ПРАВИТЕЛЬСТВО КУРГАНСКОЙ ОБЛАСТИ
ГОСУДАРСТВЕННАЯ ЖИЛИЩНАЯ ИНСПЕКЦИЯ КУРГАНСКОЙ ОБЛАСТИ
ПРИКАЗ

От 19.06.2017 года № 36
г. Курган

Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных в Государственной жилищной инспекции Курганской области.

В соответствии с частью 5 статьи 19 Федерального закона от 27 июля 2006 года №152-ФЗ «О персональных данных» в целях определения угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных,

ПРИКАЗЫВАЮ:

1. Определить угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных в Государственной жилищной инспекции Курганской области согласно приложению к настоящему Приказу.
2. Информационно-аналитической службе Государственной жилищной инспекции Курганской области руководствоваться настоящим приказом при определении угроз безопасности персональных данных, актуальных при обработке персональных данных в используемых информационных системах персональных данных в Государственной жилищной инспекции Курганской области.
3. Разместить настоящий приказ на официальном сайте Государственной жилищной инспекции Курганской области в информационно-телекоммуникационной сети «Интернет».
4. Контроль за исполнением настоящего приказа оставляю за собой.

Начальник Государственной жилищной инспекции Курганской области – главный государственный жилищный инспектор Курганской области В.В. Чупахин

Благинин С.Р.
(3522)43-26-13

Приложение
к приказу Государственной жилищной инспекции Курганской области
от 19.06.2017 года № 36
«Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных в Государственной жилищной инспекции Курганской области»

УГРОЗЫ
безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных в Государственной жилищной инспекции Курганской области.

1. Общие положения

1.1. Угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных в Государственной жилищной инспекции Курганской области (далее - Актуальные угрозы безопасности ИСПДн ГЖИ), разработаны в соответствии с частью 5 статьи 19 Федерального закона «О персональных данных».

1.2. Актуальные угрозы безопасности ИСПДн ГЖИ содержат перечень актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (далее - ИСПДн) в Государственной жилищной инспекции Курганской области (далее - ГЖИ).

1.3. При разработке Актуальных угроз безопасности ИСПДн ГЖИ использованы нормативные правовые акты, методические документы, модели угроз безопасности персональных данных, указанные в разделе 5 Актуальных угроз безопасности ИСПДн ГЖИ.

1.4. Угрозы безопасности персональных данных, обрабатываемых в ИСПДн, приведенные в Актуальных угрозах безопасности ИСПДн ГЖИ, подлежат адаптации в ходе разработки частных моделей угроз безопасности персональных данных.

При разработке частных моделей угроз безопасности персональных данных проводится анализ структурно-функциональных характеристик конкретной ИСПДн, применяемых в ней информационных технологий и особенностей ее функционирования. По результатам анализа делается вывод об отнесении ИСПДн к одному из видов ИСПДн, приведенных в пункте 1.7. Актуальных угроз безопасности ИСПДн ГЖИ.

В частной модели угроз безопасности персональных данных указываются:

- описание ИСПДн и её структурно-функциональных характеристик;
- описание угроз безопасности персональных данных с учетом совокупности предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак, возможных уязвимостей информационной системы, способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации.

Частные модели угроз безопасности информации для ГЖИ разрабатываются с учетом требований приказа Федеральной службы по техническому и экспортному контролю от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», приказа Федеральной службы безопасности

Российской Федерации от 10.07.2014 № 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» (далее – Приказ ФСБ России) и методических рекомендаций 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 (утв. ФСБ России 31 марта 2015 г. № 149/7/2/6-432).

1.5. Актуальные угрозы безопасности персональных данных, обрабатываемых в ИСПДн, содержащиеся в Актуальных угрозах безопасности ИСПДн ГЖИ, уточняются и дополняются по мере выявления новых источников угроз, развития способов и средств реализации угроз безопасности персональных данных в ИСПДн. Указанные изменения согласовываются с Федеральной службой по техническому и экспортному контролю (далее - ФСТЭК России) и Федеральной службой безопасности Российской Федерации (далее - ФСБ России) в установленном порядке.

1.6. Организаций, подведомственных Государственной жилищной инспекции Курганской области, нет. В случае появления подведомственных организаций, угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, подлежат доработке и согласованию в соответствии с законодательством РФ.

1.7. В ГЖИ создаются и эксплуатируются информационные системы, в которых могут обрабатываться персональные данные. В зависимости от предназначения такие информационные системы подразделяются на:

ИСПДн обеспечения типовой деятельности - информационные системы, предназначенные для автоматизации обеспечивающей деятельности ГЖИ в рамках исполнения типовых полномочий, предусмотренных нормативными правовыми актами, за исключением специфических полномочий, автоматизация или информационная поддержка которых предусмотрена информационными системами специальной деятельности. К ИСПДн обеспечения типовой деятельности можно отнести локальные ИСПДн: например, ИСПДн управления финансами.

ИСПДн обеспечения специальной деятельности - информационные системы ГЖИ, предназначенные для автоматизации либо информационной поддержки предоставления государственных услуг и исполнения государственных функций, предусмотренных в нормативных правовых актах в качестве полномочий государственного органа, а также исполняемых им функций. К ИСПДн обеспечения специальной деятельности относится автоматизированная информационная система «Жилищный надзор».

2. ИСПДн обеспечения типовой деятельности

ИСПДн обеспечения типовой деятельности ГЖИ характеризуются тем, что в качестве объектов информатизации выступают автономные автоматизированные рабочие места или рабочие места локальных вычислительных сетей, имеющих или не имеющих подключения к сетям общего пользования и (или) сетям международного информационного обмена.

Ввод персональных данных осуществляется как с бумажных носителей, так и с электронных носителей информации. Персональные данные субъектов могут выводиться из ИСПДн с целью передачи персональных данных третьим лицам в

предусмотренных Федеральным законом «О персональных данных» случаях, как в электронном, так и в бумажном виде.

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

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

ИСПДн управления финансами предназначены для обработки персональных данных, необходимых для бухгалтерского и управленческого финансового учета, предоставления информации в пенсионные и налоговые органы, систему обязательного медицинского страхования.

В ИСПДн управления финансами обрабатываются фамилия, имя, отчество, дата и место рождения, паспортные данные, адрес, номер телефона, идентификационный номер налогоплательщика (далее - ИНН), страховой номер индивидуального лицевого счета (СНИЛС), табельный номер, должность, номер приказа и дата приема на работу (увольнения), номер лицевого счёта для перечисления денежного содержания и иных выплат работника; фамилия, имя, отчество, паспортные данные, адрес, должность, номер телефона (либо иной вид связи), ИНН, платежные реквизиты граждан, являющихся стороной гражданско-правовых договоров.

3. ИСПДн обеспечения специальной деятельности

ИСПДн обеспечения специальной деятельности государственных органов характеризуются тем, что в качестве объектов информатизации выступают распределенные информационные системы и локальные информационные системы, подключенные или неподключенные к сетям общего пользования и (или) сетям международного информационного обмена.

Ввод персональных данных осуществляется как с бумажных носителей, так и с электронных носителей информации. Персональные данные субъектов персональных данных обрабатываются с целью получения государственных услуг и при выполнении ГЖИ своих функций. Могут выводиться из ИСПДн как в электронном, так и в бумажном виде.

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

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

ИСПДн автоматизированная информационная система «Жилищный надзор» предназначена для обеспечения деятельности и исполнения функций ГЖИ.

В ИСПДн обрабатываются персональные данные граждан, обратившихся в ГЖИ, в частности, фамилия, имя, отчество, адрес, номер телефона, необходимые для выполнения деятельности государственных органов, исполнения функций и предоставления государственных услуг, определенных в нормативных правовых актах.

4. Актуальные угрозы безопасности информационных систем персональных данных

Угрозы безопасности персональных данных рассмотрены в приказах и методических документах ФСТЭК России и ФСБ России.

Учитывая особенности обработки персональных данных в ГЖИ, а также категорию и объем обрабатываемых в ИСПДн персональных данных, основными характеристиками безопасности являются конфиденциальность, целостность и доступность.

Конфиденциальность - обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

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

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

Под актуальными угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

Угрозы безопасности персональных данных, актуальные при обработке персональных данных в ИСПДн, подразделяются на угрозы первого, второго, третьего типа.

Для определения актуальных угроз безопасности из общего перечня угроз безопасности выбираются только те угрозы, которые являются актуальными для ИСПДн в соответствии с Методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной заместителем директора ФСТЭК России 14.02.2008.

Угрозы безопасности персональным данным в ИСПДн ГЖИ относятся к 3-му типу, уровни защищенности ИСПДн ГЖИ 3-го и 4-го уровня защищенности.

Основной целью применения в ИСПДн Государственной жилищной инспекции Курганской области является защита персональных данных при информационном обмене по сетям связи общего пользования и (или) сетям международного информационного обмена.

Основными видами угроз безопасности персональным данным в ИСПДн являются:

- угрозы, связанные с преднамеренными или непреднамеренными действиями лиц, имеющх доступ к информационным ресурсам ИСПДн, включая пользователей ИСПДн;
- угрозы, связанные с преднамеренными или непреднамеренными действиями лиц, не имеющих доступа к ИСПДн, реализующие угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена;
- угрозы, возникновение которых напрямую зависит от свойств техники и программного обеспечения, используемого в ИСПДн;
- угрозы, возникающие в результате внедрения аппаратных закладок и вредоносных программ;
- угрозы, направленные на нарушение нормальной работы технических средств и средств связи, используемых в ИСПДн;

- угрозы, связанные с недостаточной квалификацией обслуживающего ИСПДн персонала.

4.1. Актуальные угрозы безопасности ИСПДн обеспечения типовой деятельности.

ИСПДн обеспечения типовой деятельности отличаются следующими особенностями:

- использованием стандартных (унифицированных) технических средств обработки информации;
- использованием типового программного обеспечения; наличием незначительного количества автоматизированных рабочих мест, участвующих в обработке персональных данных;
- дублированием информации, содержащей персональные данные, на бумажных носителях и внешних накопителях информации;
- незначительными негативными последствиями для субъектов персональных данных при реализации угроз безопасности ИСПДн;
- эксплуатацией ИСПДн (как правило) сотрудниками ГЖИ без привлечения на постоянной основе сторонних организаций;
- жесткой регламентацией процедуры взаимодействия со сторонними организациями (банки, пенсионные, страховые и налоговые органы, органы статистики).

Актуальными угрозами безопасности ИСПДн обеспечения типовой деятельности в ГЖИ, учитывая положения, изложенные в настоящем разделе, признаются:

- угрозы непреднамеренного или преднамеренного вывода из строя технических средств и не криптографических средств защиты информации (далее - СЗИ);
- угрозы несанкционированного отключения СЗИ;
- угрозы, связанные с недостаточной квалификацией обслуживающего ИСПДн персонала;
- угрозы надежности технических средств и коммуникационного оборудования;
- угрозы легитимности программного обеспечения; угрозы достаточности и качества применяемых СЗИ и средств антивирусной защиты;
- угрозы создания способов, подготовки и проведения атак без привлечения специалистов в области разработки и анализа СКЗИ;
- угрозы создания способов, подготовки и проведения атак на различных этапах жизненного цикла СКЗИ;
- угрозы проведения атак, находясь за пределами контролируемой зоны;
- угрозы получения из находящихся в свободном доступе источников, включая сети общего пользования и сети международного информационного обмена, информации об информационной системе, в которой используется СКЗИ;
- угрозы применения находящихся в свободном доступе или используемых за пределами контролируемой зоны аппаратных средств (далее - АС) и программного обеспечения (далее - ПО), включая аппаратные и программные компоненты СКЗИ и среду функционирования СКЗИ (далее - СФ), специально разработанных АС и ПО;
- угрозы проведения на этапе эксплуатации атаки из информационно-телекоммуникационных сетей, доступ к которым не ограничен определенным кругом лиц, если информационные системы, в которых используются СКЗИ, имеют выход в эти сети;
- угрозы использования на этапе эксплуатации находящихся за пределами контролируемой зоны АС и ПО из состава средств информационной системы, применяемых на местах эксплуатации СКЗИ штатных средств.

4.2. Актуальные угрозы безопасности ИСПДн обеспечения специальной деятельности.

ИСПДн обеспечения специальной деятельности отличаются следующими особенностями:

- использованием широкой номенклатуры (зачастую уникальных) технических средств получения, отображения и обработки информации;
- использованием специального (адаптированного под конкретную задачу) программного обеспечения;
- наличием значительного количества автоматизированных рабочих мест, участвующих в обработке персональных данных;
- широким применением СЗИ, сертифицированных СКЗИ при информационном обмене по сетям связи общего пользования и (или) сетям международного информационного обмена;
- сложностью дублирования больших массивов информации, содержащей персональные данные, на бумажных носителях и внешних накопителях информации;
- значительными негативными последствиями при реализации угроз безопасности ИСПДн;
- риском недостаточной квалификации пользователей и обслуживающего ИСПДн и СЗИ персонала;
- проблемами взаимодействия различных ИСПДн, вызванными несовершенством действующего законодательства и ведомственных инструкций.

Актуальными угрозами безопасности ИСПДн обеспечения специальной деятельности в ГЖИ, учитывая положения, изложенные в настоящем разделе, признаются:

- угрозы непреднамеренного или преднамеренного вывода из строя технических средств и СЗИ;
- угрозы несанкционированного отключения СЗИ;
- угрозы, связанные с недостаточной квалификацией обслуживающего ИСПДн персонала;
- угрозы надежности технических средств и коммуникационного оборудования;
- угрозы легитимности программного обеспечения; угрозы достаточности и качества применяемых СЗИ и средств антивирусной защиты;
- угрозы совершения атак на монитор виртуальных машин из физической сети;
- угрозы совершения атаки с виртуальной машины на другую виртуальную машину;
- угрозы совершения атаки на систему управления виртуальной инфраструктурой;
- угрозы создания способов, подготовки и проведения атак без привлечения специалистов в области разработки и анализа СКЗИ;
- угрозы создания способов, подготовки и проведения атак на различных этапах жизненного цикла СКЗИ;
- угрозы проведения атак, находясь за пределами контролируемой зоны;
- угрозы получения из находящихся в свободном доступе источников, включая сеть Интернет, информации об информационной системе, в которой используется СКЗИ;
- угрозы применения находящихся в свободном доступе или используемых за пределами контролируемой зоны АС и ПО, включая аппаратные и программные компоненты СКЗИ и СФ, специально разработанных АС и ПО;
- угрозы проведения на этапе эксплуатации атаки из информационно-телекоммуникационных сетей, доступ к которым не ограничен определенным кругом лиц, если информационные системы, в которых используются СКЗИ, имеют выход в эти сети;

- угрозы использования на этапе эксплуатации находящихся за пределами контролируемой зоны АС и ПО из состава средств информационной системы, применяемых на местах эксплуатации СКЗИ штатных средств.

5. Нормативные правовые акты, методические документы, использованные при разработке Актуальных угроз безопасности ИСПДн ГЖИ

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

постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

приказ ФСТЭК России от 18.02.2013 № 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 10.07.2014 № 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 ФСТЭК России 14.02.2008;

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 (утв. ФСБ России 31 марта 2015 г. № 149/7/2/6-432);

Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденная заместителем директора ФСТЭК России 15.02.2008.

Пояснительная записка

к приказу Государственной жилищной инспекции Курганской области

от 19.06.2017 года

«Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных в Государственной жилищной инспекции Курганской области»

Актуальные угрозы безопасности персональных данных, определяемые согласно требованиям Федеральной службы безопасности Российской Федерации:

№	Обобщенные 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 аппаратным средствам (далее - АС), на которых реализованы СКЗИ и среда их функционирования	нет
3	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны с физическим доступом к АС, на которых реализованы СКЗИ и среда их функционирования	нет
4	Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области анализа сигналов линейной передачи и сигналов побочного электромагнитного излучения и наводок СКЗИ)	нет
5	Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области использования для реализации атак недокументированных возможностей прикладного программного обеспечения)	нет
6	Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области использования для реализации атак недокументированных возможностей аппаратного и программного компонентов среды функционирования СКЗИ)	нет

№	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
1.1	проведение атаки при нахождении в пределах контролируемой зоны	не актуально	проводятся работы по подбору персонала; доступ в контролируемую зону, где располагается СКЗИ, обеспечивается в соответствии с условиями ограниченного доступа; представители технических, обслуживающих и других вспомогательных служб при работе в

			помещениях, где расположены СКЗИ, и сотрудники, не являющиеся пользователями СКЗИ, находятся в этих помещениях только в присутствии сотрудников по эксплуатации; сотрудники, являющиеся пользователями ИСПДн, но не являющиеся пользователями СКЗИ, проинформированы о правилах работы в ИСПДн и ответственности за несоблюдение правил обеспечения безопасности информации; пользователи СКЗИ проинформированы о правилах работы в ИСПДн, правилах работы с СКЗИ и ответственности за несоблюдение правил обеспечения безопасности информации; помещение, в которых располагаются документация на СКЗИ, СКЗИ и компоненты СФ, оснащены входными дверьми с замками, обеспечивается постоянное закрытие дверей помещений на замок и их открытие только для санкционированного прохода; утверждены правила доступа в помещения, где располагаются СКЗИ, в рабочее и нерабочее время, а также в нештатных ситуациях; утвержден перечень лиц, имеющих право доступа в помещения, где располагаются СКЗИ; осуществляется разграничение и контроль доступа пользователей к защищаемым ресурсам; осуществляется регистрация и учет действий пользователей с ПДн; осуществляется контроль целостности средств защиты; на АРМ, на которых установлены СКЗИ: используются сертифицированные средства защиты информации от несанкционированного доступа; используются сертифицированные средства антивирусной защиты.
1.2	проведение атак на этапе эксплуатации СКЗИ на следующие объекты: - документацию на СКЗИ и компоненты СФ; - помещения, в которых находится совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в	не актуально	проводятся работы по подбору персонала; доступ в контролируемую зону, где располагается СКЗИ, обеспечивается в соответствии с условиями ограниченного доступа; документация на СКЗИ хранится у ответственного за СКЗИ в металлическом сейфе; помещение, в которых располагаются документация на СКЗИ, СКЗИ и компоненты СФ, оснащены входными дверьми с замками, обеспечивается постоянное закрытие дверей

	составе других систем (далее - СВТ), на которых реализованы СКЗИ и СФ		помещений на замок и их открытие только для санкционированного прохода; утвержден перечень лиц, имеющих право доступа в помещения
1.3	получение в рамках предоставленных полномочий, а также в результате наблюдений следующей информации: - сведений о физических мерах защиты объектов, в которых размещены ресурсы информационной системы; - сведений о мерах по обеспечению контролируемой зоны объектов, в которых размещены ресурсы информационной системы; - сведений о мерах по разграничению доступа в помещения, в которых находятся СВТ, на которых реализованы СКЗИ и СФ	не актуально	проводятся работы по подбору персонала; доступ в контролируемую зону и помещения, где располагается ресурсы ИСПДн, обеспечивается в соответствии с условиями ограниченного доступа;; сведения о физических мерах защиты объектов, в которых размещены ИСПДн, доступны ограниченному кругу сотрудников; сотрудники проинформированы об ответственности за несоблюдение правил обеспечения безопасности информации
1.4	использование штатных средств ИСПДн, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий	не актуально	проводятся работы по подбору персонала; помещения, в которых располагаются СВТ, на которых располагаются СКЗИ и СФ, оснащены входными дверьми с замками, обеспечивается постоянное закрытие дверей помещений на замок и их открытие только для санкционированного прохода; сотрудники проинформированы об ответственности за несоблюдение правил обеспечения безопасности информации; осуществляется разграничение и контроль доступа пользователей к защищаемым ресурсам; осуществляется регистрация и учет действий пользователей; в ИСПДн используются сертифицированные средства защиты информации от несанкционированного доступа;
2.1	физический доступ к СВТ, на которых реализованы СКЗИ и СФ	не актуально	проводятся работы по подбору персонала; доступ в контролируемую зону и помещения, где располагается СВТ, на которых реализованы СКЗИ и СФ, обеспечивается в соответствии с условиями ограниченного

			доступа; помещения, в которых располагаются СВТ, на которых располагаются СКЗИ и СФ, оснащены входными дверьми с замками, обеспечивается постоянное закрытие дверей помещений на замок и их открытие только для санкционированного прохода
2.2	возможность воздействовать на аппаратные компоненты СКЗИ и СФ, ограниченная мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий	не актуально	проводятся работы по подбору персонала; доступ в контролируемую зону и помещения, где располагается СВТ, на которых реализованы СКЗИ и СФ, обеспечивается в соответствии с условиями ограниченного доступа; помещения, в которых располагаются СКЗИ и СФ, оснащены входными дверьми с замками, обеспечивается постоянное закрытие дверей помещений на замок и их открытие только для санкционированного прохода; представители технических, обслуживающих и других вспомогательных служб при работе в помещениях (стойках), где расположены компоненты СКЗИ и СФ, и сотрудники, не являющиеся пользователями СКЗИ, находятся в этих помещениях только в присутствии сотрудников по эксплуатации
3.1	создание способов, подготовка и проведение атак с привлечением специалистов в области анализа сигналов, сопровождающих функционирование СКЗИ и СФ, и в области использования для реализации атак недокументированных (недекларированных) возможностей прикладного ПО	не актуально	не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности; высокая стоимость и сложность подготовки реализации возможности; проводятся работы по подбору персонала; доступ в контролируемую зону и помещения, где располагается СВТ, на которых реализованы СКЗИ и СФ, обеспечивается в соответствии с условиями ограниченного доступа; помещения, в которых располагаются СКЗИ и СФ, оснащены входными дверьми с замками, обеспечивается постоянное закрытие дверей помещений на замок и их открытие только для санкционированного прохода; представители технических, обслуживающих и других вспомогательных служб при работе в помещениях (стойках), где расположены компоненты СКЗИ и СФ, и сотрудники, не являющиеся пользователями СКЗИ, находятся в этих помещениях только в присутствии сотрудников по эксплуатации; осуществляется разграничение и контроль

			доступа пользователей к защищаемым ресурсам; осуществляется регистрация и учет действий пользователей; на АРМ на которых установлены СКЗИ: используются сертифицированные средства защиты информации от несанкционированного доступа; используются сертифицированные средства антивирусной защиты
3.2	проведение лабораторных исследований СКЗИ, используемых вне контролируемой зоны, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий	не актуально	не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности; высокая стоимость и сложность подготовки реализации возможности
3.3	проведение работ по созданию способов и средств атак в научно-исследовательских центрах, специализирующихся в области разработки и анализа СКЗИ и СФ, в том числе с использованием исходных текстов входящего в СФ прикладного ПО, непосредственно использующего вызовы программных функций СКЗИ	не актуально	не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности; высокая стоимость и сложность подготовки реализации возможности
4.1	создание способов, подготовка и проведение атак с привлечением специалистов в области использования для реализации атак недокументированных (недекларированных) возможностей системного ПО	не актуально	не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности; высокая стоимость и сложность подготовки реализации возможности; проводятся работы по подбору персонала; доступ в контролируемую зону и помещения, где располагается СВТ, на которых реализованы СКЗИ и СФ, обеспечивается в соответствии с условиями ограниченного доступа; помещения, в которых располагаются СКЗИ и СФ, оснащены входными дверьми с замками,

			обеспечивается постоянное закрытие дверей помещений на замок и их открытие только для санкционированного прохода; представители технических, обслуживающих и других вспомогательных служб при работе в помещениях (стойках), где расположены компоненты СКЗИ и СФ, и сотрудники, не являющиеся пользователями СКЗИ, находятся в этих помещениях только в присутствии сотрудников по эксплуатации; осуществляется разграничение и контроль доступа пользователей к защищаемым ресурсам; осуществляется регистрация и учет действий пользователей; на АРМ на которых установлены СКЗИ: используются сертифицированные средства защиты информации от несанкционированного доступа; используются сертифицированные средства антивирусной защиты
4.2	возможность располагать сведениями, содержащимися в конструкторской документации на аппаратные и программные компоненты СФ	не актуально	не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности
4.3	возможность воздействовать на любые компоненты СКЗИ и СФ	не актуально	не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности