



АДМИНИСТРАЦИЯ ТАМБОВСКОЙ ОБЛАСТИ  
УПРАВЛЕНИЕ ОБРАЗОВАНИЯ И НАУКИ  
ТАМБОВСКОЙ ОБЛАСТИ

П Р И К А З

25.04.2018

г. Тамбов

№ 154

Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных в управлении образования и науки области

В соответствии с частью 5 статьи 19 Федерального закона от 27.07.2006. № 152-ФЗ «О персональных данных», с целью обеспечения единого подхода к определению угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных в управлении образования и науки области (далее - Управление) ПРИКАЗЫВАЮ:

1. Определить угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных в Управлении, согласно приложению.
2. Опубликовать настоящий приказ на «Официальном интернет-портале правовой информации» ([www.pravo.gov.ru](http://www.pravo.gov.ru)) и на сайте сетевого издания «Тамбовская жизнь» ([www.tamlife.ru](http://www.tamlife.ru)).
3. Контроль за исполнением настоящего приказа возложить на заместителя начальника Управления М.В.Быкову.

Начальник управления



Т.П.Котельникова

Угрозы  
безопасности персональных данных, актуальные при обработке персональных  
данных в информационных системах персональных данных в Управлении  
образования и науки области

1. Общие положения

1.1. Угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных в Управлении образования и науки области (далее - Актуальные угрозы безопасности ИСПДн), определены в соответствии с частью 5 статьи 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказом Федеральной службы по техническому и экспортному контролю (далее - ФСТЭК России) от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», приказом ФСТЭК России от 18.02.2013 № 21 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», приказом Федеральной службы безопасности Российской Федерации (далее - ФСБ России) от 10.07.2014 № 378 «Об утверждении Составы 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», Методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной заместителем директора ФСТЭК России 14.02.2008, 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, утверждёнными руководством 8-го Центра ФСБ России от 31.03.2015 №149/7/2/6-432, Базовой моделью угроз безопасности персональных данных при их обработке в информационных системах персональных данных,

утвержденной заместителем директора ФСТЭК России 15.02.2008, Банком данных угроз безопасности информации, размещенным на официальном сайте ФСТЭК России (<http://bdu.fstec.ru>) и постановлением администрации Тамбовской области от 18.12.2017 № 1248 «Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных в органах исполнительной власти области и в подведомственных им организациях».

1.2. Актуальные угрозы безопасности ИСПДн содержат перечень актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (далее - ИСПДн) Управления образования и науки области (далее - Управление).

1.3. Актуальные угрозы безопасности ИСПДн подлежат адаптации в ходе разработки частных моделей угроз безопасности персональных данных для каждой информационной системы Управления.

1.4. При разработке частных моделей угроз безопасности персональных данных проводится анализ структурно-функциональных характеристик ИС, эксплуатируемой при осуществлении Управлением функций и полномочий, а также применяемых в ней информационных технологий и особенностей ее функционирования, в том числе с использованием Банка данных угроз безопасности информации.

1.5. В частной модели угроз безопасности персональных данных указываются:

описание ИСПДн и ее структурно-функциональных характеристик;

описание угроз безопасности персональных данных с учетом совокупности предположений о способах, подготовке и проведении атак;

описание возможных уязвимостей ИС, способов реализации угроз безопасности информации и последствий нарушений безопасности информации.

1.6. Объектами информатизации в Управлении выступают ИС, имеющие сходную структуру и одноточечное подключение к сетям общего пользования и (или) информационно-телекоммуникационной сети «Интернет» (далее - сеть «Интернет») через выделенную инфраструктуру – межведомственную сеть передачи данных Тамбовской области.

1.7. В зависимости от конкретного объекта информатизации ИС Управления делятся на два вида:

локальная ИС, рабочие места и базы данных которой расположены в пределах одного здания – ЛВС «АИСТ»;

распределенные ИС, рабочие места которой расположены в пределах одного здания, а базы данных хранятся и обрабатываются в Центре обработки данных администрации области и иных организациях, расположенных на территории Российской Федерации, – ЛВС «УО», ЛВС «Контингент».

1.8. Базы данных информации, с использованием которых осуществляются сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение) персональных данных граждан Российской Федерации, находятся на территории Российской Федерации.

1.9. Ввод персональных данных в ИС и вывод данных из ИС осуществляются с использованием бумажных и электронных носителей

информации. В качестве электронных носителей информации используются учетные съемные носители информации и оптические диски. Доступ к ИСПДн ограничен перечнем государственных гражданских служащих или работников Управления.

1.10. Передача персональных данных в другие организации и в территориальные органы федеральных органов исполнительной власти по сетям общего пользования и (или) сети «Интернет» осуществляется с использованием сертифицированных шифровальных (криптографических) средств защиты информации (далее - СКЗИ).

1.11. Контролируемой зоной ИС является части первого и второго этажей в двухэтажном административном здании по адресу г. Тамбов, ул. Советская, д. 108. В пределах контролируемой зоны находятся рабочие места пользователей, серверы, сетевое и телекоммуникационное оборудование ИС. Помещение серверной располагается на цокольном этаже здания и представляет собой изолированное помещение, оборудованное охранно-пожарной сигнализацией, дверь с механическим замком и средством опечатывания. Круг лиц, имеющих право доступа в помещение серверной, определен.

1.12. В административном здании Управления:

организуется пропускной режим;

исключается неконтролируемое пребывание посторонних лиц и неконтролируемое перемещение (вынос за пределы здания) компьютеров и оргтехники;

помещения со средствами вычислительной техники оборудуются запирающимися дверями и опечатывающими устройствами;

дополнительно организовано видеонаблюдение в коридорах, вестибюлях и холлах.

1.13. Защита персональных данных в ИС Управления и сетях общего пользования, подключаемых к сети «Интернет», обеспечивается средствами защиты информации (далее - СЗИ):

СЗИ от несанкционированного доступа, сертифицированными ФСТЭК России, не ниже 4 уровня контроля отсутствия недеklarированных возможностей (далее - НДВ);

средствами антивирусной защиты, сертифицированными ФСТЭК России, не ниже 4 класса;

межсетевыми экранами, сертифицированными ФСТЭК России, не ниже 3 класса;

СКЗИ, формирующими виртуальные частные сети (VPN), сертифицированными ФСБ России по классу КС 1 и выше;

системами обнаружения вторжения не ниже 4 класса;

средством государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

## 2. Характеристики безопасности информационных систем персональных данных

2.1. Основными свойствами безопасности информации являются:

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

целостность - состояние защищенности информации, характеризуемое способностью ИС 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.

2.2. 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 ИС, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

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

2.4. Для ИСПДн Управления актуальны угрозы безопасности персональных данных третьего типа, не связанные с наличием НДВ в системном и прикладном программном обеспечении (далее - ПО), используемом в ИС.

### 3. Применение средств криптографической защиты информации в информационных системах персональных данных

3.1. Актуальность применения в ИСПДн Управления СКЗИ определяется необходимостью защиты персональных данных, в том числе при информационном обмене по сетям связи общего пользования и (или) сети «Интернет».

3.2. СКЗИ предназначены для защиты информации от действий со стороны лиц, не имеющих право доступа к этой информации.

3.3. В целях исключения возможности несанкционированного доступа потенциального нарушителя к ключевой информации СКЗИ в Управлении принимаются организационно-технические меры.

3.4. При эксплуатации СКЗИ соблюдаются требования эксплуатационно-технической документации на СКЗИ и требования действующих нормативных правовых актов в области реализации и эксплуатации СКЗИ.

3.5. Для обеспечения безопасности персональных данных при их обработке в ИСПДн используются СКЗИ, прошедшие в установленном порядке процедуру оценки соответствия.

3.6. Объектами защиты в ИСПДн являются:

персональные данные;

средства криптографической защиты информации;

среда функционирования СКЗИ (далее – СФ);

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

документы, дела, журналы, картотеки, издания, технические документы, рабочие материалы и т. п., в которых отражена защищаемая информация, относящаяся к ИСПДн и их криптографической защите, включая документацию на СКЗИ и на технические и программные компоненты среды функционирования СКЗИ;

носители защищаемой информации, используемые в ИС 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 ИС, имеющие отношение к криптографической защите персональных данных.

3.7. Реализация угроз безопасности персональных данных, обрабатываемых в ИСПДн, определяется возможностями источников атак. На основании исходных данных об объектах защиты и источниках атак в таблице 1 для Управления определены обобщенные возможности источников атак.

| Обобщенные возможности источников атак  | Да/Нет |
|---|--------|
| 1   | 2      |
| 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 | Да     |
| 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    |

3.8. В соответствии с обобщенными возможностями источников атак (таблица 1) определены две актуальные уточнённые возможности нарушителей и направления атак (соответствующие актуальные угрозы для ИС) (таблица 2).

| Уточнённые возможности нарушителей и направления атак (соответствующие актуальные угрозы) | Актуальность использования (применения) для построения и реализации атак | Обоснование отсутствия  |
|---|--|---|
| 1   | 2  | 3   |
| 1. Проведение атаки при нахождении в пределах контролируемой зоны                         | Неактуально  | <p>Проводятся работы по подбору персонала; 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 надежными замками, обеспечено постоянное закрытие дверей помещений на замок, и их открытие осуществляется только для санкционированного прохода;</p> <p>утверждены правила доступа в помещения, где располагаются СКЗИ, в рабочее и нерабочее время, а также в нештатных ситуациях;</p> <p>утвержден перечень лиц, имеющих право доступа в помещения, где располагаются СКЗИ;</p> <p>осуществляется разграничение и контроль доступа пользователей к защищаемым ресурсам;</p> <p>осуществляется регистрация и учет действий пользователей с ПДн;</p> <p>осуществляется контроль целостности средств защиты;</p> <p>на АРМ и серверах, на которых установлены СКЗИ, используются сертифицированные СЗИ от</p> |

| 1  | 2           | 3   |
|--|-------------|---|
|  |             | несанкционированного доступа (далее - НСД);<br>используются сертифицированные средства антивирусной защиты  |
| 2. Проведение атак на этапе эксплуатации СКЗИ на следующие объекты:<br>документацию на СКЗИ и компоненты СФ;<br>помещения, в которых находится совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе средств вычислительной техники (далее - СВТ) и СФ  | Неактуально | Проводятся работы по подбору персонала; документация на СКЗИ хранится у ответственного за СКЗИ в металлическом сейфе;<br>помещения, в которых располагаются документация на СКЗИ, СКЗИ и компоненты СФ, оснащены входными дверьми с надежными замками, обеспечено постоянное закрытие дверей помещений на замок, и их открытие осуществляется только для санкционированного прохода;<br>утвержден перечень лиц, имеющих право доступа в помещения |
| 3. Получение в рамках предоставленных полномочий, а также в результате наблюдений следующей информации:<br>сведений о физических мерах защиты объектов, в которых размещены ресурсы информационной системы;<br>сведений о мерах по обеспечению контролируемой зоны объектов, в которых размещены ресурсы информационной системы;<br>сведений о мерах по разграничению доступа в помещения, в которых находятся СВТ, на которых реализованы СКЗИ и СФ | Актуально   |   |
| 4. Использование штатных средств ИСПДн, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и   | Актуально   |   |



| 1  | 2           | 3  |
|--|-------------|--|
| направленными на предотвращение и пресечение несанкционированных действий  |             |  |
| 5. Физический доступ к СВТ, на которых реализованы СКЗИ и СФ   | Неактуально | 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  |
| 6. 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; 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  |
| 7. 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 НДВ прикладного ПО                   | 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; 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; |

| 1   | 2           | 3   |
|---|-------------|---|
|   |             | осуществляется регистрация и учет действий пользователей;<br>на АРМ и серверах, на которых установлены СКЗИ: используются сертифицированные СЗИ от НСД; используются сертифицированные средства антивирусной защиты   |
| 8. Проведение лабораторных исследований СКЗИ, используемых вне контролируемой зоны, ограниченными мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий   | Неактуально | Не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности;<br>высокая стоимость и сложность подготовки реализации возможности  |
| 9. Проведение работ по созданию способов и средств атак в научно-исследовательских центрах, специализирующихся в области разработки и анализа СКЗИ и СФ, в том числе с использованием исходных текстов входящего в СФ прикладного ПО, 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;<br>высокая стоимость и сложность подготовки реализации возможности  |
| 10. Создание способов, подготовка и проведение атак с привлечением специалистов в области использования для реализации атак НДВ системного ПО   | Неактуально | Не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности;<br>высокая стоимость и сложность подготовки реализации возможности;<br>проводятся работы по подбору персонала; помещения, в которых располагаются СКЗИ и СФ, оснащены входными дверьми с замками, обеспечивается постоянное закрытие дверей помещений на замок и их |

| 1  | 2           | 3  |
|--|-------------|--|
|  |             | открытие только для санкционированного прохода;<br>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;<br>осуществляется регистрация и учет действий пользователей;<br>на АРМ и серверах, на которых установлены СКЗИ, используются сертифицированные СЗИ от НСД; используются сертифицированные средства антивирусной защиты |
| 11. 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   |
| 12. 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   |

#### 4. Определение актуальных угроз безопасности персональных данных в информационных системах персональных данных

4.1. На основе проведенного анализа банка данных угроз безопасности информации ([www.bdu.fstec.ru](http://www.bdu.fstec.ru)) с учётом структурно-функциональных характеристик типовых ИС, а также применяемых в них информационных технологий и особенностей функционирования, в ИС Управления могут быть актуальны следующие угрозы безопасности ИСПДн:

- УБИ.3 Угроза анализа криптографических алгоритмов и их реализации;
- УБИ.4 Угроза аппаратного сброса пароля BIOS;
- УБИ.6 Угроза внедрения кода или данных;
- УБИ.7 Угроза воздействия на программы с высокими привилегиями;
- УБИ.8 Угроза восстановления аутентификационной информации;
- УБИ.9 Угроза восстановления предыдущей уязвимой версии BIOS;
- УБИ.12 Угроза деструктивного изменения конфигурации/среды окружения программ;

- УБИ.13 Угроза деструктивного использования декларируемого функционала BIOS;
- УБИ.14 Угроза длительного удержания вычислительных ресурсов пользователями;
- УБИ.15 Угроза доступа к защищаемым файлам с использованием обходного пути;
- УБИ.16 Угроза доступа к локальным файлам сервера при помощи URL;
- УБИ.17 Угроза доступа/перехвата/изменения HTTP cookies;
- УБИ.18 Угроза загрузки нештатной операционной системы;
- УБИ.19 Угроза заражения DNS-кеша;
- УБИ.22 Угроза избыточного выделения оперативной памяти;
- УБИ.23 Угроза изменения компонентов системы;
- УБИ.25 Угроза изменения системных и глобальных переменных;
- УБИ.26 Угроза искажения XML-схемы;
- УБИ.27 Угроза искажения вводимой и выводимой на периферийные устройства информации;
- УБИ.28 Угроза использования альтернативных путей доступа к ресурсам;
- УБИ.30 Угроза использования информации идентификации/аутентификации, заданной по умолчанию;
- УБИ.31 Угроза использования механизмов авторизации для повышения привилегий;
- УБИ.32 Угроза использования поддельных цифровых подписей BIOS;
- УБИ.33 Угроза использования слабостей кодирования входных данных;
- УБИ.34 Угроза использования слабостей протоколов сетевого/ локального обмена данными;
- УБИ.36 Угроза исследования механизмов работы программы;
- УБИ.37 Угроза исследования приложения через отчёты об ошибках;
- УБИ.39 Угроза исчерпания запаса ключей, необходимых для обновления BIOS;
- УБИ.41 Угроза межсайтового скриптинга;
- УБИ.42 Угроза межсайтовой подделки запроса;
- УБИ.45 Угроза нарушения изоляции среды исполнения BIOS;
- УБИ.49 Угроза нарушения целостности данных кеша;
- УБИ.51 Угроза невозможности восстановления сессии работы на ПЭВМ при выводе из промежуточных состояний питания;
- УБИ.53 Угроза невозможности управления правами пользователей BIOS;
- УБИ.59 Угроза неконтролируемого роста числа зарезервированных вычислительных ресурсов;
- УБИ.62 Угроза некорректного использования прозрачного прокси-сервера за счёт плагинов браузера;
- УБИ.63 Угроза некорректного использования функционала программного обеспечения;
- УБИ.67 Угроза неправомерного ознакомления с защищаемой информацией;
- УБИ.68 Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением;
- УБИ.69 Угроза неправомерных действий в каналах связи;

УБИ.71 Угроза несанкционированного восстановления удалённой защищаемой информации;

УБИ.72 Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS;

УБИ.74 Угроза несанкционированного доступа к аутентификационной информации;

УБИ.86 Угроза несанкционированного изменения аутентификационной информации;

УБИ.87 Угроза несанкционированного использования привилегированных функций BIOS;

УБИ.88 Угроза несанкционированного копирования защищаемой информации;

УБИ.89 Угроза несанкционированного редактирования реестра;

УБИ.90 Угроза несанкционированного создания учётной записи пользователя;

УБИ.91 Угроза несанкционированного удаления защищаемой информации;

УБИ.93 Угроза несанкционированного управления буфером;

УБИ.94 Угроза несанкционированного управления синхронизацией и состоянием;

УБИ.95 Угроза несанкционированного управления указателями;

УБИ.98 Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб;

УБИ.99 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.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.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.167 Угроза заражения компьютера при посещении неблагонадёжных сайтов;
- УБИ.168 Угроза «кражи» учётной записи доступа к сетевым сервисам;
- 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 скрытой регистрации вредоносной программной учетных записей администраторов;

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

УБИ.203 Угроза утечки информации с не подключенных 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.

4.2. Угрозами безопасности персональных данных при их обработке с использованием СКЗИ являются:

4.2.1. создание способов, подготовка и проведение атак без привлечения специалистов в области разработки и анализа СКЗИ;

4.2.2. создание способов, подготовка и проведение атак на различных этапах жизненного цикла СКЗИ. К этапам жизненного цикла СКЗИ относятся: разработка (модернизация) указанных средств, их производство, хранение, транспортировка, ввод в эксплуатацию (пусконаладочные работы), эксплуатация;

4.2.3. проведение атаки, находясь вне пространства, в пределах которого осуществляется контроль за пребыванием и действиями лиц и (или) транспортных средств (далее - контролируемая зона). Границей контролируемой зоны может быть: периметр охраняемой территории организации, ограждающие конструкции охраняемого здания, охраняемой части здания, выделенного помещения;

4.2.4. проведение на этапах разработки (модернизации), производства, хранения, транспортировки СКЗИ и этапе ввода в эксплуатацию СКЗИ (пусконаладочные работы) следующих атак:

внесение несанкционированных изменений в СКЗИ и (или) в компоненты аппаратных и программных средств, совместно с которыми штатно функционируют СКЗИ, в совокупности представляющие среду функционирования СКЗИ, которые способны повлиять на выполнение предъявляемых к СКЗИ требований, в том числе с использованием вредоносных программ;

4.2.5. проведение атак на этапе эксплуатации СКЗИ на:

персональные данные;

ключевую, аутентифицирующую и парольную информацию СКЗИ;

программные компоненты СКЗИ;

аппаратные компоненты СКЗИ;

программные компоненты СФ, включая программное обеспечение BIOS;

аппаратные компоненты СФ;

данные, передаваемые по каналам связи;

4.2.6. получение из находящихся в свободном доступе источников (включая информационно-телекоммуникационные сети, доступ к которым не ограничен определенным кругом лиц, в том числе информационно-телекоммуникационную сеть «Интернет») информации об ИС, в которой используется СКЗИ. При этом может быть получена следующая информация:

общие сведения об ИС, в которой используется СКЗИ (назначение, состав, оператор, объекты, в которых размещены ресурсы ИС);

сведения об информационных технологиях, базах данных, АС, ПО, используемых в ИС совместно с СКЗИ, за исключением сведений, содержащихся только в конструкторской документации на информационные технологии, базы данных, АС, ПО, используемые в ИС совместно с СКЗИ;

содержание находящейся в свободном доступе документации на аппаратные и программные компоненты СКЗИ и СФ;

общие сведения о защищаемой информации, используемой в процессе эксплуатации СКЗИ;

сведения о каналах связи, по которым передаются защищаемые СКЗИ персональные данные (далее - канал связи);

4.2.7. применение находящихся в свободном доступе или используемых за пределами контролируемой зоны АС и ПО, включая аппаратные и программные компоненты СКЗИ и СФ;

4.2.8. получение в рамках предоставленных полномочий, а также в результате наблюдений следующей информации:



сведений о физических мерах защиты объектов, в которых размещены ресурсы ИС;

сведений о мерах по обеспечению контролируемой зоны объектов, в которых размещены ресурсы ИС;

сведений о мерах по разграничению доступа в помещения, в которых находятся СВТ, на которых реализованы СКЗИ и СФ;

4.2.9. использование штатных средств, ограниченное мерами, реализованными в ИС, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий.