ПРИНЯТО

Педагогическим советом МБОУ «Лицей №1 ЗМР РТ»
протокол от 28.12.2018 №3
председатель педагогического совета
_____ С.Ю.Кудрявцева

УТВЕРЖДАЮ

Директор МБОУ «Лицей №1 ЗМР РТ»
_____ С.Ю.Кудрявцева
Введено в действие приказом
от 28.12.2018 №379-о

ПОЛОЖЕНИЕ
об определении актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных МБОУ «Лицей №1 ЗМР РТ»

1. Общие положения

1.1. Настоящее Положение определяет перечень угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых Муниципальным бюджетным общеобразовательным учреждением «Лицей №1 Зеленодольского муниципального района Республики Татарстан (далее – Лицей), при осуществлении им соответствующих видов деятельности, с учетом содержания персональных данных, характера и способов их обработки. Указанный перечень уточняется по мере выявления новых угроз безопасности персональных данных и их источников, развития способов и средств их реализации.

1.2. Настоящее Положение не регулирует отношения, связанные с обеспечением безопасности персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну.

1.3. Настоящее Положение применяется Лицеем при решении ими следующих задач:

определение угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных;

анализ защищенности информационных систем персональных данных от актуальных угроз безопасности персональных данных в ходе выполнения мероприятий по информационной безопасности (защите информации);

модернизация системы защиты персональных данных в Лицее;

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

предотвращение несанкционированного воздействия на технические средства информационных систем персональных данных;

контроль за обеспечением уровня защищенности персональных данных педагогов и учащихся.

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

группы актуальных угроз безопасности персональных данных в информационных системах персональных данных, приведенные в разделе 6 настоящего Положения;

расширенный перечень угроз безопасности персональных данных в информационных системах персональных данных, приведенный в приложении № 1 к настоящему Положению;

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

1.5. При определении актуальных угроз безопасности персональных данных в информационных системах персональных данных Лицей руководствуется положениями следующих нормативных правовых актов:

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

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

постановление Правительства Российской Федерации от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»;

постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

приказ Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 года № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

приказ Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 года № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

приказ Федеральной службы безопасности Российской Федерации от 10 июля 2014 года № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;

Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденная заместителем директора Федеральной службы по техническому и экспортному контролю от 14 февраля 2008 года;

Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденная заместителем директора Федеральной службы по техническому и экспортному контролю от 15 февраля 2008 года;

Методические рекомендации по составлению Частной модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных учреждений здравоохранения, социальной сферы, труда и занятости, разработанные Министерством здравоохранения и социального развития Российской Федерации, согласованные с Федеральной службой по техническому и экспортному контролю 22 декабря 2009 года;

Модель угроз типовой медицинской информационной системы типового лечебного профилактического учреждения, разработанная Министерством здравоохранения и социального развития Российской Федерации, согласованная с Федеральной службой по техническому и экспортному контролю 27 ноября 2009 года;

Модель угроз и нарушителя безопасности персональных данных, обрабатываемых в типовых информационных системах персональных данных отрасли, согласованная с Федеральной службой по техническому и экспортному контролю, Федеральной службой безопасности Российской Федерации и одобренная решением секции № 1 Научно-технического совета Министерства связи и массовых коммуникаций Российской Федерации «Научно-техническое и стратегическое развитие отрасли» от 21 апреля 2010 года № 2;

Руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации», утвержденный решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 года;

Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К), утвержденные решением Коллегии Государственной технической комиссии при Президенте Российской Федерации № 7.2/02.03.01 г.;

Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности, утвержденные руководством 8 Центра Федеральной службы безопасности Российской Федерации (от 31 марта 2015 года № 149/7/2/6-432).

1.6. В настоящем Положении используются термины и понятия, установленные Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными

постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной заместителем директора Федеральной службы по техническому и экспортному контролю от 14 февраля 2008 года.

В настоящем Положении применяются следующие сокращения:

АРМ – автоматизированное рабочее место;

ГИСТ РТ – Государственная интегрированная система телекоммуникаций Республики Татарстан;

ИСПДн – информационная система персональных данных;

ПО – программное обеспечение;

ПЭВМ – персональная электронно-вычислительная машина (АРМ);

реестр – стандартный реестр операционной системы;

ТС – технические средства.

2. Владельцы и операторы информационных систем персональных данных, сети передачи данных

2.1. Владельцами ИСПДн и их операторами является Лицей.

2.2. Владельцы ИСПДн и их операторы расположены в Лицее.

2.3. Контролируемой зоной ИСПДн, функционирующих в Лицее, являются здания и отдельные помещения, принадлежащие ему или арендуемые этим Лицеем. Все средства вычислительной техники, участвующие в обработке персональных данных, располагаются в пределах контролируемой зоны Лицея. Вне контролируемой зоны находятся линии передачи данных и телекоммуникационное оборудование оператора связи (провайдера), используемое для информационного обмена по сетям связи общего пользования (сетям международного информационного обмена) и расположенное за пределами территории Лицея.

2.4. Локальные вычислительные сети передачи данных в Лицее организованы по топологии «звезда» и имеют подключения к следующим сетям:

внешним сетям (сетям провайдера), подключение к которым организовано посредством проводных (медных и оптоволоконных) каналов связи операторов связи (провайдеров);

сетям Лицея, организаций, расположенных на территории Российской Федерации. Подключение к указанным сетям осуществляется в соответствии с разработанными регламентами взаимодействия. Органы исполнительной власти Республики Татарстан имеют подключение к ГИСТ РТ посредством защищенных каналов связи;

иным сетям, взаимодействие с которыми организовано Лицеем с целью исполнения своих полномочий.

2.5. Подключение к сетям связи общего пользования осуществляется Лицеем при условии соблюдения ими мер по защите передаваемой информации, в том числе мер по защите подключения для передачи данных.

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

3.1. При определении Лицеем угрозы безопасности персональным данным в конкретной ИСПДн защите подлежат следующие объекты, входящие в ИСПДн:

персональные данные, обрабатываемые в ИСПДн;

информационные ресурсы ИСПДн (файлы, базы данных и т.п.);

средства вычислительной техники, участвующие в обработке персональных данных посредством ИСПДн;

средства криптографической защиты информации и средства защиты информации;

среда функционирования средств криптографической защиты информации;

информация, относящаяся к криптографической защите персональных данных, включая ключевую, парольную и аутентифицирующую информацию средств криптографической защиты информации;

документы, дела, журналы, картотеки, издания, технические документы, видео-, кино- и фотоматериалы, рабочие материалы и т.п., в которых отражена защищаемая информация, относящаяся к ИСПДн и их криптографической защите, включая документацию на средства криптографической защиты информации и на технические и программные компоненты среды функционирования средств криптографической защиты информации;

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

используемые ИСПДн каналы (линии) связи, включая кабельные системы;

сети передачи данных, не выходящие за пределы контролируемой зоны ИСПДн;

помещения, в которых обрабатываются персональные данные посредством ИСПДн и располагаются компоненты ИСПДн;

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

3.2. В состав средств вычислительной техники, участвующих в обработке персональных данных посредством ИСПДн, входят:

АРМ пользователей с различными уровнями доступа (правами);

терминальная станция;

серверное оборудование;

сетевое и телекоммуникационное оборудование;

общесистемное ПО (операционные системы физических серверов, виртуальных серверов, АРМ и т.п.).

3.3. Ввод персональных данных в ИСПДн в Лицее осуществляется как с бумажных, так и с электронных носителей информации. Персональные данные

выводятся из ИСПДн как в электронном, так и в бумажном виде с целью их хранения и (или) передачи третьим лицам.

4. Информационные системы персональных данных

4.1. В целях исполнения своих полномочий Лицеем обрабатываются все категории персональных данных. Состав персональных данных, подлежащих обработке в конкретной ИСПДн, цели обработки, действия (операции), совершаемые с персональными данными в ИСПДн, определяются Лицеем, являющимся оператором ИСПДн.

4.2. Обработка персональных данных в ИСПДн осуществляется в соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных». Перечень обрабатываемых персональных данных в ИСПДн должен соответствовать целям их обработки.

4.3. ИСПДн подразделяются на:

ИСПДн, оператором которых является сам Лицей;

ИСПДн, эксплуатируемые Лицеем, не в качестве ее оператора.

4.4. ИСПДн и ее компоненты должны быть расположены в Российской Федерации.

4.5. ИСПДн подразделяются в зависимости от технологии обработки персональных данных, целей и состава персональных данных на следующие категории:

информационно-справочные;

сегментные;

республиканские;

ведомственные;

служебные.

Для всех категорий персональных данных вышеуказанных категорий ИСПДн необходимо обеспечивать следующие характеристики безопасности: конфиденциальность, целостность, доступность. В рамках ИСПДн возможна модификация и передача персональных данных.

4.5.1. Информационно-справочные ИСПДн используются в целях официального доведения любой информации до определенного или неопределенного круга лиц.

К информационно-справочным ИСПДн относятся:

официальные порталы (сайты) Лицея;

информационные порталы (сайты), которые ведутся Лицеем в целях реализации проекта и (или) проведения мероприятия на территории Республики Татарстан (далее – информационные порталы (сайты));

закрытые порталы для нескольких групп участников Лицея;

Портал государственных и муниципальных услуг Республики Татарстан.

4.5.1.1. Официальные порталы (сайты) Лицея содержат сведения о деятельности Лицея, в том числе сведения, подлежащие обязательному размещению в указанных ИСПДн в соответствии с законодательством.

Категории персональных данных, которые могут подлежать обработке в ИСПДн:

общедоступные;

иные.

Режим обработки персональных данных в ИСПДн: многопользовательский. ИСПДн предусматривает разграничение доступа. Обработка персональных данных осуществляется посредством веб-интерфейса сотрудниками Лицея, являющегося оператором ИСПДн, гражданами Российской Федерации и других государств. Персональные данные хранятся в базе данных ИСПДн и отображаются по запросу соответствующей страницы ИСПДн пользователям в соответствии с предоставленными правами.

Типы субъектов персональных данных, которые могут подлежать обработке в ИСПДн: сотрудники Лицея, являющегося оператором ИСПДн, граждане Российской Федерации и других государств.

Структура ИСПДн: локальная, функционирующая в контролируемой зоне Лицея, и (или) на серверном оборудовании иного Органа в пределах его контролируемой зоны, и (или) на вычислительных ресурсах облачного провайдера.

ИСПДн подключены к сетям связи общего пользования (сетям международного информационного обмена). По типу подключения ИСПДн делятся на:

подключенные посредством ГИСТ РТ;

подключенные с использованием иных каналов связи.

Средства вычислительной техники, участвующие в обработке: АРМ, серверное оборудование, сетевое и телекоммуникационное оборудование.

4.5.1.2. Информационные порталы (сайты) содержат сведения о мероприятиях, проводимых Органами в соответствии с их функциями и полномочиями.

Категории персональных данных, которые могут подлежать обработке в ИСПДн:

общедоступные;

иные.

Режим обработки персональных данных в ИСПДн: многопользовательский. ИСПДн предусматривает разграничение доступа. Обработка персональных данных осуществляется посредством веб-интерфейса сотрудниками Лицея, являющегося оператором ИСПДн, гражданами Российской Федерации и других государств. Персональные данные хранятся в базе данных ИСПДн и отображаются по запросу соответствующей страницы ИСПДн пользователям в соответствии с предоставленными правами.

Типы субъектов персональных данных, которые могут подлежать обработке в ИСПДн: сотрудники Лицея, являющегося оператором ИСПДн, граждане Российской Федерации и других государств.

Структура ИСПДн: локальная, функционирующая в контролируемой зоне Лицея, и (или) на серверном оборудовании иного Лицея в пределах его контролируемой зоны, и (или) на вычислительных ресурсах облачного провайдера.

ИСПДн подключены к сетям связи общего пользования (сетям международного информационного обмена). По типу подключения ИСПДн делятся на:

подключенные посредством ГИСТ РТ;

подключенные с использованием иных каналов связи.

Средства вычислительной техники, участвующие в обработке: АРМ, серверное оборудование, сетевое и телекоммуникационное оборудование.

4.5.1.3. Закрытые порталы для нескольких групп участников Лицея содержат сведения, предоставляемые ограниченному кругу лиц из числа Лицея в соответствии с их функциями и полномочиями.

Категории персональных данных, которые могут подлежать обработке в ИСПДн:

общедоступные;

иные.

Режим обработки персональных данных в ИСПДн: многопользовательский. ИСПДн предусматривает разграничение доступа. Обработка персональных данных осуществляется сотрудниками Лицея посредством веб-интерфейса в соответствии с предоставленными правами. Персональные данные хранятся в базе данных ИСПДн и отображаются по запросу соответствующей страницы ИСПДн пользователям в соответствии с предоставленными правами.

Типы субъектов персональных данных, которые могут подлежать обработке в ИСПДн: сотрудники Лицея

Структура ИСПДн: локальная, функционирующая в контролируемой зоне Лицея, и (или) на серверном оборудовании иного Лицея в пределах его контролируемой зоны, и (или) на вычислительных ресурсах облачного провайдера.

ИСПДн подключены к сетям связи общего пользования (сетям международного информационного обмена). По типу подключения ИСПДн делятся на:

подключенные посредством ГИСТ РТ;

подключенные с использованием иных каналов связи.

Средства вычислительной техники, участвующие в обработке: АРМ, серверное оборудование, сетевое и телекоммуникационное оборудование.

4.5.1.4. Портал государственных и муниципальных услуг Республики Татарстан содержит социально значимую информацию и сведения, необходимые для получения гражданами государственных и муниципальных услуг в электронном виде.

Категории персональных данных, которые могут подлежать обработке в ИСПДн:

общедоступные;

иные.

Режим обработки персональных данных в ИСПДн: многопользовательский, ИСПДн предусматривает разграничение доступа. Обработка персональных данных осуществляется в соответствии с предоставленными правами сотрудниками Лицея, гражданами Российской Федерации и других государств посредством веб-интерфейса.

Персональные данные обрабатываются в деперсонифицированном (обезличенном) виде. Запрашиваемые данные не позволяют однозначно идентифицировать субъекта персональных данных без использования сторонних баз данных. После получения запрашиваемых данных ИСПДн в целях получения ответа на запрос субъекта персональных данных передает его данные по закрытым каналам связи в ИСПДн иных Лицеев, в чью компетенцию входит предоставление информации по запросу субъекта. Ответ на запрос (сведения о ходе исполнения запроса) субъекта отображается в указанной ИСПДн.

Типы субъектов персональных данных, которые могут подлежать обработке в ИСПДн: сотрудники Органа, являющегося оператором ИСПДн, граждане Российской Федерации и других государств.

Структура ИСПДн: локальная, функционирующая в контролируемой зоне Органа, и (или) на серверном оборудовании иного Лицея в пределах его контролируемой зоны, и (или) на вычислительных ресурсах облачного провайдера.

ИСПДн подключены к сетям связи общего пользования (сетям международного информационного обмена). По типу подключения ИСПДн делятся на:

подключенные посредством ГИСТ РТ;

подключенные с использованием иных каналов связи.

Средства вычислительной техники, участвующие в обработке: АРМ, серверное оборудование, сетевое и телекоммуникационное оборудование.

4.5.2. Сегментные ИСПДн представляют собой сегменты федеральных информационных систем, создаются и эксплуатируются в Республике Татарстан на основании предоставляемых оператором федеральной информационной системы рекомендаций (правовых, организационных, технических) и используются для сбора, обработки, свода данных в Республике Татарстан и передачи их оператору федеральной информационной системы, и наоборот, при этом цели и задачи создания (модернизации), эксплуатации данных информационной системы определяются оператором федеральной информационной системы. Данные ИСПДн предназначены для реализации полномочий федеральных органов власти и исполнения функций Лицеев.

Обработке в ИСПДн могут подлежать все категории персональных данных.

Режим обработки персональных данных в ИСПДн: многопользовательский. ИСПДн предусматривает разграничение доступа. Обработка персональных данных осуществляется в соответствии с предоставленными правами сотрудниками Лицея в специализированных программах и (или) посредством веб-интерфейса, а в отдельных случаях – гражданами Российской Федерации и других государств в режиме веб-интерфейса (с ограниченными правами доступа).

Типы субъектов персональных данных, которые могут подлежать обработке в ИСПДн: граждане Российской Федерации и других государств.

Структура ИСПДн: распределенная или локальная, функционирующая в контролируемой зоне Лицея.

ИСПДн подключены к сетям связи общего пользования (сетям международного информационного обмена). По типу подключения ИСПДн делятся на:

подключенные посредством ГИСТ РТ;

подключенные с использованием иных каналов связи.

Обмен (передача и получение) персональными данными с федеральным уровнем (федеральным сегментом), между региональными сегментами ИСПДн (при наличии) и с иными ИСПДн 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 ГИСТ РТ;

с использованием иных средств защиты информации, передаваемой по открытым каналам связи.

Средства вычислительной техники, участвующие в обработке: АРМ, терминальная станция, серверное оборудование, сетевое и телекоммуникационное оборудование.

По технологии обработки ИСПДн подразделяются на:

построенные по технологии «толстого клиента»: на рабочие места пользователей ИСПДн устанавливается специальное клиентское приложение, осуществляющее подключение к серверному сегменту, располагающемуся в пределах контролируемой зоны Лицея и передающее данные на центральный сегмент или напрямую в центральный;

построенные по технологии «толстого клиента»: на рабочие места пользователей ИСПДн 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 ИСПДн передается только графическая информация, сама обработка данных осуществляется на удаленном серверном сегменте, располагающемся в пределах контролируемой зоны Лицея, и передающем данные на центральный сегмент, или на центральном сегменте.

ИСПДн, 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) электронного сертификата, 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) электронного сертификата, и (или) сертификата электронной подписи в соответствии с Федеральным законом от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи».

4.5.3. Республиканские ИСПДн создаются и эксплуатируются по желанию (на основании решения) Республики Татарстан или Лицея в интересах нескольких учреждений, при этом цели и задачи создания (модернизации), эксплуатации данных ИСПДн, а также требования к ним определяются Республикой Татарстан или Лицеем соответственно.

По выполняемым функциям республиканские ИСПДн подразделяются на:

интеграционные;

многопрофильные;

ИСПДн для организаций Республики Татарстан.

4.5.3.1. ИСПДн интеграционные характеризуются отсутствием пользователей (кроме администраторов ИСПДн и администраторов безопасности ИСПДн) и функционируют исключительно в целях интеграции и передачи данных между ИСПДн иных категорий.

Категории персональных данных, которые могут подлежать обработке в ИСПДн:

общедоступные;

специальные;

иные.

Режим обработки персональных данных в ИСПДн: многопользовательский. ИСПДн предусматривает разграничение доступа. Обработка персональных данных осуществляется сотрудниками Лицея в специализированных программах и (или) посредством веб-интерфейса в соответствии с предоставленными правами.

Типы субъектов персональных данных, которые могут подлежать обработке в ИСПДн: граждане Российской Федерации и других государств.

Структура ИСПДн: локальная или распределенная, функционирующая в контролируемой зоне Органа.

ИСПДн подключены к сетям связи общего пользования (сетям международного информационного обмена). По типу подключения ИСПДн делятся на:

подключенные посредством ГИСТ РТ;

подключенные с использованием иных каналов связи.

Обмен (передача и получение) персональными данными с федеральным уровнем и иными ИСПДн 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 ГИСТ РТ;

с использованием иных средств защиты информации, передаваемой по открытым каналам связи.

Средства вычислительной техники, участвующие в обработке: АРМ, серверное оборудование, сетевое и телекоммуникационное оборудование.

4.5.3.2. ИСПДн многопрофильные предназначены для централизованной автоматизации делопроизводства и документооборота, учета корреспонденции, обращений граждан, обеспечения доступа к электронным документам в Органах.

Категории персональных данных, которые могут подлежать обработке в ИСПДн:

общедоступные;

специальные;

иные.

Режим обработки персональных данных в ИСПДн: многопользовательский. ИСПДн предусматривает разграничение доступа. Обработка персональных данных осуществляется сотрудниками Лицея в специализированных программах в соответствии с предоставленными правами.

Типы субъектов персональных данных, которые могут подлежать обработке в ИСПДн: граждане Российской Федерации и других государств.

Структура ИСПДн: локальная или распределенная, функционирующая в контролируемой зоне Лицея.

ИСПДн подключена к сетям связи общего пользования (сетям международного информационного обмена). По типу подключения ИСПДн делятся на:

подключенные посредством ГИСТ РТ;

подключенные с использованием иных каналов связи.

Обмен (передача и получение) персональными данными с иными ИСПДн осуществляется в зависимости от технологии подключения к сетям связи общего пользования (сетям международного информационного обмена):

посредством ГИСТ РТ;

с использованием сторонних средств криптографической защиты информации.

Средства вычислительной техники, участвующие в обработке: АРМ, серверное оборудование, сетевое и телекоммуникационное оборудование.

4.5.3.3. ИСПДн для учреждений и организаций Республики Татарстан предназначены для автоматизации совместной деятельности учреждений и организаций Республики Татарстан, в том числе деятельности, которая необходима к исполнению в соответствии с требованиями законодательства.

Категории персональных данных, которые могут подлежать обработке в ИСПДн:

общедоступные;

иные.

Режим обработки персональных данных в ИСПДн: многопользовательский. ИСПДн предусматривает разграничение доступа. Обработка персональных данных осуществляется в соответствии с предоставленными правами сотрудниками Органов и организаций Республики Татарстан в специализированных программах в режиме веб-интерфейса.

Типы субъектов персональных данных, которые могут подлежать обработке в ИСПДн: сотрудники организаций Республики Татарстан.

Структура ИСПДн: локальная, функционирующая в контролируемой зоне Лицея.

ИСПДн подключены к сетям связи общего пользования (сетям международного информационного обмена). По типу подключения ИСПДн делятся на:

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

подключенные посредством ГИСТ РТ;

подключенные с использованием иных каналов связи.

Обмен (передача и получение) персональными данными с иными ИСПДн 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 ГИСТ РТ;

с использованием сторонних средств криптографической защиты информации.

Средства вычислительной техники, участвующие в обработке: АРМ, серверное оборудование, сетевое и телекоммуникационное оборудование.

По архитектуре республиканские ИСПДн подразделяются на:

сегментированные;

централизованные;

смешанные.

Сегментированные ИСПДн 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 АРМ, а также АРМ, выполняющее функции сервера, или серверное оборудование. Пользователи периферийных сегментов подключаются к расположенному в пределах контролируемой зоны АРМ, 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 ИСПДн подразделяются на:

построенные по технологии «толстого клиента»: на рабочие места пользователей ИСПДн устанавливается специальное клиентское приложение, осуществляющее подключение к АРМ, выполняющему функции сервера, или серверному сегменту, располагающемуся в пределах контролируемой зоны Лицея и передающему данные на центральный сегмент;

построенные по технологии «тонкого клиента»: на рабочие места пользователей ИСПДн передается только графическая информация, сама обработка данных осуществляется на серверном сегменте, располагающемся в пределах контролируемой зоны Лицея и передающем данные на центральный сегмент.

ИСПДн, 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 ИСПДн делятся на сегменты (центральный и периферийный).

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

В состав периферийных сегментов входят только АРМ, являющиеся непосредственно точками, которые отвечают 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 ИСПДн подразделяются на:

построенные по технологии «толстого клиента»: на рабочие места пользователей ИСПДн устанавливается специальное клиентское приложение, осуществляющее подключение к центральному сегменту;

построенные по технологии «толстого клиента»: на рабочие места пользователей ИСПДн 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 ИСПДн передается только графическая информация, сама обработка данных осуществляется на центральном сегменте.

ИСПДн, 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 ИСПДн построены с одновременным применением сегментированных и централизованных архитектур. Указанные ИСПДн могут объединять в себе технологии обработки, характерные как для сегментированных ИСПДн, так и для централизованных ИСПДн.

4.5.4. Ведомственные ИСПДн создаются (эксплуатируются) по решению Органа в своих интересах, цели и задачи создания (модернизации), эксплуатации которых определяются Лицеем. Ведомственные ИСПДн предназначены для исполнения функций учреждений.

Категории персональных данных, которые могут подлежать обработке в ИСПДн:

специальные;

иные.

Режим обработки персональных данных в ИСПДн: многопользовательский. ИСПДн предусматривает разграничение доступа. Обработка персональных данных осуществляется сотрудниками учреждений в специализированных программах и (или) посредством веб-интерфейса в соответствии с предоставленными правами.

Типы субъектов персональных данных, которые могут подлежать обработке в ИСПДн: сотрудники оператора ИСПДн и иных учреждений, а также сторонние граждане.

Структура ИСПДн: распределенная или локальная, функционирующая в контролируемой зоне Лицея.

ИСПДн подключены к сетям связи общего пользования (сетям международного информационного обмена). По типу подключения ИСПДн делятся на:

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

подключенные посредством ГИСТ РТ;

подключенные с использованием иных каналов связи.

Обмен (передача и получение) персональными данными между сегментами ИСПДн (при наличии) и с иными ИСПДн 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 ГИСТ РТ;

с использованием сторонних средств криптографической защиты информации.

Также обмен персональными данными между сегментами ИСПДн (при наличии) и с иными ИСПДн осуществляется посредством собственных корпоративных сетей Лицея.

Средства вычислительной техники, участвующие в обработке: АРМ, терминальная станция, серверное оборудование, сетевое и телекоммуникационное оборудование.

По архитектуре ведомственные ИСПДн подразделяются на:

сегментированные;

централизованные;

смешанные.

Сегментированные ИСПДн 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 АРМ, а также АРМ, выполняющее функции сервера, или серверное оборудование. Пользователи периферийных сегментов подключаются к расположенному в пределах контролируемой зоны АРМ, 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 ИСПДн подразделяются на:

построенные по технологии «толстого клиента»: на рабочие места пользователей ИСПДн устанавливается специальное клиентское приложение, осуществляющее подключение к АРМ, выполняющему функции сервера, или серверному сегменту, располагающемуся в пределах контролируемой зоны Лицея и передающему данные на центральный сегмент;

построенные по технологии «тонкого клиента»: на рабочие места пользователей ИСПДн передается только графическая информация, сама обработка данных осуществляется на серверном сегменте, располагающемся в пределах контролируемой зоны Органа и передающем данные на центральный сегмент.

ИСПДн, 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 ИСПДн делятся на сегменты (центральный и периферийный).

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

В состав периферийных сегментов входят только АРМ, являющиеся непосредственно точками, которые отвечают 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 ИСПДн подразделяются на:

построенные по технологии «толстого клиента»: на рабочие места пользователей ИСПДн устанавливается специальное клиентское приложение, осуществляющее подключение к центральному сегменту;

построенные по технологии «толстого клиента»: на рабочие места пользователей ИСПДн 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 ИСПДн передается только графическая информация, сама обработка данных осуществляется на центральном сегменте.

ИСПДн, 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 ИСПДн построены с одновременным применением сегментированных и централизованных архитектур. Указанные ИСПДн могут объединять в себе технологии обработки, характерные как для сегментированных ИСПДн, так и для централизованных ИСПДн.

4.5.5. Служебные ИСПДн создаются (эксплуатируются) на основании решения Органа и его должностных лиц в интересах Лицея, цели и задачи создания (модернизации), эксплуатации которых определяются Органом и используются для автоматизации определенной области деятельности или типовой деятельности, неспецифичной относительно полномочий конкретного Лицея. Служебные ИСПДн предназначены для управления процессами в Лицее.

К основным служебным ИСПДн относятся:

ИСПДн бухгалтерского учета и управления финансами;

ИСПДн кадрового учета и управления персоналом;

ИСПДн документооборота и делопроизводства;

ИСПДн поддерживающие.

4.5.5.1. ИСПДн бухгалтерского учета и управления финансами предназначены для автоматизации деятельности Лицея, связанной с ведением бухгалтерского учета и управлением финансами.

Обработке в ИСПДн подлежат иные категории персональных данных.

Режим обработки персональных данных в ИСПДн: многопользовательский. ИСПДн предусматривает разграничение доступа. Обработка персональных данных осуществляется сотрудниками учреждений в специализированных программах и (или) посредством веб-интерфейса в соответствии с предоставленными правами.

Типы субъектов персональных данных, которые могут подлежать обработке в ИСПДн: сотрудники Органа, являющегося оператором ИСПДн.

Структура ИСПДн: локальная, функционирующая в контролируемой зоне Лицея.

ИСПДн подключены к сетям связи общего пользования (сетям международного информационного обмена). По типу подключения ИСПДн делятся на:

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

подключенные посредством ГИСТ РТ;

подключенные с использованием иных каналов связи.

Передача персональных данных в иные ИСПДн 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 сторонних средств криптографической защиты информации.

Средства вычислительной техники, участвующие в обработке: АРМ, серверное оборудование, сетевое и телекоммуникационное оборудование.

По технологии обработки ИСПДн подразделяются на:

построенные по технологии «толстого клиента»: на рабочие места пользователей ИСПДн устанавливается специальное клиентское приложение, осуществляющее подключение к базе данных, которая хранится на серверном сегменте (сервере или АРМ, выполняющем функцию сервера), располагающемся в пределах контролируемой зоны Лицея;

построенные по технологии «тонкого клиента»: на рабочие места пользователей ИСПДн передается только графическая информация, сама обработка данных осуществляется на удаленном серверном сегменте (сервере или АРМ, выполняющем функцию сервера), располагающемся в пределах контролируемой зоны Лицея.

Доступ к персональным данным в ИСПДн предоставляется пользователю после ввода логина и пароля (предъявления идентификатора).

4.5.5.2. ИСПДн кадрового учета и управления персоналом предназначены для автоматизации деятельности Лицея, связанной с ведением кадрового учета и управления персоналом.

Категории персональных данных, которые могут подлежать обработке в ИСПДн:

специальные;

иные.

Режим обработки персональных данных в ИСПДн: многопользовательский. ИСПДн предусматривает разграничение доступа. Обработка персональных данных осуществляется сотрудниками учреждений в специализированных и (или) стандартных офисных программах, и (или) посредством веб-интерфейса в соответствии с предоставленными правами.

Типы субъектов персональных данных, которые могут подлежать обработке в ИСПДн: сотрудники Лицея, являющегося оператором ИСПДн, граждане Российской Федерации, устанавливающие (имеющие) трудовые отношения (трудовые договоры, служебные контракты) с Лицеем.

Структура ИСПДн: локальная, функционирующая в контролируемой зоне Лицея.

ИСПДн подключены к сетям связи общего пользования (сетям международного информационного обмена). По типу подключения ИСПДн делятся на:

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

подключенные посредством ГИСТ РТ;

подключенные с использованием иных каналов связи.

Передача персональных данных в иные ИСПДн 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 сторонних средств криптографической защиты информации.

Средства вычислительной техники, участвующие в обработке: АРМ, серверное оборудование, сетевое и телекоммуникационное оборудование.

Технология обработки персональных данных в ИСПДн построена по принципу «толстого клиента»: на рабочие места пользователей ИСПДн устанавливается специальное клиентское приложение, осуществляющее подключение к базе данных, которая хранится на серверном сегменте (сервере или АРМ, выполняющем функцию сервера), располагающемся в пределах контролируемой зоны Лицея. Доступ к персональным данным в ИСПДн предоставляется пользователю после ввода логина и пароля (предъявления идентификатора).

4.5.5.3. ИСПДн документооборота и делопроизводства предназначены для автоматизации деятельности Лицея, связанной с осуществлением документооборота и делопроизводства.

Категории персональных данных, которые могут подлежать обработке в ИСПДн:

общедоступные;

специальные;

иные.

Режим обработки персональных данных в ИСПДн: многопользовательский. ИСПДн предусматривает разграничение доступа. Обработка персональных данных осуществляется сотрудниками учреждений в специализированных программах в соответствии с предоставленными правами.

Типы субъектов персональных данных, которые могут подлежать обработке в ИСПДн: сотрудники Лицея, являющегося оператором ИСПДн, граждане Российской Федерации и других государств.

Структура ИСПДн: локальная, функционирующая в контролируемой зоне Лицея.

ИСПДн подключены к сетям связи общего пользования (сетям международного информационного обмена). По типу подключения ИСПДн делятся на:

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

подключенные с использованием иных каналов связи.

Передача персональных данных в иные ИСПДн 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 ГИСТ РТ;

с использованием сторонних средств криптографической защиты информации.

Средства вычислительной техники, участвующие в обработке: АРМ, серверное оборудование, сетевое и телекоммуникационное оборудование.

Технология обработки персональных данных в ИСПДн построена по принципу «толстого клиента»: на рабочие места пользователей ИСПДн устанавливается специальное клиентское приложение, осуществляющее подключение к базе данных, которая хранится на серверном сегменте (сервере или АРМ, выполняющем функцию сервера), располагающемся в пределах контролируемой зоны Органа. Доступ к персональным данным в ИСПДн предоставляется пользователю после ввода логина и пароля (предъявления идентификатора).

4.5.5.4. ИСПДн поддерживающие. Предназначены для автоматизации деятельности Лицея, связанной с осуществлением им (его сотрудниками) своих функций, полномочий и задач.

Категории персональных данных, которые могут подлежать обработке в ИСПДн:

общедоступные;

специальные;

иные.

Режим обработки персональных данных в ИСПДн: многопользовательский. ИСПДн предусматривает разграничение доступа. Обработка персональных данных осуществляется сотрудниками учреждений в специализированных и (или) стандартных офисных программах, и (или) посредством веб-интерфейса в соответствии с предоставленными правами.

Типы субъектов персональных данных, которые могут подлежать обработке в ИСПДн: сотрудники Лицея, являющегося оператором ИСПДн, граждане Российской Федерации и других государств.

Структура ИСПДн: локальная, функционирующая в контролируемой зоне Лицея.

ИСПДн подключены к сетям связи общего пользования (сетям международного информационного обмена). По типу подключения ИСПДн делятся на:

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

подключенные посредством ГИСТ РТ;

подключенные с использованием иных каналов связи.

Передача персональных данных в иные ИСПДн не осуществляется.

Средства вычислительной техники, участвующие в обработке: АРМ, серверное оборудование, сетевое и телекоммуникационное оборудование.

По технологии обработки ИСПДн подразделяются на:

построенные по принципу «толстого клиента»: на рабочие места пользователей ИСПДн устанавливается специальное клиентское приложение, осуществляющее подключение к серверному сегменту (серверу или АРМ, выполняющему функцию сервера), располагающемуся в пределах контролируемой зоны Лицея;

построенные на базе стандартного офисного ПО: ИСПДн представляет собой базу данных в формате стандартного офисного приложения, обрабатываемую и хранящуюся на АРМ;

построенные по веб-технологии: пользователи работают в ИСПДн посредством веб-интерфейса, подключающегося к локальному веб-серверу, располагающемуся в пределах контролируемой зоны Лицея.

Доступ к персональным данным в ИСПДн предоставляется пользователю после ввода логина и пароля (предъявления идентификатора).

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

5.1. Источниками угрозы безопасности персональных данных выступают:
носитель вредоносной программы;
аппаратная закладка;
нарушитель.

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

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

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

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

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

пакеты передаваемых по компьютерной сети сообщений;

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

5.1.2. Аппаратная закладка. Потенциально может рассматриваться возможность применения аппаратных средств, предназначенных для регистрации вводимой в ИСПДн с клавиатуры АРМ 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 др.

Ввиду отсутствия возможности неконтролируемого пребывания физических лиц в служебных помещениях, в которых размещены технические средства ИСПДн, или в непосредственной близости от них, соответственно исключается вероятность установки аппаратных закладок посторонними лицами.

5.1.3. Нарушитель. Под нарушителем безопасности информации понимается физическое лицо, случайно или преднамеренно совершающее действия, следствием

которых является нарушение безопасности персональных данных при их обработке в ИСПДн.

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

внешний нарушитель. Указанный тип нарушителя не имеет права постоянного или имеет право разового (контролируемого) доступа в контролируемую зону, также не имеет доступа к техническим средствам и ресурсам ИСПДн, расположенным в пределах контролируемой зоны, или он ограничен и контролируется. Указанный тип нарушителя может реализовывать угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена;

внутренний нарушитель, имеющий доступ к ИСПДн. Указанный тип нарушителя имеет право постоянного (периодического) доступа на территорию контролируемой зоны, а также доступ к техническим средствам и ресурсам ИСПДн, расположенным в пределах контролируемой зоны. Указанный тип нарушителя может проводить атаки с использованием внутренней (локальной) сети передачи данных и непосредственно в ИСПДн;

внутренний нарушитель, не имеющий доступа к ИСПДн. Указанный тип нарушителя имеет право постоянного (периодического) доступа на территорию контролируемой зоны, но не имеет доступ к техническим средствам и ресурсам ИСПДн, расположенным в пределах контролируемой зоны. Указанный тип нарушителя может проводить атаки с использованием внутренней (локальной) сети передачи данных.

5.2. Основными угрозами безопасности персональных данных в ИСПДн являются:

угрозы утечки информации по техническим каналам;

угрозы использования штатных средств ИСПДн с целью совершения несанкционированного доступа к информации;

угрозы нарушения доступности информации;

угрозы нарушения целостности информации;

угрозы недекларированных возможностей в системном ПО и прикладном ПО;

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 ИСПДн/системы информационной безопасности ИСПДн;

угрозы ошибочных/деструктивных действий лиц;

угрозы нарушения конфиденциальности;

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 ПО и оборудования;

угрозы физического доступа к компонентам ИСПДн;

угрозы эксплуатации уязвимостей в системном ПО, прикладном ПО, средствах защиты информации, средствах криптографической защиты информации, аппаратных компонентах ИСПДн, 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 ИСПДн;

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

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

6.1. В настоящем разделе приведены группы актуальных угроз безопасности персональных данных в ИСПДн из групп, указанных в пункте 5.2 настоящего Положения, исходя из содержания персональных данных, характера и способов их обработки.

6.2. Информационно-справочные ИСПДн:

6.2.1. Официальные порталы (сайты) Органов:

угрозы утечки информации по техническим каналам;

угрозы использования штатных средств ИСПДн с целью совершения несанкционированного доступа к информации;

угрозы нарушения доступности информации;

угрозы нарушения целостности информации;

угрозы недекларированных возможностей в системном ПО и прикладном ПО;

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 ИСПДн/системы информационной безопасности ИСПДн;

угрозы ошибочных/деструктивных действий лиц;

угрозы нарушения конфиденциальности;

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 ПО и оборудования;

угрозы физического доступа к компонентам ИСПДн;

угрозы эксплуатации уязвимостей в системном ПО, прикладном ПО, средствах защиты информации, средствах криптографической защиты информации, аппаратных компонентах ИСПДн, 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 ИСПДн;

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

6.2.2. Информационные порталы (сайты):

угрозы утечки информации по техническим каналам;

угрозы использования штатных средств ИСПДн с целью совершения несанкционированного доступа к информации;

угрозы нарушения доступности информации;

угрозы нарушения целостности информации;

угрозы недекларированных возможностей в системном ПО и прикладном ПО;

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 ИСПДн/системы информационной безопасности ИСПДн;

угрозы ошибочных/деструктивных действий лиц;

угрозы нарушения конфиденциальности;

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 ПО и оборудования;

угрозы физического доступа к компонентам ИСПДн;

угрозы эксплуатации уязвимостей в системном ПО, прикладном ПО, средствах защиты информации, средствах криптографической защиты информации, аппаратных компонентах ИСПДн, 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 ИСПДн;

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

6.2.3. Закрытые порталы для нескольких групп участников Органов:

угрозы утечки информации по техническим каналам;

угрозы использования штатных средств ИСПДн с целью совершения несанкционированного доступа к информации;

угрозы нарушения доступности информации;

угрозы нарушения целостности информации;

угрозы недекларированных возможностей в системном ПО и прикладном ПО;

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 ИСПДн/системы информационной безопасности ИСПДн;

угрозы ошибочных/деструктивных действий лиц;

угрозы нарушения конфиденциальности;

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 ПО и оборудования;

угрозы физического доступа к компонентам ИСПДн;

угрозы эксплуатации уязвимостей в системном ПО, прикладном ПО, средствах защиты информации, средствах криптографической защиты информации, аппаратных компонентах ИСПДн, 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 ИСПДн;

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

6.2.4. Портал государственных и муниципальных услуг Республики Татарстан:

угрозы утечки информации по техническим каналам;

угрозы использования штатных средств ИСПДн с целью совершения несанкционированного доступа к информации;

угрозы нарушения доступности информации;

угрозы нарушения целостности информации;

угрозы недекларированных возможностей в системном ПО и прикладном ПО;

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 ИСПДн/системы информационной безопасности ИСПДн;

угрозы ошибочных/деструктивных действий лиц;

угрозы нарушения конфиденциальности;

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 ПО и оборудования;

угрозы физического доступа к компонентам ИСПДн;

угрозы эксплуатации уязвимостей в системном ПО, прикладном ПО, средствах защиты информации, средствах криптографической защиты информации, аппаратных компонентах ИСПДн, 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 ИСПДн;

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

6.3. Сегментные ИСПДн:

угрозы утечки информации по техническим каналам;

угрозы использования штатных средств ИСПДн с целью совершения несанкционированного доступа к информации;

угрозы нарушения доступности информации;

угрозы нарушения целостности информации;

угрозы недекларированных возможностей в системном ПО и прикладном ПО;

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 ИСПДн/системы информационной безопасности ИСПДн;

угрозы ошибочных/деструктивных действий лиц;

угрозы нарушения конфиденциальности;

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 ПО и оборудования;

угрозы физического доступа к компонентам ИСПДн;

угрозы эксплуатации уязвимостей в системном ПО, прикладном ПО, средствах защиты информации, средствах криптографической защиты информации, аппаратных компонентах ИСПДн, 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 ИСПДн;

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

6.4. Республиканские ИСПДн:

6.4.1. ИСПДн интеграционные:

угрозы утечки информации по техническим каналам;

угрозы использования штатных средств ИСПДн с целью совершения несанкционированного доступа к информации;

угрозы нарушения доступности информации;

угрозы нарушения целостности информации;

угрозы недекларированных возможностей в системном ПО и прикладном ПО;

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 ИСПДн/системы информационной безопасности ИСПДн;

угрозы ошибочных/деструктивных действий лиц;

угрозы нарушения конфиденциальности;

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 ПО и оборудования;

угрозы физического доступа к компонентам ИСПДн;

угрозы эксплуатации уязвимостей в системном ПО, прикладном ПО, средствах защиты информации, средствах криптографической защиты информации, аппаратных компонентах ИСПДн, 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 ИСПДн;

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

6.4.2. ИСПДн многопрофильные:

угрозы утечки информации по техническим каналам;

угрозы использования штатных средств ИСПДн с целью совершения несанкционированного доступа к информации;

угрозы нарушения доступности информации;

угрозы нарушения целостности информации;

угрозы недекларированных возможностей в системном ПО и прикладном ПО;

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 ИСПДн/системы информационной безопасности ИСПДн;

угрозы ошибочных/деструктивных действий лиц;

угрозы нарушения конфиденциальности;

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 ПО и оборудования;

угрозы физического доступа к компонентам ИСПДн;

угрозы эксплуатации уязвимостей в системном ПО, прикладном ПО, средствах защиты информации, средствах криптографической защиты информации, аппаратных компонентах ИСПДн, 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 ИСПДн;

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

6.4.3. ИСПДн для учреждений и организаций Республики Татарстан:

угрозы утечки информации по техническим каналам;

угрозы использования штатных средств ИСПДн с целью совершения несанкционированного доступа к информации;

угрозы нарушения доступности информации;

угрозы нарушения целостности информации;

угрозы недекларированных возможностей в системном ПО и прикладном ПО;

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 ИСПДн/системы информационной безопасности ИСПДн;

угрозы ошибочных/деструктивных действий лиц;

угрозы нарушения конфиденциальности;

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 ПО и оборудования;

угрозы физического доступа к компонентам ИСПДн;

угрозы эксплуатации уязвимостей в системном ПО, прикладном ПО, средствах защиты информации, средствах криптографической защиты информации, аппаратных компонентах ИСПДн, 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 ИСПДн;

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

6.5. Ведомственные ИСПДн:

угрозы утечки информации по техническим каналам;

угрозы использования штатных средств ИСПДн с целью совершения несанкционированного доступа к информации;

угрозы нарушения доступности информации;

угрозы нарушения целостности информации;

угрозы недекларированных возможностей в системном ПО и прикладном ПО;

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 ИСПДн/системы информационной безопасности ИСПДн;

угрозы ошибочных/деструктивных действий лиц;

угрозы нарушения конфиденциальности;

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 ПО и оборудования;

угрозы физического доступа к компонентам ИСПДн;

угрозы эксплуатации уязвимостей в системном ПО, прикладном ПО, средствах защиты информации, средствах криптографической защиты информации, аппаратных компонентах ИСПДн, 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 ИСПДн;

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

6.6. Служебные ИСПДн:

6.6.1. ИСПДн бухгалтерского учета и управления финансами:

грозы утечки информации по техническим каналам;

грозы использования штатных средств ИСПДн с целью совершения несанкционированного доступа к информации;

угрозы нарушения доступности информации;

угрозы нарушения целостности информации;

угрозы недекларированных возможностей в системном ПО и прикладном ПО;

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 ИСПДн/системы информационной безопасности ИСПДн;

угрозы ошибочных/деструктивных действий лиц;

угрозы нарушения конфиденциальности;

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 ПО и оборудования;

угрозы физического доступа к компонентам ИСПДн;

угрозы эксплуатации уязвимостей в системном ПО, прикладном ПО, средствах защиты информации, средствах криптографической защиты информации, аппаратных компонентах ИСПДн, 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 ИСПДн;

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

6.6.2. ИСПДн кадрового учета и управления персоналом:

угрозы утечки информации по техническим каналам;

угрозы использования штатных средств ИСПДн с целью совершения несанкционированного доступа к информации;

угрозы нарушения доступности информации;

угрозы нарушения целостности информации;

угрозы недекларированных возможностей в системном ПО и прикладном ПО;

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 ИСПДн/системы информационной безопасности ИСПДн;

угрозы ошибочных/деструктивных действий лиц;

угрозы нарушения конфиденциальности;

угрозы программно-математических воздействий;

угрозы, связанные с нарушением правил эксплуатации машинных носителей;

угрозы, связанные с нарушением процедур установки/обновления ПО и оборудования;

угрозы физического доступа к компонентам ИСПДн;

угрозы эксплуатации уязвимостей в системном ПО, прикладном ПО, средствах защиты информации, средствах криптографической защиты информации, аппаратных компонентах ИСПДн, 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 ИСПДн;

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

6.6.3. ИСПДн документооборота и делопроизводства:

угрозы утечки информации по техническим каналам;

угрозы использования штатных средств ИСПДн с целью совершения несанкционированного доступа к информации;

угрозы нарушения доступности информации;

угрозы нарушения целостности информации;

угрозы недекларированных возможностей в системном ПО и прикладном ПО;

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 ИСПДн/системы информационной безопасности ИСПДн;

угрозы ошибочных/деструктивных действий лиц;

угрозы нарушения конфиденциальности;

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 ПО и оборудования;

угрозы физического доступа к компонентам ИСПДн;

угрозы эксплуатации уязвимостей в системном ПО, прикладном ПО, средствах защиты информации, средствах криптографической защиты информации, аппаратных компонентах ИСПДн, 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 ИСПДн;

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

6.6.4. ИСПДн поддерживающие:

угрозы утечки информации по техническим каналам;

угрозы использования штатных средств ИСПДн с целью совершения несанкционированного доступа к информации;

угрозы нарушения доступности информации;

угрозы нарушения целостности информации;

угрозы недекларированных возможностей в системном ПО и прикладном ПО;

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 ИСПДн/системы информационной безопасности ИСПДн;

угрозы ошибочных/деструктивных действий лиц;

угрозы нарушения конфиденциальности;

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 ПО и оборудования;

угрозы физического доступа к компонентам ИСПДн;

угрозы эксплуатации уязвимостей в системном ПО, прикладном ПО, средствах защиты информации, средствах криптографической защиты информации, аппаратных компонентах ИСПДн, 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 ИСПДн;

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

Приложение № 1
к Положению об определении
актуальных угроз безопасности
персональных данных при их
обработке в информационных
системах персональных данных
МБОУ «Лицей №1 ЗМР РТ»

Расширенный перечень
угроз безопасности персональных данных в информационных системах персональных данных

№ п/п	Наименование угрозы безопасности персональных данных в ИСПДн*	Источники угрозы безопасности персональных данных	Объект воздействия
1	2	3	4
1.	Угрозы утечки информации по техническим каналам		
1.1.	Угрозы утечки акустической информации		
1.1.1.	Использование направленных (ненаправленных) микрофонов воздушной проводимости для съема акустического излучения информативного речевого сигнала		
1.1.2.	Использование «контактных микрофонов» для съема виброакустических сигналов		
1.1.3.	Использование «лазерных микрофонов» для съема виброакустических сигналов		
1.1.4.	Использование средств ВЧ-навязывания для съема электрических сигналов, возникающих за счет «микрофонного эффекта» в технических средствах обработки информации и		

1	2	3	4
	вспомогательных технических средствах и системах (распространяются по проводам и линиям, выходящим за пределы служебных помещений)		
1.1.5.	Применение средств ВЧ-облучения для съема радиоизлучения, модулированного информативным сигналом, возникающего при непосредственном облучении технических средств обработки информации и вспомогательных технических средств и систем ВЧ-сигналом		
1.1.6.	Применение акустооптических модуляторов на базе волоконно-оптической связи, находящихся в поле акустического сигнала («оптических микрофонов»)		
1.2.	Угрозы утечки видовой информации		
1.2.1.	Визуальный просмотр на экранах дисплеев и других средств отображения средств вычислительной техники, измерительно-вычислительного комплекса, входящих в состав информационных систем		
1.2.2.	Визуальный просмотр с помощью оптических (оптико-электронных) средств на экранах дисплеев и других средств отображения средств вычислительной техники, измерительно-вычислительного комплекса, входящих в состав информационной системы		
1.2.3.	Использование специальных электронных устройств съема видовой информации (видеозакладки)		
1.3.	Угрозы утечки информации по каналам побочных электромагнитных излучений и наводок		
1.3.1.	Применение специальных средств регистрации побочных электромагнитных излучений и наводок от ТС и линий передачи информации (программно-аппаратный комплекс, сканерные приемники, цифровые анализаторы спектра, селективные микровольтметры)		

1	2	3	4
1.3.2.	Применение токосъемников для регистрации наводок информативных сигналов, обрабатываемых ТС, на цепи электропитания и линии связи, выходящих за пределы служебных помещений		
1.3.3.	Применение специальных средств регистрации радиоизлучений, модулированных информативным сигналом, возникающих при работе различных генераторов, входящих в состав ТС информационной системы, или при наличии паразитной генерации в узлах ТС		
1.3.4.	Применение специальных средств регистрации радиоизлучений, формируемых в результате ВЧ-облучения ТС информационной системы, в которых проводится обработка информативных сигналов – параметрических каналов утечки		
2.	Угрозы использования штатных средств ИСПДн с целью совершения несанкционированного доступа к информации		
2.1.	Угроза некорректного использования функционала ПО	Внешний нарушитель со средним потенциалом, внутренний нарушитель со средним потенциалом	Системное ПО, прикладное ПО, сетевое ПО, микропрограммное обеспечение, аппаратное обеспечение
2.2.	Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением	Внешний нарушитель со средним потенциалом, внутренний нарушитель со средним потенциалом	Системное ПО, прикладное ПО, сетевое ПО, микропрограммное обеспечение, реестр
2.3.	Угроза несанкционированного изменения аутентификационной информации	Внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	Системное ПО, объекты файловой системы, учетные данные пользователя, реестр
2.4.	Угроза несанкционированного использования привилегированных функций BIOS	Внешний нарушитель с высоким потенциалом, внутренний нарушитель с низким потенциалом	Аппаратное обеспечение, микропрограммное обеспечение BIOS/UEFI

1	2	3	4
2.5.	Доступ в операционную среду (локальную операционную систему отдельного ТС информационной системы) с возможностью выполнения несанкционированного доступа, вызовом штатных процедур или запуска специально разработанных программ		
3.	Угрозы нарушения доступности информации		
3.1.	Угроза длительного удержания вычислительных ресурсов пользователями	Внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	Информационная система, сетевой узел, носитель информации, системное ПО, сетевое ПО, сетевой трафик
3.2.	Угроза нарушения работоспособности грид-системы при нетипичной сетевой нагрузке	Внешний нарушитель со средним потенциалом, внутренний нарушитель со средним потенциалом	Грид-система, сетевой трафик
3.3.	Угроза несанкционированного доступа к гипервизору из виртуальной машины и (или) физической сети	Внешний нарушитель со средним потенциалом, внутренний нарушитель со средним потенциалом	Гипервизор
3.4.	Угроза отказа в загрузке входных данных неизвестного формата хранилищем больших данных	Внутренний нарушитель с низким потенциалом	Хранилище больших данных, метаданные
3.5.	Угроза отказа в обслуживании системой хранения данных суперкомпьютера	Внутренний нарушитель с низким потенциалом	Система хранения данных суперкомпьютера
3.6.	Угроза перегрузки грид-системы вычислительными заданиями	Внутренний нарушитель с низким потенциалом	Ресурсные центры грид-системы
3.7.	Угроза повреждения системного реестра	Внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	Объекты файловой системы, реестр
3.8.	Угроза приведения системы в состояние «отказ в обслуживании»	Внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	Информационная система, сетевой узел, системное ПО, сетевое ПО, сетевой трафик

Приложение № 2
к Положению об определении
актуальных угроз безопасности
персональных данных при их
обработке в информационных
системах персональных данных
МБОУ «Лицей №1 ЗМР РТ»

Типовые возможности
нарушителей безопасности информации и направления атак

№ п/п	Возможности нарушителей безопасности информации и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия (при наличии)
1	2	3	4
1.	Проведение атаки при нахождении в пределах контролируемой зоны		
2.	Проведение атак на этапе эксплуатации средств криптографической защиты информации на следующие объекты: документация на средства криптографической защиты информации и компоненты среды функционирования средств криптографической защиты информации; помещения, в которых находится совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем (средств вычислительной техники), на которых реализованы средства криптографической защиты информации и среды функционирования средств криптографической защиты информации		

1	2	3	4
3.	Получение в рамках предоставленных полномочий, а также в результате наблюдений следующей информации: сведения о физических мерах защиты объектов, в которых размещены ресурсы информационной системы; сведения о мерах по обеспечению контролируемой зоны объектов, в которых размещены ресурсы информационной системы; сведения о мерах по разграничению доступа в помещения, в которых находятся средства вычислительной техники, на которых реализованы средства криптографической защиты информации и среды функционирования средств криптографической защиты информации		
4.	Использование штатных средств ИСПДн, ограниченное мерами, реализованными в информационной системе, в которой используется средство криптографической защиты информации, и направленными на предотвращение и пресечение несанкционированных действий		
5.	Физический доступ к средствам вычислительной техники, на которых реализованы средства криптографической защиты информации и среды функционирования средств криптографической защиты информации		
6.	Возможность воздействовать на аппаратные компоненты средств криптографической защиты информации и среды функционирования средств криптографической защиты информации, ограниченная мерами, реализованными в информационной системе, в которой используется средство криптографической защиты информации, и направленными на предотвращение и пресечение несанкционированных действий		
7.	Создание способов, подготовка и проведение атак с привлечением специалистов в области анализа сигналов, сопровождающих функционирование средств криптографической защиты информации и сред функционирования средств криптографической защиты информации, и в области использования для реализации атак недокументированных (недекларированных) возможностей прикладного программного обеспечения		

1	2	3	4
8.	Проведение лабораторных исследований средств криптографической защиты информации, используемых вне контролируемой зоны, ограниченное мерами, реализованными в информационной системе, в которой используется средство криптографической защиты информации, и направленными на предотвращение и пресечение несанкционированных действий		
9.	Проведение работ по созданию способов и средств атак в научно-исследовательских центрах, специализирующихся в области разработки и анализа средств криптографической защиты информации и сред функционирования средств криптографической защиты информации, в том числе с использованием исходных текстов, входящих 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 с привлечением специалистов в области использования для реализации атак недокументированных (недекларированных) возможностей системного программного обеспечения		
11.	Возможность располагать сведениями, содержащимися в конструкторской документации на аппаратные и программные компоненты среды функционирования средств криптографической защиты информации		
12.	Возможность воздействовать на любые компоненты средств криптографической защиты информации и сред функционирования средств криптографической защиты информации		