8.45.		Угроза использования ресурсов информационной системы до прохождения процедур идентификации и авторизации***			
8.46.		Угрозы несанкционированного подключения к информационной системе с использованием санкционированной сессии удаленного доступа***			
8.47.		Угроза подбора идентификационных данных для удаленного доступа к информационной системе***			
8.48.		Угроза использования слабостей или уязвимостей защиты протоколов удаленного доступа***			
8.49.		Угроза бесконтрольного использования технологий беспроводного доступа, в том числе с мобильных устройств***			
8.50.		Угроза получения доступа к информационной системе с использованием технологий беспроводного доступа, в том числе мобильных устройств, без			

1	2	3	4	5	6
		прохождения процедуры идентификации и авторизации***			
8.51.		Угроза получения доступа к информационной системе с использованием технологий беспроводного доступа с неконтролируемых устройств***			
8.52.		Угроза несанкционированной автоматической передачи конфиденциальной информации на запросы сторонних информационных систем***			
8.53.		Угроза получения несанкционированного доступа к средствам управления персональными идентификаторами или учетными записями, в том числе с повышенными правами доступа***			
8.54.		Угроза получения несанкционированного доступа к средствам управления средствами идентификации и аутентификации***			
8.55.		Угроза перехвата идентифицирующих и аутентифицирующих данных в процессе идентификации и аутентификации пользователей***			
8.56.		Угроза бесконтрольного доступа к информации неопределенным кругом лиц***			
8.57.		Угроза получения доступа к данным, не предназначенным для пользователя***			
8.58.		Угроза удаленного управления и использования периферийных устройств для получения информации или выполнения иных деструктивных целей***			
8.59.		Угроза модификации, подмены, удаления атрибутов безопасности (меток безопасности) при взаимодействии с иными информационными системами***			
8.60.		Угроза использования технологий мобильного кода для совершения попыток несанкционированного доступа к информационной системе при использовании в информационной системе мобильных устройств***			
8.61.		Угроза использования встроенных в информаци-			

1	2	3	4	5	6
		онную систему недекларированных возможностей, скрытых каналов передачи информации в обход реализованных мер защиты			
8.62.		Отсутствие отказоустойчивых централизованных средств управления учетными записями			
8.63.		Отсутствие автоматического блокирования учетных записей по истечении их срока действия, а также в результате превышения допустимого числа попыток доступа к информационной системе, выявления попыток несанкционированного доступа			
8.64.		Угроза отсутствия необходимых методов управления доступом для разграничения прав доступа в соответствии с технологией обработки и угрозами безопасности информации			
8.65.		Угроза передачи информации разной степени конфиденциальности без разграничения информационных потоков			
8.66.		Угроза передачи информации без соблюдения атрибутов (меток) безопасности, связанных с передаваемой информацией			
8.67.		Отсутствие динамического анализа и управления информационными потоками в зависимости от состояния информационной системы, условий ее функционирования, изменений в технологии обработки передаваемых данных			
8.68.		Угроза обхода правил управления информационными потоками за счет манипуляций с передаваемыми данными			
8.69.		Угроза несанкционированного доступа к средствам управления информационными потоками			
8.70.		Угроза возложения функционально различных должностных обязанностей/ролей на одно должностное лицо			
8.71.		Угроза предоставления расширенных прав и при-			

1	2	3	4	5	6
		вилегий пользователям, в том числе внешним			
8.72.		Отсутствие информирования пользователя о применении средств защиты информации и необходимости соблюдения установленных оператором правил и ограничений на работу с информацией, о предыдущем успешном доступе к информационной системе, о количестве успешных или неуспешных попыток доступа, об изменении сведений об учетной записи пользователя, о превышении числа параллельных сеансов доступа			
8.73.		Отсутствие информирования администратора о превышении числа параллельных сеансов доступа пользователей			
8.74.		Угроза использования одних и тех же учетных записей для параллельного доступа к информационной системе с двух и более различных устройств			
8.75.		Отсутствие блокирования сеанса пользователя (на мониторе пользователя не должна отображаться информация сеанса пользователя) после времени бездействия в течение пяти минут			
8.76.		Угроза использования незавершенных сеансов пользователей			
8.77.		Угроза наличия удаленного доступа от имени привилегированных пользователей для администрирования информационной системы, системы защиты, в том числе с использованием технологий беспроводного доступа			
8.78.		Отсутствие автоматизированного мониторинга и контроля удаленного доступа			
8.79.		Угроза использования уязвимых или незащищенных технологий удаленного доступа			
8.80.		Угроза взаимодействия с иными информационными системами, не обеспеченными системой защиты			
8.81.		Отсутствие механизмов автоматизированного			

1	2	3	4	5	6
		контроля параметров настройки компонентов программного обеспечения, влияющих на безопасность информации			
8.82.		Отсутствие механизмов автоматизированного реагирования на несанкционированное изменение параметров настройки компонентов программного обеспечения, влияющих на безопасность информации			
8.83.		Отсутствие контроля за используемыми интерфейсами ввода/вывода			
9.	Угрозы ошибок или внесения уязвимостей при проектировании, внедрении информационной системы персональных данных или системы защиты информационной системы персональных данных				
9.1.	УБИ.111	Угроза передачи данных по скрытым каналам	внешний нарушитель со средним потенциалом, внутренний нарушитель со средним потенциалом	сетевой узел, сетевое программное обеспечение, сетевой трафик	нарушение конфиденциальности
9.2.	УБИ.166	Угроза внедрения системной избыточности	внутренний нарушитель со средним потенциалом	программное обеспечение, информационная система, ключевая система информационной инфраструктуры	нарушение доступности
9.3.	УБИ.165	Угроза включения в проект недостоверно испытанных компонентов	внутренний нарушитель со средним потенциалом	программное обеспечение, техническое средство, информационная система, ключевая система информационной инфраструктуры	нарушение конфиденциальности, целостности, доступности
9.4.		Угроза ошибок при моделировании угроз и нарушителей***			
9.5.		Угроза внедрения системы защиты, не обеспечивающей нивелирования актуальных угроз и нарушителей информационной безопасности***			
10.	Угрозы ошибочных или деструктивных действий лиц				
10.1.	УБИ.127	Угроза подмены действия пользователя путем обмана	внешний нарушитель с низким потенциалом	сетевой узел, сетевое программное обеспечение	нарушение конфиденциальности

1	2	3	4	5	6
10.2.	УБИ.175	Угроза «фишинга»	внешний нарушитель с низким потенциалом	рабочая станция, сетевое программное обеспечение, сетевой трафик	нарушение конфиденциальности
10.3.	УБИ.177	Угроза неподтвержденного ввода данных оператором в систему, связанную с безопасностью	внутренний нарушитель с низким потенциалом	системное программное обеспечение, сетевое программное обеспечение, прикладное программное обеспечение, аппаратное обеспечение	нарушение целостности, доступности
10.4.		Реализация угроз с использованием возможности непосредственного доступа к техническим средствам и части программных средств информационной системы, средствам защиты информации и средствам криптографической защиты информации (далее – СКЗИ) в соответствии с установленными для них административными полномочиями***			
10.5.		Внесение изменений в конфигурацию программных средств и технических средств, которые приводят к отключению или частичному отключению информационной системы, модулей, компонентов или сегментов информационной системы, средств защиты информации (в случае сговора с внешними нарушителями)***			
10.6.		Создание неконтролируемых точек доступа для получения удаленного доступа к информационной системе***			
10.7.		Переконфигурирование средств защиты информации и СКЗИ для реализации угроз в информационной системе***			
10.8.		Осуществление угроз с использованием локальных линий связи, систем электропитания и заземления***			
10.9.		Хищение ключей шифрования, идентификаторов и паролей***			
10.10.		Внесение программно-аппаратных закладок в про-			

1	2	3	4	5	6
		граммно-аппаратные средства информационной системы, обеспечивающих съем информации с использованием непосредственного подключения к техническим средствам обработки информации***			
10.11.		Создание методов и средств реализации атак, а также самостоятельное проведение атаки			
10.12.		Ошибки при конфигурировании и обслуживании модулей или компонентов информационной системы			
10.13.		Создание ситуаций, препятствующих функционированию сети (остановка, сбой серверов; уничтожение или модификация программного обеспечения; создание множественных, ложных информационных сообщений)			
10.14.		Несанкционированный съем информации, блокирование работы отдельных пользователей, перестройка планов маршрутизации и политик доступа сети			
10.15.		Непреднамеренное разглашение персональных данных лицам, не имеющим права доступа к ним			
10.16.		Нарушение правил хранения ключевой информации			
10.17.		Передача защищаемой информации по открытым каналам связи			
10.18.		Несанкционированная модификация или уничтожение информации легитимным пользователем			
10.19.		Копирование информации на незарегистрированный носитель информации, в том числе вывод на печать			
10.20.		Несанкционированное отключение средств защиты информации			
10.21.		Угрозы социальной инженерии			
11.	Угрозы программно-математических воздействий				
11.1.	УБИ.6	Угроза внедрения кода или данных	внешний нарушитель с низким потенциалом	системное программное обеспечение, прикладное	нарушение конфиденциальности, целостно-

1	2	3	4	5	6
				программное обеспечение, сетевое программное обеспечение	сти, доступности
11.2.	УБИ.8	Угроза восстановления аутентификационной информации	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	системное программное обеспечение, микропрограммное обеспечение, учетные данные пользователя	нарушение конфиденциальности
11.3.	УБИ.12	Угроза деструктивного изменения конфигурации/среды окружения программ	внутренний нарушитель с низким потенциалом	системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение, микропрограммное обеспечение, метаданные, объекты файловой системы, реестр	нарушение конфиденциальности, целостности, доступности
11.4.	УБИ.22	Угроза избыточного выделения оперативной памяти	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	аппаратное обеспечение, системное программное обеспечение, сетевое программное обеспечение	нарушение доступности
11.5.	УБИ.26	Угроза искажения схемы расширяемого языка разметки (XML-схемы)	внешний нарушитель со средним потенциалом, внутренний нарушитель со средним потенциалом	сетевой узел, сетевое программное обеспечение, сетевой трафик	нарушение целостности, доступности
11.6.	УБИ.27	Угроза искажения вводимой и выводимой на периферийные устройства информации	внешний нарушитель с высоким потенциалом, внутренний нарушитель с низким потенциалом	системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение, аппаратное обеспечение	нарушение целостности
11.7.	УБИ.33	Угроза использования слабостей кодирования входных данных	внешний нарушитель со средним потенциалом, внутренний наруши-	системное программное обеспечение, прикладное программное обеспечение,	нарушение целостности, доступности

1	2	3	4	5	6
			тель со средним потенциалом	сетевое программное обеспечение, микропрограммное обеспечение, реестр	
11.8.	УБИ.41	Угроза межсайтового скриптинга	внешний нарушитель с низким потенциалом	сетевой узел, сетевое программное обеспечение	нарушение конфиденциальности, целостности, доступности
11.9.	УБИ.42	Угроза межсайтовой подделки запроса	внешний нарушитель со средним потенциалом	сетевой узел, сетевое программное обеспечение	нарушение конфиденциальности, целостности, доступности
11.10.	УБИ.72	Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS	внутренний нарушитель с низким потенциалом	микропрограммное и аппаратное обеспечение BIOS/UEFI	нарушение конфиденциальности, целостности, доступности
11.11.	УБИ.115	Угроза перехвата вводимой и выводимой на периферийные устройства информации	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	системное программное обеспечение, прикладное программное обеспечение, аппаратное обеспечение	нарушение конфиденциальности
11.12.	УБИ.129	Угроза подмены резервной копии программного обеспечения BIOS	внутренний нарушитель с низким потенциалом	микропрограммное и аппаратное обеспечение BIOS/UEFI	нарушение целостности
11.13.	УБИ.145	Угроза пропуска проверки целостности программного обеспечения	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение	нарушение целостности, доступности
11.14.	УБИ.167	Угроза заражения компьютера при посещении неблагонадежных сайтов	внутренний нарушитель с низким потенциалом	сетевой узел, сетевое программное обеспечение	нарушение конфиденциальности, целостности, доступности
11.15.	УБИ.170	Угроза неправомерного шифрования информации	внешний нарушитель с низким потенциалом	объект файловой системы	нарушение доступности
11.16.	УБИ.171	Угроза скрытного включения вычислительного устройства в состав бот-сети	внешний нарушитель с низким потенциалом	сетевой узел, сетевое программное обеспечение	нарушение доступности
11.17.	УБИ.172	Угроза распространения «почтовых червей»	внешний нарушитель с низким потенциалом	сетевое программное обеспечение	нарушение конфиденциальности, целостности, доступности
11.18.	УБИ.186	Угроза внедрения вредоносного кода через рекла-	внутренний наруши-	сетевое программное обес-	нарушение целостности,

1	2	3	4	5	6
		му, сервисы и контент	тель с низким потенциалом	печение	доступности
11.19.	УБИ.189	Угроза маскирования действий вредоносного кода	внешний нарушитель со средним потенциалом	системное программное обеспечение, сетевое программное обеспечение	нарушение целостности, доступности
11.20.	УБИ.190	Угроза внедрения вредоносного кода за счет посещения зараженных сайтов в информационно-телекоммуникационной сети «Интернет»	внешний нарушитель со средним потенциалом	сетевое программное обеспечение	нарушение конфиденциальности, целостности, доступности
11.21.	УБИ.191	Угроза внедрения вредоносного кода в дистрибутив программного обеспечения	внутренний нарушитель с низким потенциалом, внешний нарушитель с низким потенциалом	прикладное программное обеспечение, сетевое программное обеспечение, системное программное обеспечение	нарушение конфиденциальности, целостности, доступности
11.22.	УБИ.193	Угроза утечки информации за счет применения вредоносным программным обеспечением алгоритмов шифрования трафика	внешний нарушитель со средним потенциалом	информационные ресурсы, объекты файловой системы	нарушение конфиденциальности
11.23.		Внедрение программных закладок***			
11.24.		Угроза внедрения в информационные системы вредоносного программного обеспечения с устройств, подключаемых с использованием технологий беспроводного доступа***			
11.25.		Применение специально созданных программных продуктов для несанкционированного доступа***			
11.26.		Угроза внедрения через легитимные схемы информационного обмена между информационными системами вредоносного программного обеспечения***			
11.27.		Отсутствие централизованной системы управления средствами антивирусной защиты информации			
12.	Угрозы, связанные с использованием «облачных» услуг				
12.1.	УБИ.20	Угроза злоупотребления возможностями, предоставленными потребителям «облачных» услуг	внутренний нарушитель с низким потенциалом	«облачная» система, виртуальная машина	нарушение конфиденциальности, целостности, доступности
12.2.	УБИ.21	Угроза злоупотребления доверием потребителей «облачных» услуг	внешний нарушитель с низким потенциалом	«облачная» система	нарушение конфиденциальности, целостно-

1	2	3	4	5	6
					сти
12.3.	УБИ.43	Угроза нарушения доступности «облачного» сервера	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	«облачная» система, «облачный» сервер	нарушение доступности
12.4.	УБИ.52	Угроза невозможности миграции образов виртуальных машин из-за несовместимости аппаратного и программного обеспечения	внешний нарушитель с низким потенциалом	«облачная» инфраструктура, виртуальная машина, аппаратное обеспечение, системное программное обеспечение	нарушение целостности, доступности
12.5.	УБИ.54	Угроза недобросовестного исполнения обязательств поставщиками «облачных» услуг	внешний нарушитель с низким потенциалом	информационная система, сервер, носитель информации, метаданные, объекты файловой системы	нарушение конфиденциальности, целостности, доступности
12.6.	УБИ.55	Угроза незащищенного администрирования «облачных» услуг	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	«облачная» система, рабочая станция, сетевое программное обеспечение	нарушение конфиденциальности, целостности, доступности
12.7.	УБИ.56	Угроза некачественного переноса инфраструктуры в «облако»	внешний нарушитель с низким потенциалом	информационная система, иммигрированная в «облако», «облачная» система	нарушение конфиденциальности, целостности, доступности
12.8.	УБИ.58	Угроза неконтролируемого роста числа виртуальных машин	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	«облачная» система, консоль управления «облачной» инфраструктурой, «облачная» инфраструктура	нарушение доступности
12.9.	УБИ.64	Угроза некорректной реализации политики лицензирования в «облаке»	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение	нарушение доступности
12.10.	УБИ.65	Угроза неопределенности в распределении ответственности между ролями в «облаке»	внешний нарушитель с низким потенциалом, внутренний наруши-	системное программное обеспечение	нарушение конфиденциальности, целостности, доступности

1	2	3	4	5	6
			тель с низким потенциалом		
12.11.	УБИ.66	Угроза неопределенности ответственности за обеспечение безопасности «облака»	внешний нарушитель с низким потенциалом	«облачная» система	нарушение конфиденциальности, целостности, доступности
12.12.	УБИ.70	Угроза непрерывной модернизации «облачной» инфраструктуры	внутренний нарушитель со средним потенциалом	«облачная» инфраструктура	нарушение целостности, доступности
12.13.	УБИ.96	Угроза несогласованности политик безопасности элементов «облачной» инфраструктуры	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	системное программное обеспечение, «облачная» система	нарушение конфиденциальности, целостности, доступности
12.14.	УБИ.101	Угроза общедоступности «облачной» инфраструктуры	внешний нарушитель со средним потенциалом	объекты файловой системы, аппаратное обеспечение, «облачный» сервер	нарушение конфиденциальности, целостности, доступности
12.15.	УБИ.134	Угроза потери доверия к поставщику «облачных» услуг	внутренний нарушитель со средним потенциалом	объекты файловой системы, информационная система, иммигрированная в «облако»	нарушение конфиденциальности, целостности, доступности
12.16.	УБИ.135	Угроза потери и утечки данных, обрабатываемых в «облаке»	внутренний нарушитель с низким потенциалом	системное программное обеспечение, метаданные, объекты файловой системы	нарушение конфиденциальности, целостности, доступности
12.17.	УБИ.137	Угроза потери управления «облачными» ресурсами	внешний нарушитель с высоким потенциалом	сетевой трафик, объекты файловой системы	нарушение конфиденциальности, целостности, доступности
12.18.	УБИ.138	Угроза потери управления собственной инфраструктурой при переносе ее в «облако»	внутренний нарушитель со средним потенциалом	информационная система, иммигрированная в «облако», системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение	нарушение конфиденциальности, целостности, доступности
12.19.	УБИ.141	Угроза привязки к поставщику «облачных» услуг	внутренний нарушитель с низким потенци-	информационная система, иммигрированная в «обла-	нарушение доступности

1	2	3	4	5	6
			алом	ко», системное программное обеспечение, сетевое программное обеспечение, сетевой трафик, объекты файловой системы	
12.20.	УБИ.142	Угроза приостановки оказания «облачных» услуг вследствие технических сбоев		системное программное обеспечение, аппаратное обеспечение, канал связи	нарушение доступности
12.21.	УБИ.164	Угроза распространения состояния «отказ в обслуживании» в «облачной» инфраструктуре	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	«облачная» инфраструктура, созданная с использованием технологий виртуализации	нарушение конфиденциальности, целостности, доступности
13.	Угрозы, связанные с использованием технологий виртуализации				
13.1.	УБИ.10	Угроза выхода процесса за пределы виртуальной машины	внешний нарушитель со средним потенциалом, внутренний нарушитель со средним потенциалом	информационная система, сетевой узел, носитель информации, объекты файловой системы, учетные данные пользователя, образ виртуальной машины	нарушение конфиденциальности, целостности, доступности
13.2.	УБИ.44	Угроза нарушения изоляции пользовательских данных внутри виртуальной машины	внешний нарушитель со средним потенциалом, внутренний нарушитель со средним потенциалом	виртуальная машина, гипервизор	нарушение конфиденциальности, целостности, доступности
13.3.	УБИ.48	Угроза нарушения технологии обработки информации путем несанкционированного внесения изменений в образы виртуальных машин	внешний нарушитель со средним потенциалом, внутренний нарушитель со средним потенциалом	образ виртуальной машины, сетевой узел, сетевое программное обеспечение, виртуальная машина	нарушение конфиденциальности, целостности, доступности
13.4.	УБИ.59	Угроза неконтролируемого роста числа зарезервированных вычислительных ресурсов	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	информационная система, сервер	нарушение доступности
13.5.	УБИ.75	Угроза несанкционированного доступа к вирту-	внешний нарушитель с	сетевое программное обес-	нарушение конфиден-

1	2	3	4	5	6
		альным каналам передачи	низким потенциалом, внутренний нарушитель с низким потенциалом	печение, сетевой трафик, виртуальные устройства	циальности
13.6.	УБИ.77	Угроза несанкционированного доступа к данным за пределами зарезервированного адресного пространства, в том числе выделенного под виртуальное аппаратное обеспечение	внешний нарушитель со средним потенциалом, внутренний нарушитель со средним потенциалом	сервер, рабочая станция, виртуальная машина, гипервизор, машинный носитель информации, метаданные	нарушение целостности, доступности
13.7.	УБИ.78	Угроза несанкционированного доступа к защищаемым виртуальным машинам из виртуальной и (или) физической сети	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	виртуальная машина	нарушение конфиденциальности, целостности, доступности
13.8.	УБИ.79	Угроза несанкционированного доступа к защищаемым виртуальным машинам со стороны других виртуальных машин	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	виртуальная машина	нарушение конфиденциальности, целостности, доступности
13.9.	УБИ.80	Угроза несанкционированного доступа к защищаемым виртуальным устройствам из виртуальной и (или) физической сети	внешний нарушитель со средним потенциалом, внутренний нарушитель со средним потенциалом	виртуальные устройства хранения, обработки и передачи данных	нарушение конфиденциальности, целостности, доступности
13.10.	УБИ.84	Угроза несанкционированного доступа к системе хранения данных из виртуальной и (или) физической сети	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	виртуальные устройства хранения данных, виртуальные диски	нарушение конфиденциальности, целостности, доступности
13.11.	УБИ.85	Угроза несанкционированного доступа к хранимой в виртуальном пространстве защищаемой информации	внешний нарушитель со средним потенциалом, внутренний нарушитель со средним потенциалом	носитель информации, объекты файловой системы	нарушение конфиденциальности
13.12.	УБИ.108	Угроза ошибки обновления гипервизора	внутренний наруши-	системное программное	нарушение конфиден-

1	2	3	4	5	6
			тель с низким потенциалом	обеспечение, гипервизор	циальности, целостности, доступности
13.13.	УБИ.119	Угроза перехвата управления гипервизором	внешний нарушитель со средним потенциалом, внутренний нарушитель со средним потенциалом	системное программное обеспечение, гипервизор, консоль управления гипервизором	нарушение конфиденциальности, целостности, доступности
13.14.	УБИ.120	Угроза перехвата управления средой виртуализации	внешний нарушитель со средним потенциалом, внутренний нарушитель со средним потенциалом	информационная система, системное программное обеспечение	нарушение конфиденциальности, целостности, доступности
13.15.		Нарушение доверенной загрузки виртуальных серверов информационной системы, перехват загрузки***			
13.16.		Нарушение целостности конфигурации виртуальных серверов – подмена или искажение образов (данных и оперативной памяти)***			
13.17.		Несанкционированный доступ к консоли управления виртуальной инфраструктурой***			
13.18.		Несанкционированный доступ к виртуальному серверу информационной системы, в том числе несанкционированное сетевое подключение и проведение сетевых атак на виртуальный сервер информационной системы***			
13.19.		Несанкционированный удаленный доступ к ресурсам гипервизора вследствие сетевых атак типа «переполнение буфера»***			
13.20.		Угроза несанкционированного доступа к объектам виртуальной инфраструктуры без прохождения процедуры идентификации и аутентификации***			
13.21.		Угроза несанкционированного доступа к виртуальной инфраструктуре, компонентам виртуальной инфраструктуры, виртуальным машинам или объектам внутри виртуальных машин***			

1	2	3	4	5	6
13.22.		Угроза отсутствия средств регистрации событий в виртуальной инфраструктуре***			
14.	Угрозы, связанные с нарушением правил эксплуатации машинных носителей информации				
14.1.	УБИ.71	Угроза несанкционированного восстановления удаленной защищаемой информации	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	машинный носитель информации	нарушение конфиденциальности
14.2.	УБИ.91	Угроза несанкционированного удаления защищаемой информации	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	метаданные, объекты файловой системы, реестр	нарушение доступности
14.3.	УБИ.156	Угроза утраты носителей информации	внутренний нарушитель с низким потенциалом	носитель информации	нарушение конфиденциальности, доступности
14.4.	УБИ.158	Угроза форматирования носителей информации	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	носитель информации	нарушение целостности, доступности
14.5.		Повреждение носителя информации			
14.6.		Доступ к снятым с эксплуатации носителям информации (содержащим остаточные данные)			
14.7.		Угроза подключения к информационной системе неучтенных машинных носителей***			
14.8.		Угроза подключения к информационной системе неперсонифицированных машинных носителей			
14.9.		Угроза несанкционированного копирования информации на машинные носители***			
14.10.		Угроза несанкционированной модификации или удаления информации на машинных носителях***			
14.11.		Угроза хищения машинных носителей***			
14.12.		Угроза подмены машинных носителей***			
14.13.		Угроза встраивания программно-аппаратных за-			

1	2	3	4	5	6
		кладок в машинные носители***			
14.14.		Угроза несанкционированного доступа к информации, хранящейся на машинном носителе***			
14.15.		Угроза использования машинных носителей для хранения информации разных уровней конфиденциальности и целей обработки			
14.16.		Угроза использования неконтролируемых портов средств вычислительной техники для вывода информации на внешние машинные носители***			
14.17.		Угроза передачи информации или фрагментов информации между пользователями, сторонними организациями при неполном уничтожении или стирании информации с машинных носителей***			
14.18.		Угроза несанкционированного использования машинных носителей			
14.19.		Угроза несанкционированного выноса машинных носителей за пределы контролируемой зоны			
15.	Угрозы, связанные с нарушением процедур установки или обновления программного обеспечения и оборудования				
15.1.	УБИ.5	Угроза внедрения вредоносного кода в BIOS	внутренний нарушитель с высоким потенциалом	микропрограммное и аппаратное обеспечение BIOS/UEFI	нарушение конфиденциальности, целостности, доступности
15.2.	УБИ.23	Угроза изменения компонентов системы	внутренний нарушитель с низким потенциалом	информационная система, сервер, рабочая станция, виртуальная машина, системное программное обеспечение, прикладное программное обеспечение, аппаратное обеспечение	нарушение целостности, доступности
15.3.	УБИ.39	Угроза исчерпания запаса ключей, необходимых для обновления BIOS	внешний нарушитель со средним потенциалом	микропрограммное обеспечение BIOS/UEFI	нарушение целостности
15.4.	УБИ.188	Угроза подмены программного обеспечения	внутренний нарушитель со средним потенциалом	прикладное программное обеспечение, сетевое программное обеспечение, системное программное обеспечение	нарушение конфиденциальности, целостности, доступности

1	2	3	4	5	6
15.5.		Установка программного обеспечения, содержащего уязвимости***			
15.6.		Установка нелицензионного программного обеспечения***			
15.7.		Угроза ошибочного запуска или ошибочной установки программного обеспечения***			
15.8.		Угроза неправильной установки программного обеспечения***			
15.9.		Угроза автоматического запуска вредоносного, нелегального или неразрешенного программного обеспечения при запуске операционной системы и (или) обновлений программного обеспечения			
15.10.		Угроза удаленного запуска или установки вредоносного, нелегального или неразрешенного программного обеспечения			
16.	Угрозы физического доступа к компонентам информационной системы персональных данных				
16.1.	УБИ.139	Угроза преодоления физической защиты	внешний нарушитель со средним потенциалом	сервер, рабочая станция, носитель информации, аппаратное обеспечение	нарушение конфиденциальности, целостности, доступности
16.2.	УБИ.157	Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	внешний нарушитель с низким потенциалом	сервер, рабочая станция, носитель информации, аппаратное обеспечение	нарушение целостности, доступности
16.3.	УБИ.160	Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации	внешний нарушитель с низким потенциалом	сервер, рабочая станция, носитель информации, аппаратное обеспечение	нарушение конфиденциальности, доступности
16.4.		Угроза несанкционированного доступа к СКЗИ***			
16.5.		Угроза нарушения функционирования внутренних машинных носителей и других систем хранения данных***			
16.6.		Угроза доступа к системам обеспечения, их повреждения***			
16.7.		Угроза нарушения функционирования кабельных линий связи, технических средств***			
16.8.		Угроза несанкционированного доступа в контролируемую зону***			

1	2	3	4	5	6
16.9.		Отсутствие средств автоматизированного контроля доступа			
17.	Угрозы эксплуатации уязвимостей системного или прикладного программного обеспечения, средств защиты информации, СКЗИ, аппаратных компонентов информационной системы персональных данных, микропрограммного обеспечения				
17.1.	УБИ.3	Угроза анализа криптографических алгоритмов и их реализации	внешний нарушитель со средним потенциалом	метаданные, системное программное обеспечение	нарушение конфиденциальности, целостности
17.2.	УБИ.9	Угроза восстановления предыдущей уязвимой версии BIOS	внутренний нарушитель с низким потенциалом	микропрограммное обеспечение BIOS/UEFI	нарушение конфиденциальности, целостности, доступности
17.3.	УБИ.13	Угроза деструктивного использования декларированного функционала BIOS	внутренний нарушитель с низким потенциалом	микропрограммное обеспечение BIOS/UEFI	нарушение целостности
17.4.	УБИ.32	Угроза использования поддельных цифровых подписей BIOS	внешний нарушитель со средним потенциалом	микропрограммное и аппаратное обеспечение BIOS/UEFI	нарушение целостности
17.5.	УБИ.35	Угроза использования слабых криптографических алгоритмов BIOS	внешний нарушитель с высоким потенциалом	микропрограммное обеспечение BIOS/UEFI	нарушение конфиденциальности, целостности, доступности
17.6.	УБИ.73	Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети	внешний нарушитель со средним потенциалом, внутренний нарушитель со средним потенциалом	сетевое оборудование, микропрограммное обеспечение, сетевое программное обеспечение, виртуальные устройства	нарушение конфиденциальности, целостности, доступности
17.7.	УБИ.102	Угроза опосредованного управления группой программ через совместно используемые данные	внешний нарушитель со средним потенциалом, внутренний нарушитель со средним потенциалом	системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение	нарушение целостности, доступности
17.8.	УБИ.107	Угроза отключения контрольных датчиков	внешний нарушитель с высоким потенциалом, внутренний нарушитель с низким потенциалом	системное программное обеспечение	нарушение целостности, доступности
17.9.	УБИ.143	Угроза программного выведения из строя средств	внешний нарушитель со	носитель информации,	нарушение доступности

1	2	3	4	5	6
		хранения, обработки и (или) ввода/вывода/передачи информации	средним потенциалом, внутренний нарушитель со средним потенциалом	микропрограммное обеспечение, аппаратное обеспечение	
17.10.	УБИ.150	Угроза сбоя процесса обновления BIOS	внутренний нарушитель со средним потенциалом	микропрограммное и аппаратное обеспечение BIOS/UEFI, каналы связи	нарушение доступности
17.11.	УБИ.154	Угроза установки уязвимых версий обновления программного обеспечения BIOS	внешний нарушитель со средним потенциалом, внутренний нарушитель со средним потенциалом	микропрограммное обеспечение BIOS/UEFI	нарушение конфиденциальности, целостности, доступности
17.12.	УБИ.163	Угроза перехвата исключения/сигнала из привилегированного блока функций	внешний нарушитель со средним потенциалом, внутренний нарушитель со средним потенциалом	системное программное обеспечение	нарушение конфиденциальности, целостности, доступности
17.13.	УБИ.169	Угроза наличия механизмов разработчика	внутренний нарушитель со средним потенциалом	программное обеспечение, техническое средство	нарушение конфиденциальности, целостности, доступности
17.14.	УБИ.173	Угроза «спама» веб-сервера	внешний нарушитель с низким потенциалом	сетевое программное обеспечение	нарушение доступности
17.15.	УБИ.192	Угроза использования уязвимых версий программного обеспечения	внутренний нарушитель с низким потенциалом, внешний нарушитель с низким потенциалом	прикладное программное обеспечение, сетевое программное обеспечение, системное программное обеспечение	нарушение конфиденциальности, целостности, доступности
18.	Угрозы, связанные с использованием сетевых технологий				
18.1.	УБИ.11	Угроза деавторизации санкционированного клиента беспроводной сети	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	сетевой узел	нарушение доступности
18.2.	УБИ.19	Угроза заражения кеша системы доменных имен (DNS-кеша)	внешний нарушитель с низким потенциалом	сетевой узел, сетевое программное обеспечение, сетевой трафик	нарушение конфиденциальности

1	2	3	4	5	6
18.3.	УБИ.34	Угроза использования слабостей протоколов сетевого/локального обмена данными	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	системное программное обеспечение, сетевое программное обеспечение, сетевой трафик	нарушение конфиденциальности
18.4.	УБИ.69	Угроза неправомерных действий в каналах связи	внешний нарушитель с низким потенциалом	сетевой трафик	нарушение конфиденциальности, целостности
18.5.	УБИ.92	Угроза несанкционированного удаленного внеполосного доступа к аппаратным средствам	внешний нарушитель с высоким потенциалом	информационная система, аппаратное обеспечение	нарушение конфиденциальности, целостности, доступности
18.6.	УБИ.125	Угроза подключения к беспроводной сети в обход процедуры аутентификации	внешний нарушитель с низким потенциалом	сетевой узел, сетевое программное обеспечение	нарушение конфиденциальности, целостности, доступности
18.7.	УБИ.126	Угроза подмены беспроводного клиента или точки доступа	внешний нарушитель с низким потенциалом	сетевой узел, сетевое программное обеспечение, аппаратное обеспечение, точка беспроводного доступа	нарушение конфиденциальности, доступности
18.8.	УБИ.128	Угроза подмены доверенного пользователя	внешний нарушитель с низким потенциалом	сетевой узел, сетевое программное обеспечение	нарушение конфиденциальности
18.9.	УБИ.131	Угроза подмены субъекта сетевого доступа	внешний нарушитель со средним потенциалом	прикладное программное обеспечение, сетевое программное обеспечение, сетевой трафик	нарушение конфиденциальности, целостности
18.10.	УБИ.174	Угроза «фарминга»	внешний нарушитель с низким потенциалом	рабочая станция, сетевое программное обеспечение, сетевой трафик	нарушение конфиденциальности
18.11.		Угроза удаленного запуска приложений			
18.12.		Угроза навязывания ложных маршрутов***			
18.13.		Угроза внедрения ложных объектов сети***			
18.14.		Угроза проведения атак или попыток несанкционированного доступа в информационную систему с использованием протоколов сетевого доступа***			
18.15.		Угроза отсутствия механизмов реагирования (блокирования) атак или вторжений***			

1	2	3	4	5	6
18.16.		Угроза отсутствия системы анализа сетевого трафика при обмене данными между информационными системами на наличие атак или вторжений***			
18.17.		Угроза отсутствия системы анализа сетевого трафика между сегментами информационной системы на наличие атак или вторжений***			
18.18.		Угроза использования неактуальных версий сигнатур обнаружения атак***			
18.19.		Угроза отсутствия централизованной системы управления средствами защиты от атак или вторжений			
18.20.		Угроза использования слабостей или уязвимостей защиты протоколов удаленного доступа***			
18.21.		Угроза бесконтрольного использования технологий беспроводного доступа, в том числе с мобильных устройств***			
18.22.		Угроза подмены устройств, подключаемых к информационной системе с использованием технологии удаленного доступа***			
18.23.		Угроза использования неконтролируемых сетевых протоколов для модификации или перехвата управления информационной системой***			
18.24.		Угроза перехвата, искажения, модификации, подмены, перенаправления трафика между разными категориями пользователей и средствами защиты информации***			
18.25.		Угроза подмены сетевых адресов, определяемых по сетевым именам***			
18.26.		Угроза отсутствия проверки подлинности сетевых соединений***			
18.27.		Отсутствие подтверждения факта отправки и получения информации конкретными пользователями***			
18.28.		Угроза получения несанкционированного доступа			

1	2	3	4	5	6
		при двунаправленной передаче информации между сегментами, информационными системами			
18.29.		Отсутствие контроля соединений между средствами вычислительной техники информационной системы			
18.30.		Угроза несанкционированного доступа к средствам управления информационными потоками			
18.31.		Угроза отсутствия/неиспользования средств разделения информационных потоков, содержащих различные виды (категории) информации, а также отделение информации управления от пользовательской информации			
18.32.		Отсутствие средств анализа сетевого трафика на наличие вредоносного программного обеспечения			
18.33.		Угроза доступа к информационной системе с использованием беспроводного доступа из-за границ контролируемой зоны			
19.	Угрозы инженерной инфраструктуры				
19.1.		Угроза сбоев в сети электропитания			
19.2.		Угроза выхода из строя технических средств в результате нарушения климатических параметров работы			
19.3.		Угрозы нарушения схем электропитания***			
19.4.		Угроза, связанная с отсутствием заземления или неправильным заземлением***			
20.	Угрозы, связанные с отсутствием системы регистрации событий информационной безопасности				
20.1.		Угроза отсутствия системы регистрации событий информационной безопасности***			
20.2.		Угроза автоматического удаления или затирания событий информационной безопасности новыми событиями***			
20.3.		Угроза переполнения журналов информационной безопасности***			
20.4.		Угроза отсутствия подсистемы централизованного сбора событий информационной безопасности от			

1	2	3	4	5	6
		различных программных и аппаратных продуктов, средств защиты информации***			
20.5.		Угроза неправильного отнесения событий к событиям информационной безопасности***			
20.6.		Угроза отсутствия централизованной системы анализа журналов информационной безопасности, формируемых программными и аппаратными средствами, средствами защиты информации***			
20.7.		Угроза отключения журналов информационной безопасности***			
20.8.		Угроза модификации или удаления журнала информационной безопасности***			
20.9.		Угроза задержек при получении журналов информационной безопасности			
20.10.		Угроза ошибок ведения журнала регистрации событий информационной безопасности, в том числе связанных с неправильными настройками времени			
20.11.		Угроза отсутствия необходимых сведений в журналах информационной безопасности для проведения проверки, расследования и анализа событий информационной безопасности***			
20.12.		Угроза отключения или отказа системы регистрации событий информационной безопасности			
20.13.		Угроза несанкционированного изменения правил ведения журнала регистрации событий			
20.14.		Отсутствие оповещений (предупреждений) администратора о сбоях, критических событиях в работе системы регистрации событий информационной безопасности			
21.	Угрозы, связанные с контролем защищенности информационной системы персональных данных				
21.1.		Угроза отсутствия контроля за уязвимостями информационной системы, ее компонентов, программного обеспечения***			
21.2.		Угроза использования неактуальных версий баз			

1	2	3	4	5	6
		данных уязвимостей, применяемых средствами анализа защищенности***			
21.3.		Угроза установки программного обеспечения или обновлений без проведения анализа уязвимостей			
21.4.		Угроза отсутствия регулярного контроля за защищенностью информационной системы, в том числе средств защиты информации, с учетом новых угроз безопасности информации			
21.5.		Угроза отсутствия анализа изменения настроек информационной системы, ее компонентов, средств защиты информации на предмет появления уязвимостей***			
21.6.		Отсутствие журнала анализа защищенности			
22.	Угрозы, связанные с перехватом защищаемой информации при ее передаче по каналам связи				
22.1.	УБИ.17	Угроза доступа/перехвата/изменения HTTP cookies (фрагментов данных, передаваемых с использованием протокола передачи гипертекста)	внешний нарушитель с низким потенциалом	прикладное программное обеспечение, сетевое программное обеспечение	нарушение конфиденциальности, доступности
22.2.	УБИ.116	Угроза перехвата данных, передаваемых по вычислительной сети	внешний нарушитель с низким потенциалом	сетевой узел, сетевой трафик	нарушение конфиденциальности
22.3.		Угроза перехвата данных, передаваемых с использованием технологий беспроводного доступа***			
23.	Угрозы, связанные с использованием мобильных устройств				
23.1.	УБИ.184	Угроза агрегирования данных, обрабатываемых с помощью мобильного устройства	внутренний нарушитель со средним потенциалом	мобильное устройство	нарушение конфиденциальности
23.2.	УБИ.194	Угроза несанкционированного использования привилегированных функций мобильного устройства	внешний нарушитель с высоким потенциалом	мобильное устройство	нарушение конфиденциальности, целостности, доступности
23.3.		Угроза установки на мобильные устройства вредоносных или уязвимых версий программного обеспечения***			

* Идентификаторы угроз приведены в соответствии с банком данных угроз безопасности информации, размещенным на официальном сайте Федеральной службы по техническому и экспортному контролю в информационно-телекоммуникационной сети «Интернет».

** Данные по незаполненным ячейкам таблицы заполняются при разработке частной модели угроз безопасности персональных данных и определении угроз безопасности персональных данных, актуальных при обработке персональных данных в соответствующей информационной системе персональных данных, эксплуатируемой органом исполнительной власти Чувашской Республики или подведомственной ему организацией.

*** Базовые угрозы безопасности персональных данных при обработке персональных данных в информационных системах персональных данных.

_____

Приложение № 2
к угрозам безопасности персональных данных, актуальным при обработке персональных данных в информационных системах персональных данных, эксплуатируемых в органах исполнительной власти Чувашской Республики и подведомственных им организациях

ТИПОВЫЕ ВОЗМОЖНОСТИ
нарушителей безопасности информации и направления атак

№ пп	Возможности нарушителей безопасности информации и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак*	Обоснование отсутствия (при наличии)*
1	2	3	4
1.	Проведение атаки при нахождении за пределами контролируемой зоны		
2.	Проведение атаки при нахождении в пределах контролируемой зоны		
3.	Проведение атак на этапе эксплуатации средств криптографической защиты информации (далее – СКЗИ) на: документацию на СКЗИ и компоненты среды их функционирования; помещения, в которых находится совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем, на которых реализованы СКЗИ и среда их функционирования		
4.	Получение в рамках предоставленных полномочий, а также в результате наблюдений: сведений о физических мерах защиты объектов, в которых размещены ресурсы информационной системы персональных данных (далее также – информационная система); 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 средства вычислительной техники, на которых реализованы СКЗИ и среда их функционирования		

1	2	3	4
5.	Использование штатных средств информационной системы, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий		
	Физический доступ к средствам вычислительной техники, на которых реализованы СКЗИ и среда их функционирования		
6.	Возможность воздействовать на аппаратные компоненты СКЗИ и среду их функционирования, ограниченная мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий		
7.	Создание способов, подготовка и проведение атак с привлечением специалистов в области анализа сигналов, сопровождающих функционирование СКЗИ и среды их функционирования, и в области использования для реализации атак недокументированных (недекларированных) возможностей прикладного программного обеспечения		
8.	Проведение лабораторных исследований СКЗИ, используемых вне контролируемой зоны, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий		
9.	Проведение работ по созданию способов и средств атак в научно-исследовательских центрах, специализирующихся в области разработки и анализа СКЗИ и среды их функционирования, в том числе с использованием исходных текстов входящего в среду функционирования прикладного программного обеспечения, непосредственно использующего вызовы программных функций СКЗИ		
10.	Создание способов, подготовка и проведение атак с привлечением специалистов в области использования недокументированных (недекларированных) возможностей системного программного обеспечения для реализации атак		
11.	Возможность располагать сведениями, содержащимися в конструкторской документации на аппаратные и программные компоненты среды функционирования СКЗИ		
12.	Возможность воздействовать на любые компоненты СКЗИ и среду их функционирования		

---

* Данные по незаполненным ячейкам таблицы заполняются при разработке органами исполнительной власти Чувашской Республики или подведомственными им организациями частной модели угроз безопасности персональных данных и определении угроз безопасности персональных данных, актуальных при обработке персональных данных в соответствующей информационной системе персональных данных, эксплуатируемой органом исполнительной власти Чувашской Республики или подведомственной ему организацией.