Утверждено приказом
директора МБУК «ЦБС»
от 04.03.2024 №36

МОДЕЛЬ УГРОЗ

безопасности персональных данных при их обработке в информационных системах
Муниципального бюджетного учреждения культуры
«Централизованная библиотечная система»

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

АРМ - автоматизированное рабочее место

ИСПДн - информационная система персональных данных

КЗ - контролируемая зона

НДВ - недекларированные возможности

НСД - несанкционированный доступ

ОБПДн - обеспечение безопасности персональных данных

ОС - операционная система

ПДн - персональные данные

ПО - программное обеспечение

СВТ - средство вычислительной техники

СЗИ - средство защиты информации

СКЗИ – средство криптографической защиты информации

ВТСС - вспомогательные технические средства и системы

ТСОИ - технические средства обработки информации

УБПДн - угрозы безопасности персональных данных

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

В настоящем документе используются следующие термины и их определения:

Автоматизированная система - система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Аутентификация отправителя данных - подтверждение того, что отправитель полученных данных соответствует заявленному.

Безопасность персональных данных - состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

Блокирование персональных данных - временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи.

Вирус (компьютерный, программный) - исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Вредоносная программа - программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

Доступ в операционную среду компьютера (информационной системы персональных данных) - получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ.

Доступ к информации - возможность получения информации и ее использования.

Закладочное устройство - элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации).

Защищаемая информация - информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Идентификация - присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информационная система персональных данных - это информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

Нарушитель безопасности персональных данных - физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных.

Недекларированные возможности - функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Несанкционированный доступ (несанкционированные действия) - доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по своим функциональному предназначению и техническим характеристикам.

Носитель информации - физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Обработка персональных данных - действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

Персональные данные - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Пользователь информационной системы персональных данных - лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

Правила разграничения доступа - совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Программная закладка - скрытно внесенный в программное обеспечение функциональный объект, который при определенных условиях способен обеспечить несанкционированное программное воздействие. Программная закладка может быть реализована в виде вредоносной программы или программного кода.

Программное (программно-математическое) воздействие - несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

Технические средства информационной системы персональных данных - средства

вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации.

Угрозы безопасности персональных данных - совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

Уничтожение персональных данных - действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

Утечка (защищаемой) информации по техническим каналам - неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

Уязвимость - некая слабость, которую можно использовать для нарушения системы или содержащейся в ней информации.

1.ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Настоящий документ разработан в соответствии с требованием п. 7 Требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства Российской Федерации от 1 ноября 2012 г. №1119.

Определение нарушителей и угроз безопасности персональных данных приих обработке и последующее формирование на их основе модели угроз и нарушителей является одним из необходимых мероприятий по обеспечению безопасности ПДн в информационных системах.

Выявление и учет угроз безопасности ПДн в конкретных условиях составляют основу для планирования и осуществления мероприятий, направленных на обеспечение безопасности ПДн при их обработке в информационных системах ПДн.

Настоящая Модель угроз и нарушителей учитывает требования следующих законодательных актов и нормативно-методических документов:

- Федеральный закон №152-ФЗ от 27 июля 2006 года «О персональных данных»; постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Приказ ФСТЭК Российской Федерации № 21 от 18.02.2013 «Состав и содержание технических и организационных мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Выписка ФСТЭК Российской Федерации 15.02.2008 «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных

данных»;

- Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утверждена зам. директора ФСТЭК России 14.02.2008;

1.2. Актуальные угрозы безопасности ИСПДн содержат перечень актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (далее - ИСПДн) МБУК «Централизованная библиотечная система» (далее – ЦБС).

1.2.1. Угрозы 1-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в информационной системе.

1.2.2. Угрозы 2-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе.

1.2.3. 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.

1.3. Определение типа угроз безопасности персональных данных, актуальных для информационной системы, производится оператором с учетом оценки возможного вреда, проведенной во исполнение п.5 ч. 1 ст.18.1 ФЗ №152 "О персональных данных", и в соответствии с нормативными правовыми актами, принятыми во исполнение ч.5 ст. 19 данного закона.

1.3. Актуальные угрозы безопасности ИСПДн подлежат адаптации в ходе разработки ЦБС частной модели угроз безопасности персональных данных (далее - ИС).

1.4. В 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. Информационная система ЦБС относится к локальной информационной системе, рабочие места и базы данных которой расположены в пределах одного здания – Центральной городской библиотеки (далее – ЦГБ).

1.7. 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.

1.8. Ввод персональных данных в ИС и вывод данных из ИС осуществляются с использованием электронных носителей информации. В качестве электронных носителей информации используются учтенные съемные носители информации. Доступ к ИСПДн ограничен перечнем лиц, имеющих самостоятельный доступ к штатным средствам объектов вычислительной техники ЦГБ, являющейся владельцем ИС.

1.9. 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).

1.10. Контролируемой зоной ИС является здание ЦГБ. В пределах контролируемой зоны находятся

рабочие места пользователей, серверы, сетевое и телекоммуникационное оборудование ИС. Вне контролируемой зоны находятся линии передачи данных и телекоммуникационное оборудование, используемое для информационного обмена по сетям общего пользования и сети Интернет.

1.11. В здании ЦГБ:

- исключено неконтролируемое пребывание посторонних лиц и неконтролируемое перемещение (вынос за пределы здания) компьютеров и оргтехники;
- помещения со средствами вычислительной техники (сервера) должны быть оборудованы запирающимися дверями и опечатывающими устройствами;
- дополнительно должно быть организовано видеонаблюдение в коридорах, вестибюлях и холлах.

1.12. Защита персональных данных в ИС ЦБС и сетях общего пользования, подключаемых к сети Интернет, обеспечивается средствами защиты информации (далее - СЗИ).

2. ХАРАКТЕРИСТИКА 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 даннымпри их обработке в ИС, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

3. СОСТАВ ПО ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Для данной ИСПДн в целом необходимо обеспечить следующие характеристики безопасности информации - конфиденциальность, целостность.

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

Целостность информации - способность средства вычислительной техники или информационной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного воздействий на нее в процессе обработки или хранения.

В ЦБС обработка персональных данных осуществляется в многопользовательском режиме с разграничением прав доступа.

Режим обработки предусматривает следующие действия с персональными данными: сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение

персональных данных. Все пользователи ИСПДн имеют собственные роли таблица №1

Таблица №1

Группа	Уровень доступа к ПДн	Разрешенные
Администратор ИСПДн	Обладает полной информацией о системном и прикладном программном обеспечении ИСПДн. Обладает полной информацией о технических средствах и конфигурации ИСПДн. Имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн. Обладает правами конфигурирования и административной настройки технических средств ИСПДн.	- сбор - систематизация - накопление - хранение - уточнение - использование - уничтожение
Работник ответственный за обработку ПДн в автоматизированном режиме	Обладает всеми необходимыми атрибутами и правами, обеспечивающими доступ ко всем ПДн – персональный логин и пароль	- сбор - хранение - уточнение - использование

Предоставление или прекращение доступа к ИСПДн осуществляется в соответствии с приказом о назначении на должность или приказом об увольнении.

4. КЛАССИФИКАЦИЯ УГРОЗ БЕЗОПАСНОСТИ

Перечень угроз, уязвимостей и технических каналов утечки информации сформирован в соответствии с требованиями руководящих документов ФСТЭК России.

Состав и содержание УБПДн определяется совокупностью условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к ПДн, обрабатываемым в ИСПДн ЦБС.

ИСПДн ЦБС представляет собой совокупность информационных и программноаппаратных элементов и их особенностей как объектов обеспечения безопасности. Основными элементами ИСПДн являются:

- персональные данные, обрабатываемые в ИСПДн;
- информационные технологии, как совокупность приемов, способов и методов применения средств вычислительной техники при обработке ПДн;
- технические средства ИСПДн, осуществляющие обработку ПДн (средства вычислительной техники (СВТ), информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн;
- программные средства (операционные системы, системы управления базами данных и т.п.);
- средства защиты информации (СЗИ), включая СКЗИ;
- вспомогательные технические средства и системы (технические средства и системы, их коммуникации, не предназначенные для обработки ПДн, но размещенные в помещениях, в которых расположены ИСПДн, такие как средства вычислительной техники, средства и системы охранной и пожарной сигнализации, средства и системы кондиционирования, средства электронной оргтехники и т.п.) (далее - ВТСС);
- документация на СКЗИ и на технические и программные компоненты ИСПДн;

- ключевая, аутентифицирующая и парольная информация;
- помещения, в которых находятся защищаемые ресурсы.

Возможности источников УБПДн обусловлены совокупностью методов и способов несанкционированного и (или) случайного доступа к ПДн, в результате которого возможно нарушение конфиденциальности (копирование, неправомерное распространение), целостности (уничтожение, изменение) и доступности (блокирование) ПДн.

Угроза безопасности ПДн реализуется в результате образования канала реализации УБПДн между источником угрозы и носителем (источником) ПДн, что создает необходимые условия для нарушения безопасности ПДн (несанкционированный или случайный доступ).

Основными элементами канала реализации УБПДн являются:

- источник УБПДн - субъект, материальный объект или физическое явление, создающие УБПДн;
- среда (путь) распространения ПДн или воздействий, в которой физическое поле, сигнал, данные или программы могут распространяться и воздействовать на защищаемые свойства (конфиденциальность, целостность, доступность) ПДн;
- носитель ПДн - физическое лицо или материальный объект, в том числе физическое поле, в котором ПДн находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Источниками угроз НСД в ИСПДн могут быть:

- нарушитель;
- носитель вредоносной программы.

По признаку принадлежности к ИСПДн все нарушители делятся на две группы:

- внешние нарушители - физические лица, не имеющие права пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИСПДн;
- внутренние нарушители - физические лица, имеющие право пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИСПДн.

Система разграничения доступа ИСПДн обеспечивает разграничение прав пользователей на доступ к информационным, программным, аппаратным и другим ресурсам ИСПДн.

Носитель вредоносной программы – аппаратный элемент средств вычислительной техники из состава ИСПДн или ПО, выполняющее роль программного контейнера. В качестве ее носителя выступают: дискета; оптический диск; лазерный диск; флэш-память; внешний жесткий диск.

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

5. УРОВЕНЬ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Уровень защищенности при обработке ПДн в ИСПДн ЦБС установлен в соответствии с Постановлением Правительства РФ от 1 ноября 2012 г. N 1119 (п.12, 13).

12. 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.

13. Для обеспечения 4-го уровня защищенности персональных данных при их обработке в информационных системах необходимо выполнение следующих требований:

а) организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

б) обеспечение сохранности носителей персональных данных;

в) утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;

г) использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз.

6. ПРИМЕНЕНИЕ СРЕДСТВ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Актуальность применения в ИСПДн ЦБС 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 права доступа к этой информации.

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

3.4. При эксплуатации СКЗИ должны соблюдаться 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;
- информация, относящаяся к криптографической защите персональных данных, включая ключевую, парольную и аутентифицирующуюинформацию 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 ЦБС, определяется актуальными возможностями источников атак. На основании исходных данных об объектах защиты и источниках атак в таблице №2 для ЦГБ определены обобщенные возможности источников атак.

Таблица №2

№	Обобщенные возможности источников атак	Да/Нет
1	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак только за пределами контролируемой зоны	Да
2	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемойзоны, но без физического доступа к аппаратным средствам (далее - АС), на которых реализованы СКЗИ и среда их функционирования	Да

3.8. В соответствии с обобщенными возможностями источников атак (таблица №2) определены две актуальные уточнённые возможности нарушителей направления атак (соответствующие актуальные угрозы для ИС) (таблица №3).

Таблица №3

Уточнённые возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак
1. Получение в рамках предоставленных пол номочий, а также в результате наблюдений с ледующей информации: сведений о физичес ких мерах защиты объектов, в которых разме щены 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.	Актуально
2. Использование штатных средств ИСПДн, ограниченное мерами, реализованными в ин формационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий	Актуально

7. ОПЕРЕДЕЛЕНИЕ АКТУАЛЬНЫХ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

7.1. На основе проведенного анализа данных угроз безопасности информации с учётом структурно-функциональных характеристик типовых ИС, а также применяемых в них информационных технологий и особенностей функционирования, в ИС ЦБС могут быть актуальны следующие угрозы безопасности ИСПДн:

- Угроза анализа криптографических алгоритмов и их реализации;
- Угроза аппаратного сброса пароля BIOS;
- Угроза внедрения кода или данных;
- Угроза воздействия на программы с высокими привилегиями;
- Угроза восстановления аутентификационной информации;
- Угроза восстановления предыдущей уязвимой версии BIOS;
- Угроза деструктивного изменения конфигурации/среды окружения программ;
- Угроза деструктивного использования декларированного функционала BIOS;
- Угроза доступа к защищаемым файлам с использованием обходного пути;
- Угроза использования альтернативных путей доступа к ресурсам;
- Угроза использования информации идентификации/ аутентификации, заданной по умолчанию;
- Угроза использования поддельных цифровых подписей BIOS;
- Угроза некорректного использования функционала программного обеспечения;
- Угроза неправомерного ознакомления с защищаемой информацией;
- Угроза неправомерных действий в каналах связи;
- Угроза несанкционированного восстановления удалённой защищаемой информации;
- Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS;
- Угроза несанкционированного доступа к аутентификационной информации;
- Угроза несанкционированного изменения аутентификационной информации;
- Угроза несанкционированного использования привилегированных функций BIOS;
- Угроза несанкционированного копирования защищаемой информации;
- Угроза утечки информации за счет применения вредоносным программным обеспечением алгоритмов шифрования трафика;
- Угроза хищения аутентификационной информации из временных файлов cookie;
- Угроза скрытной регистрации вредоносной программной учетных записей администраторов;
- Угроза утечки пользовательских данных при использовании функций автоматического заполнения аутентификационной информации в браузере;
- Угроза утечки информации с неподключенных к сети Интернет компьютеров;
- Угроза несанкционированного изменения вредоносной программой значений параметров п рограммируемых логических контроллеров;
- Угроза нарушения работы компьютера и блокирования доступа к его данным из-за некорректной работы установленных на нем средств защиты.

7.2. Угрозами безопасности персональных данных при их обработке сиспользованием 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.