БЕЛГОРОДСКАЯ ОБЛАСТЬ

ПРАВИТЕЛЬСТВО БЕЛГОРОДСКОЙ ОБЛАСТИ

ПОСТАНОВЛЕНИЕ

Белгород

«26» февраля 2018 г. № 58-пп

Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных органов исполнительной власти и государственных органов Белгородской области

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

1. Определить угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных органов исполнительной власти и государственных органов Белгородской области согласно приложению к настоящему постановлению.

2. Органам исполнительной власти и государственным органам Белгородской области руководствоваться настоящим постановлением.

3. Рекомендовать органам местного самоуправления муниципальных районов и городских округов руководствоваться настоящим постановлением при организации работ по защите персональных данных.

4. Контроль за исполнением постановления возложить на управление информационных технологий и связи Администрации Губернатора Белгородской области (Мирошников Е.В.).

5. Настоящее постановление вступает в силу со дня его официального опубликования.

Администрация Губернатора Белгородской области
Отдел сопровождения правовых актов
Для документов

Губернатор Белгородской области **Е.Савченко**

Приложение
к постановлению Правительства
Белгородской области

от 26 февраля **2018 г.**

№ 58-пп

Угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных органов исполнительной власти и государственных органов Белгородской области

I. Общие положения

Угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных (далее - ИСПДн) органов исполнительной власти и государственных органов Белгородской области (далее - Актуальные угрозы безопасности ИСПДн), разработаны в соответствии с частью 5 статьи 19 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных».

Под Актуальными угрозами безопасности ИСПДн понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в ИСПДн, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия в соответствии с пунктом 6 требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

В качестве исходного перечня вероятных угроз безопасности информации целесообразно использовать угрозы, приведенные в Актуальных угрозах безопасности ИСПДн. Рассматриваемые угрозы подлежат адаптации при разработке моделей угроз безопасности персональных данных ИСПДн.

Типовая форма частной модели угроз безопасности персональных данных для органов исполнительной власти и государственных органов Белгородской области разрабатывается с учетом требований:

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

– Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных»;

– Постановления Правительства Российской Федерации от 21 марта 2012 года № 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»;

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

– приказа Федеральной службы по техническому и экспортному контролю Российской Федерации 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»;

– приказа 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»;

– Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной заместителем директора ФСТЭК России 15 февраля 2008 года;

– Методики определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной заместителем директора ФСТЭК России 14 февраля 2008 года;

– 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, утвержденных руководством 8 Центра ФСБ России от 31 марта 2015 года № 149/7/2/6-432;

– Банка данных угроз ФСТЭК России (www.bdu.fstec.ru).

При разработке частных моделей угроз безопасности персональных данных проводится анализ структурно-функциональных характеристик конкретной ИСПДн и применяемых в ней информационных технологий, особенностей её функционирования.

В частной модели угроз безопасности персональных данных указываются:

– структурно-функциональное построение ИСПДн, ее описание;

– описание ИСПДн по структуре (разноплановые системы) в том случае, если применяются сертифицированные средства криптографической защиты информации (далее - СКЗИ);

– описание угроз безопасности персональных данных с учетом совокупности предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак;

– описание возможных уязвимостей информационной системы, способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации;

– описание модели нарушителя.

Актуальные угрозы безопасности ИСПДн уточняются и дополняются по мере выявления новых источников угроз, развития способов и средств реализации угроз безопасности персональных данных в ИСПДн.

Информационные системы персональных данных органов исполнительной власти и государственных органов Белгородской области характеризуются тем, что разноплановы и могут иметь любую структуру из шести типовых, рассмотренных в Базовой модели угроз безопасности персональных данных при их обработке в ИСПДн, утвержденной заместителем директора ФСТЭК России 15 февраля 2008 года:

1) автоматизированные рабочие места, не имеющие подключения к сетям связи общего пользования и (или) сетям международного информационного обмена;

2) автоматизированные рабочие места, имеющие подключение к сетям связи общего пользования и (или) сетям международного информационного обмена;

3) локальные информационные системы персональных данных, не имеющие подключения к сетям связи общего пользования и (или) сетям международного информационного обмена;

4) локальные информационные системы персональных данных, имеющие подключение к сетям связи общего пользования и (или) сетям международного информационного обмена;

5) распределенные ИСПДн, не имеющие подключение к сетям связи общего пользования и (или) сетям международного информационного обмена;

6) распределенные ИСПДн, имеющие подключение к сетям связи общего пользования и (или) сетям международного информационного обмена.

Ввод персональных данных в ИСПДн и вывод данных из ИСПДн осуществляются с использованием бумажных и электронных носителей информации. В качестве электронных носителей информации используются учтенные съемные носители информации и компакт-диски.

Персональные данные субъектов персональных данных обрабатываются в целях:

– обеспечения деятельности Губернатора и Правительства Белгородской области;

– предоставления государственных и муниципальных услуг;

– приема и рассмотрения поступивших в адрес Губернатора Белгородской области документов, обращений граждан и организаций, а также регистрации и отправки исходящей корреспонденции;

– обеспечения кадровой работы, в том числе в целях содействия гражданским служащим, работникам в прохождении государственной гражданской службы Белгородской области, выполнении работы, в обучении и должностном росте, обеспечения личной безопасности гражданских служащих, работников и членов их семей, обеспечения сохранности принадлежащего им имущества и имущества государственных органов, учета результатов исполнения ими должностных обязанностей, обеспечения установленных законодательством Российской Федерации условий осуществления служебной деятельности и труда, гарантий и компенсаций;

– формирования кадрового резерва на государственной гражданской службе Белгородской области, резерва управленческих кадров Белгородской области, противодействия коррупции;

– реализации процедур по представлению граждан к награждению;

– рассмотрения вопросов, связанных с помилованием осужденных и лиц, отбывших назначенное судом наказание и имеющих не снятую судимость.

При осуществлении информационного обмена по сетям связи общего пользования и (или) сетям международного информационного обмена применяются сертифицированные СКЗИ.

Автоматизированные рабочие места пользователей, серверы, сетевое и телекоммуникационное оборудование ИСПДн находятся в пределах контролируемой зоны. Для ИСПДн контролируемой зоной являются административные здания либо отдельные помещения. 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.

В административных зданиях установлен пропускной режим, неконтролируемое пребывание посторонних лиц и неконтролируемое перемещение (вынос за пределы здания) компьютеров и оргтехники запрещены. Помещения оборудованы запирающимися дверями с опечатывающими устройствами (при использовании СКЗИ). В коридорах, вестибюлях и холлах ведется видеонаблюдение.

Технические средства и базы данных ИСПДн органов исполнительной власти и государственных органов Белгородской области размещаются на территории Российской Федерации.

II. Угрозы безопасности ИСПДн

Учитывая особенности обработки персональных данных в органах исполнительной власти и государственных органах Белгородской области, а также категорию и объем обрабатываемых в ИСПДн персональных данных, основными характеристиками безопасности являются конфиденциальность, целостность и доступность.

Система защиты персональных данных включает в себя организационные и (или) технические меры, определенные с учетом актуальных угроз

безопасности персональных данных и информационных технологий, используемых в информационных системах.

Безопасность информации (данных) - состояние защищенности информации (данных), при котором обеспечены ее (их) конфиденциальность, доступность и целостность.

Конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

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 (ресурсов информационной системы), при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно.

Основной целью применения в ИСПДн органов исполнительной власти и государственных органов Белгородской области СКЗИ является защита персональных данных, в том числе при информационном обмене по сетям связи общего пользования и (или) сетям международного информационного обмена.

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, распространение персональных данных, а также иные неправомерные действия с персональными данными.

В зависимости от состава обрабатываемых персональных данных и типа актуальных угроз, необходимый уровень защищенности персональных данных для каждой ИСПДн определяется индивидуально.

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

III. Объекты защиты

К объектам защиты относятся:

- персональные данные (ПДн);
- средства защиты информации (СЗИ);
- программно-аппаратные средства;
- системное, сетевое и прикладное программное обеспечение;
- телекоммуникационное оборудование;
- средства криптографической защиты информации (СКЗИ);
- среда функционирования СЗИ;

– среда функционирования СКЗИ (СФ);

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

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

– носители защищаемой информации, используемые в информационной системе в процессе криптографической защиты персональных данных, носители ключевой, парольной и аутентифицирующей информации СКЗИ и порядок доступа к ним;

– используемые информационной системой каналы (линии) связи, включая кабельные системы;

– помещения, в которых находятся ресурсы информационной системы, имеющие отношение к криптографической защите персональных данных.

IV. Актуальные угрозы безопасности в ИСПДн органов исполнительной власти и государственных органов Белгородской области

1. Угрозы безопасности информации из состава Банка данных угроз безопасности информации (www.bdu.fstec.ru), потенциально опасные для информационных систем персональных данных:

УБИ. 003 Угроза анализа криптографических алгоритмов и их реализации;

УБИ. 004 Угроза аппаратного сброса пароля BIOS;

УБИ. 006 Угроза внедрения кода или данных;

УБИ. 008 Угроза восстановления аутентификационной информации;

УБИ. 009 Угроза восстановления предыдущей уязвимой версии BIOS;

УБИ. 012 Угроза деструктивного изменения конфигурации/среды окружения программ;

УБИ. 013 Угроза деструктивного использования декларированного функционала BIOS;

УБИ. 014 Угроза длительного удержания вычислительных ресурсов пользователями;

УБИ. 015 Угроза доступа к защищаемым файлам с использованием обходного пути;

УБИ. 016 Угроза доступа к локальным файлам сервера при помощи URL;

УБИ. 017 Угроза доступа/перехвата/изменения HTTP cookies;

УБИ. 018 Угроза загрузки нештатной операционной системы;

УБИ. 019 Угроза заражения DNS-кеша;

УБИ. 022 Угроза избыточного выделения оперативной памяти;
УБИ. 023 Угроза изменения компонентов системы;
УБИ. 025 Угроза изменения системных и глобальных переменных;
УБИ. 026 Угроза искажения XML-схемы;
УБИ. 027 Угроза искажения вводимой и выводимой на периферийные устройства информации;
УБИ. 028 Угроза использования альтернативных путей доступа к ресурсам;
УБИ. 029 Угроза использования вычислительных ресурсов суперкомпьютера «паразитными» процессами;
УБИ. 030 Угроза использования информации идентификации/аутентификации, заданной по умолчанию;
УБИ. 031 Угроза использования механизмов авторизации для повышения привилегий;
УБИ. 032 Угроза использования поддельных цифровых подписей BIOS;
УБИ. 033 Угроза использования слабостей кодирования входных данных;
УБИ. 034 Угроза использования слабостей протоколов сетевого/локального обмена данными;
УБИ. 036 Угроза исследования механизмов работы программы;
УБИ. 037 Угроза исследования приложения через отчёты об ошибках;
УБИ. 038 Угроза исчерпания вычислительных ресурсов хранилища больших данных;
УБИ. 039 Угроза исчерпания запаса ключей, необходимых для обновления BIOS;
УБИ. 040 Угроза конфликта юрисдикций различных стран;
УБИ. 041 Угроза межсайтового скриптинга;
УБИ. 042 Угроза межсайтовой подделки запроса;
УБИ. 045 Угроза нарушения изоляции среды исполнения BIOS;
УБИ. 049 Угроза нарушения целостности данных кеша;
УБИ. 051 Угроза невозможности восстановления сессии работы на ПЭВМ при выводе из промежуточных состояний питания;
УБИ. 053 Угроза невозможности управления правами пользователей BIOS;
УБИ. 061 Угроза некорректного задания структуры данных транзакции;
УБИ. 063 Угроза некорректного использования функционала программного обеспечения;
УБИ. 067 Угроза неправомерного ознакомления с защищаемой информацией;
УБИ. 068 Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением;
УБИ. 069 Угроза неправомерных действий в каналах связи;
УБИ. 071 Угроза несанкционированного восстановления удалённой защищаемой информации;

УБИ. 072 Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS;

УБИ. 074 Угроза несанкционированного доступа к аутентификационной информации;

УБИ. 086 Угроза несанкционированного изменения аутентификационной информации;

УБИ. 087 Угроза несанкционированного использования привилегированных функций BIOS;

УБИ. 088 Угроза несанкционированного копирования защищаемой информации;

УБИ. 089 Угроза несанкционированного редактирования реестра;

УБИ. 090 Угроза несанкционированного создания учётной записи пользователя;

УБИ. 091 Угроза несанкционированного удаления защищаемой информации;

УБИ. 093 Угроза несанкционированного управления буфером;

УБИ. 094 Угроза несанкционированного управления синхронизацией и состоянием;

УБИ. 095 Угроза несанкционированного управления указателями;

УБИ. 098 Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб;

УБИ. 099 Угроза обнаружения хостов;

УБИ. 100 Угроза обхода некорректно настроенных механизмов аутентификации;

УБИ. 102 Угроза опосредованного управления группой программ через совместно используемые данные;

УБИ. 103 Угроза определения типов объектов защиты;

УБИ. 104 Угроза определения топологии вычислительной сети;

УБИ. 107 Угроза отключения контрольных датчиков;

УБИ. 109 Угроза перебора всех настроек и параметров приложения;

УБИ. 111 Угроза передачи данных по скрытым каналам;

УБИ. 112 Угроза передачи запрещённых команд на оборудование с числовым программным управлением;

УБИ. 113 Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники;

УБИ. 114 Угроза переполнения целочисленных переменных;

УБИ. 115 Угроза перехвата вводимой и выводимой на периферийные устройства информации;

УБИ. 116 Угроза перехвата данных, передаваемых по вычислительной сети;

УБИ. 117 Угроза перехвата привилегированного потока;

УБИ. 118 Угроза перехвата привилегированного процесса;

УБИ. 121 Угроза повреждения системного реестра;

УБИ. 122 Угроза повышения привилегий;

УБИ. 123 Угроза подбора пароля BIOS;

УБИ. 124 Угроза подделки записей журнала регистрации событий;
УБИ. 127 Угроза подмены действия пользователя путём обмана;
УБИ. 128 Угроза подмены доверенного пользователя;
УБИ. 129 Угроза подмены резервной копии программного обеспечения BIOS;
УБИ. 130 Угроза подмены содержимого сетевых ресурсов;
УБИ. 131 Угроза подмены субъекта сетевого доступа;
УБИ. 132 Угроза получения предварительной информации об объекте защиты;
УБИ. 139 Угроза преодоления физической защиты;
УБИ. 140 Угроза приведения системы в состояние «отказ в обслуживании»;
УБИ. 143 Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации;
УБИ. 144 Угроза программного сброса пароля BIOS;
УБИ. 145 Угроза пропуска проверки целостности программного обеспечения;
УБИ. 149 Угроза сбоя обработки специальным образом изменённых файлов;
УБИ. 150 Угроза сбоя процесса обновления BIOS;
УБИ. 151 Угроза сканирования веб-сервисов, разработанных на основе языка описания WSDL;
УБИ. 152 Угроза удаления аутентификационной информации;
УБИ. 153 Угроза усиления воздействия на вычислительные ресурсы пользователей при помощи сторонних серверов;
УБИ. 154 Угроза установки уязвимых версий обновления программного обеспечения BIOS;
УБИ. 155 Угроза утраты вычислительных ресурсов;
УБИ. 156 Угроза утраты носителей информации;
УБИ. 157 Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации;
УБИ. 158 Угроза форматирования носителей информации;
УБИ. 159 Угроза «форсированного веб-браузинга»;
УБИ. 160 Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации;
УБИ. 162 Угроза эксплуатации цифровой подписи программного кода;
УБИ. 163 Угроза перехвата исключения/сигнала из привилегированного блока функций;
УБИ. 165 Угроза включения в проект не достоверно испытанных компонентов;
УБИ. 166 Угроза внедрения системной избыточности;
УБИ. 167 Угроза заражения компьютера при посещении неблагонадёжных сайтов;
УБИ. 168 Угроза «кражи» учётной записи доступа к сетевым сервисам;
УБИ. 169 Угроза наличия механизмов разработчика;

УБИ. 170 Угроза неправомерного шифрования информации;

УБИ. 171 Угроза скрытного включения вычислительного устройства в состав бот-сети;

УБИ. 172 Угроза распространения «почтовых червей»;

УБИ. 173 Угроза «спама» веб-сервера;

УБИ. 174 Угроза «фарминга»;

УБИ. 175 Угроза «фишинга»;

УБИ. 176 Угроза нарушения технологического/производственного процесса из-за временных задержек, вносимых средством защиты;

УБИ. 177 Угроза неподтверждённого ввода данных оператором в систему, связанную с безопасностью;

УБИ. 178 Угроза несанкционированного использования системных и сетевых утилит;

УБИ. 179 Угроза несанкционированной модификации защищаемой информации;

УБИ. 180 Угроза отказа подсистемы обеспечения температурного режима;

УБИ. 181 Угроза перехвата одноразовых паролей в режиме реального времени;

УБИ. 182 Угроза физического устаревания аппаратных компонентов;

УБИ. 183 Угроза перехвата управления автоматизированной системой управления технологическими процессами;

УБИ. 185 Угроза несанкционированного изменения параметров настройки средств защиты информации;

УБИ. 186 Угроза внедрения вредоносного кода через рекламу, сервисы и контент;

УБИ. 187 Угроза несанкционированного воздействия на средство защиты информации;

УБИ. 188 Угроза подмены программного обеспечения;

УБИ. 189 Угроза маскирования действий вредоносного кода;

УБИ. 190 Угроза внедрения вредоносного кода за счет посещения зараженных сайтов в сети Интернет;

УБИ. 191 Угроза внедрения вредоносного кода в дистрибутив программного обеспечения;

УБИ. 192 Угроза использования уязвимых версий программного обеспечения;

УБИ. 193 Угроза утечки информации за счет применения вредоносным программным обеспечением алгоритмов шифрования трафика;

УБИ. 197 Угроза хищения аутентификационной информации из временных файлов cookie;

УБИ. 198 Угроза скрытной регистрации вредоносной программой учетных записей администраторов;

УБИ. 201 Угроза утечки пользовательских данных при использовании функций автоматического заполнения аутентификационной информации в браузере;

УБИ. 203 Угроза утечки информации с неподключенных к сети Интернет компьютеров;

УБИ. 204 Угроза несанкционированного изменения вредоносной программой значений параметров программируемых логических контроллеров;

УБИ. 205 Угроза нарушения работы компьютера и блокирования доступа к его данным из-за некорректной работы установленных на нем средств защиты;

УБИ. 207 Угроза несанкционированного доступа к параметрам настройки оборудования за счет использования «мастер-кодов» (инженерных паролей).

2. В случае, если ИСПДн не имеет подключения к сетям общего пользования, то актуальными будут угрозы:

Угрозы безопасности информации из состава Банка данных угроз безопасности информации (www.bdu.fstec.ru), потенциально опасные для информационных систем персональных данных, не имеющих подключения к сетям общего пользования:

УБИ. 004 Угроза аппаратного сброса пароля BIOS;

УБИ. 008 Угроза восстановления аутентификационной информации;

УБИ. 009 Угроза восстановления предыдущей уязвимой версии BIOS;

УБИ. 010 Угроза выхода процесса за пределы виртуальной машины;

УБИ. 011 Угроза деавторизации санкционированного клиента беспроводной сети;

УБИ. 012 Угроза деструктивного изменения конфигурации/среды окружения программ;

УБИ. 013 Угроза деструктивного использования декларированного функционала BIOS;

УБИ. 014 Угроза длительного удержания вычислительных ресурсов пользователями;

УБИ. 015 Угроза доступа к защищаемым файлам с использованием обходного пути;

УБИ. 018 Угроза загрузки нештатной операционной системы;

УБИ. 022 Угроза избыточного выделения оперативной памяти;

УБИ. 023 Угроза изменения компонентов системы;

УБИ. 025 Угроза изменения системных и глобальных переменных;

УБИ. 026 Угроза искажения XML-схемы;

УБИ. 027 Угроза искажения вводимой и выводимой на периферийные устройства информации;

УБИ. 028 Угроза использования альтернативных путей доступа к ресурсам;

УБИ. 029 Угроза использования вычислительных ресурсов суперкомпьютера «паразитными» процессами;

УБИ. 030 Угроза использования информации идентификации/аутентификации, заданной по умолчанию;

УБИ. 031 Угроза использования механизмов авторизации для повышения привилегий;

УБИ. 033 Угроза использования слабостей кодирования входных данных;

УБИ. 034 Угроза использования слабостей протоколов сетевого/локального обмена данными;

УБИ. 036 Угроза исследования механизмов работы программы;

УБИ. 037 Угроза исследования приложения через отчёты об ошибках;

УБИ. 038 Угроза исчерпания вычислительных ресурсов хранилища больших данных;

УБИ. 045 Угроза нарушения изоляции среды исполнения BIOS;

УБИ. 049 Угроза нарушения целостности данных кеша;

УБИ. 051 Угроза невозможности восстановления сессии работы на ПЭВМ при выводе из промежуточных состояний питания;

УБИ. 053 Угроза невозможности управления правами пользователей BIOS;

УБИ. 061 Угроза некорректного задания структуры данных транзакции;

УБИ. 063 Угроза некорректного использования функционала программного обеспечения;

УБИ. 067 Угроза неправомерного ознакомления с защищаемой информацией;

УБИ. 068 Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением;

УБИ. 071 Угроза несанкционированного восстановления удалённой защищаемой информации;

УБИ. 072 Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS;

УБИ. 074 Угроза несанкционированного доступа к аутентификационной информации;

УБИ. 086 Угроза несанкционированного изменения аутентификационной информации;

УБИ. 087 Угроза несанкционированного использования привилегированных функций BIOS;

УБИ. 088 Угроза несанкционированного копирования защищаемой информации;

УБИ. 089 Угроза несанкционированного редактирования реестра;

УБИ. 090 Угроза несанкционированного создания учётной записи пользователя;

УБИ. 091 Угроза несанкционированного удаления защищаемой информации;

УБИ. 093 Угроза несанкционированного управления буфером;

УБИ. 094 Угроза несанкционированного управления синхронизацией и состоянием;

УБИ. 095 Угроза несанкционированного управления указателями;

УБИ. 100 Угроза обхода некорректно настроенных механизмов аутентификации;

УБИ. 102 Угроза опосредованного управления группой программ через совместно используемые данные;

УБИ. 107 Угроза отключения контрольных датчиков;

УБИ. 109 Угроза перебора всех настроек и параметров приложения;

УБИ. 111 Угроза передачи данных по скрытым каналам;

УБИ. 112 Угроза передачи запрещённых команд на оборудование с числовым программным управлением;

УБИ. 113 Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники;

УБИ. 114 Угроза переполнения целочисленных переменных;

УБИ. 115 Угроза перехвата вводимой и выводимой на периферийные устройства информации;

УБИ. 117 Угроза перехвата привилегированного потока;

УБИ. 118 Угроза перехвата привилегированного процесса;

УБИ. 121 Угроза повреждения системного реестра;

УБИ. 122 Угроза повышения привилегий;

УБИ. 123 Угроза подбора пароля BIOS;

УБИ. 124 Угроза подделки записей журнала регистрации событий;

УБИ. 129 Угроза подмены резервной копии программного обеспечения BIOS;

УБИ. 140 Угроза приведения системы в состояние «отказ в обслуживании»;

УБИ. 143 Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации;

УБИ. 144 Угроза программного сброса пароля BIOS;

УБИ. 145 Угроза пропуска проверки целостности программного обеспечения;

УБИ. 149 Угроза сбоя обработки специальным образом изменённых файлов;

УБИ. 150 Угроза сбоя процесса обновления BIOS;

УБИ. 152 Угроза удаления аутентификационной информации;

УБИ. 153 Угроза усиления воздействия на вычислительные ресурсы пользователей при помощи сторонних серверов;

УБИ. 154 Угроза установки уязвимых версий обновления программного обеспечения BIOS;

УБИ. 155 Угроза утраты вычислительных ресурсов;

УБИ. 156 Угроза утраты носителей информации;

УБИ. 158 Угроза форматирования носителей информации;

УБИ. 162 Угроза эксплуатации цифровой подписи программного кода;

УБИ. 163 Угроза перехвата исключения/сигнала из привилегированного блока функций;

УБИ. 165 Угроза включения в проект не достоверно испытанных компонентов;

УБИ. 166 Угроза внедрения системной избыточности;

УБИ. 167 Угроза заражения компьютера при посещении неблагонадёжных сайтов;

УБИ. 169 Угроза наличия механизмов разработчика;

УБИ. 177 Угроза неподтверждённого ввода данных оператором в систему, связанную с безопасностью;

УБИ. 178 Угроза несанкционированного использования системных и сетевых утилит;

УБИ. 179 Угроза несанкционированной модификации защищаемой информации;

УБИ. 180 Угроза отказа подсистемы обеспечения температурного режима;

УБИ. 182 Угроза физического устаревания аппаратных компонентов;

УБИ. 183 Угроза перехвата управления автоматизированной системой управления технологическими процессами;

УБИ. 185 Угроза несанкционированного изменения параметров настройки средств защиты информации;

УБИ. 186 Угроза внедрения вредоносного кода через рекламу, сервисы и контент;

УБИ. 187 Угроза несанкционированного воздействия на средство защиты информации;

УБИ. 188 Угроза подмены программного обеспечения;

УБИ. 191 Угроза внедрения вредоносного кода в дистрибутив программного обеспечения;

УБИ. 192 Угроза использования уязвимых версий программного обеспечения;

УБИ. 203 Угроза утечки информации с неподключенных к сети Интернет компьютеров;

УБИ. 207 Угроза несанкционированного доступа к параметрам настройки оборудования за счет использования «мастер-кодов» (инженерных паролей).

В соответствии с методическими рекомендациями 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, утвержденных руководством 8 Центра ФСБ России 31 марта 2015 года № 149/7/2/6-432, на основании исходных данных об информационных системах, объектах защиты и источниках атак определяются обобщенные возможности источников атак.

Определение обобщенных возможностей источников атак представлено в разделе V.

Реализация угроз безопасности персональных данных, обрабатываемых в информационных системах персональных данных, определяется возможностями источников атак. Таким образом, актуальность использования возможностей источников атак определяет наличие соответствующих актуальных угроз.

На основании обобщенных возможностей источников атак и в соответствии с правилами, приведенными в методических рекомендациях, определяются актуальные угрозы, а для неактуальных угроз в разделе VI приводятся обоснования признания их неактуальности.

Если системы разноплановые и при этом угрозы, которые могут быть нейтрализованы только с помощью СКЗИ, являются актуальными, то при разработке для имеющихся ИСПДн частных моделей угроз необходимо руководствоваться разделом 3 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, утвержденных руководством 8 Центра ФСБ России от 31 марта 2015 года № 149/7/2/6-432.

В случае, если не имеется актуальных угроз, которые могли бы быть нейтрализованы с помощью СКЗИ, руководствоваться требованиями нормативных правовых актов, указанных в разделе I Актуальных угроз безопасности ИСПДн.

V. Обобщённые возможности источников атак

№ п/п	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, 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 аппаратным средствам, 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

№ п/п	Обобщенные возможности источников атак	Да/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

VI. Обоснование признания неактуальности угроз

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия актуальности угроз
1.1.	Проведение атаки при нахождении в пределах контролируемой зоны	Неактуально	Проводятся работы по подбору персонала; доступ в контролируемую зону, где располагается СКЗИ, обеспечивается в соответствии с контрольно-пропускным режимом; представители технических, обслуживающих и других вспомогательных служб при работе в помещениях (стойках), 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; помещения, в которых располагаются СКЗИ, 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

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия актуальности угроз
			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 АРМах и серверах, 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	Неактуально	Проводятся работы по подбору персонала; доступ в контролируемую зону, где располагается СКЗИ, обеспечивается в соответствии с контрольно-пропускным режимом; документация на СКЗИ хранится у ответственного за СКЗИ в металлическом сейфе; помещения, в которых располагаются документация на СКЗИ, СКЗИ и компоненты СФ, оснащены входными дверьми с замками, обеспечивается постоянное закрытие дверей

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия актуальности угроз
	функционировать самостоятельно или в 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	Неактуально	Проводятся работы по подбору персонала; доступ в контролируемую зону и помещения, где располагается ресурсы ИСПДн, обеспечивается в соответствии с контрольно-пропускным режимом; 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	Неактуально	Проводятся работы по подбору персонала; помещения, в которых располагаются СВТ, на которых располагаются СКЗИ и СФ, оснащены входными дверьми с

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия актуальности угроз
	системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий		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, сертифицированные средства антивирусной защиты
2.1.	Физический доступ к СВТ, на которых реализованы СКЗИ и СФ	Неактуально	Проводятся работы по подбору персонала; доступ в контролируемую зону и помещения, где располагается СВТ, на которых реализованы СКЗИ и СФ, обеспечивается в соответствии с контрольно-пропускным режимом; 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

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия актуальности угроз
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	Неактуально	Проводятся работы по подбору персонала; доступ в контролируемую зону и помещения, где располагается СВТ, на которых реализованы СКЗИ и СФ, обеспечивается в соответствии с контрольно-пропускным режимом; 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	Неактуально	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

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия актуальности угроз
	недокументированных (недекларированных) возможностей прикладного программного обеспечения		располагается СВТ, на которых реализованы СКЗИ и СФ, обеспечивается в соответствии с контрольно-пропускным режимом; 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 АРМах и серверах, на которых установлены СКЗИ: используются сертифицированные средства защиты информации от несанкционированного доступа, используются сертифицированные средства антивирусной защиты
3.2.	Проведение лабораторных исследований СКЗИ, используемых	Неактуально	Не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия актуальности угроз
	вне контролируемой зоны, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий		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 программного обеспечения, непосредственно использующего вызовы программных функций СКЗИ	Неактуально	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

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия актуальности угроз
4.1.	Создание способов, подготовка и проведение атак с привлечением специалистов в области использования для реализации атак недокументированных (недекларированных) возможностей системного программного обеспечения	Неактуально	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 контрольно-пропускным режимом; 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 АРМах и серверах, на которых установлены СКЗИ: используются сертифицированные средства защиты информации от несанкционированного доступа, используются сертифицированные средства антивирусной защиты

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия актуальности угроз
4.2.	Возможность располагать сведениями, содержащимися в конструкторской документации на аппаратные и программные компоненты СФ.	Неактуально	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.	Неактуально	Не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности