

ПОЛОЖЕНИЕ

об определении угроз безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных в ТОГБПОУ «Уваровский политехнический колледж»

1. Общие положения

1.1 «Положение об определении угроз безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных в ТОГБПОУ «Уваровский политехнический колледж»» (далее – Положение) разработано в соответствии с Федеральным законом 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, и Банком данных угроз безопасности информации, размещенным на официальном сайте ФСТЭК России.

2. Характеристика безопасности информационных систем персональных данных.

2.1. Основными свойствами безопасности информационных систем ТОГБПОУ Положение определяет перечень актуальных угроз безопасности персональных данных при их обработке в информационной системе персональных данных (далее - ИСПДн).
Общее описание информационных систем персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности
Угрозы 3-го типа актуальны для информационной системы, если для нее актуальны угрозы, не связанные с наличием недокументированных (недекларированных)

возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

Необходимость обеспечения 4-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает общедоступные персональные данные;

б) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает иные категории персональных данных сотрудников оператора или иные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

Возможны три случая:

1. ИСПДн имеют сходную структуру, однотипны. В дальнейшем такие системы будут именоваться "однотипными системами". Примером может служить описание федеральным органом исполнительной власти угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах территориальных подразделений этого органа.

В указанном случае целесообразно в проекте НПА указывать наиболее полную информацию об ИСПДн и среде их функционирования.

Следует отметить, что в зависимости от вида деятельности, для которого разрабатывается НПА, в проекте НПА может выделяться несколько категорий однотипных систем.

2. ИСПДн разноплановы, имеют различную структуру и могут содержать различные категории персональных данных. В дальнейшем такие системы будут именоваться "разноплановыми системами".

В этом случае целесообразно перечислить имеющиеся системы и указать общую информацию о возможной среде их функционирования, если такая информация имеется.

3. Эксплуатируются как одна или несколько однотипных, так и разноплановые системы.

В этом случае целесообразно указывать наиболее полную информацию о категориях однотипных систем и среде их функционирования, а также общую информацию о разноплановых системах и среде их функционирования. При описании информационных систем следует, в частности, указывать:
- общие сведения об информационных системах (назначение, оператор (уполномоченное лицо):

В соответствии с проведенным анализом комиссия сделала вывод о том, что ИСПДн АРМ-203 имеет сходную структуру, то есть относится к «однотипным системам»; обрабатывает общедоступные персональные данные; для нее актуальны угрозы, не связанные с наличием недокументированных (не декларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе, поэтому для нее актуальны угрозы 3-го типа. Необходимость обеспечения 4-го уровня защищенности персональных данных при их обработке в информационной системе.

- объем и содержание персональных данных, обрабатываемых в информационных системах:

Объем обрабатываемых персональных данных менее 1000 субъектов персональных данных.

- характеристики безопасности (конфиденциальность, целостность, доступность, подлинность), которые необходимо обеспечивать для обрабатываемых персональных данных.

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, характеризующееся 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.

При описании однотипных систем следует также указывать:

- объекты, в которых размещены ресурсы информационных систем.

4. 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.
- физические меры защиты объектов, в которых размещены ресурсы информационных систем;
 - меры по обеспечению контролируемой зоны;
- типы информационных систем (например, единая информационная система для всех обрабатываемых персональных данных или совокупность изолированных и (или) взаимосвязанных информационных подсистем. В последнем случае необходимо приводить описание взаимосвязей между подсистемами и указывать объем и содержание персональных данных, обрабатываемых в каждой подсистеме);
- наличие или отсутствие информационного взаимодействия каждой подсистемы информационной системы или информационной системы в целом с другими информационными системами, а также наличие факта передачи персональных данных между ними;
- используемые в каждой подсистеме или в информационной системе в целом каналы (линии) связи, включая кабельные системы, и меры по ограничению несанкционированного доступа к защищаемой информации, передаваемой по этим каналам (линиям) связи, с указанием каналов (линий) связи, в которых невозможен несанкционированный доступ к передаваемой по ним защищаемой информации, и реализуемые для обеспечения этого качества меры;
- носители защищаемой информации, используемые в каждой подсистеме информационной системы или в информационной системе в целом (за исключением каналов (линий) связи).

Таблица 1

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

3.1. 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).

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	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; утверждены правила доступа в помещения, где располагаются СКЗИ, в рабочее и нерабочее время, а также в нестандартных 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 и серверах, на которых установлены СКЗИ, используются сертифицированные СЗИ от несанкционированного доступа (далее - НСД); используются сертифицированные средства антивирусной защиты
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 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; 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; утвержден перечень лиц, имеющих право доступа в помещения
3. Получение в рамках предоставленных полномочий, а также в результате наблюдений следующей информации: сведений о физических мерах защиты объектов, в которых размещены ресурсы информационной	Актуально	

<p>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</p>		
<p>4. Использование штатных средств ИСПДн, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий</p>	<p>Актуально</p>	
<p>5. Физический доступ к СВТ, на которых реализованы СКЗИ и СФ</p>	<p>Неактуально</p>	<p>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</p>
<p>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</p>	<p>Неактуально</p>	<p>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</p>

<p>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</p>	<p>Неактуально</p>	<p>Не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности;</p> <p>высокая стоимость и сложность подготовки реализации возможности;</p> <p>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;</p> <p>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;</p> <p>осуществляется регистрация и учет действий пользователей; на АРМ и серверах, на которых установлены СКЗИ: используются сертифицированные СЗИ от НСД; используются сертифицированные средства антивирусной защиты</p>
<p>8. 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</p>	<p>Неактуально</p>	<p>Не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности;</p> <p>высокая стоимость и сложность подготовки реализации возможности</p>

<p>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</p>	<p>Неактуально</p>	<p>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</p>
<p>10. Создание способов, подготовка и проведение атак с привлечением специалистов в области использования для реализации атак НДВ системного ПО</p>	<p>Неактуально</p>	<p>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; осуществляется регистрация и учет действий пользователей; на АРМ и серверах, на которых установлены СКЗИ, используются сертифицированные СЗИ от НСД; используются сертифицированные средства антивирусной защиты</p>
<p>11. Возможность располагать сведениями, содержащимися в конструкторской документации на аппаратные и программные компоненты СФ</p>	<p>Неактуально</p>	<p>Не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности</p>

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
--	-------------	--

1. Определение актуальных угроз безопасности персональных данных в информационных системах персональных данных

4.1. На основе проведенного анализа банка данных угроз безопасности информации с учётом структурно-функциональных характеристик типовых ИС, а также применяемых в них информационных технологий и особенностей функционирования, в ИС органов власти 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 декларированного 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 HTTPcookies;
- 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.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 кэша;
- 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.1 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 Угрозанесанкционированного 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.112 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.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 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.