МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ
ДОПОЛНИТЕЛЬНОГО ОБРАЗОВАНИЯ
СПОРТИВНАЯ ШКОЛА № 5 ГОРОДА СТАВРОПОЛЯ

ПРИКАЗ

03.06.2025 г. Ставрополь № 102-ОД

Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных в МБУ ДО СШ № 5 г. Ставрополь

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 МБУ ДО СШ № 5 г. Ставрополя

ПРИКАЗЫВАЮ:

1. Утвердить и ввести в действие Положение об угрозах безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных в МБУ ДО СШ № 5 г. Ставрополя согласно Приложению.
2. Контроль за исполнением настоящего Приказа оставляю за собой.

Директор Е.И. Пащенко

Исп. Павлова Т.В.
В дело № _____
_____ _____ 2025

Приложение
к приказу МБУ ДО № 5
г. Ставрополя
от 03.06.2025 г. № 102 – ОД

Положение об угрозах безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных в МБУ ДО СШ № 5 г. Ставрополя

1. Общие положения

1.1. Угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных в МБУ ДО СШ № 5 г. Ставрополя (далее - Актуальные угрозы безопасности ИСПДн, Учреждение), 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», приказами 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» и от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», приказом Федеральной службы безопасности Российской Федерации (далее - ФСБ России) от10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности», 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 (ШрДМи.Шес.ги).

1.2. Актуальные угрозы безопасности ИСПДн содержат перечень актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (далее - ИСПДн) в Учреждении.

1.3. Актуальные угрозы безопасности ИСПДн подлежат адаптации в ходе разработки администрацией Учреждения частных моделей угроз безопасности персональных данных для каждой информационной системы (далее - ИС).

1.4. 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.

1.5. В зависимости от конкретного объекта информатизации ИС Учреждения делятся на два вида:

локальная ИС, рабочие места и базы данных которой расположены в пределах одного здания;

распределенная ИС, рабочие места которой расположены в пределах одного здания, а базы данных хранятся и обрабатываются в Центре обработки данных администрации области.

1.6. 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.

1.7. Ввод персональных данных в ИС и вывод данных из ИС осуществляются с использованием бумажных и электронных носителей информации. В качестве электронных носителей информации используются учтенные съемные носители информации и оптические диски.

1.8. 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).

1.9. Контролируемой зоной ИС являются административное здание Учреждения. В пределах контролируемой зоны находятся рабочие места пользователей. Вне контролируемой зоны находятся линии передачи данных и телекоммуникационное оборудование, используемое для

информационного обмена по сетям общего пользования и (или) сети «Интернет».

1.10. В административном здание Учреждения:

должен быть организован пропускной режим;

должно быть исключено неконтролируемое пребывание посторонних лиц и неконтролируемое перемещение (вынос за пределы здания) компьютеров и оргтехники;

помещения со средствами вычислительной техники должны быть оборудованы запирающимися дверями и опечатывающими устройствами;

дополнительно может быть организовано видеонаблюдение в коридорах, вестибюлях и холлах.

1.11. Защита персональных данных в ИС Учреждении 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 недекларированных 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 (УРЫ), 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. Характеристики безопасности информационных систем персональных данных

1.12. 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.

1.13. 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.

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

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

2. Применение средств криптографической защиты информации в информационных системах персональных данных

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

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

2.3. Принятыми организационно-техническими мерами в Учреждении должна быть исключена возможность несанкционированного доступа потенциального нарушителя к ключевой информации СКЗИ.

2.4. При эксплуатации СКЗИ должны соблюдаться требования эксплуатационно-технической документации на СКЗИ и требования действующих нормативных правовых актов в области реализации и эксплуатации СКЗИ.

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

2.6. 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.

2.7. 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 Учреждения определены обобщенные возможности источников атак.

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	Нет

2.8. 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).

Таблица 2

Уточнённые возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
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 нештатных ситуациях; утвержден перечень лиц, имеющих право доступа в помещения, где располагаются СКЗИ; осуществляется разграничение и контроль доступа пользователей к защищаемым ресурсам; осуществляется регистрация и учет действий пользователей с ПДн; осуществляется контроль целостности средств защиты; на АРМ 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	Актуально	

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		
4. Использование штатных средств ИСПДн, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий	Актуально	
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,	Неактуально	Не осуществляется обработка сведений,

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		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
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	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
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	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

исходных текстов входящего в СФ прикладного ПО, непосредственно использующего вызовы программных функций СКЗИ		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
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; 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
11. Возможность располагать сведениями, содержащимися в конструкторской документации на аппаратные и	Неактуально	Не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности

программные компоненты СФ		
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

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

3.1. 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 Учреждения могут быть актуальны следующие угрозы безопасности ИСПДн:

УБИ.3 Угроза анализа криптографических алгоритмов и их реализации;

УБИ.4 Угроза аппаратного сброса пароля B108;

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 B108;

УБИ.12 Угроза деструктивного изменения конфигурации/среды окружения программ;

УБИ.13 Угроза деструктивного использования декларированного функционала ВЮ8;

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 ШЪ;

УБИ.17 Угроза доступа/перехвата/изменения HTTP соокшз;

УБИ. 18 Угроза загрузки нештатной операционной системы;

УБИ. 19 Угроза заражения БШ-кеша;

УБИ.22 Угроза избыточного выделения оперативной памяти;

УБИ.23 Угроза изменения компонентов системы;

УБИ.26 Угроза искажения ХМЬ-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 B108;

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 B108;

УБИ.41 Угроза межсайтового скриптинга;

УБИ.42 Угроза межсайтовой подделки запроса;

УБИ.45 Угроза нарушения изоляции среды исполнения B108;

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 B108;

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 B108;

УБИ.74 Угроза несанкционированного доступа к аутентификационной информации;

УБИ.86 Угроза несанкционированного изменения аутентификационной информации;

УБИ.87 Угроза несанкционированного использования привилегированных функций B108;

УБИ.88 Угроза несанкционированного копирования защищаемой информации;

УБИ.89 Угроза несанкционированного редактирования реестра;

УБИ.90 Угроза несанкционированногосоздания 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 некорректнонастроенных 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 В108;

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 В108;

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 БЮ8;

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 БЮ8;

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 ботсети;

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 соокш;

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.

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

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

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;

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;

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;

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 БЮ8;

аппаратные компоненты СФ;

данные, передаваемые по каналам связи;

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);

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

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;

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