ПРАВИТЕЛЬСТВО ОРЕНБУРГСКОЙ ОБЛАСТИ

П О С Т А Н О В Л Е Н И Е

28.06.2019 г. Оренбург № 418-пп

Об утверждении положения об угрозах безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных органов исполнительной власти Оренбургской области

В соответствии с частью 5 статьи 19 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» и в целях обеспечения единого подхода к определению угроз безопасности, актуальных при обработке персональных данных в информационных системах органов исполнительной власти Оренбургской области, Правительство Оренбургской области п о с т а н о в л я е т:

1. Утвердить положение об угрозах безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных органов исполнительной власти Оренбургской области (далее – положение), согласно приложению.

2. Органам исполнительной власти Оренбургской области при составлении частных моделей угроз руководствоваться положением.

3. Рекомендовать органам местного самоуправления муниципальных образований Оренбургской области при составлении частных моделей угроз руководствоваться положением.

4. Контроль за исполнением настоящего постановления возложить на директора департамента информационных технологий Оренбургской области.

5. Постановление вступает в силу после его официального опубликования.

Временно исполняющий обязанности Губернатора Д.В.Паслер

АППАРАТ ГУБЕРНАТОРА И ПРАВИТЕЛЬСТВА ОРЕНБУРГСКОЙ ОБЛАСТИ
УПРАВЛЕНИЕ ДОКУМЕНТАЦИОННОГО ОБЕСПЕЧЕНИЯ

Приложение
к постановлению
Правительства области
от 28.06.2019 № 418-пп

Положение
об угрозах безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных органов исполнительной власти Оренбургской области

I. Общие положения

1. Настоящее Положение определяет угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, владельцами и операторами которых являются органы исполнительной власти Оренбургской области, государственные учреждения и предприятия Оренбургской области (далее – органы власти и организации).

2. При определении угроз безопасности персональных данных, актуальных для конкретной информационной системы персональных данных, следует проводить анализ угроз безопасности информации и уязвимостей программного обеспечения с учетом угроз и уязвимостей, содержащихся в банке данных угроз безопасности информации Федеральной службы по техническому и экспортному контролю bdu.fstec.ru в информационно-телекоммуникационной сети «Интернет».

3. Органами власти и организациями в целях реализации полномочий и осуществления функций обрабатываются все категории персональных данных. Состав персональных данных, подлежащих обработке в конкретной информационной системе персональных данных, цели такой обработки, действия (операции), совершаемые с персональными данными в информационных системах персональных данных, определяются оператором информационных систем персональных данных.

II. Участники взаимодействия и сети передачи данных

4. Контролируемой зоной информационных систем персональных данных являются здания и отдельные помещения, принадлежащие органам власти и организациям или арендуемые ими (далее – контролируемая зона). Все средства вычислительной техники, участвующие в обработке персональных данных, располагаются в пределах контролируемой зоны. Вне контролируемой зоны находятся линии передачи данных и телекоммуникационное оборудование оператора связи (провайдера), используемые для информационного обмена по сетям связи общего пользования (сетям международного информационного обмена).

5. Локальные вычислительные сети передачи данных в органах власти и организациях организованы по топологии «звезда» и имеют подключения к следующим сетям:

1) внешние сети (сети провайдера). Подключение к внешним сетям (сетям провайдера) организовано посредством следующих типов каналов связи:

оптоволоконные каналы связи операторов связи (провайдеров);

проводные каналы связи операторов связи (провайдеров);

2) сети органов власти и организаций, организаций (предприятий, учреждений), расположенных на территории Российской Федерации. Подключение к таким сетям осуществляется в соответствии с разработанными регламентами взаимодействия. Органы власти и организации подключены к единой информационно-телекоммуникационной сети посредством защищенных каналов связи;

3) иные сети, взаимодействие с которыми организовано органами власти и организациями с целью реализации своих полномочий.

6. Подключение к сетям связи общего пользования осуществляется органами власти и организациями с применением средств криптографической защиты информации.

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

7. При определении органами власти и организациями угроз безопасности персональных данных в конкретной информационной системе персональных данных защите подлежат следующие объекты, входящие в информационные системы персональных данных:

персональные данные, обрабатываемые в информационных системах персональных данных;

информационные ресурсы информационных систем персональных данных (файлы, базы данных и другое);

средства вычислительной техники, участвующие в обработке персональных данных посредством информационных систем персональных данных;

средства криптографической защиты информации и средства защиты информации;

среда функционирования средств криптографической защиты информации;

информация, относящаяся к криптографической защите персональных данных, в том числе ключевая, парольная и аутентифицирующая информация средств криптографической защиты информации;

документы, дела, журналы, картотеки, издания, технические документы, видео-, кино- и фотоматериалы, рабочие и другие материалы, отражающие защищаемую информацию, относящуюся к информационным системам персональных данных и их криптографической защите, включая документацию на средства криптографической защиты информации, технические и

программные компоненты среды функционирования средств криптографической защиты информации;

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

каналы (линии) связи, включая кабельные системы, используемые информационными системами персональных данных;

сети передачи данных, не выходящие за пределы контролируемой зоны информационной системы персональных данных;

помещения, в которых обрабатываются персональные данные посредством информационных систем персональных данных и располагаются компоненты информационной системы персональных данных;

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

8. К средствам вычислительной техники, участвующей в обработке персональных данных посредством информационных систем персональных данных, относятся:

автоматизированные рабочие места пользователей с различными уровнями доступа (правами) – программно-аппаратный комплекс, позволяющий осуществлять доступ пользователей к информационной системе персональных данных и предназначенный для локальной обработки информации;

терминальная станция – программно-аппаратный комплекс, позволяющий осуществлять доступ пользователей к информационной системе персональных данных, но не предназначенный для локальной обработки информации;

серверное оборудование – программно-аппаратный комплекс, предназначенный для обработки и консолидированного хранения данных информационных систем персональных данных. Серверное оборудование может быть представлено автоматизированными рабочими местами пользователей, выполняющими функции сервера;

сетевое и телекоммуникационное оборудование, используемое для информационного обмена между серверным оборудованием, автоматизированным рабочим местом пользователя, терминальными станциями (коммутаторы, маршрутизаторы и другое);

общесистемное программное обеспечение (операционные системы физических серверов, виртуальных серверов, автоматизированных рабочих мест).

9. Ввод персональных данных в информационные системы персональных данных в органах власти и организациях осуществляется как с бумажных, так и с электронных носителей информации. Персональные данные хранятся и (или) передаются третьим лицам как в электронном, так и в бумажном виде.

IV. Информационные системы персональных данных

10. С целью реализации полномочий и осуществления функций органами власти и организациями обрабатываются все категории персональных данных. Состав персональных данных, подлежащих обработке в конкретной информационной системе персональных данных, цели обработки, действия (операции), совершаемые с персональными данными в информационной системе персональных данных, определяются владельцем или оператором информационной системы персональных данных.

11. Обработка персональных данных в информационной системе персональных данных осуществляется с соблюдением принципов и правил, предусмотренных Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных». Перечень обрабатываемых персональных данных в информационной системе персональных данных соответствует целям их обработки и не является избыточным.

12. Информационные системы персональных данных подразделяются на:

информационные системы персональных данных, операторами которых являются органы власти и организации;

информационные системы персональных данных, эксплуатируемые органами власти и организациями, но не в качестве их операторов.

13. В зависимости от технологии обработки персональных данных, целей и состава персональных данных информационные системы персональных данных подразделяются на:

информационно-справочные;

сегментные;

внутриобластные;

ведомственные;

служебные.

14. Для всех категорий персональных данных информационных систем персональных данных, указанных в пунктах 12, 13 настоящего Положения, необходимо обеспечивать следующие характеристики безопасности:

конфиденциальность;

целостность;

доступность;

подлинность.

При этом должна сохраняться возможность модификации и передачи персональных данных.

15. Информационно-справочные информационные системы персональных данных используются для официального доведения любой информации до определенного или неопределенного круга лиц, при этом факт доведения такой информации не порождает правовых последствий, однако может являться обязательным согласно законодательству Российской Федерации.

15.1. К основным информационно-справочным информационным системам персональных данных относятся:

«Официальные порталы (сайты) органов власти и организаций»;

«Информационные порталы (сайты), которые ведутся конкретным органом власти и организацией и посвящаются определенному проекту и (или) мероприятию, проводимому на территории Оренбургской области» (далее – «Информационные порталы (сайты)»;

«Закрытые порталы для нескольких групп участников органов власти и организаций»;

«Специализированная информационная система «Портал государственных услуг Оренбургской области».

15.2. Информационно-справочные информационные системы персональных данных «Официальные порталы (сайты) органов власти и организаций» содержат сведения о деятельности органов власти и организаций, в том числе сведения, подлежащие обязательному опубликованию в соответствии с законодательством Российской Федерации и Оренбургской области.

К категориям персональных данных, которые могут подлежать обработке в информационных системах персональных данных «Официальные порталы (сайты) органов власти и организаций», относятся:

общедоступные;

иные.

Режим обработки персональных данных в информационных системах персональных данных «Официальные порталы (сайты) органов власти и организаций» является многопользовательским, то есть данная информационная система персональных данных предусматривает разграничение доступа. Обработка персональных данных осуществляется посредством веб-интерфейса сотрудниками органов власти и организаций, являющихся операторами информационной системы персональных данных «Официальные порталы (сайты) органов власти и организаций», и гражданами всех стран мира. Персональные данные хранятся в базе данных информационной системы персональных данных «Официальные порталы (сайты) органов власти и организаций» и отображаются по запросу соответствующей страницы данной информационной системы персональных данных пользователям в соответствии с предоставленными правами.

Типами субъектов персональных данных, которые могут подлежать обработке в информационных системах персональных данных «Официальные порталы (сайты) органов власти и организаций», являются сотрудники органов власти и организаций, являющихся операторами данной информационной системы персональных данных, и граждане всех стран мира.

Структура информационных систем персональных данных «Официальные порталы (сайты) органов власти и организаций» – локальная, функционирующая в контролируемой зоне органа власти и организации, и (или) на серверном оборудовании иного органа власти и организации в пределах их контролируемых зон, и (или) на вычислительных ресурсах «облачного» провайдера.

Информационные системы персональных данных «Официальные порталы (сайты) органов власти и организаций» подключены к сетям связи общего пользования (сетям международного информационного обмена). По типу подключения данные информационные системы персональных данных делятся на:

подключенные посредством единой информационно-телекоммуникационной сети;

подключенные с использованием иных каналов связи.

Средствами вычислительной техники, участвующими в обработке информации, являются автоматизированные рабочие места пользователей, серверное оборудование, сетевое и телекоммуникационное оборудование.

Уровень защищенности информационных систем персональных данных «Официальные порталы (сайты) органов власти и организаций» – четвертый.

15.3. Информационно-справочные информационные системы персональных данных «Информационные порталы (сайты)» содержат сведения о мероприятиях, проводимых органами власти и организациями в соответствии с их функциями и полномочиями.

К категориям персональных данных, которые могут подлежать обработке в информационных системах персональных данных «Информационные порталы (сайты)», относятся:

общедоступные;

иные.

Режим обработки персональных данных в информационных системах персональных данных «Информационные порталы (сайты)» является многопользовательским, то есть, данные информационные системы персональных данных предусматривают разграничение доступа. Обработка персональных данных осуществляется посредством веб-интерфейса сотрудниками органов власти и организаций, являющихся операторами информационных систем персональных данных «Информационные порталы (сайты)», и гражданами всех стран мира. Персональные данные хранятся в базе данных информационных систем персональных данных «Информационные порталы (сайты)» и отображаются по запросу соответствующей страницы информационной системы персональных данных пользователям в соответствии с предоставленными правами.

Типами субъектов персональных данных, которые могут подлежать обработке в информационных системах персональных данных «Информационные порталы (сайты)», являются сотрудники органов власти и организаций, являющихся операторами данных информационных систем персональных данных, и граждане всех стран мира.

Структура информационных систем персональных данных «Информационные порталы (сайты)» – локальная, функционирующая в контролируемой зоне органа власти и организации, и (или) на серверном оборудовании иного органа власти и организации в пределах их контролируемой зоны, и (или) на вычислительных ресурсах «облачного» провайдера.

Информационные системы персональных данных «Информационные порталы (сайты)» подключены к сетям связи общего пользования (сетям международного информационного обмена). По типу подключения данные информационные системы персональных данных делятся на подключенные посредством:

единой информационно-телекоммуникационной сети;

иных каналов связи.

Средствами вычислительной техники, участвующими в обработке информации, являются автоматизированные рабочие места пользователей, серверное оборудование, сетевое и телекоммуникационное оборудование.

Уровень защищенности информационно-справочных систем персональных данных «Информационные порталы (сайты)» – четвертый.

15.4. Информационно-справочные информационные системы персональных данных «Закрытые порталы для нескольких групп участников органов власти и организаций» содержат сведения, предоставляемые ограниченному круг лиц из числа органов власти и организаций в соответствии с функциями и полномочиями органов власти и организаций.

К категориям персональных данных, которые могут подлежать обработке в информационных системах персональных данных «Закрытые порталы для нескольких групп участников органов власти и организаций», относятся:

общедоступные;

иные.

Режим обработки персональных данных в информационных системах персональных данных «Закрытые порталы для нескольких групп участников органов власти и организаций» является многопользовательским, то есть данные информационные системы персональных данных предусматривают разграничение доступа. Обработка персональных данных осуществляется сотрудниками органов власти и организаций посредством веб-интерфейса в соответствии с предоставленными правами. Персональные данные хранятся в базе данных информационных систем персональных данных и отображаются по запросу соответствующей страницы информационной системы персональных данных пользователям в соответствии с предоставленными правами.

Типами субъектов персональных данных, которые могут подлежать обработке в информационных системах персональных данных «Закрытые порталы для нескольких групп участников органов власти и организаций», являются сотрудники органов власти и организаций.

Структура информационной системы персональных данных «Закрытые порталы для нескольких групп участников органов власти и организаций» – локальная, функционирующая в контролируемых зонах органа власти и организации, и (или) на серверном оборудовании иного органа власти и организации в пределах их контролируемых зон, и (или) на вычислительных ресурсах «облачного» провайдера.

Информационные системы персональных данных «Закрытые порталы для нескольких групп участников органов власти и организаций» подключены к сетям связи общего пользования (сетям международного информационного обмена). По типу подключения информационные системы персональных данных «Закрытые порталы для нескольких групп участников органов власти и организаций» делятся на подключенные посредством:

единой информационно-телекоммуникационной сети;

иных каналов связи.

Средствами вычислительной техники, участвующими в обработке информации, являются автоматизированные рабочие места пользователей, серверное оборудование, сетевое и телекоммуникационное оборудование.

Уровни защищенности информационных систем персональных данных «Закрытые порталы для нескольких групп участников органов власти и организаций» – третий, четвертый.

15.5. Информационно-справочная информационная система персональных данных «Специализированная информационная система «Портал государственных услуг Оренбургской области» содержит социально значимую информацию и сведения, необходимые для получения гражданами государственных и муниципальных услуг в электронном виде.

К категориям персональных данных, которые могут подлежать обработке в информационной системе персональных данных «Специализированная информационная система «Портал государственных услуг Оренбургской области», относятся:

общедоступные;

иные.

Режим обработки персональных данных в информационной системе персональных данных «Специализированная информационная система «Портал государственных услуг Оренбургской области» является многопользовательским, то есть данная информационная система персональных данных предусматривает разграничение доступа. Обработка персональных данных осуществляется в соответствии с предоставленными правами сотрудниками органов власти и организаций и гражданами всех стран мира в режиме веб-интерфейса.

Персональные данные обрабатываются в деперсонифицированном (обезличенном) виде. Запрашиваемые данные не позволяют однозначно идентифицировать субъект персональных данных без использования сторонних баз данных. После получения запрашиваемых данных информационная система персональных данных «Специализированная информационная система «Портал государственных услуг Оренбургской области» для получения ответа на запрос субъекта персональных данных передает его данные по закрытым каналам связи в информационные системы персональных данных иных органов власти и организаций, в чью компетенцию входит предоставление информации по запросу субъекта. Ответ на запрос (сведения о ходе исполнения запроса) субъекта отображается в данной информационной системе персональных данных.

Типами субъектов персональных данных, которые могут подлежать обработке в информационной системе персональных данных «Специализированная информационная система «Портал государственных услуг Оренбургской области», являются сотрудники органов власти и организаций, являющихся операторами данной информационной системы персональных данных, и граждане всех стран мира.

Структура информационной системы персональных данных «Специализированная информационная система «Портал государственных услуг Оренбургской области» – локальная, функционирующая в контролируемых зонах органа власти и организации, и (или) на серверном оборудовании иного органа власти и организации в пределах их контролируемых зон, и (или) на вычислительных ресурсах «облачного» провайдера.

Информационная система персональных данных «Специализированная информационная система «Портал государственных услуг Оренбургской области» подключена к сетям связи общего пользования (сетям международного информационного обмена). Существует два типа подключения данной информационной системы персональных данных к сетям связи общего пользования:

посредством единой информационно-телекоммуникационной сети;

посредством иных каналов связи.

Средствами вычислительной техники, участвующими в обработке информации, являются автоматизированные рабочие места пользователей, серверное оборудование, сетевое и телекоммуникационное оборудование.

Уровни защищенности информационной системы персональных данных «Специализированная информационная система «Портал государственных услуг Оренбургской области» – второй, третий, четвертый.

16. Сегментные информационные системы персональных данных представляют собой сегменты федеральных информационных систем, создаются и эксплуатируются в Оренбургской области на основании рекомендаций (правовых, организационных, технических), предоставляемых владельцами данных информационных систем персональных данных (федеральными органами государственной власти), и используются для сбора, обработки, свода данных по Оренбургской области и передачи их в федеральные органы государственной власти и наоборот, при этом цели и задачи создания (модернизации), эксплуатации сегментных информационных систем персональных данных определяются федеральными органами государственной власти. Данные информационные системы персональных данных предназначены для реализации полномочий федеральных органов государственной власти и осуществления функций органов власти и организаций.

16.1. К основным сегментным информационным системам персональных данных относятся:

региональный сегмент единой государственной информационной системы в сфере здравоохранения Оренбургской области;

государственная информационная система жилищно-коммунального хозяйства;

государственная информационная система о государственных муниципальных платежах.

К категориям персональных данных, которые могут подлежать обработке в сегментных информационных системах персональных данных, относятся:

специальные;

сотрудников оператора;

общедоступные;

иные.

Режим обработки персональных данных в сегментных информационных системах персональных данных является многопользовательским, то есть данные информационные системы персональных данных предусматривают разграничение доступа. Обработка персональных данных осуществляется в соответствии с предоставленными правами сотрудниками органов власти и организаций в специализированных программах и (или) посредством веб-интерфейса, в отдельных случаях – гражданами всех стран мира в режиме веб-интерфейса (с ограниченными правами доступа).

Типами субъектов персональных данных, которые могут подлежать обработке в сегментных информационных системах персональных данных, являются граждане всех стран мира.

Структура сегментных информационных систем персональных данных – распределенная или локальная, функционирующая в контролируемых зонах органа власти и организации.

Сегментные информационные системы персональных данных подключены к сетям связи общего пользования (сетям международного информационного обмена).

По типу подключения сегментные информационные системы персональных данных делятся на подключенные посредством:

единой информационно-телекоммуникационной сети;

иных каналов связи.

Обмен (передача и получение) персональных данных с иными информационными системами персональных данных осуществляется в зависимости от технологии подключения к сетям связи общего пользования (сетям международного информационного обмена):

без подключения (передача персональных данных осуществляется с использованием машинных носителей);

посредством единой информационно-телекоммуникационной сети;

с использованием средств криптографической защиты информации.

Средствами вычислительной техники, участвующими в обработке информации, являются автоматизированные рабочие места пользователей, терминальная станция, серверное оборудование, сетевое и телекоммуникационное оборудование.

16.2. По технологии обработки сегментные информационные системы персональных данных подразделяются на:

построенные по технологии толстого клиента: на рабочие места пользователей сегментных информационных систем персональных данных устанавливается специальное клиентское приложение, осуществляющее подключение к серверному сегменту, располагающемуся в пределах контролируемой зоны органа власти и организации и передающее данные на центральный сегмент или напрямую в центральный сегмент;

построенные по технологии толстого клиента: на рабочие места пользователей сегментных информационных систем персональных данных устанавливается специальное клиентское приложение, осуществляющее выгрузку данных на локальный носитель и последующую передачу выгруженных данных посредством защищенного канала связи или нарочно;

построенные по технологии тонкого клиента: на рабочие места пользователей сегментных информационных систем персональных данных передается только графическая информация, сама обработка данных осуществляется на удаленном серверном сегменте, располагающемся в пределах контролируемой зоны органа власти и организации и передающем данные на центральный сегмент, или на центральном сегменте.

16.3. Сегментные информационные системы персональных данных, реализованные по технологии тонкого клиента, подразделяются на:

реализованные посредством веб-интерфейса с применением веб-браузера и авторизацией с помощью логина и пароля и (или) сертификата электронной подписи в соответствии с Федеральным законом от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи»;

реализованные с использованием терминального доступа с авторизацией с помощью логина и пароля и (или) сертификата электронной подписи в соответствии с Федеральным законом от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи».

Уровни защищенности сегментных информационных систем персональных данных – первый, второй, третий.

17. Внутриобластные информационные системы персональных данных создаются и эксплуатируются по желанию (на основании решения) органа власти и организации в интересах нескольких органов власти и организаций, при этом цели и задачи создания (модернизации), эксплуатации данных информационных систем персональных данных, а также требования к ним определяются на уровне органа власти и организации.

17.1. По осуществляемым функциям внутриобластные информационные системы персональных данных подразделяются на:

интеграционные (государственная автоматизированная информационная система «Электронный социальный регистр населения Оренбургской области»);

многопрофильные (единая автоматизированная система электронного документооборота и делопроизводства в органах исполнительной власти Оренбургской области, государственная информационная система «Автоматизированная информационная система поддержки деятельности много-

функциональных центров предоставления государственных и муниципальных услуг и межведомственных запросов Оренбургской области»);

информационные системы персональных данных для органов власти и организаций и иных организаций (предприятий, учреждений) Оренбургской области (информационная система удостоверяющего центра электронной подписи).

17.2. Внутриобластные информационные системы персональных данных интеграционные характеризуются отсутствием пользователей (кроме администраторов информационных систем персональных данных и администраторов безопасности информационных систем персональных данных) и функционируют исключительно в целях интеграции и передачи данных между информационными системами персональных данных иных категорий.

К категориям персональных данных, которые могут подлежать обработке во внутриобластных информационных системах персональных данных интеграционных, относятся:

специальные;

общедоступные.

иные.

Режим обработки персональных данных во внутриобластных информационных системах персональных данных интеграционных является многопользовательским, то есть данные информационные системы персональных данных предусматривают разграничение доступа. Обработка персональных данных осуществляется сотрудниками органов власти и организаций в специализированных программах и (или) посредством веб-интерфейса в соответствии с предоставленными правами.

Типами субъектов персональных данных, которые могут подлежать обработке во внутриобластных информационных системах персональных данных интеграционных, являются граждане всех стран мира.

Структура во внутриобластных информационных системах персональных данных интеграционных – локальная или распределенная, функционирующая в контролируемых зонах органа власти и организации.

Внутриобластные информационные системы персональных данных интеграционные подключены к сетям связи общего пользования (сетям международного информационного обмена). По типу подключения внутриобластные информационные системы персональных данных интеграционные делятся на:

подключенные посредством единой информационно-телекоммуникационной сети;

подключенные с использованием иных каналов связи.

Обмен (передача и получение) персональных данных с иными информационными системами персональных данных осуществляется в зависимости от технологии подключения к сетям связи общего пользования (сетям международного информационного обмена):

без подключения (передача персональных данных осуществляется с использованием машинных носителей);

посредством единой информационно-телекоммуникационной сети;

с использованием средств криптографической защиты информации.

Средствами вычислительной техники, участвующими в обработке информации, являются автоматизированные рабочие места пользователей, серверное оборудование, сетевое и телекоммуникационное оборудование.

Уровни защищенности внутриобластной информационных систем персональных данных интеграционных – первый, второй, третий.

17.3. Внутриобластные информационные системы персональных данных многопрофильные предназначены для централизованной автоматизации делопроизводства и документооборота, учета корреспонденции, обращений граждан, обеспечения доступа к электронным документам в органах власти и организациях.

К категориям персональных данных, которые могут подлежать обработке во внутриобластных информационных системах персональных данных многопрофильных, относятся:

специальные;

общедоступные;

иные.

Режим обработки персональных данных во внутриобластных информационных системах персональных данных многопрофильных является многопользовательским, то есть данные информационные системы персональных данных предусматривают разграничение доступа. Обработка персональных данных осуществляется сотрудниками органов власти и организаций в специализированных программах в соответствии с предоставленными правами.

Типами субъектов персональных данных, которые могут подлежать обработке во внутриобластных информационных системах персональных данных многопрофильных, являются граждане всех стран мира.

Структура внутриобластных информационных систем персональных данных многопрофильных – локальная или распределенная, функционирующая в контролируемых зонах органа власти и организации.

Внутриобластные информационные системы персональных данных многопрофильные подключены к сетям связи общего пользования (сетям международного информационного обмена). По типу подключения данные информационные системы персональных данных делятся на:

подключенные посредством единой информационно-телекоммуникационной сети;

подключенные с использованием иных каналов связи.

Обмен (передача и получение) персональных данных с иными информационными системами персональных данных осуществляется в зависимости от технологии подключения к сетям связи общего пользования (сетям международного информационного обмена):

посредством единой информационно-телекоммуникационной сети;

с использованием средств криптографической защиты информации.

Средствами вычислительной техники, участвующими в обработке информации, являются автоматизированные рабочие места пользователей, серверное оборудование, сетевое и телекоммуникационное оборудование.

Уровни защищенности внутриобластных информационных систем персональных данных многопрофильных – второй, третий.

17.4. Внутриобластные информационные системы персональных данных для органов власти и организаций и иных организаций (предприятий, учреждений) Оренбургской области (далее – внутриобластные информационные системы персональных данных для органов власти и организаций) предназначены для автоматизации совместной деятельности органов власти и организаций и иных организаций (предприятий, учреждений) Оренбургской области, в том числе деятельности, необходимой в соответствии с требованиями законодательства Российской Федерации и Оренбургской области.

К категориям персональных данных, которые могут подлежать обработке во внутриобластных информационных системах персональных данных для органов власти и организаций, относятся:

общедоступные;

иные.

Режим обработки персональных данных во внутриобластных информационных системах персональных данных для органов власти и организаций является многопользовательским, то есть данные информационные системы персональных данных предусматривают разграничение доступа. Обработка персональных данных осуществляется в соответствии с предоставленными правами сотрудниками органов власти и организаций и организациями (предприятиями, учреждениями) Оренбургской области в специализированных программах в режиме веб-интерфейса.

Типами субъектов персональных данных, которые могут подлежать обработке во внутриобластных информационных системах персональных данных для органов власти и организаций, являются сотрудники органов власти и организаций и организаций (предприятий, учреждений) Оренбургской области.

Структура внутриобластных информационных систем персональных данных для органов власти и организаций – локальная, функционирующая в контролируемых зонах органа власти и организации.

Внутриобластные информационные системы персональных данных для органов власти и организаций подключены к сетям связи общего пользования (сетям международного информационного обмена). По типу подключения такие информационные системы персональных данных делятся на:

без подключения (передача персональных данных осуществляется с использованием машинных носителей);

подключенные посредством единой информационно-телекоммуникационной сети;

с использованием средств криптографической защиты информации.

Обмен (передача и получение) персональных данных с иными информационными системами передачи данных осуществляется в зависимости от технологии подключения к сетям связи общего пользования (сетям международного информационного обмена):

без подключения (передача персональных данных осуществляется с использованием машинных носителей);

посредством единой информационно-телекоммуникационной сети;

с использованием средств криптографической защиты информации.

Средствами вычислительной техники, участвующими в обработке информации, являются автоматизированные рабочие места пользователей, серверное оборудование, сетевое и телекоммуникационное оборудование.

Уровни защищенности внутриобластных информационных систем персональных данных для органов власти и организаций – второй, третий.

По архитектуре внутриобластные информационные системы персональных данных для органов власти и организаций подразделяются на:

сегментированные;

централизованные;

смешанные.

Сегментированные внутриобластные информационные системы персональных данных для органов власти и организаций делятся на сегменты (центральный и периферийный), функционирующие независимо. Центральный сегмент является единой точкой консолидации информации, получаемой от периферийных сегментов. Периферийные сегменты являются непосредственно точками, которые отвечают за наполнение и первоначальную обработку информации. В состав периферийных сегментов входят автоматизированные рабочие места пользователей, а также автоматизированное рабочее место пользователя, выполняющее функции сервера, или серверное оборудование. Пользователи периферийных сегментов подключаются к расположенному в пределах контролируемых зон автоматизированному рабочему месту пользователя, выполняющему функции сервера, или серверному оборудованию, осуществляющему консолидацию сведений на уровне периферийного сегмента, который в свою очередь передает полученные данные в центральный сегмент.

По технологии обработки сегментированные внутриобластные информационные системы персональных данных для органов власти и организаций подразделяются на:

построенные по технологии толстого клиента: на рабочие места пользователей данных информационных систем персональных данных устанавливается специальное клиентское приложение, осуществляющее подключение к автоматизированному рабочему месту пользователя, выполняющему функции сервера, или серверному сегменту, располагающемуся в пределах контролируемых зон органа власти и организации и передающему данные на центральный сегмент;

построенные по технологии тонкого клиента: на рабочие места пользователей данных информационных систем персональных данных передается

только графическая информация, сама обработка данных осуществляется на серверном сегменте, располагающемся в пределах контролируемых зон органа власти и организации и передающем данные на центральный сегмент.

Сегментированные внутриобластные информационные системы персональных данных для органов власти и организаций, реализованные по технологии тонкого клиента, подразделяются на:

реализованные посредством веб-интерфейса с применением веб-браузера и с авторизацией с помощью логина и пароля и (или) сертификата электронной подписи в соответствии с Федеральным законом от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи»;

реализованные с использованием терминального доступа с авторизацией с помощью логина и пароля и (или) сертификата электронной подписи в соответствии с Федеральным законом от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи».

Централизованные внутриобластные информационные системы персональных данных для органов власти и организаций делятся на сегменты (центральный и периферийный).

Центральный сегмент является единой точкой консолидации информации, получаемой от периферийных сегментов.

В состав периферийных сегментов входят только автоматизированные рабочие места пользователей, которые являются непосредственно точками, отвечающими за наполнение и первоначальную обработку информации. Пользователи периферийных сегментов подключаются напрямую к центральному сегменту и осуществляют обработку данных непосредственно на нем.

По технологии обработки централизованные внутриобластные информационные системы персональных данных для органов власти и организаций подразделяются на:

построенные по технологии толстого клиента: на рабочие места пользователей данных информационных систем персональных данных устанавливается специальное клиентское приложение, осуществляющее подключение к центральному сегменту;

построенные по технологии толстого клиента: на рабочие места пользователей данных информационных систем персональных данных устанавливается специальное клиентское приложение, осуществляющее выгрузку данных на локальный носитель и последующую передачу выгруженных данных посредством защищенного канала связи или нарочно;

построенные по технологии тонкого клиента: на рабочие места пользователей данных информационных систем персональных данных передается только графическая информация, сама обработка данных осуществляется на центральном сегменте.

Централизованные внутриобластные информационные системы персональных данных для органов власти и организаций, реализованные по технологии тонкого клиента, подразделяются на:

реализованные посредством веб-интерфейса с применением веб-браузера и с авторизацией с помощью логина и пароля и (или) сертификата электронной подписи в соответствии с Федеральным законом от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи»;

реализованные с использованием терминального доступа с авторизацией с помощью логина и пароля и (или) сертификата электронной подписи в соответствии с Федеральным законом от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи».

Смешанные внутриобластные информационные системы персональных данных для органов власти и организаций построены с одновременным применением сегментированных и централизованных архитектур. Данные информационные системы персональных данных могут объединять в себе технологии обработки, характерные как для сегментированных внутриобластных информационных систем персональных данных для органов власти и организаций, так и для централизованных внутриобластных информационных систем персональных данных для органов власти и организаций.

18. Ведомственные информационные системы персональных данных создаются (эксплуатируются) на основании решения органа власти и организации в интересах органа власти и организации. Ведомственные информационные системы персональных данных предназначены для осуществления функций органов власти и организаций.

18.1. К категориям персональных данных, которые могут подлежать обработке в ведомственных информационных системах персональных данных, относятся:

специальные;

общедоступные;

иные.

Режим обработки персональных данных в ведомственных информационных системах персональных данных является многопользовательским, то есть данные информационные системы персональных данных предусматривают разграничение доступа. Обработка персональных данных осуществляется сотрудниками органов власти и организаций в специализированных программах и (или) посредством веб-интерфейса в соответствии с предоставленными правами.

Типами субъектов персональных данных, которые могут подлежать обработке в ведомственных информационных системах персональных данных, являются сотрудники оператора информационной системы персональных данных, иных органов власти и организаций, а также сторонние граждане.

Структура ведомственных информационных систем персональных данных – распределенная или локальная, функционирующая в контролируемых зонах органа власти и организации.

Ведомственные информационные системы персональных данных подключены к сетям связи общего пользования (сетям международного инфор-

мационного обмена). По типу подключения ведомственные информационные системы персональных данных делятся на:

без подключения (передача персональных данных осуществляется с использованием машинных носителей);

подключенные посредством единой информационно-телекоммуникационной сети;

подключенные с использованием иных каналов связи.

Обмен (передача и получение) персональными данными между сегментами ведомственных информационных систем персональных данных (при наличии) и иными информационными системами персональных данных осуществляется в зависимости от технологии подключения к сетям связи общего пользования (сетям международного информационного обмена):

без подключения (передача персональных данных осуществляется с использованием машинных носителей);

посредством единой информационно-телекоммуникационной сети;

с использованием средств криптографической защиты информации.

Обмен персональными данными между сегментами ведомственных информационных систем персональных данных (при наличии) и иными информационными системами персональных данных также может осуществляться посредством собственных корпоративных сетей органа власти и организации.

Средствами вычислительной техники, участвующими в обработке информации, являются автоматизированные рабочие места пользователей, терминальная станция, серверное оборудование, сетевое и телекоммуникационное оборудование.

Уровни защищенности ведомственных информационных систем персональных данных – первый, второй, третий.

18.2. По архитектуре ведомственные информационные системы персональных данных подразделяются на:

сегментированные;

централизованные;

смешанные.

18.3. Сегментированные ведомственные информационные системы персональных данных делятся на сегменты (центральный и периферийный), функционирующие независимо.

Центральный сегмент является единой точкой консолидации информации, получаемой от периферийных сегментов.

Периферийные сегменты являются непосредственно точками, отвечающими за наполнение и первоначальную обработку информации. В состав периферийных сегментов входят автоматизированные рабочие места пользователей, а также автоматизированные рабочие места пользователей, выполняющие функции сервера, или серверное оборудование. Пользователи периферийных сегментов подключаются к расположенному в пределах контролируемой зоны автоматизированному рабочему месту пользователя, выполняющему функции сервера, или серверному оборудованию, осуществляю-

щему консолидацию сведений на уровне периферийного сегмента, который в свою очередь передает полученные данные в центральный сегмент.

По технологии обработки сегментированные ведомственные информационные системы персональных данных подразделяются на:

построенные по технологии толстого клиента: на рабочие места пользователей данных информационных систем персональных данных устанавливается специальное клиентское приложение, осуществляющее подключение к автоматизированному рабочему месту пользователя, выполняющему функции сервера, или серверному сегменту, располагающемуся в пределах контролируемых зон органа власти и организации и передающему данные на центральный сегмент;

построенные по технологии тонкого клиента: на рабочие места пользователей данных информационных систем персональных данных передается только графическая информация, сама обработка данных осуществляется на серверном сегменте, располагающемся в пределах контролируемых зон органа власти и организации и передающем данные на центральный сегмент.

Сегментированные ведомственные информационные системы персональных данных, реализованные по технологии тонкого клиента, подразделяются на:

реализованные посредством веб-интерфейса с применением веб-браузера и с авторизацией с помощью логина и пароля и (или) сертификата электронной подписи в соответствии с Федеральным законом от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи»;

реализованные с использованием терминального доступа с авторизацией с помощью логина и пароля и (или) сертификата электронной подписи в соответствии с Федеральным законом от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи».

18.4. Централизованные ведомственные информационные системы персональных данных делятся на сегменты (центральный и периферийный).

Центральный сегмент является единой точкой консолидации информации, получаемой от периферийных сегментов.

В состав периферийных сегментов входят только автоматизированные рабочие места пользователей, которые являются непосредственно точками, отвечающими за наполнение и первоначальную обработку информации. Пользователи периферийных сегментов подключаются напрямую к центральному сегменту и осуществляют обработку данных непосредственно на нем.

По технологии обработки централизованные ведомственные информационные системы персональных данных подразделяются на:

построенные по технологии толстого клиента: на рабочие места пользователей данных информационных систем персональных данных устанавливается специальное клиентское приложение, осуществляющее подключение к центральному сегменту;

построенные по технологии толстого клиента: на рабочие места пользователей данных информационных систем персональных данных устанав-

ливается специальное клиентское приложение, осуществляющее выгрузку данных на локальный носитель и последующую передачу выгруженных данных посредством защищенного канала связи или нарочно;

построенные по технологии тонкого клиента: на рабочие места пользователей данных информационных систем персональных данных передается только графическая информация, сама обработка данных осуществляется на центральном сегменте.

Централизованные ведомственные информационные системы персональных данных, реализованные по технологии тонкого клиента, подразделяются на:

реализованные посредством веб-интерфейса с применением веб-браузера и с авторизацией с помощью логина и пароля и (или) сертификата электронной подписи в соответствии с Федеральным законом от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи»;

реализованные с использованием терминального доступа с авторизацией с помощью логина и пароля и (или) сертификата электронной подписи в соответствии с Федеральным законом от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи».

18.5. Смешанные ведомственные информационные системы персональных данных построены с одновременным применением сегментированных и централизованных архитектур. Данные информационные системы персональных данных могут объединять в себе технологии обработки, характерные как для сегментированных информационных систем персональных данных, так и для централизованных информационных систем персональных данных.

19. Служебные информационные системы персональных данных создаются (эксплуатируются) на основании решения органа власти и организации в интересах органа власти и организации, цели и задачи создания (модернизации), эксплуатации которых определяются органом власти и организацией, и используются для автоматизации определенной области деятельности или типовой деятельности, неспецифичной относительно полномочий определенных органа власти и организации. Служебные информационные системы персональных данных предназначены для управления бизнес-процессами в органе власти и организации.

19.1. Служебными информационными системами персональных данных являются:

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.

19.2. Информационные системы персональных данных бухгалтерского учета и управления финансами предназначены для автоматизации деятельно-

сти органа власти и организации, связанной с ведением бухгалтерского учета и управлением финансами.

Обработке в служебных информационных системах персональных данных бухгалтерского учета и управления финансами подлежат иные категории персональных данных.

Режим обработки персональных данных в служебных информационных системах персональных данных бухгалтерского учета и управления финансами является многопользовательским, то есть данная информационная система персональных данных предусматривает разграничение доступа. Обработка персональных данных осуществляется сотрудниками органов власти и организаций в специализированных программах и (или) посредством веб-интерфейса в соответствии с предоставленными правами.

Типами субъектов персональных данных, которые могут подлежать обработке в служебных информационных системах персональных данных бухгалтерского учета и управления финансами являются сотрудники органа власти и организации.

Структура служебных информационных систем персональных данных бухгалтерского учета и управления финансами – локальная, функционирующая в контролируемых зонах органа власти и организации.

Служебные информационные системы персональных данных бухгалтерского учета и управления финансами подключены к сетям связи общего пользования (сетям международного информационного обмена). По типу подключения данные информационные системы персональных данных делятся на:

без подключения (передача персональных данных осуществляется с использованием машинных носителей);

подключенные посредством единой информационно-телекоммуникационной сети;

подключенные с использованием иных каналов связи.

Передача персональных данных в иные информационные системы персональных данных осуществляется в зависимости от технологии подключения к сетям связи общего пользования (сетям международного информационного обмена):

без подключения (передача персональных данных осуществляется с использованием машинных носителей);

с использованием средств криптографической защиты информации.

Средствами вычислительной техники, участвующими в обработке информации, являются автоматизированные рабочие места пользователей, серверное оборудование, сетевое и телекоммуникационное оборудование.

По технологии обработки служебные информационные системы персональных данных бухгалтерского учета и управления финансами подразделяются на:

построенные по технологии толстого клиента: на рабочие места пользователей данных информационных систем персональных данных устанавливается специальное клиентское приложение, осуществляющее подключе-

ние к базе данных, которая хранится на серверном сегменте (сервере или автоматизированном рабочем месте пользователя, выполняющем функцию сервера), располагающемся в пределах контролируемых зон органа власти и организации;

построенные по технологии тонкого клиента: на рабочие места пользователей данных информационных систем персональных данных передается только графическая информация, сама обработка данных осуществляется на удаленном серверном сегменте (сервере или автоматизированном рабочем месте пользователя, выполняющем функцию сервера), располагающемся в пределах контролируемых зон органа власти и организации.

Доступ к персональным данным в служебных информационных системах персональных данных бухгалтерского учета и управления финансами предоставляется пользователю после ввода логина и пароля (предъявления идентификатора).

Уровень защищенности служебных информационных систем персональных данных бухгалтерского учета и управления финансами – четвертый.

19.3. Служебные информационные системы персональных данных кадрового учета и управления персоналом предназначены для автоматизации деятельности органа власти и организации, связанной с ведением кадрового учета и управления персоналом.

К категориям персональных данных, которые могут подлежать обработке в служебных информационных системах персональных данных кадрового учета и управления персоналом, относятся:

специальные;

иные.

Режим обработки персональных данных в служебных информационных системах персональных данных кадрового учета и управления персоналом является многопользовательским, то есть данные информационные системы персональных данных предусматривают разграничение доступа. Обработка персональных данных осуществляется сотрудниками органов власти и организаций в специализированных и (или) стандартных офисных программах и (или) посредством веб-интерфейса в соответствии с предоставленными правами.

Типами субъектов персональных данных, которые могут подлежать обработке в данных информационных системах персональных данных являются сотрудники органа власти и организации, являющихся оператором информационной системы персональных данных, граждане Российской Федерации, устанавливающие (имеющие) трудовые отношения (трудовые договоры, служебные контракты) с органом власти и организацией.

Структура служебных информационных систем персональных данных кадрового учета и управления персоналом – локальная, функционирующая в контролируемых зонах органа власти и организации.

Служебные информационные системы персональных данных кадрового учета и управления персоналом подключены к сетям связи общего пользо-

вания (сетям международного информационного обмена). По типу подключения информационные системы персональных данных делятся на:

без подключения (передача персональных данных осуществляется с использованием машинных носителей);

подключенные посредством единой информационно-телекоммуникационной сети;

подключенные с использованием иных каналов связи.

Передача персональных данных в иные информационные системы персональных данных осуществляется в зависимости от технологии подключения к сетям связи общего пользования (сетям международного информационного обмена):

без подключения (передача персональных данных осуществляется с использованием машинных носителей);

с использованием средств криптографической защиты информации.

Средствами вычислительной техники, участвующими в обработке информации, являются автоматизированные рабочие места пользователей, серверное оборудование, сетевое и телекоммуникационное оборудование.

Технология обработки персональных данных в служебных информационных системах персональных данных кадрового учета и управления персоналом построена по принципу толстого клиента: на рабочие места пользователей данных информационных систем персональных данных устанавливается специальное клиентское приложение, осуществляющее подключение к базе данных, которая хранится на серверном сегменте (сервере или автоматизированном рабочем месте пользователя, выполняющем функцию сервера), располагающемся в пределах контролируемых зон органа власти и организации. Доступ к персональным данным в служебных информационных системах персональных данных кадрового учета и управления персоналом предоставляется пользователю после ввода логина и пароля (предъявления идентификатора).

Уровень защищенности служебных информационных систем персональных кадрового учета и управления персоналом – четвертый.

19.4. Служебные информационные системы персональных данных документооборота и делопроизводства предназначены для автоматизации деятельности органа власти и организации, связанной с осуществлением документооборота и делопроизводства.

К категориям персональных данных, которые могут подлежать обработке в служебных информационных системах персональных данных документооборота и делопроизводства, относятся:

специальные;

общедоступные;

иные.

Режим обработки персональных данных в служебных информационных системах персональных данных документооборота и делопроизводства является многопользовательским, то есть данные информационные системы персональных данных предусматривают разграничение доступа. Обработка

персональных данных осуществляется сотрудниками органов власти и организаций в специализированных программах в соответствии с предоставленными правами.

Типами субъектов персональных данных документооборота и делопроизводства, которые могут подлежать обработке в данных информационных системах персональных данных являются сотрудники органа власти и организации, являющихся операторами информационной системы персональных данных, и граждане всех стран мира.

Структура информационных систем персональных данных документооборота и делопроизводства – локальная, функционирующая в контролируемых зонах органа власти и организации.

Служебные информационные системы персональных данных документооборота и делопроизводства подключены к сетям связи общего пользования (сетям международного информационного обмена). По типу подключения служебные информационные системы персональных данных документооборота и делопроизводства делятся на:

без подключения (передача персональных данных осуществляется с использованием машинных носителей);

подключенные посредством единой информационно-телекоммуникационной сети;

подключенные с использованием иных каналов связи.

Передача персональных данных в иные информационные системы персональных данных осуществляется в зависимости от технологии подключения к сетям связи общего пользования (сетям международного информационного обмена):

без подключения (передача персональных данных осуществляется с использованием машинных носителей);

посредством единой информационно-телекоммуникационной сети;

с использованием сторонних средств криптографической защиты информации.

Средствами вычислительной техники, участвующими в обработке информации, являются автоматизированные рабочие места пользователей, серверное оборудование, сетевое и телекоммуникационное оборудование.

Технология обработки персональных данных в служебных информационных системах персональных данных документооборота и делопроизводства построена по принципу толстого клиента: на рабочие места пользователей информационных систем персональных данных устанавливается специальное клиентское приложение, осуществляющее подключение к базе данных, которая хранится на серверном сегменте (сервере или автоматизированном рабочем месте пользователя, выполняющем функцию сервера), располагающемся в пределах контролируемых зон органа власти и организации. Доступ к персональным данным в служебных информационных системах персональных данных документооборота и делопроизводства предоставляется пользователю после ввода логина и пароля (предъявления идентификатора).

Уровень защищенности служебных информационных систем персональных данных документооборота и делопроизводства – четвертый.

V. Угрозы безопасности персональных данных, выявленные при функционировании информационной системы персональных данных

20. Источниками угроз безопасности персональных данных в информационной системе персональных данных являются:

носитель вредоносной программы;

аппаратная закладка;

нарушитель.

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

отчуждаемый носитель, то есть дискета, оптический диск, флэш-память, отчуждаемый жесткий магнитный диск и другое;

встроенные носители информации (жесткие магнитные диски, 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, микросхемы прямого доступа к памяти, шин передачи данных, портов ввода/вывода.

В случае если вредоносная программа ассоциируется с какой-либо прикладной программой, файлами, имеющими определенные расширения или иные атрибуты, сообщениями, передаваемыми по сети, то ее носителями являются пакеты передаваемых по компьютерной сети сообщений или файлы (текстовые, графические, исполняемые и другое).

20.2. Под аппаратной закладкой потенциально может рассматриваться возможность применения аппаратных средств, предназначенных для регистрации вводимой в информационную систему персональных данных с клавиатуры автоматизированного рабочего места пользователя информации (персональных данных): аппаратная закладка внутри клавиатуры, считывание данных с кабеля клавиатуры бесконтактным методом, включение устройства в разрыв кабеля, аппаратная закладка внутри системного блока и другое. Однако в виду отсутствия возможности неконтролируемого пребывания физических лиц в служебных помещениях, в которых размещены технические средства информационной системы персональных данных, или в непосредственной близости от них установка аппаратных закладок посторонними лицами невозможна.

Существование данного источника маловероятно также из-за несоответствия стоимости аппаратных закладок, сложности их скрытой установки и полученной в результате информации.

20.3. Под нарушителями безопасности информации понимаются физические лица, случайно или преднамеренно совершающие действия, следстви-

ем которых является нарушение безопасности персональных данных при их обработке в информационных системах персональных данных.

По наличию права постоянного или разового доступа в информационные системы персональных данных нарушители безопасности информации подразделяются на два типа:

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

внутренние нарушители – нарушители, имеющие правомерный доступ к информационным системам персональных данных, включая пользователей информационной системы персональных данных, и реализующие угрозы непосредственно в информационной системе персональных данных.

VI. Основные угрозы безопасности в информационных системах персональных данных

21. Основными видами угроз безопасности 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 недекларированных возможностей в системном программном обеспечении и 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 (внесения уязвимостей) при проектировании, внедрении информационной системы персональных данных (системы информационной безопасности информационной системы персональных данных);

угрозы ошибочных (деструктивных) действий лиц;

угрозы получения нарушителем сведений о структуре, конфигурации и настройках информационной системы персональных данных и ее системы защиты;

угрозы программно-математических воздействий;

угрозы, связанные с использованием «облачных» услуг;

угрозы, связанные с использованием суперкомпьютерных технологий;

угрозы, связанные с использованием технологий виртуализации;

угрозы, связанные с нарушением правил эксплуатации машинных носителей;

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

угрозы физического доступа к компонентам информационной системы персональных данных;

угрозы эксплуатации уязвимостей в системном программном обеспечении, прикладном программном обеспечении, средств защиты информации, средств криптографической защиты информации, аппаратных компонентах информационной системы персональных данных, микропрограммном обеспечении;

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.

VII. Актуальные угрозы безопасности персональных данных в информационных системах персональных данных

22. В настоящем разделе рассматриваются актуальные угрозы безопасности персональных данных в информационных системах персональных данных, указанных в разделе IV настоящего Положения.

23. К информационно-справочным информационным системам персональных данных относятся:

23.1. «Официальные порталы (сайты) органов власти и организаций». Видами актуальных угроз безопасности для данных информационных систем являются:

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

угрозы нарушения доступности информации;

угрозы нарушения целостности информации;

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 (внесения уязвимостей) при проектировании, внедрении информационной системы персональных данных (системы информационной безопасности информационной системы персональных данных);

угрозы ошибочных (деструктивных) действий лиц;

угрозы получения нарушителем сведений о структуре, конфигурации и настройках информационной системы персональных данных и ее системы защиты;

угрозы программно-математических воздействий;

угрозы, связанные с использованием «облачных» услуг;

угрозы, связанные с использованием технологий виртуализации;

угрозы, связанные с нарушением правил эксплуатации машинных носителей;

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

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.

23.2. «Информационные порталы (сайты)». Видами актуальных угроз безопасности для данных информационных систем являются:

угрозы использования штатных средств информационной системы персональных данных с целью совершения несанкционированного доступа к информации;

угрозы нарушения доступности информации;

угрозы нарушения целостности информации;

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 (внесения уязвимостей) при проектировании, внедрении информационной системы персональных данных (системы информационной безопасности информационной системы персональных данных);

угрозы ошибочных (деструктивных) действий лиц;

угрозы получения нарушителем сведений о структуре, конфигурации и настройках информационной системы персональных данных и ее системы защиты;

угрозы программно-математических воздействий;

угрозы, связанные с использованием «облачных» услуг;

угрозы, связанные с использованием технологий виртуализации;

угрозы, связанные с нарушением правил эксплуатации машинных носителей;

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

угрозы физического доступа к компонентам информационной системы персональных данных;

угрозы эксплуатации уязвимостей в системном программном обеспечении, прикладном программном обеспечении, средствах защиты информации, средствах криптографической защиты информации, аппаратных компонентах информационной системы персональных данных, микропрограммном обеспечении;

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.

23.3. «Закрытые порталы для нескольких групп участников органов власти и организаций». Видами актуальных угроз безопасности для данных информационных систем являются:

угрозы использования штатных средств информационной системы персональных данных с целью совершения несанкционированного доступа к информации;

угрозы нарушения доступности информации;

угрозы нарушения целостности информации;

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 (внесения уязвимостей) при проектировании, внедрении информационной системы персональных данных (системы информационной безопасности информационной системы персональных данных);

угрозы ошибочных (деструктивных) действий лиц;

угрозы получения нарушителем сведений о структуре, конфигурации и настройках информационной системы персональных данных и ее системы защиты;

угрозы программно-математических воздействий;

угрозы, связанные с использованием «облачных» услуг;

угрозы, связанные с использованием технологий виртуализации;

угрозы, связанные с нарушением правил эксплуатации машинных носителей;

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

угрозы физического доступа к компонентам информационной системы персональных данных;

угрозы эксплуатации уязвимостей в системном программном обеспечении, прикладном программном обеспечении, средствах защиты информации, средствах криптографической защиты информации, аппаратных компонентах информационной системы персональных данных, микропрограммном обеспечении;

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.

23.4. «Специализированная информационная система «Портал государственных услуг Оренбургской области». Видами актуальных угроз безопасности для данных информационных систем являются:

угрозы использования штатных средств информационной системы персональных данных с целью совершения несанкционированного доступа к информации;

угрозы нарушения доступности информации;

угрозы нарушения целостности информации;

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 (внесения уязвимостей) при проектировании, внедрении информационной системы персональных данных (системы информационной безопасности информационной системы персональных данных);

угрозы ошибочных (деструктивных) действий лиц;

угрозы получения нарушителем сведений о структуре, конфигурации и настройках информационной системы персональных данных и ее системы защиты;

угрозы программно-математических воздействий;

угрозы, связанные с использованием «облачных» услуг;

угрозы, связанные с использованием технологий виртуализации;

угрозы, связанные с нарушением правил эксплуатации машинных носителей;

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

угрозы физического доступа к компонентам информационной системы персональных данных;

угрозы эксплуатации уязвимостей в системном программном обеспечении, прикладном программном обеспечении, средств защиты информации, средств криптографической защиты информации, аппаратных компонентах

информационной системы персональных данных, микропрограммном обеспечении;

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.

24. Видами актуальных угроз безопасности для сегментных информационных систем персональных данных являются:

угрозы использования штатных средств информационной системы персональных данных с целью совершения несанкционированного доступа к информации;

угрозы нарушения доступности информации;

угрозы нарушения целостности информации;

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 (внесения уязвимостей) при проектировании, внедрении информационной системы персональных данных (системы информационной безопасности информационной системы персональных данных);

угрозы ошибочных (деструктивных) действий лиц;

угрозы получения нарушителем сведений о структуре, конфигурации и настройках информационной системы персональных данных и ее системы защиты;

угрозы программно-математических воздействий;

угрозы, связанные с использованием технологий виртуализации;

угрозы, связанные с нарушением правил эксплуатации машинных носителей;

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

угрозы физического доступа к компонентам информационной системы персональных данных;

угрозы эксплуатации уязвимостей в системном программном обеспечении, прикладном программном обеспечении, средств защиты информации, средств криптографической защиты информации, аппаратных компонентах информационной системы персональных данных, микропрограммном обеспечении;

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.

25. К внутриобластным информационным системам персональных данных относятся:

25.1. Информационные системы персональных данных интеграционные. Видами актуальных угроз безопасности для данных информационных систем являются:

угрозы использования штатных средств информационной системы персональных данных с целью совершения несанкционированного доступа к информации;

угрозы нарушения доступности информации;

угрозы нарушения целостности информации;

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 (внесения уязвимостей) при проектировании, внедрении информационной системы персональных данных (системы информационной безопасности информационной системы персональных данных);

угрозы ошибочных (деструктивных) действий лиц;

угрозы получения нарушителем сведений о структуре, конфигурации и настройках информационной системы персональных данных и ее системы защиты;

угрозы программно-математических воздействий;

угрозы, связанные с использованием технологий виртуализации;

угрозы, связанные с нарушением правил эксплуатации машинных носителей;

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

угрозы физического доступа к компонентам информационной системы персональных данных;

угрозы эксплуатации уязвимостей в системном программном обеспечении, прикладном программном обеспечении, средств защиты информации, средств криптографической защиты информации, аппаратных компонентах информационной системы персональных данных, микропрограммном обеспечении;

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.

25.2. Информационные системы персональных данных многопрофильные. Видами актуальных угроз безопасности для данных информационных систем являются:

угрозы использования штатных средств информационной системы персональных данных с целью совершения несанкционированного доступа к информации;

угрозы нарушения доступности информации;

угрозы нарушения целостности информации;

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 (внесения уязвимостей) при проектировании, внедрении информационной системы персональных данных (системы информационной безопасности информационной системы персональных данных);

угрозы ошибочных (деструктивных) действий лиц;

угрозы получения нарушителем сведений о структуре, конфигурации и настройках информационной системы персональных данных и ее системы защиты;

угрозы программно-математических воздействий;

угрозы, связанные с использованием технологий виртуализации;

угрозы, связанные с нарушением правил эксплуатации машинных носителей;

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

угрозы физического доступа к компонентам информационной системы персональных данных;

угрозы эксплуатации уязвимостей в системном программном обеспечении, прикладном программном обеспечении, средствах защиты информации, средствах криптографической защиты информации, аппаратных компонентах информационной системы персональных данных, микропрограммном обеспечении;

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.

25.3. Информационные системы персональных данных для органов власти и организаций. Видами актуальных угроз безопасности для данных информационных систем являются:

угрозы использования штатных средств информационной системы персональных данных с целью совершения несанкционированного доступа к информации;

угрозы нарушения доступности информации;

угрозы нарушения целостности информации;

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 (внесения уязвимостей) при проектировании, внедрении информационной системы персональных данных (системы информационной безопасности информационной системы персональных данных);

угрозы ошибочных (деструктивных) действий лиц;

угрозы получения нарушителем сведений о структуре, конфигурации и настройках информационной системы персональных данных и ее системы защиты;

угрозы программно-математических воздействий;

угрозы, связанные с использованием технологий виртуализации;

угрозы, связанные с нарушением правил эксплуатации машинных носителей;

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

угрозы физического доступа к компонентам информационной системы персональных данных;

угрозы эксплуатации уязвимостей в системном программном обеспечении прикладном программном обеспечении, средств защиты информации, средств криптографической защиты информации, аппаратных компонентах информационной системы персональных данных, микропрограммном обеспечении;

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.

26. Видами актуальных угроз безопасности для ведомственных информационных систем персональных данных являются:

угрозы использования штатных средств информационной системы персональных данных с целью совершения несанкционированного доступа к информации;

угрозы нарушения доступности информации;

угрозы нарушения целостности информации;

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 (внесения уязвимостей) при проектировании, внедрении информационной системы персональных данных (системы информационной безопасности информационной системы персональных данных);

угрозы ошибочных (деструктивных) действий лиц;

угрозы получения нарушителем сведений о структуре, конфигурации и настройках информационной системы персональных данных и ее системы защиты;

угрозы программно-математических воздействий;

угрозы, связанные с использованием технологий виртуализации;

угрозы, связанные с нарушением правил эксплуатации машинных носителей;

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

угрозы физического доступа к компонентам информационной системы персональных данных;

угрозы эксплуатации уязвимостей в системном программном обеспечении, прикладном программном обеспечении, средств защиты информации, средств криптографической защиты информации, аппаратных компонентах информационной системы персональных данных, микропрограммном обеспечении;

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.

27. К служебным информационным системам персональных данных относятся:

27.1. Информационные системы персональных данных бухгалтерского учета и управления финансами. Видами актуальных угроз безопасности для данных информационных систем являются:

угрозы использования штатных средств информационной системы персональных данных с целью совершения несанкционированного доступа к информации;

угрозы нарушения доступности информации;

угрозы нарушения целостности информации;

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 (внесения уязвимостей) при проектировании, внедрении информационной системы персональных данных (системы информационной безопасности информационной системы персональных данных);

угрозы ошибочных (деструктивных) действий лиц;

угрозы получения нарушителем сведений о структуре, конфигурации и настройках информационной системы персональных данных и ее системы защиты;

угрозы программно-математических воздействий;

угрозы, связанные с использованием технологий виртуализации;

угрозы, связанные с нарушением правил эксплуатации машинных носителей;

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

угрозы физического доступа к компонентам информационной системы персональных данных;

угрозы эксплуатации уязвимостей в системном программном обеспечении, прикладном программном обеспечении, средствах защиты информации, средствах криптографической защиты информации, аппаратных компонентах информационной системы персональных данных, микропрограммном обеспечении;

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.

27.2. Информационные системы персональных данных кадрового учета и управления персоналом. Видами актуальных угроз безопасности для данных информационных систем являются:

угрозы использования штатных средств информационной системы персональных данных с целью совершения несанкционированного доступа к информации;

угрозы нарушения доступности информации;

угрозы нарушения целостности информации;

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 (внесения уязвимостей) при проектировании, внедрении информационной системы персональных данных (системы информационной безопасности информационной системы персональных данных);

угрозы ошибочных (деструктивных) действий лиц;

угрозы получения нарушителем сведений о структуре, конфигурации и настройках информационной системы персональных данных и ее системы защиты;

угрозы программно-математических воздействий;

угрозы, связанные с использованием технологий виртуализации;

угрозы, связанные с нарушением правил эксплуатации машинных носителей;

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

угрозы физического доступа к компонентам информационной системы персональных данных;

угрозы эксплуатации уязвимостей в системном программном обеспечении, прикладном программном обеспечении, средствах защиты информации, средствах криптографической защиты информации, аппаратных компонентах информационной системы персональных данных, микропрограммном обеспечении;

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.

27.3. Информационные системы персональных данных документооборота и делопроизводства. Видами актуальных угроз безопасности для данных информационных систем являются:

Угрозы использования штатных средств информационной системы персональных данных с целью совершения несанкционированного доступа к информации;

угрозы нарушения доступности информации;

угрозы нарушения целостности информации;

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 (внесения уязвимостей) при проектировании, внедрении информационной системы персональных данных (системы информационной безопасности информационной системы персональных данных);

угрозы ошибочных (деструктивных) действий лиц;

угрозы получения нарушителем сведений о структуре, конфигурации и настройках информационной системы персональных данных и ее системы защиты;

угрозы программно-математических воздействий;

угрозы, связанные с использованием технологий виртуализации;

угрозы, связанные с нарушением правил эксплуатации машинных носителей;

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

угрозы физического доступа к компонентам информационной системы персональных данных;

угрозы эксплуатации уязвимостей в системном программном обеспечении, прикладном программном обеспечении, средствах защиты информации, средствах криптографической защиты информации, аппаратных компонентах информационной системы персональных данных, микропрограммном обеспечении;

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.

28. Обобщенные возможности источников атак представлены в приложении № 1 к настоящему Положению.

29. Уточненные возможности нарушителей и направления атак представлены в приложении № 2 к настоящему Положению.

30. Расширенный перечень угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, представлен в приложении № 3 к настоящему Положению.

Приложение № 1
к положению об угрозах
безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных органов исполнительной власти Оренбургской области

Обобщенные возможности источников атак

№ п/п	Наименование обобщенной возможности источников атак	Да/нет
1.	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак только за пределами контролируемой зоны	да
2.	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны, но без физического доступа к автоматизированной системе, на которой реализованы средства криптографической защиты информации и среда их функционирования	да
3.	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны с физическим доступом к автоматизированной системе, на которой реализованы средства криптографической защиты информации и среда их функционирования	нет
4.	Возможность привлекать специалистов, имеющих опыт разработки и анализа средств криптографической защиты информации (включая специалистов в области анализа сигналов линейной передачи и сигналов побочного электромагнитного излучения и наводок средства криптографической защиты информации)	нет
5.	Возможность привлекать специалистов, имеющих опыт разработки и анализа средств криптографической защиты информации (включая специалистов в области использования для реализации атак недокументированных возможностей прикладного программного обеспечения)	нет
6.	Возможность привлекать специалистов, имеющих опыт разработки и анализа средств криптографической защиты информации (включая специалистов в области использования для реализации атак недокументированных возможностей аппаратного и программного компонентов среды функционирования средств криптографической защиты информации)	нет

Приложение № 2
к положению об угрозах безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных органов исполнительной власти Оренбургской области

Уточненные возможности нарушителей и направления атак

№ п/п	Наименование уточненной возможности нарушителей и направления атак	Актуальность применения	Обоснование отсутствия возможности нарушителей и направления атак
1	2	3	4
1.	Проведение атак при нахождении в пределах контролируемой зоны	актуально	-
2.	Проведение атак на этапе эксплуатации средств криптографической защиты информации на следующие объекты: документация на средства криптографической защиты информации и среда функционирования средств криптографической защиты информации; помещения, в которых находятся программные и технические элементы систем обработки данных, способных функционировать самостоятельно или в составе других систем (далее – средства вычислительной техники), на которых реализованы средства криптографической защиты информации и среда функционирования средств криптографической защиты информации	неактуально	проведение работ по подбору персонала; обеспечение доступа в контролируемую зону, где находятся средства криптографической защиты информации, в соответствии с контрольно-пропускным режимом; хранение документации на средства криптографической защиты информации в металлическом сейфе у ответственного за средства криптографической защиты информации; оснащение помещений, в которых располагаются документация на средства криптографической защиты информации, компоненты среды функционирования средств криптографической защиты информации, входными дверьми с замками; обеспечение постоянного закрытия дверей помещений на замок и их открытия только для санкционированного про-

1	2	3	4
			хода; утверждение перечня лиц, имеющих право доступа в помещения
3.	Получение в рамках предоставленных полномочий, а также в результате наблюдений следующих сведений о: физических мерах защиты объектов, в которых размещены ресурсы информационной системы; мерах по обеспечению контролируемой зоны объектов, в которых размещены ресурсы информационной системы; мерах по разграничению доступа в помещения, в которых находятся средства вычислительной техники, на которых реализованы средства криптографической защиты информации и среда функционирования средств криптографической защиты информации	неактуально	проведение работ по подбору персонала; обеспечение доступа в контролируемую зону и помещения, где располагаются ресурсы информационной системы персональных данных, в соответствии с контрольно-пропускным режимом; доступность сведений о физических мерах защиты объектов, в которых размещены информационные системы персональных данных, ограниченному кругу сотрудников; информирование сотрудников об ответственности за несоблюдение правил обеспечения безопасности информации
4.	Использование штатных средств информационной системы персональных данных, ограниченных мерами, реализованными в информационной системе, в которой используются средства криптографической защиты информации, и направленных на предотвращение и пресечение несанкционированных действий	неактуально	проведение работ по подбору персонала; оснащение помещений, в которых располагаются средства вычислительной техники, на которых реализованы средства криптографической защиты информации и среда функционирования средств криптографической защиты информации, входными дверьми с замками, обеспечение постоянного закрытия дверей помещений на замок и их открытия только для санкционированного прохода; информирование сотрудников

1	2	3	4
			об ответственности за несоблюдение правил обеспечения безопасности информации; осуществление разграничения и контроля доступа пользователей к защищаемым ресурсам; осуществление регистрации и учета действий пользователей; использование в информационной системе персональных данных сертифицированных средств защиты информации от несанкционированного доступа, сертифицированных средств антивирусной защиты
5.	Физический доступ к средствам вычислительной техники, на которых реализованы средства криптографической защиты информации и среда функционирования средств криптографической защиты информации	неактуально	проведение работ по подбору персонала; обеспечение доступа в контролируемую зону и помещения, где располагаются средства вычислительной техники, на которых реализованы средства криптографической защиты информации и среда функционирования средства криптографической защиты информации, в соответствии с контрольно-пропускным режимом; оснащение помещений, в которых располагаются средства вычислительной техники, на которых реализованы средства криптографической защиты информации и среда функционирования средств криптографической защиты информации, входными дверьми с замками; обеспечение постоянного закрытия дверей помещений на замок и их открытия только для санкционированного прохода

1	2	3	4
6.	Возможность воздействовать на аппаратные компоненты средств криптографической защиты информации и среду функционирования средств криптографической защиты информации, ограниченную мерами, реализованными в информационной системе, в которой используются средства криптографической защиты информации, и направленными на предотвращение и пресечение несанкционированных действий	неактуально	проведение работ по подбору персонала; обеспечение доступа в контролируемую зону и помещения, где располагаются средства вычислительной техники, на которых реализованы средства криптографической защиты информации и среда функционирования средств криптографической защиты информации, в соответствии с контрольно-пропускным режимом; оснащение помещений, в которых располагаются средства криптографической защиты информации и среда функционирования средств криптографической защиты информации, входными дверьми с замками; обеспечение постоянного закрытия дверей помещений на замок и их открытия только для санкционированного прохода; нахождение представителей технических, обслуживающих и других вспомогательных служб при работе в помещениях (стойках), где расположены компоненты средства криптографической защиты информации и среда функционирования средств криптографической защиты информации, и сотрудников, не являющихся пользователями средств криптографической защиты информации, только в присутствии сотрудников по эксплуатации
7.	Создание способов, подготовка и проведение атак с привлечением специалистов в	неактуально	отсутствие обработки сведений, составляющих государственную тайну, а также иных

1	2	3	4
	области анализа сигналов, сопровождающих функционирование средств криптографической защиты информации и среду функционирования средств криптографической защиты информации, и в области использования прикладного программного обеспечения для реализации атак недокументированных (недекларированных) возможностей		сведений, представляющих интерес для реализации возможности; высокая стоимость и сложность подготовки реализации возможности; проведение работ по подбору персонала; обеспечение доступа в контролируемую зону и помещения, где располагаются средства вычислительной техники, на которых реализованы средства криптографической защиты информации и среда функционирования средств криптографической защиты информации, в соответствии с контрольно-пропускным режимом; оснащение помещений, в которых располагаются средства криптографической защиты информации и среда функционирования средств криптографической защиты информации, входными дверьми с замками; обеспечение постоянного закрытия дверей помещений на замок и их открытия только для санкционированного прохода; нахождение представителей технических, обслуживающих и других вспомогательных служб при работе в помещениях (стойках), где расположены компоненты средства криптографической защиты информации и среда функционирования средств криптографической защиты информации, и сотрудников, не являющихся пользователями средств крип-

1	2	3	4
			тографической защиты информации, только в присутствии сотрудников по эксплуатации; осуществление разграничения и контроля доступа пользователей к защищаемым ресурсам; осуществление регистрации и учета действий пользователей; использование на автоматизированных рабочих местах пользователей и серверах, на которых установлены средства криптографической защиты информации, сертифицированных средств защиты информации от несанкционированного доступа и сертифицированных средств антивирусной защиты
8.	Проведение лабораторных исследований средств криптографической защиты информации, используемых вне контролируемой зоны, ограниченное мерами, реализованными в информационной системе, в которой используются средства криптографической защиты информации, и направленными на предотвращение и пресечение несанкционированных действий	неактуально	отсутствие обработки сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности; высокая стоимость и сложность подготовки реализации возможности
9.	Проведение работ по созданию способов и средств атак в научно-исследовательских центрах, специализирующихся в области разработки и анализа средств криптографической защиты информации и среды функционирования средств криптографической защиты информации, в том числе с использованием	неактуально	отсутствие обработки сведений, составляющих государственную тайну, а также иных сведений, представляющих интерес для реализации возможности; высокая стоимость и сложность подготовки реализации возможности

1	2	3	4
	исходных текстов входящего в среду функционирования средств криптографической защиты информации прикладного программного обеспечения, непосредственно использующего вызовы программных функций средств криптографической защиты информации		
10.	Создание способов, подготовка и проведение атак с привлечением специалистов в области использования недокументированных (недекларированных) возможностей системного программного обеспечения	неактуально	отсутствие обработки сведений, составляющих государственную тайну, а также иных сведений, представляющих интерес для реализации возможности; высокая стоимость и сложность подготовки реализации возможности; проведение работ по подбору персонала; обеспечение доступа в контролируемую зону и помещения, где располагаются средства вычислительной техники, на которых реализованы средства криптографической защиты информации и среда функционирования средств криптографической защиты информации, в соответствии с контрольно-пропускным режимом; оснащение помещений, в которых располагаются средства криптографической защиты информации и среда функционирования средств криптографической защиты информации, входными дверьми с замками; обеспечение постоянного закрытия дверей помещений на замок и их открытия только для санкционированного про-

1	2	3	4
			хода; нахождение представителей технических, обслуживающих и других вспомогательных служб при работе в помещениях (стойках), где расположены компоненты средств криптографической защиты информации и среда функционирования средств криптографической защиты информации, и сотрудников, не являющихся пользователями средств криптографической защиты информации, только в присутствии сотрудников по эксплуатации; осуществление разграничения и контроля доступа пользователей к защищаемым ресурсам; осуществление регистрации и учета действий пользователей; использование на автоматизированных рабочих местах пользователей и серверах, на которых установлены средства криптографической защиты информации, сертифицированных средств защиты информации от несанкционированного доступа и сертифицированных средств антивирусной защиты
11.	Возможность располагать сведениями, содержащимися в конструкторской документации на аппаратные и программные компоненты среды функционирования средств криптографической защиты информации	неактуально	отсутствие обработки сведений, составляющих государственную тайну, а также иных сведений, представляющих интерес для реализации возможности
12.	Возможность воздействовать на любые компоненты средств криптографической	неактуально	отсутствие обработки сведений, составляющих государственную тайну, а также иных

1	2	3	4
	защиты информации и среду функционирования средств криптографической защиты информации		сведений, представляющих интерес для реализации возможности

Приложение № 3
к положению об угрозах безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных органов исполнительной власти Оренбургской области

Расширенный перечень угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных

№ п/п	Наименование угрозы безопасности персональных данных	Наименование источника угроз безопасности персональных данных	Наименование объекта воздействия
1	2	3	4
I. Угрозы использования штатных средств информационной системы с целью совершения несанкционированного доступа к информации			
1.	Угроза некорректного использования функционала программного обеспечения	внешний нарушитель со средним потенциалом; внутренний нарушитель со средним потенциалом	системное программное обеспечение; прикладное программное обеспечение; сетевое программное обеспечение; микропрограммное обеспечение; аппаратное обеспечение
2.	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 операционной системы
3.	Угроза несанкционированного изменения аутентификационной информации	внешний нарушитель с низким потенциалом; внутренний наруши-	системное программное обеспечение; объекты файловой системы, учетные данные пользователя;

1	2	3	4
		тель с низким потенциалом	реестр операционной системы
4.	Доступ в операционную среду (локальную операционную систему отдельного технического средства информационной системы) с возможностью получения несанкционированного доступа вызовом штатных процедур или запуска специально разработанных программ	-[1)]	-[1)]
II. Угрозы нарушения доступности информации			
5.	Угроза длительного удержания вычислительных ресурсов пользователями	внешний нарушитель с низким потенциалом; внутренний нарушитель с низким потенциалом	информационная система; сетевой узел; носитель информации; системное программное обеспечение; сетевое программное обеспечение; сетевой трафик
6.	Угроза несанкционированного доступа к гипервизору из виртуальной машины и (или) физической сети	внешний нарушитель со средним потенциалом; внутренний нарушитель со средним потенциалом	гипервизор
7.	Угроза повреждения системного реестра	внешний нарушитель с низким потенциалом; внутренний нарушитель с низким потенциалом	объекты файловой системы; реестр операционной системы
8.	Угроза приведения 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

1	2	3	4
9.	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
10.	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
11.	Угроза вывода из строя (выхода из строя) отдельных технических средств[2)]	-[1)]	-[1)]
12.	Угроза вывода из строя незарезервированных технических (программных) средств (каналов связи)	-[1)]	-[1)]
13.	Угроза отсутствия актуальных резервных копий[2)]	-[1)]	-[1)]
14.	Угроза потери информации в процессе ее обработки технически и (или) программными средствами и при передаче по каналам связи[2)]	-[1)]	-[1)]
15.	Угроза переполнения канала связи вследствие множества параллельных попыток авторизации[2)]	-[1)]	-[1)]
16.	Угроза нехватки ресурсов информационных систем для выполнения штатных задач в результате обработки множества параллельных задач, выполняемых одной учетной записью[2)]	-[1)]	-[1)]

1	2	3	4
III. Угрозы нарушения целостности информации			
17.	Угроза нарушения целостности данных кэша	внешний нарушитель с низким потенциалом; внутренний нарушитель с низким потенциалом	сетевое программное обеспечение
18.	Угроза некорректного задания структуры данных транзакции	внутренний нарушитель со средним потенциалом	сетевой трафик; база данных; сетевое программное обеспечение
19.	Угроза сбоя обработки файлов, измененных специальным образом	внешний нарушитель со средним потенциалом; внутренний нарушитель со средним потенциалом	метаданные; объекты файловой системы; системное программное обеспечение
20.	Угроза отсутствия контроля целостности обрабатываемой в информационной системе информации, применяемого программного обеспечения, в том числе средств защиты информации[2)]	-[1)]	-[1)]
21.	Угроза отсутствия целостных резервных копий информации, программного обеспечения, средств защиты информации в случае реализации угроз информационной безопасности[2)]	-[1)]	-[1)]
22.	Угроза отсутствия контроля за поступающими в информационную систему данными, в том числе незапрашиваемыми[2)]	-[1)]	-[1)]
23.	Отсутствие средств централизованного управления за поступающими в информационную систему данными, в том числе незапрашиваемыми	-[1)]	-[1)]

1	2	3	4
24.	Отсутствие автоматизированных фильтров, осуществляющих обработку поступающей в информационную систему информации	-[1)]	-[1)]
25.	Угроза доступа в информационную систему информации от неаутентифицированных серверов (пользователей)	-[1)]	-[1)]
26.	Угроза отсутствия контроля за данными, передаваемыми из информационной системы[2)]	-[1)]	-[1)]
27.	Отсутствие резервного копирования информации, передаваемой из информационной системы	-[1)]	-[1)]
28.	Угроза ввода (передачи) недостоверных (ошибочных) данных[2)]	-[1)]	-[1)]
29.	Угроза подмены используемых информационной системой файлов[2)]	-[1)]	-[1)]
30.	Угроза модификации (удаления) файлов журналов системного, прикладного программного обеспечения, средств защиты[2)]	-[1)]	-[1)]
31.	Угроза установки (запуска) модифицированного программного обеспечения и (или) модифицированных обновлений программного обеспечения	-[1)]	-[1)]
32.	Угроза модификации, стирания или удаления данных системы регистрации событий информационной безопасности	-[1)]	-[1)]
33.	Отсутствие графика осуществления контроля целостности применяемых программных средств, в том числе средств защиты информации	-[1)]	-[1)]

1	2	3	4
34.	Угроза отсутствия контроля целостности информации, обрабатываемой информационной системой, и ее структуры	-[1)]	-[1)]
IV. Угрозы недекларированных возможностей в системном программном обеспечении и прикладном программном обеспечении			
35.	Угроза возникновения ошибок функционирования системного программного обеспечения, реализация недекларированных возможностей системного программного обеспечения	-[1)]	-[1)]
36.	Угроза использования встроенных недекларированных возможностей для получения несанкционированного доступа к информационной системе	-[1)]	-[1)]
V. Угрозы, не являющиеся атаками			
37.	Угроза исчерпания вычислительных ресурсов хранилища больших данных	внутренний нарушитель с низким потенциалом	информационная система
38.	Угроза невозможности восстановления сессии работы на автоматизированном рабочем месте при выводе из промежуточных состояний питания	внутренний нарушитель с низким потенциалом	рабочая станция; носитель информации; системное программное обеспечение, метаданные; объекты файловой системы; реестр операционной системы
39.	Угроза неконтролируемого копирования данных внутри хранилища больших данных	внутренний нарушитель с низким потенциалом	хранилище больших данных; метаданные; защищаемые данные
40.	Угроза неконтролируемого уничтожения информации хранилищем больших данных	внутренний нарушитель с низким потенциалом	хранилище больших данных; метаданные; защищаемые данные

1	2	3	4
41.	Угроза выхода из строя (отказа) отдельных технических, программных средств, каналов связи	-[1]	-[1]
VI. Угрозы несанкционированного доступа, создающие предпосылки для реализации несанкционированного доступа в результате нарушения процедуры авторизации и аутентификации			
42.	Угроза нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия	внешний нарушитель с низким потенциалом; внутренний нарушитель с низким потенциалом	сетевой узел; сетевое программное обеспечение; метаданные; учетные данные пользователя
43.	Угроза обхода некорректно настроенных механизмов аутентификации	внешний нарушитель с низким потенциалом; внутренний нарушитель с низким потенциалом	системное программное обеспечение; сетевое программное обеспечение
44.	Угроза получения доступа к информационной системе, ее компонентам, информации, обрабатываемой информационной системой без прохождения процедуры идентификации и аутентификации[2]	-[1]	-[1]
45.	Угроза получения доступа к информационной системе вследствие ошибок подсистемы идентификации и аутентификации[2]	-[1]	-[1]
46.	Угроза получения несанкционированного доступа в результате сбоев (ошибок) подсистемы идентификации и аутентификации[2]	-[1]	-[1]
47.	Угроза получения несанкционированного доступа сторонними лицами, устройствами[2]	-[1]	-[1]
48.	Угроза отсутствия (слабости) процедур аутентификации при доступе пользователей (устройств) к ресурсам информационной системы	-[1]	-[1]

1	2	3	4
49.	Угрозы авторизации с использованием устаревших, но неотключенных учетных записей[2)]	-[1)]	-[1)]
50.	Угроза использования «слабых» методов идентификации и аутентификации пользователей, в том числе при использовании удаленного доступа	-[1)]	-[1)]
51.	Угроза применения только программных методов двухфакторной аутентификации	-[1)]	-[1)]
52.	Угроза использования долговременных паролей для подключения к информационной системе посредством удаленного доступа	-[1)]	-[1)]
53.	Угроза передачи аутентифицирующей информации по открытым каналам связи без использования средства криптографической защиты информации	-[1)]	-[1)]
54.	Угроза доступа к информационной системе неаутентифицированных устройств и пользователей	-[1)]	-[1)]
55.	Угроза повторного использования идентификаторов в течение как минимум 1 года	-[1)]	-[1)]
56.	Угроза использования идентификаторов, не используемых более 45 дней	-[1)]	-[1)]
57.	Угроза раскрытия используемых идентификаторов пользователя в публичном доступе	-[1)]	-[1)]
58.	Отсутствие управления идентификаторами внешних пользователей	-[1)]	-[1)]
59.	Угроза использования «слабых» (предсказуемых) паролей	-[1)]	-[1)]

1	2	3	4
60.	Отсутствие отказоустойчивой централизованной системы идентификации и аутентификации	-[1)]	-[1)]
61.	Угроза использования пользователями идентичных идентификаторов в разных информационных системах	-[1)]	-[1)]
62.	Угроза использования неподписанных программных средств	-[1)]	-[1)]
63.	Угроза запуска несанкционированных процессов и служб от имени системных пользователей	-[1)]	-[1)]
64.	Угроза отсутствия регламента работы с персональными идентификаторами	-[1)]	-[1)]
65.	Отсутствие в централизованной системе идентификации и аутентификации атрибутов, позволяющих однозначно определить внешних и внутренних пользователей	-[1)]	-[1)]
66.	Угроза бесконтрольного доступа пользователей к процессу загрузки	-[1)]	-[1)]
67.	Угроза подмены (модификации) базовой системы ввода-вывода, программного обеспечения телекоммуникационного оборудования	-[1)]	-[1)]
VII. Угрозы несанкционированного доступа к информации в результате слабости процедур разграничения ролей и полномочий, правил управления доступом			
68.	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

1	2	3	4
69.	Угроза доступа к защищаемым файлам с использованием обходного пути	внешний нарушитель с низким потенциалом; внутренний нарушитель с низким потенциалом	объекты файловой системы
70.	Угроза доступа к локальным файлам сервера при помощи единого определителя ресурса (URL)	внешний нарушитель со средним потенциалом	сетевое программное обеспечение
71.	Угроза изменения системных и глобальных переменных	внутренний нарушитель со средним потенциалом	системное программное обеспечение; прикладное программное обеспечение; сетевое программное обеспечение
72.	Угроза использования альтернативных путей доступа к ресурсам	внешний нарушитель с низким потенциалом; внутренний нарушитель с низким потенциалом	сетевой узел; объекты файловой системы; прикладное программное обеспечение; системное программное обеспечение
73.	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
74.	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
75.	Угроза неправомерного ознакомления с защищаемой информацией	внутренний нарушитель с низким потенциалом	аппаратное обеспечение; носители информации; объекты файловой системы

1	2	3	4
76.	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 операционной системы; машинные носители информации
77.	Угроза несанкционированного копирования защищаемой информации	внешний нарушитель с низким потенциалом; внутренний нарушитель с низким потенциалом	объекты файловой системы; машинный носитель информации
78.	Угроза несанкционированного редактирования реестра операционной системы	внешний нарушитель с низким потенциалом; внутренний нарушитель с низким потенциалом	системное программное обеспечение, использующее реестр операционной системы; реестр операционной системы
79.	Угроза несанкционированного создания учетной записи пользователя	внешний нарушитель с низким потенциалом; внутренний нарушитель с низким потенциалом	системное программное обеспечение
80.	Угроза несанкционированного управления буфером	внешний нарушитель с низким потенциалом; внутренний нарушитель с низким потенциалом	системное программное обеспечение; прикладное программное обеспечение; сетевое программное обеспечение
81.	Угроза несанкционированного управления синхронизацией и состоянием системы	внешний нарушитель со средним потенциалом; внутренний нарушитель со средним потенциалом	системное программное обеспечение; прикладное программное обеспечение; сетевое программное обеспечение; микропрограммное обеспечение

1	2	3	4
82.	Угроза несанкционированного управления указателями	внешний нарушитель со средним потенциалом; внутренний нарушитель со средним потенциалом	системное программное обеспечение; прикладное программное обеспечение; сетевое программное обеспечение
83.	Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники	внешний нарушитель с низким потенциалом; внутренний нарушитель с низким потенциалом	системное программное обеспечение; аппаратное обеспечение
84.	Угроза перехвата привилегированного потока	внешний нарушитель со средним потенциалом; внутренний нарушитель со средним потенциалом	системное программное обеспечение; прикладное программное обеспечение; сетевое программное обеспечение
85.	Угроза перехвата привилегированного процесса	внешний нарушитель со средним потенциалом; внутренний нарушитель со средним потенциалом	системное программное обеспечение; прикладное программное обеспечение; сетевое программное обеспечение
86.	Угроза повышения привилегий	внешний нарушитель со средним потенциалом; внутренний нарушитель со средним потенциалом	системное программное обеспечение; сетевое программное обеспечение; информационная система
87.	Угроза подделки записей журнала регистрации событий	внешний нарушитель с низким потенциалом; внутренний нарушитель с низким потенциалом	системное программное обеспечение

1	2	3	4
88.	Угроза удаления аутентификационной информации	внешний нарушитель с низким потенциалом; внутренний нарушитель с низким потенциалом	системное программное обеспечение; микропрограммное обеспечение; учетные данные пользователя
89.	Угроза «форсированного веб-браузинга»	внешний нарушитель с низким потенциалом	сетевой узел; сетевое программное обеспечение
90.	Угроза получения несанкционированного доступа к средствам управления персональными идентификаторами (учетными записями), в том числе с повышенными правами доступа[2)]	-[1)]	-[1)]
91.	Угроза получения доступа к данным в обход механизмов разграничения доступа, в том числе с повышенными правами доступа[2)]	-[1)]	-[1)]
92.	Угроза бесконтрольной передачи данных как внутри информационной системы, так и между информационными системами[2)]	-[1)]	-[1)]
93.	Угроза получения дополнительных данных, не предусмотренных технологией обработки[2)]	-[1)]	-[1)]
94.	Угроза получения пользователями и лицами, обеспечивающими функционирование информационной системы персональных данных, доступа к данным и полномочиям, не предназначенным для данных лиц в связи с их должностными обязанностями[2)]	-[1)]	-[1)]
95.	Угроза предоставления прав доступа, не необходимых для исполнения должностных обязанностей и функционирования информационной системы, для совершения деструктивных действий[2)]	-[1)]	-[1)]

1	2	3	4
96.	Отсутствие ограничения на количество неудачных попыток входа в информационную систему[2)]	-[1)]	-[1)]
97.	Угроза использования (подключения) к открытому (незаблокированному) сеансу пользователя[2)]	-[1)]	-[1)]
98.	Угроза использования ресурсов информационной системы до прохождения процедур идентификации и авторизации[2)]	-[1)]	-[1)]
99.	Угрозы несанкционированного подключения к информационной системе с использованием санкционированной сессии удаленного доступа[2)]	-[1)]	-[1)]
100.	Угроза подбора идентификационных данных для удаленного доступа к информационной системе[2)]	-[1)]	-[1)]
101.	Угроза использования слабостей (уязвимостей) защиты протоколов удаленного доступа[2)]	-[1)]	-[1)]
102.	Угроза получения доступа к информационной системе с использованием технологий беспроводного доступа с неконтролируемых устройств[2)]	-[1)]	-[1)]
103.	Угроза несанкционированной автоматической передачи конфиденциальной информации на запросы сторонних информационных систем[2)]	-[1)]	-[1)]
104.	Угроза получения несанкционированного доступа к средствам управления персональными идентификаторами (учетными записями), в том числе с повышенными правами доступа[2)]	-[1)]	-[1)]

1	2	3	4
105.	Угроза получения несанкционированного доступа к средствам управления средствами идентификации и аутентификации[2)]	-[1)]	-[1)]
106.	Угроза перехвата идентифицирующих и аутентифицирующих данных в процессе идентификации и аутентификации пользователей[2)]	-[1)]	-[1)]
107.	Угроза бесконтрольного доступа к информации неопределенным кругом лиц[2)]	-[1)]	-[1)]
108.	Угроза получения доступа к данным, не предназначенным для пользователя[2)]	-[1)]	-[1)]
109.	Угроза удаленного управления и использования периферийных устройств для получения информации или выполнения иных деструктивных целей[2)]	-[1)]	-[1)]
110.	Угроза модификации, подмены, удаления атрибутов безопасности (меток безопасности) при взаимодействии с иными информационными системами[2)]	-[1)]	-[1)]
111.	Угроза использования встроенных в информационную систему недекларированных возможностей, скрытых каналов передачи информации в обход реализованных мер защиты	-[1)]	-[1)]
112.	Отсутствие отказоустойчивых централизованных средств управления учетными записями	-[1)]	-[1)]
113.	Отсутствие автоматического блокирования учетных записей по истечении их срока действия в результате исчерпания попыток доступа к информационной системе, выявления попыток несанкционированного доступа	-[1)]	-[1)]

1	2	3	4
114.	Угроза отсутствия необходимых методов управления доступом для разграничения прав доступа в соответствии с технологией обработки и угрозами безопасности информации	-[1)]	-[1)]
115.	Угроза передачи информации разной степени конфиденциальности без разграничения информационных потоков	-[1)]	-[1)]
116.	Угроза передачи информации без соблюдения атрибутов (меток) безопасности, связанных с передаваемой информацией	-[1)]	-[1)]
117.	Отсутствие динамического анализа и управления информационными потоками в зависимости от состояния информационной системы, условий ее функционирования, изменений в технологии обработки, передаваемых данных	-[1)]	-[1)]
118.	Угроза обхода правил управления информационными потоками за счет манипуляций с передаваемыми данными	-[1)]	-[1)]
119.	Угроза несанкционированного доступа к средствам управления информационными потоками	-[1)]	-[1)]
120.	Угроза возложения функционально различных должностных обязанностей (ролей) на одно должностное лицо	-[1)]	-[1)]
121.	Угроза предоставления расширенных прав и привилегий пользователям, в том числе внешним	-[1)]	-[1)]
122.	Отсутствие информирования пользователя о применении средств защиты информации и необходимости соблюдения установленных опера-	-[1)]	-[1)]

1	2	3	4
	тором правил и ограничений на работу с информацией, предыдущем успешном доступе к информационной системе, количестве успешных (безуспешных) попыток доступа, об изменении сведений об учетной записи пользователя, о превышении числа параллельных сеансов доступа		
123.	Отсутствие информирования администратора о превышении числа параллельных сеансов доступа пользователями	-[1)]	-[1)]
124.	Угроза использования одних и тех же учетных записей для параллельного доступа к информационной системе с двух и более различных устройств	-[1)]	-[1)]
125.	Отсутствие блокирования сеанса пользователя (на мониторе пользователя не должна отображаться информация сеанса пользователя) после времени бездействия 5 минут	-[1)]	-[1)]
126.	Угроза использования незавершенных сеансов пользователей	-[1)]	-[1)]
127.	Угроза наличия удаленного доступа от имени привилегированных пользователей для администрирования информационной системы, системы защиты, в том числе с использованием технологий беспроводного доступа	-[1)]	-[1)]
128.	Отсутствие автоматизированного мониторинга и контроля удаленного доступа	-[1)]	-[1)]
129.	Угроза использования уязвимых (незащищенных) технологий удаленного доступа	-[1)]	-[1)]

1	2	3	4
130.	Угроза взаимодействия с иными информационными системами, не обеспеченными системой защиты	-[1)]	-[1)]
131.	Отсутствие механизмов автоматизированного контроля параметров настройки компонентов программного обеспечения, влияющих на безопасность информации	-[1)]	-[1)]
132.	Отсутствие механизмов автоматизированного реагирования на несанкционированное изменение параметров настройки компонентов программного обеспечения, влияющих на безопасность информации	-[1)]	-[1)]
133.	Отсутствие контроля за используемыми интерфейсами ввода/вывода	-[1)]	-[1)]
VIII. Угрозы ошибок (внесения уязвимостей) при проектировании, внедрении информационной системы и ее системы информационной безопасности			
134.	Угроза внедрения системной избыточности	внутренний нарушитель со средним потенциалом	программное обеспечение; информационная система; ключевая система информационной инфраструктуры
135.	Угроза ошибок при моделировании угроз и нарушителей информационной безопасности[2)]	-[1)]	-[1)]
136.	Угроза внедрения системы защиты, не обеспечивающей нивелирования актуальных угроз и нарушителей информационной безопасности[2)]	-[1)]	-[1)]
IX. Угрозы ошибочных (деструктивных) действий лиц			
137.	Угроза подмены действия пользователя путем обмана	внешний нарушитель со средним потенциалом	прикладное программное обеспечение; сетевое программное обеспечение

1	2	3	4
138.	Угроза «фишинга»	внешний нарушитель с низким потенциалом	рабочая станция; сетевое программное обеспечение; сетевой трафик
139.	Реализация угроз с использованием возможности непосредственного доступа к техническим и части программных средств информационной системы, средств защиты информации и средств криптографической защиты информации, в соответствии с установленными для них административными полномочиями[2)]	-[1)]	-[1)]
140.	Внесение изменений в конфигурацию программных и технических средств в соответствии с установленными полномочиями, приводящими к отключению (частичному отключению) информационной системы, модулей, компонентов, сегментов информационной системы, средств защиты информации (в случае сговора с внешними нарушителями безопасности информации) [2)]	-[1)]	-[1)]
141.	Создание неконтролируемых точек доступа (лазеек) в систему для удаленного доступа к информационной системе[2)]	-[1)]	-[1)]
142.	Переконфигурирование средств защиты информации и средств криптографической защиты информации для реализации угроз информационной системе[2)]	-[1)]	-[1)]
143.	Осуществление угроз с использованием локальных линий связи, систем электропитания и заземления[2)]	-[1)]	-[1)]

1	2	3	4
144.	Хищение ключей шифрования, идентификаторов и известных паролей[2)]	-[1)]	-[1)]
145.	Внесение программно-аппаратных закладок в программно-аппаратные средства информационной системы, обеспечивающих съем информации, используя непосредственное подключение к техническим средствам обработки информации[2)]	-[1)]	-[1)]
146.	Создание методов и средств реализации атак, а также самостоятельное проведение атаки	-[1)]	-[1)]
147.	Ошибки при конфигурировании и обслуживании модулей (компонентов) информационной системы	-[1)]	-[1)]
148.	Создание ситуаций, препятствующих функционированию сети (остановка, сбой серверов; уничтожение и (или) модификация программного обеспечения; создание множественных, ложных информационных сообщений). Несанкционированный съем информации, блокирование работы отдельных пользователей, перестройка планов маршрутизации и политик доступа сети	-[1)]	-[1)]
149.	Разглашение персональных данных лицам, не имеющим права доступа к ним	-[1)]	-[1)]
150.	Нарушение правил хранения ключевой информации	-[1)]	-[1)]
151.	Передача защищаемой информации по открытым каналам связи	-[1)]	-[1)]
152.	Несанкционированная модификация (уничтожение) информации легитимным пользователем	-[1)]	-[1)]

1	2	3	4
153.	Копирование информации на незарегистрированный носитель информации, в том числе печать	-[1)]	-[1)]
154.	Несанкционированное отключение средств защиты	-[1)]	-[1)]
X. Угрозы получения нарушителем сведений о структуре, конфигурации и настройках информационной системы и ее системы защиты			
155.	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
156.	Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб	внешний нарушитель с низким потенциалом	сетевой узел; сетевое программное обеспечение; сетевой трафик
157.	Угроза обнаружения хостов	внешний нарушитель с низким потенциалом	сетевой узел; сетевое программное обеспечение; сетевой трафик
158.	Угроза определения типов объектов защиты	внешний нарушитель с низким потенциалом	сетевой узел; сетевое программное обеспечение; сетевой трафик
159.	Угроза определения топологии вычислительной сети	внешний нарушитель с низким потенциалом	сетевой узел; сетевое программное обеспечение; сетевой трафик
160.	Угроза получения предварительной информации об объекте защиты	внешний нарушитель со средним потенциалом	сетевой узел; сетевое программное обеспечение; сетевой трафик; прикладное программное обеспечение

1	2	3	4
161.	Угроза сканирования веб-сервисов, разработанных на основе языка описания WSDL	внешний нарушитель с низким потенциалом	сетевое программное обеспечение; сетевой узел
162.	Сканирование сети для изучения логики работы информационной системы, выявления протоколов, портов[2)]	-[1)]	-[1)]
163.	Анализ сетевого трафика для изучения логики работы информационной системы, выявления протоколов, портов, перехвата служебных данных (в том числе идентификаторов и паролей), их подмены[2)]	-[1)]	-[1)]
164.	Применение специальных программ для выявления пароля (IP-спуфинг, разные виды перебора)[2)]	-[1)]	-[1)]
XI. Угрозы программно-математических воздействий			
165.	Угроза внедрения кода или данных	внешний нарушитель с низким потенциалом	системное программное обеспечение; прикладное программное обеспечение; сетевое программное обеспечение
166.	Угроза восстановления аутентификационной информации	внешний нарушитель с низким потенциалом; внутренний нарушитель с низким потенциалом	системное программное обеспечение; микропрограммное обеспечение; учетные данные пользователя
167.	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 операционной системы

1	2	3	4
168.	Угроза избыточного выделения оперативной памяти	внешний нарушитель с низким потенциалом; внутренний нарушитель с низким потенциалом	аппаратное обеспечение; системное программное обеспечение; сетевое программное обеспечение
169.	Угроза искажения XML-схемы	внешний нарушитель со средним потенциалом; внутренний нарушитель со средним потенциалом	сетевой узел; сетевое программное обеспечение; сетевой трафик
170.	Угроза использования слабостей кодирования входных данных	внешний нарушитель со средним потенциалом; внутренний нарушитель со средним потенциалом	системное программное обеспечение; прикладное программное обеспечение; сетевое программное обеспечение; микропрограммное обеспечение; реестр операционной системы
171.	Угроза межсайтового скриптинга	внешний нарушитель с низким потенциалом	сетевой узел; сетевое программное обеспечение
172.	Угроза межсайтовой подделки запроса	внешний нарушитель со средним потенциалом	сетевой узел; сетевое программное обеспечение
173.	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
174.	Угроза неправомерного шифрования информации	внешний нарушитель с низким потенциалом	объект файловой системы
175.	Угроза скрытного включения вычислительного устройства в состав бот-сети	внешний нарушитель с низким потенциалом	сетевой узел; сетевое программное обеспечение

1	2	3	4
176.	Угроза распространения «почтовых червей»	внешний нарушитель с низким потенциалом	сетевое программное обеспечение
177.	Внедрение программных закладок[2)]	-[1)]	-[1)]
178.	Угроза внедрения в информационную систему вредоносного программного обеспечения с устройств, подключаемых с использованием технологий беспроводного доступа[2)]	-[1)]	-[1)]
179.	Применение специально созданных программных продуктов для несанкционированного доступа[2)]	-[1)]	-[1)]
180.	Угроза внедрения через легитимные схемы информационного обмена между информационными системами вредоносного программного обеспечения[2)]	-[1)]	-[1)]
181.	Отсутствие централизованной системы управления средствами антивирусной защиты	-[1)]	-[1)]
XII. Угрозы, связанные с использованием «облачных» услуг			
182.	Угроза злоупотребления возможностями, предоставленными потребителям «облачных» услуг	внутренний нарушитель с низким потенциалом	«облачная» система; виртуальная машина
183.	Угроза злоупотребления доверием потребителей «облачных» услуг	внешний нарушитель с низким потенциалом	«облачная» система
184.	Угроза нарушения доступности «облачного» сервера	внешний нарушитель с низким потенциалом; внутренний нарушитель с низким потенциалом	«облачная» система; «облачный» сервер
185.	Угроза невозможности миграции образов виртуальных машин из-за несовместимости аппарат-	внешний нарушитель с низким потенциалом	«облачная» инфраструктура; виртуальная машина;

1	2	3	4
	ного и программного обеспечения		аппаратное обеспечение; системное программное обеспечение
186.	Угроза недобросовестного исполнения обязательств поставщиками «облачных» услуг	внешний нарушитель с низким потенциалом	информационная система; сервер; носитель информации; метаданные; объекты файловой системы
187.	Угроза незащищенного администрирования «облачных» услуг	внешний нарушитель с низким потенциалом; внутренний нарушитель с низким потенциалом	«облачная» система; рабочая станция; сетевое программное обеспечение
188.	Угроза некачественного переноса инфраструктуры в «облако»	внешний нарушитель с низким потенциалом	информационная система, иммигрированная в «облако»; «облачная» система
189.	Угроза неконтролируемого роста числа виртуальных машин	внешний нарушитель с низким потенциалом; внутренний нарушитель с низким потенциалом	«облачная» система; консоль управления «облачной» инфраструктурой; «облачная» инфраструктура
190.	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
191.	Угроза неопределенности в распределении ответственности между ролями в «облаке»	внешний нарушитель с низким потенциалом; внутренний нарушитель с низким потенциалом	системное программное обеспечение

1	2	3	4
192.	Угроза неопределенности ответственности за обеспечение безопасности «облака»	внешний нарушитель с низким потенциалом	«облачная» система
193.	Угроза непрерывной модернизации «облачной» инфраструктуры	внутренний нарушитель со средним потенциалом	«облачная» инфраструктура
194.	Угроза несогласованности политик безопасности элементов «облачной» инфраструктуры	внешний нарушитель с низким потенциалом; внутренний нарушитель с низким потенциалом	системное программное обеспечение; «облачная» система
195.	Угроза общедоступности «облачной» инфраструктуры	внешний нарушитель со средним потенциалом	объекты файловой системы; аппаратное обеспечение; «облачный» сервер
196.	Угроза потери доверия к поставщику «облачных» услуг	внутренний нарушитель со средним потенциалом	объекты файловой системы; информационная система, иммигрированная в «облако»
197.	Угроза потери и утечки данных, обрабатываемых в «облаке»	внутренний нарушитель с низким потенциалом	системное программное обеспечение; метаданные; объекты файловой системы
198.	Угроза потери управления «облачными» ресурсами	внешний нарушитель с высоким потенциалом	сетевой трафик; объекты файловой системы
199.	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
200.	Угроза привязки к поставщику «облачных» услуг	внутренний нарушитель с низким потенциалом	информационная система, иммигрированная в облако; системное программное обеспечение;

1	2	3	4
			сетевое программное обеспечение; сетевой трафик; объекты файловой системы
201.	Угроза приостановки оказания «облачных» услуг вследствие технических сбоев	-[1)]	системное программное обеспечение; аппаратное обеспечение; канал связи
202.	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
XIII. Угрозы, связанные с использованием технологий виртуализации			
203.	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
204.	Угроза нарушения изоляции пользовательских данных внутри виртуальной машины	внешний нарушитель со средним потенциалом; внутренний нарушитель со средним потенциалом	виртуальная машина; гипервизор
205.	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

1	2	3	4
206.	Угроза неконтролируемого роста числа зарезервированных вычислительных ресурсов	внешний нарушитель с низким потенциалом; внутренний нарушитель с низким потенциалом	информационная система; сервер
207.	Угроза несанкционированного доступа к виртуальным каналам передачи	внешний нарушитель с низким потенциалом; внутренний нарушитель с низким потенциалом	сетевое программное обеспечение; сетевой трафик; виртуальные устройства
208.	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
209.	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
210.	Угроза несанкционированного доступа к защищаемым виртуальным машинам со стороны других виртуальных машин	внешний нарушитель с низким потенциалом; внутренний нарушитель с низким потенциалом	виртуальная машина
211.	Угроза несанкционированного доступа к системе хранения данных из виртуальной и (или) физической сети	внешний нарушитель с низким потенциалом; внутренний наруши-	виртуальные устройства хранения данных; виртуальные диски

1	2	3	4
		тель с низким потенциалом	
212.	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
213.	Угроза ошибки обновления гипервизора	внутренний нарушитель с низким потенциалом	системное программное обеспечение; гипервизор
214.	Угроза перехвата управления гипервизором	внешний нарушитель со средним потенциалом; внутренний нарушитель со средним потенциалом	системное программное обеспечение; гипервизор; консоль управления гипервизором
215.	Угроза перехвата управления средой виртуализации	внешний нарушитель со средним потенциалом; внутренний нарушитель со средним потенциалом	информационная система; системное программное обеспечение
216.	Нарушение доверенной загрузки виртуальных серверов информационных систем, перехват загрузки[2)]	-[1)]	-[1)]
217.	Нарушение целостности конфигурации виртуальных серверов-подмена (искажение) образов (данных и оперативной памяти)[2)]	-[1)]	-[1)]
218.	Угроза несанкционированного доступа к консоли управления виртуальной инфраструктурой[2)]	-[1)]	-[1)]

1	2	3	4
219.	Угроза несанкционированного доступа к виртуальному серверу информационной системы, в том числе несанкционированного сетевого подключения и проведения сетевых атак на виртуальный сервер информационной системы[2)]	-[1)]	-[1)]
220.	Угроза несанкционированного доступа к ресурсам гипервизора вследствие сетевых атак типа «переполнение буфера»[2)]	-[1)]	-[1)]
221.	Угроза несанкционированного доступа к объектам виртуальной инфраструктуры без прохождения процедуры идентификации и аутентификации[2)]	-[1)]	-[1)]
222.	Угроза несанкционированного доступа к виртуальной инфраструктуре (компонентам виртуальной инфраструктуры или виртуальным машинам или объектам внутри виртуальных машин)[2)]	-[1)]	-[1)]
223.	Угроза отсутствия средств регистрации событий в виртуальной инфраструктуре[2)]	-[1)]	-[1)]
XIV. Угрозы, связанные с нарушением правил эксплуатации машинных носителей			
224.	Угроза несанкционированного восстановления удаленной защищаемой информации	внешний нарушитель с низким потенциалом; внутренний нарушитель с низким потенциалом	машинный носитель информации
225.	Угроза несанкционированного удаления защищаемой информации	внешний нарушитель с низким потенциалом; внутренний нарушитель с низким потенциалом	метаданные; объекты файловой системы; реестр операционной системы

1	2	3	4
226.	Угроза утраты носителей информации	внутренний нарушитель с низким потенциалом	носитель информации
227.	Угроза форматирования носителей информации	внешний нарушитель с низким потенциалом; внутренний нарушитель с низким потенциалом	носитель информации
228.	Повреждение носителя информации	-[1)]	-[1)]
229.	Доступ к снятым с эксплуатации носителям информации (содержащим остаточные данные)	-[1)]	-[1)]
230.	Угроза подключения к информационной системе неучтенных машинных носителей[2)]	-[1)]	-[1)]
231.	Угроза подключения к информационной системе не персонифицированных машинных носителей	-[1)]	-[1)]
232.	Угроза несанкционированного копирования информации на машинные носители[2)]	-[1)]	-[1)]
233.	Угроза несанкционированной модификации (удаления) информации на машинных носителях[2)]	-[1)]	-[1)]
234.	Угроза хищения машинных носителей[2)]	-[1)]	-[1)]
235.	Угроза подмены машинных носителей[2)]	-[1)]	-[1)]
236.	Угроза встраивания программно-аппаратных закладок в машинные носители[2)]	-[1)]	-[1)]
237.	Угроза несанкционированного доступа к информации, хранящейся на машинном носителе[2)]	-[1)]	-[1)]
238.	Угроза использования машинных носителей для хранения информации разных уровней конфиденциальности и целей обработки	-[1)]	-[1)]

1	2	3	4
239.	Угроза использования неконтролируемых портом средства вычислительной техники для вывода информации на сторонние машинные носители[2)]	-[1)]	-[1)]
240.	Угроза передачи информации (фрагментов информации) между пользователями, сторонними организациями при неполном уничтожении (стирании) информации с машинных носителей[2)]	-[1)]	-[1)]
241.	Угроза несанкционированного использования машинных носителей	-[1)]	-[1)]
242.	Угроза несанкционированного выноса машинных носителей за пределы контролируемой зоны	-[1)]	-[1)]
XV. Угрозы, связанные с нарушением процедур установки (обновления) программного обеспечения и оборудования			
243.	Угроза запуска (установки) вредоносного (шпионского или неразрешенного) программного обеспечения и (или) обновлений программного обеспечения[2)]	-[1)]	-[1)]
244.	Установка программного обеспечения, содержащего известные уязвимости[2)]	-[1)]	-[1)]
245.	Установка нелицензионного программного обеспечения[2)]	-[1)]	-[1)]
246.	Угроза ошибочного запуска (установки) программного обеспечения[2)]	-[1)]	-[1)]
247.	Угроза неправильной установки программного обеспечения[2)]	-[1)]	-[1)]
248.	Угроза автоматического запуска вредоносного (шпионского или неразрешенного) программного обеспечения при запуске операционной сис-	-[1)]	-[1)]

1	2	3	4
	темы и (или) обновлений программного обеспечения		
249.	Угроза удаленного запуска (удаленной установки) вредоносного (шпионского или неразрешенного) программного обеспечения	-[1)]	-[1)]
250.	Угроза несанкционированного запуска программного обеспечения в нерабочее время	-[1)]	-[1)]
XVI. Угрозы физического доступа к компонентам информационных систем			
251.	Угроза преодоления физической защиты	внешний нарушитель со средним потенциалом	сервер; рабочая станция; носитель информации; аппаратное обеспечение
252.	Угроза физического выведения из строя средств хранения, обработки и (или) ввода, вывода или передачи информации	внешний нарушитель с низким потенциалом	сервер; рабочая станция; носитель информации; аппаратное обеспечение
253.	Угроза хищения средств хранения, обработки и (или) ввода, вывода или передачи информации	внешний нарушитель с низким потенциалом	сервер; рабочая станция; носитель информации; аппаратное обеспечение
254.	Угроза несанкционированного доступа к средства криптографической защиты информации[2)]	-[1)]	-[1)]
255.	Угроза нарушения функционирования жестких магнитных дисков и других систем хранения данных[2)]	-[1)]	-[1)]
256.	Угроза доступа к системам обеспечения, их повреждения[2)]	-[1)]	-[1)]
257.	Угроза нарушения функционирования кабельных линий связи, телекоммуникационных систем[2)]	-[1)]	-[1)]

1	2	3	4
258.	Угроза несанкционированного доступа в контролируемую зону[2)]	-[1)]	-[1)]
259.	Отсутствие средств автоматизированного контроля доступа	-[1)]	-[1)]
XVII. Угрозы эксплуатации уязвимостей в системном программном обеспечении, прикладном программном обеспечении, средствах защиты информации, средствах криптографической защиты информации, аппаратных компонентах информационной системы, микропрограммном обеспечении			
260.	Угроза анализа криптографических алгоритмов и их реализации	внешний нарушитель со средним потенциалом	метаданные; системное программное обеспечение
261.	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
262.	Угроза перехвата (исключения) сигнала из привилегированного блока функций	внешний нарушитель со средним потенциалом; внутренний нарушитель со средним потенциалом	системное программное обеспечение
263.	Угроза наличия механизмов разработчика	внутренний нарушитель со средним потенциалом	программное обеспечение; техническое средство
XVIII. Угрозы, связанные с использованием сетевых технологий			
264.	Угроза деавторизации санкционированного клиента беспроводной сети	внешний нарушитель с низким потенциалом; внутренний нарушитель с низким потенциалом	сетевой узел

1	2	3	4
265.	Угроза доступа (перехвата или изменения HTTP cookies)	внешний нарушитель с низким потенциалом	прикладное программное обеспечение; сетевое программное обеспечение
266.	Угроза заражения DNS-кэша	внешний нарушитель с низким потенциалом	сетевой узел; сетевое программное обеспечение; сетевой трафик
267.	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
268.	Угроза неправомерных действий в каналах связи	внешний нарушитель с низким потенциалом	сетевой трафик
269.	Угроза перехвата данных, передаваемых по вычислительной сети	внешний нарушитель с низким потенциалом	сетевой узел; сетевой трафик
270.	Угроза подмены доверенного пользователя	внешний нарушитель с низким потенциалом	сетевой узел; сетевое программное обеспечение
271.	Угроза подмены субъекта сетевого доступа	внешний нарушитель со средним потенциалом	прикладное программное обеспечение; сетевое программное обеспечение; сетевой трафик
272.	Угроза «фарминга»	внешний нарушитель с низким потенциалом	рабочая станция; сетевое программное обеспечение; сетевой трафик
273.	Угроза удаленного запуска приложений	-[1)]	-[1)]
274.	Угроза навязывания ложных маршрутов[2)]	-[1)]	-[1)]
275.	Угроза перехвата данных[2)]	-[1)]	-[1)]
276.	Угроза внедрения ложных объектов сети[2)]	-[1)]	-[1)]
277.	Угроза проведения атак (попыток) несанкционированного доступа к информационной систе-	-[1)]	-[1)]

1	2	3	4
	ме с использованием протоколов сетевого доступа[2)]		
278.	Угроза отсутствия механизмов реагирования (блокирования) атак (вторжений)[2)]	-[1)]	-[1)]
279.	Угроза отсутствия системы анализа сетевого трафика при обмене данными между информационными системами на наличие атак (вторжений)[2)]	-[1)]	-[1)]
280.	Угроза отсутствия системы анализа сетевого трафика между сегментами информационной системы на наличие атак (вторжений)[2)]	-[1)]	-[1)]
281.	Угроза использования неактуальных версий сигнатур обнаружения атак[2)]	-[1)]	-[1)]
282.	Угроза отсутствия централизованной системы управления средствами защиты от атак (вторжений)	-[1)]	-[1)]
283.	Угроза использования слабостей (уязвимостей) защиты протоколов удаленного доступа[2)]	-[1)]	-[1)]
284.	Угроза перехвата данных, передаваемых с использованием технологий беспроводного доступа[2)]	-[1)]	-[1)]
285.	Угроза подмены устройств, подключаемых к информационной системе с использованием технологии удаленного доступа[2)]	-[1)]	-[1)]
286.	Угроза использования неконтролируемых сетевых протоколов для модификации (перехвата управления) информационной системой[2)]	-[1)]	-[1)]

1	2	3	4
287.	Угроза перехвата, искажения, модификации, подмены, перенаправления трафика между разными категориями пользователей и средствами защиты информации[2)]	-[1)]	-[1)]
288.	Угроза отсутствия проверки подлинности сетевых соединений[2)]	-[1)]	-[1)]
289.	Отсутствие подтверждения факта отправки (получения) информации конкретными пользователями[2)]	-[1)]	-[1)]
290.	Угроза получения несанкционированного доступа при двунаправленной передаче информации между сегментами, информационными системами	-[1)]	-[1)]
291.	Отсутствие контроля соединений между средствами вычислительной техники информационной системы	-[1)]	-[1)]
292.	Угроза несанкционированного доступа к средствам управления информационными потоками	-[1)]	-[1)]
293.	Угроза отсутствия (неиспользования) средств разделения информационных потоков, содержащих различные виды (категории) информации, а также отделение информации управления от пользовательской информации	-[1)]	-[1)]
294.	Отсутствие средств анализа сетевого трафика на наличие вредоносного программного обеспечения	-[1)]	-[1)]
295.	Угроза доступа к информационной системе с использованием беспроводного доступа из-за границ контролируемой зоны	-[1)]	-[1)]

1	2	3	4
XIX. Угрозы инженерной инфраструктуры			
296.	Угрозы сбоев в сети электропитания	-[1)]	-[1)]
297.	Угроза выхода из строя технических средств в результате нарушения климатических параметров работы	-[1)]	-[1)]
298.	Угрозы нарушения схем электропитания[2)]	-[1)]	-[1)]
299.	Угрозы связанные с отсутствием заземления (неправильным заземлением)[2)]	-[1)]	-[1)]
XX. Угрозы, связанные с отсутствием системы регистрации событий информационной безопасности			
300.	Угроза отсутствия системы регистрации событий информационной безопасности[2)]	-[1)]	-[1)]
301.	Угроза автоматического удаления (затирания) событий информационной безопасности новыми события[2)]	-[1)]	-[1)]
302.	Угроза переполнения журналов информационной безопасности[2)]	-[1)]	-[1)]
303.	Угроза отсутствия централизованной подсистемы централизованного сбора событий информационной безопасности от различных программных и аппаратных продуктов, средств защиты информации[2)]	-[1)]	-[1)]
304.	Угроза неправильного отнесения событий, к событиям информационной безопасности[2)]	-[1)]	-[1)]
305.	Угроза отсутствия централизованной системы анализа журналов информационной безопасности от различных программных и аппаратных продуктов, средств защиты информации[2)]	-[1)]	-[1)]
306.	Угроза отключения журналов информационной безопасности[2)]	-[1)]	-[1)]

1	2	3	4
307.	Угроза модификации (удаления) журналов информационной безопасности[2)]	-[1)]	-[1)]
308.	Угроза задержек при получении журналов информационной безопасности	-[1)]	-[1)]
309.	Угроза ошибок ведения журнала регистрации событий информационной безопасности, в том числе связанных с неправильными настройками времени	-[1)]	-[1)]
310.	Угроза отсутствия необходимых сведений в журналах информационной безопасности для проведения проверки, расследования или анализа событий информационной безопасности[2)]	-[1)]	-[1)]
311.	Угроза отключения (отказа) системы регистрации событий информационной безопасности	-[1)]	-[1)]
312.	Угроза несанкционированного изменения правил ведения журнала регистрации событий	-[1)]	-[1)]
313.	Отсутствие оповещений (предупреждений) администратора о сбоях, критических событиях в работе системы регистрации событий информационной безопасности	-[1)]	-[1)]
XXI. Угрозы, связанные с контролем защищенности информационной системы			
314.	Угроза отсутствия контроля за уязвимостями информационной системы и ее компонентов и наличием неразрешенного программного обеспечения[2)]	-[1)]	-[1)]
315.	Угроза использования неактуальных версий баз данных уязвимостей средств анализа защищенности[2)]	-[1)]	-[1)]

1	2	3	4
316.	Угроза установки программного обеспечения (обновлений) без проведения анализа уязвимостей	-[1)]	-[1)]
317.	Угроза отсутствия регулярного контроля за защищенностью информационной системы, в том числе средств защиты информации, с учетом новых угроз безопасности информации	-[1)]	-[1)]
318.	Угроза отсутствия анализа изменения настроек информационной системы, компонентов информационной системы, в том числе средств защиты информации на предмет появления уязвимостей[2)]	-[1)]	-[1)]
319.	Отсутствие журнала анализа защищенности	-[1)]	-[1)]

[1)] Определяются в частных моделях угроз и нарушителя безопасности информации для каждой информационной системы персональных данных.

[2)] Базовые угрозы безопасности персональных данных в информационной системе персональных данных.