

**АДМИНИСТРАЦИЯ**

**МОНАСТЫРЩИНСКОГО СЕЛЬСКОГО ПОСЕЛЕНИЯ**

**БОГУЧАРСКОГО МУНИЦИПАЛЬНОГО РАЙОНА**

**ВОРОНЕЖСКОЙ ОБЛАСТИ**

**РАСПОРЯЖЕНИЕ**

от «24» сентября 2018 года № 41- р

 с.Монастырщина

**Об определении угроз безопасности**

 **персональных данных, актуальных**

**при обработке персональных данных**

**в информационных системах персональных**

**данных администрации Монастырщинского**

 **сельского поселения Богучарского**

**муниципального района**

В соответствии с пунктом 1 части 2 статьи 19 Федерального закона от 27.07.2006 № 152 – ФЗ «О персональных данных», Федеральным законом от 06.10.2003 № 131 - ФЗ «Об общих принципах организации местного самоуправления в Российской Фе­дерации», постановление правительства Воронежской области от 02.11.2017 года № 809 «Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных правительства Воронежской области, исполнительных органов государственной власти Воронежской области и подведомственных им организаций», Уставом Монастырщинского сельского поселения Богучарского муниципального района:

1.Утвердить угрозы безопасности персональных данных, актуальные при обработке данных в информационных системах персональных данных в администрации Монастырщинского сельского поселения Богучарского муниципального района, согласно приложению.

2. Контроль за исполнением настоящего распоряжения оставляю за собой.

Глава Монастырщинского сельского поселения Ю.Н.Сывороткин

Приложение

к распоряжению администрации

Монастырщинского сельского поселения

 Богучарского муниципального района

24.09.2018 № 41-р

**Угрозы безопасности персональных данных, актуальные при обработке**

**данных в информационных системах персональных данных в администрации Монастырщинского сельского поселения Богучарского муниципального района**

1. Общие положения

 Угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных администрации Монастырщинского сельского поселения Богучарского муниципального района (далее - Актуальные угрозы), определены в соответствии с частью 5 статьи 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

 Под угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия при их обработке в информационной системе персональных данных (нарушение конфиденциальности, целостности и доступности обрабатываемых персональных данных).

Для информационных систем персональных данных администрации Монастырщинского сельского поселения Богучарского муниципального района (далее - ИСПДн) целью защиты информации является обеспечение конфиденциальности, целостности и доступности обрабатываемых персональных данных.

* 1. В качестве источников угроз безопасности персональных данных могут выступать субъекты (физические лица, организации) или явления (техногенные аварии, стихийные бедствия, иные природные явления). При этом источники угроз могут быть следующих типов:

антропогенные источники (антропогенные угрозы);

техногенные источники (техногенные угрозы);

стихийные источники (угрозы стихийных бедствий, иных природных явлений).

Источниками антропогенных угроз безопасности персональных данных могут выступать лица, осуществляющие преднамеренные действия с целью доступа к персональным данным (воздействия на персональные данные), содержащимся в информационной системе, или нарушения функционирования информационной системы или обслуживающей ее инфраструктуры (преднамеренные угрозы безопасности персональных данных);

лица, имеющие доступ к информационной системе, не преднамеренные действия которых могут привести к нарушению безопасности персональных данных (непреднамеренные угрозы безопасности персональных данных).

Преднамеренные угрозы безопасности персональных данных могут быть реализованы за счет утечки персональных данных по техническим каналам (технические каналы утечки информации, обрабатываемой в технических средствах информационной системы, технические каналы перехвата информации при ее передаче по каналам (линиям) связи, технические каналы утечки акустической (речевой) информации) либо за счет несанкционированного доступа.

* 1. Настоящие Актуальные угрозы содержат перечень актуальных угроз безопасности персональных данных, которые могут быть реализованы в типовых ИСПДн, эксплуатируемых при осуществлении соответствующих видов деятельности, с учетом содержания персональных данных, характера и способов их обработки. Актуальные угрозы также содержат совокупность предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак для рассматриваемых типов ИСПДн, в случае применения в них для обеспечения безопасности персональных данных средств криптографической защиты информации (далее - СКЗИ).

Актуальные угрозы дополнительно устанавливают единый подход к определению угроз безопасности персональных данных, актуальных при обработке персональных данных в конкретных ИСПДн, и разработке на их основе частных моделей угроз безопасности персональных данных (далее - Частные модели угроз) для этих ИСПДн.

* 1. Настоящие Актуальные угрозы также распространяются на государственные информационные системы (далее — ГИС) Воронежской области, в которых осуществляется обработка персональных данных. Такие ГИС Воронежской области в рамках настоящего документа будут рассматриваться как ИСПДн.

В случае если в ГИС Воронежской области кроме персональных данных обрабатывается иная информация ограниченного доступа, не содержащая сведения, составляющие государственную тайну, то для определения угроз безопасности такой информации и разработки моделей угроз безопасности информации кроме настоящих Актуальных угроз должны дополнительно применяться нормативные правовые и методические документы ФСТЭК России и ФСБ России.

* 1. Актуальные угрозы разработаны с использованием следующих документов:

Федерального закона Российской Федерации от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

постановления Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»;

постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

постановления правительства Воронежской области от 18.11.2014 № 1024-ДСП «Об утверждении концепции защиты информации в Воронежской области»;

базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной заместителем директора ФСТЭК России 15.02.2008 (далее - Базовая модель угроз);

методики определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной заместителем директора ФСТЭК России 14.02.2008;

методических рекомендаций по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности, утвержденных руководством 8-го Центра ФСБ России 31.03.2015 № 149/7/2/6-432.

Настоящие Актуальные угрозы, а также угрозы безопасности персональных данных, актуальные при обработке персональных данных в ИСПДн, определяются по результатам оценки возможностей (потенциала) внешних и внутренних нарушителей, уровня исходной защищенности ИСПДн, анализа возможных способов реализации угроз безопасности персональных данных и последствий от нарушения свойств безопасности персональных данных (конфиденциальности, целостности, доступности).

* 1. Источником данных об угрозах безопасности информации, на основе которых определяются Актуальные угрозы, являются:

банк данных угроз безопасности информации ФСТЭК России (<http://bdu.fstec.ru>, далее - Банк данных угроз);

Базовая модель угроз.

В качестве источника данных об угрозах безопасности информации, актуальных при обработке персональных данных в ИСПДн, используются настоящие Актуальные угрозы.

Определение угроз безопасности персональных данных, актуальных при обработке персональных данных в ИСПДн, осуществляется администрацией Богучарского муниципального района, которая является оператором.

ИСПДн.

В администрации Монастырщинского сельского поселения Богучарского муниципального района актом руководителя утверждается перечень ИСПДн, оператором которых она является (далее - Оператор).

Определение угроз безопасности персональных данных, актуальных при обработке персональных данных в ИСПДн, является обязательным для их Оператора и оформляется документально в виде Частных моделей угроз, которые утверждаются руководителем Оператора.

В случае если Оператором в соответствии с пунктом 2.12 настоящих Актуальных угроз принято решение применения СКЗИ для обеспечения безопасности персональных данных в ИСПДн, то при определении угроз безопасности персональных данных, актуальных при обработке персональных данных в данной ИСПДн, Оператор дополнительно формирует совокупность предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак.

* 1. При определении угроз безопасности персональных данных, актуальных при обработке персональных данных в ИСПДн, и разработке Частных моделей угроз для этих ИСПДн использование настоящих Актуальных угроз Оператором обязательно.

Настоящие Актуальные угрозы применяются на этапах создания ИСПДн для определения и оценки угроз безопасности персональных данных, а также в ходе эксплуатации ИСПДн при периодическом пересмотре (переоценке) угроз безопасности персональных данных.

* 1. Настоящие Актуальные угрозы подлежат адаптации Оператором в ходе определения угроз безопасности персональных данных, актуальных при обработке персональных данных в ИСПДн.

Адаптация Актуальных угроз направлена на уточнение (уменьшение) перечня угроз безопасности персональных данных, актуальных при обработке персональных данных в ИСПДн, и осуществляется с учетом их структурно­-функциональных характеристик, применяемых информационных технологий и особенностей функционирования (в том числе исключение угроз, которые непосредственно связаны с информационными технологиями, не используемыми в ИСПДн, или структурно-функциональными характеристиками, не свойственными ИСПДн).

* 1. В целях снижения субъективных факторов при оценке угроз безопасности персональных данных в ИСПДн и разработки Частных моделей угроз Оператор может привлекать нескольких сотрудников из разных подразделений (ответственных за обеспечение безопасности персональных данных, администраторов безопасности информации, системных администраторов и т.д.).
	2. В рамках одной Частной модели угроз Оператор рассматривает угрозы безопасности персональных данных только для одной ИСПДн.
	3. Частная модель угроз должна содержать:

описание ИСПДн и особенностей ее функционирования, в том числе цель и задачи, решаемые ИСПДн, структурно-функциональные характеристики ИСПДн (тип, к которому отнесена ИСПДн), физические и логические границы ИСПДн, применяемые в ней информационные технологии, сегменты ИСПДн и их типизацию, взаимосвязи между сегментами ИСПДн и другими информационными системами и информационно-телекоммуникационными сетями, в том числе с сетью Интернет, технологии обработки информации в ИСПДн, возможные уязвимости ИСПДн;

границы контролируемой зоны (контролируемых зон отдельных сегментов) ИСПДн;

категории и объем обрабатываемых персональных данных, а также тип актуальных угроз безопасности персональных данных и обеспечиваемый уровень их защищенности;

обеспечиваемые характеристики безопасности обрабатываемых персональных данных (конфиденциальность, целостность, доступность) и последствия от их нарушения;

исходный уровень защищенности ИСПДн;

оценку возможностей (типа, вида, потенциала) нарушителей, необходимых им для реализации угроз безопасности персональных данных;

возможные способы реализации угроз безопасности персональных данных;

обоснование необходимости (или отсутствия таковой) применения для обеспечения безопасности персональных данных СКЗИ;

совокупность предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак, в случае применения в ИСПДн для обеспечения безопасности персональных данных СКЗИ и определение требуемого класса СКЗИ;

актуальные угрозы безопасности персональных данных.

* 1. В случае если ИСПДн имеет сегменты, которые эксплуатируют иные органы государственной власти, органы местного самоуправления или организации, то определение угроз безопасности персональных данных, актуальных при обработке персональных данных в такой ИСПДн, с учетом всех имеющихся сегментов осуществляется ее Оператором.
	2. При необходимости для определения угроз безопасности персональных данных, актуальных при обработки персональных данных в ИСПДн, и разработки Частных моделей угроз Операторами могут привлекаться юридические лица или индивидуальные предприниматели, имеющие лицензию на осуществление деятельности по технической защите конфиденциальной информации.
	3. Согласование Оператором угроз безопасности персональных данных, актуальных при обработке персональных данных в ИСПДн, и Частных моделей угроз, разработанных с использованием настоящих Актуальных угроз, с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, не требуется.

Исключение составляют только Частные модели угроз, разрабатываемые для вновь создаваемых муниципальных информационных систем Богучарского района, которые в соответствии с пунктом 3 требований к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации муниципальных информационных систем и дальнейшего хранения содержащейся в их базах данных информации, утвержденных постановлением Правительства Российской Федерации от 06.07.2015 № 676, согласуются с федеральным органом исполнительной власти в области обеспечения безопасности и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий в части, касающейся выполнения установленных требований о защите информации.

* 1. Настоящие Актуальные угрозы подлежат пересмотру (переоценке): при изменении законодательства Российской Федерации в части определения угроз безопасности персональных данных при их обработке в информационных системах;

при появлении новых угроз в источниках данных об угрозах безопасности информации, используемых в настоящих Актуальных угрозах, которые будут актуальными для рассматриваемых типов ИСПДн;

при изменении структурно-функциональных характеристик, применяемых информационных технологий или особенностей функционирования ИСПДн, следствием которых стало возникновение новых актуальных угроз безопасности персональных данных;

при повышении возможности реализации или опасности существующих угроз безопасности персональных данных;

при появлении сведений и фактов о новых возможностях нарушителей. Угрозы безопасности персональных данных, актуальные при обработке персональных данных в ИСПДн, подлежат пересмотру (переоценке) Оператором:

при внесении изменений в настоящие Актуальные угрозы для соответствующего типа ИСПДн;

при изменении структурно-функциональных характеристик или особенностей функционирования ИСПДн, вследствие чего изменился тип, к которому относится ИСПДн;

при применении в ИСПДн информационных технологий, посредством которых могут формироваться новые угрозы безопасности персональных данных, исключенные из базового (предварительного) перечня угроз безопасности персональных данных для этой ИСПДн Оператором в соответствии с пунктом 4.4 настоящих Актуальных угроз;

при повышении возможности реализации существующих угроз безопасности персональных данных;

в иных случаях по решению Оператора.

2.Угрозы безопасности ИСПДн

Учитывая особенности обработки персональных данных в администрации района, а также категорию и объем обрабатываемых в ИСПДн персональных данных, основными характеристиками безопасности являются конфиденциальность, целостность и доступность.

Система защиты персональных данных включает в себя организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах.

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

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

Целостность - состояние защищенности информации, характеризуемое способностью автоматизированной системы обеспечивать сохранность и неизменность информации при попытках несанкционированных воздействий на нее в процессе обработки или хранения.

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

Основной целью применения в ИСПДн администрации района СКЗИ является защита персональных данных, в том числе при информационном обмене по сетям связи общего пользования и (или) сетям международного информационного обмена.

Под актуальными угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иные неправомерные действия с персональными данными.

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

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

3.Объекты защиты

К объектам защиты относятся:

* персональные данные (ПДн);
* средства защиты информации (СЗИ);
* программно-аппаратные средства;
* системное, сетевое и прикладное программное обеспечение;
* телекоммуникационное оборудование;
* средства криптографической защиты информации (СКЗИ);
* среда функционирования СЗИ;
* среда функционирования СКЗИ (СФ);
* информация, относящаяся к криптографической защите персональных данных, включая ключевую, парольную и аутентифицирующую информацию СКЗИиСЗИ;
* документы, дела, журналы, картотеки, издания, технические документы, видео-, кино- и фотоматериалы, рабочие материалы и т.п., в которых отражена защищаемая информация, относящаяся к информационным системам персональных данных и их криптографической защите, включая документацию на СКЗИ и на технические и программные компоненты среды функционирования СКЗИ;
* носители защищаемой информации, используемые в информационной системе в процессе криптографической защиты персональных данных, носители ключевой, парольной и аутентифицирующей информации СКЗИ и порядок доступа к ним;
* используемые информационной системой каналы (линии) связи, включая кабельные системы;
* помещения, в которых находятся ресурсы информационной системы, имеющие отношение к криптографической защите персональных данных.

4.Актуальные угрозы безопасности в ИСПДн администрации Монастырщинского сельского поселения Богучарского муниципального района

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

УБИ. 003 Угроза анализа криптографических алгоритмов и их реализации;

УБИ. 004 Угроза аппаратного сброса пароля BIOS;

УБИ. 006 Угроза внедрения кода или данных;

УБИ. 008 Угроза восстановления аутентификационной информации;

УБИ. 009 Угроза восстановления предыдущей уязвимой версии BIOS;

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

УБИ. 013 Угроза деструктивного использования декларированного функционала BIOS;

УБИ. 014 Угроза длительного удержания вычислительных ресурсов пользователями;

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

УБИ. 016 Угроза доступа к локальным файлам сервера при помощи

URL;

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

УБИ. 018 Угроза загрузки нештатной операционной системы;

УБИ. 019 Угроза заражения DNS-кеша;

УБИ. 022 Угроза избыточного выделения оперативной памяти;

УБИ. 023 Угроза изменения компонентов системы;

УБИ. 025 Угроза изменения системных и глобальных переменных;

УБИ. 026 Угроза искажения XML-схемы;

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

УБИ. 028 Угроза использования альтернативных путей доступа к ресурсам;

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

УБИ. 030 Угроза использования

информации идентификации/аутентификации, заданной по умолчанию;

УБИ. 031 Угроза использования механизмов авторизации для повышения привилегий;

УБИ. 032 Угроза использования поддельных цифровых подписей

BIOS;

УБИ. 033 Угроза использования слабостей кодирования входных данных;

УБИ. 034 Угроза использования слабостей

протоколов сетевого/локального обмена данными;

УБИ. 036 Угроза исследования механизмов работы программы;

УБИ. 037 Угроза исследования приложения через отчёты об ошибках;

УБИ. 038 Угроза исчерпания вычислительных ресурсов хранилища больших данных;

УБИ. 039 Угроза исчерпания запаса ключей, необходимых для обновления BIOS;

УБИ. 040 Угроза конфликта юрисдикции различных стран;

УБИ. 041 Угроза межсайтового скриптинга;

УБИ. 042 Угроза межсайтовой подделки запроса;

УБИ. 045 Угроза нарушения изоляции среды исполнения BIOS;

УБИ. 049 Угроза нарушения целостности данных кеша;

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

УБИ. 053 Угроза невозможности управления правами пользователей

BIOS;

 УБИ. 061Угроза некорректного задания структуры данных

транзакции;

УБИ. 063 Угроза некорректного использования функционала программного обеспечения;

УБИ. 067 Угроза неправомерного ознакомления с защищаемой информацией;

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

УБИ. 069 Угроза неправомерных действий в каналах связи;

УБИ. 071 Угроза несанкционированного восстановления удалённой защищаемой информации;

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

УБИ.074 Угроза несанкционированного доступа к аутентификационной информации;

 УБИ.086 Угроза несанкционированного изменения аутентификационной информации;

УБИ. 087 Угроза несанкционированного

использования привилегированных функций BIOS;

УБИ. 088 Угроза несанкционированного копирования защищаемой информации;

УБИ. 089 Угроза несанкционированного редактирования реестра;

УБИ. 090 Угроза несанкционированного создания учётной записи пользователя;

УБИ. 091 Угроза несанкционированного удаления защищаемой информации;

УБИ. 093 Угроза несанкционированного управления буфером;

УБИ. 094 Угроза несанкционированного управления синхронизацией и состоянием;

УБИ. 095 Угроза несанкционированного управления указателями;

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

УБИ. 099 Угроза обнаружения хостов;

УБИ. 100 Угроза обхода некорректно настроенных механизмов аутентификации;

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

УБИ. 103 У гроза определения типов объектов защиты;

УБИ. 104 Угроза определения топологии вычислительной сети;

УБИ. 107 Угроза отключения контрольных датчиков;

УБИ. 109 Угроза перебора всех настроек и параметров приложения;

УБИ. 111 Угроза передачи данных по скрытым каналам;

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

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

УБИ. 114 Угроза переполнения целочисленных переменных;

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

УБИ. 116 Угроза перехвата данных, передаваемых по вычислительной

сети;

УБИ. 117 Угроза перехвата привилегированного потока;

УБИ. 118 Угроза перехвата привилегированного процесса;

УБИ. 121 Угроза повреждения системного реестра;

УБИ. 122 Угроза повышения привилегий;

УБИ. 123 Угроза подбора пароля BIOS;

УБИ. 124 Угроза подделки записей журнала регистрации событий;

УБИ. 127 Угроза подмены действия пользователя путём обмана;

УБИ. 128 У гроза подмены доверенного пользователя;

УБИ. 129 Угроза подмены резервной копии программного обеспечения

BIOS;

УБИ. 130 Угроза подмены содержимого сетевых ресурсов;

УБИ. 131 Угроза подмены субъекта сетевого доступа;

УБИ. 132 Угроза получения предварительной информации об объекте защиты;

УБИ. 139 Угроза преодоления физической защиты;

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

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

УБИ. 144 Угроза программного сброса пароля BIOS;

УБИ. 145 Угроза пропуска проверки целостности программного обеспечения;

УБИ. 149 Угроза сбоя обработки специальным образом изменённых файлов;

УБИ. 150 Угроза сбоя процесса обновления BIOS;

УБИ. 151 Угроза сканирования веб-сервисов, разработанных на основе языка описания WSDL;

УБИ. 152 Угроза удаления аутентификационной информации;

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

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

УБИ. 155 Угроза утраты вычислительных ресурсов;

УБИ. 156 Угроза утраты носителей информации;

УБИ. 157 Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации;

УБИ. 158 Угроза форматирования носителей информации;

УБИ. 159 Угроза «форсированного веб-браузинга»;

УБИ. 160 Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации;

УБИ. 162 Угроза эксплуатации цифровой подписи программного

кода;

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

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

УБИ. 166 Угроза внедрения системной избыточности;

УБИ. 167 Угроза заражения компьютера при посещении неблагонадёжных сайтов;

УБИ. 168 Угроза «кражи» учётной записи доступа к сетевым сервисам;

УБИ. 169 Угроза наличия механизмов разработчика;

УБИ. 170 Угроза неправомерного шифрования информации;

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

УБИ. 172 Угроза распространения «почтовых червей»;

УБИ. 173 Угроза «спама» веб-сервера;

УБИ. 174 Угроза «фарминга»;

УБИ. 175 Угроза «фишинга»;

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

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

УБИ. 178 Угроза несанкционированного использования системных и сетевых утилит;

УБИ. 179 Угроза несанкционированной модификации защищаемой информации;

УБИ. 180 Угроза отказа подсистемы обеспечения температурного режима;

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

УБИ. 182 Угроза физического устаревания аппаратных компонентов;

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

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

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

УБИ. 187 Угроза несанкционированного воздействия на средство защиты информации;

 УБИ. 188 Угроза подмены программного обеспечения;

УБИ. 189 Угроза маскирования действий вредоносного кода;

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

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

УБИ. 192 Угроза использования уязвимых версий программного обеспечения;

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

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

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

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

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

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

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

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

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

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

УБИ. 004 Угроза аппаратного сброса пароля BIOS;

УБИ. 008 Угроза восстановления аутентификационной информации;

УБИ. 009 Угроза восстановления предыдущей уязвимой версии BIOS;

УБИ. 010 Угроза выхода процесса за пределы виртуальной машины;

УБИ.011 Угроза деавторизации санкционированного клиента беспроводной сети;

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

УБИ. 013 Угроза деструктивного использования декларированного функционала BIOS;

УБИ, 014 Угроза длительного удержания вычислительных ресурсов пользователями;

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

УБИ. 018 Угроза загрузки нештатной операционной системы;

УБИ. 022 Угроза избыточного выделения оперативной памяти;

УБИ. 023 Угроза изменения компонентов системы;

УБИ. 025 Угроза изменения системных и глобальных переменных;

УБИ. 026 Угроза искажения XML-схемы;

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

УБИ. 028 Угроза использования альтернативных путей доступа к ресурсам;

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

УБИ. 030 Угроза использования информации

идентификации/аутентификации, заданной по умолчанию;

УБИ. 031 Угроза использования механизмов авторизации для повышения привилегий;

УБИ. 033 Угроза использования слабостей кодирования входных данных;

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

УБИ. 036 Угроза исследования механизмов работы программы;

УБИ. 037 Угроза исследования приложения через отчёты об ошибках; УБИ. 038 Угроза исчерпания вычислительных ресурсов хранилища больших данных;

УБИ. 045 Угроза нарушения изоляции среды исполнения BIOS;

УБИ. 049 Угроза нарушения целостности данных кеша;

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

УБИ. 053 Угроза невозможности управления правами пользователей

BIOS;

УБИ. 061 Угроза некорректного задания структуры данных

транзакции;

УБИ. 063 Угроза некорректного использования функционала программного обеспечения;

УБИ. 067 Угроза неправомерного ознакомления с защищаемой информацией;

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

УБИ. 071 Угроза несанкционированного восстановления удалённой защищаемой информации;

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

УБИ. 074 Угроза несанкционированного доступа к аутентификационной информации;

УБИ. 086 Угроза несанкционированного изменения

аутентификационной информации;

УБИ. 087 Угроза несанкционированного использования

привилегированных функций BIOS;

УБИ. 088 Угроза несанкционированного копирования защищаемой информации;

УБИ. 089 Угроза несанкционированного редактирования реестра;

УБИ. 090 Угроза несанкционированного создания учётной записи пользователя;

УБИ. 091 Угроза несанкционированного удаления защищаемой информации;

УБИ. 093 Угроза несанкционированного управления буфером;

УБИ. 094 Угроза несанкционированного управления синхронизацией и состоянием;

УБИ. 095 Угроза несанкционированного управления указателями;

УБИ. 100 Угроза обхода некорректно настроенных механизмов аутентификации;

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

УБИ. 107 Угроза отключения контрольных датчиков;

УБИ. 109 Угроза перебора всех настроек и параметров приложения;

УБИ. 111 Угроза передачи данных по скрытым каналам;

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

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

УБИ. 114 Угроза переполнения целочисленных переменных;

УБИ. 315 Угроза перехвата вводимой и выводимой на периферийные устройства информации;

УБИ. 117 Угроза перехвата привилегированного потока;

УБИ. 118 Угроза перехвата привилегированного процесса;

УБИ. 121 Угроза повреждения системного реестра;

УБИ. 122 Угроза повышения привилегий;

УБИ. 123 Угроза подбора пароля BIOS;

УБИ. 124 Угроза подделки записей журнала регистрации событий;

УБИ. 129 Угроза подмены резервной копии программного обеспечения

BIOS;

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

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

УБИ. 144 Угроза программного сброса пароля BIOS;

УБИ. 145 Угроза пропуска проверки целостности программного обеспечения;

УБИ. 149 Угроза сбоя обработки специальным образом изменённых файлов;

УБИ. 150 Угроза сбоя процесса обновления BIOS;

УБИ. 152 Угроза удаления аутентификационной информации;

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

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

УБИ. 155 Угроза утраты вычислительных ресурсов;

УБИ. 156 Угроза утраты носителей информации;

УБИ. 158 Угроза форматирования носителей информации;

УБИ. 162 Угроза эксплуатации цифровой подписи программного

кода;

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

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

УБИ. 166 Угроза внедрения системной избыточности;

УБИ.167 Угроза заражения компьютера при посещении неблагонадёжных сайтов;

УБИ.169 Угроза наличия механизмов разработчика;

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

УБИ.178 Угроза несанкционированного использования системных и сетевых утилит;

УБИ.179 Угроза несанкционированной модификации защищаемой информации;

УБИ.180 Угроза отказа подсистемы обеспечения температурного режима;

УБИ.182 Угроза физического устаревания аппаратных компонентов;

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

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

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

УБИ.187 Угроза несанкционированного воздействия на средство защиты информации;

УБИ.188 Угроза подмены программного обеспечения;

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

УБИ.192 Угроза использования уязвимых версий программного обеспечения;

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

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

В соответствии с методическими рекомендациями по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности, утвержденных руководством 8 Центра ФСБ России 31 марта 2015 года № 149/7/2/6-432, на основании исходных данных об информационных системах, объектах защиты и источниках атак определяются обобщенные возможности источников атак.

Определение обобщенных возможностей источников атак представлено в разделе 5.

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

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

Если системы разноплановые и при этом угрозы, которые могут быть нейтрализованы только с помощью СКЗИ, являются актуальными, то при разработке для имеющихся ИСПДн частных моделей угроз необходимо руководствоваться разделом 3 Методических рекомендаций по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности, утвержденных руководством 8 Центра ФСБ России от 31 марта 2015 года № 149/7/2/6-432.

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

5. Обобщённые возможности источников атак

|  |  |  |
| --- | --- | --- |
| №п/п | Обобщенные возможности источников атак | Да/нет |
| 1. | Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак только за пределами контролируемой зоны | Да |
| 2. | Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны, но без физического доступа к аппаратным средствам, на которых реализованы СКЗИ и среда их функционирования | Нет |
| 3. | Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны с физическим доступом к аппаратным средствам, на которых реализованы СКЗИ и среда их функционирования | Нет |
| 4. | Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области анализа сигналов линейной передачи и сигналов побочного электромагнитного излучения и наводок СКЗИ) | Нет |
| 5. | Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области использования для реализации атак недокументированных возможностей прикладного программного обеспечения) | Нет |
| 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 |

6. Обоснование признания неактуальности угроз

|  |  |  |  |
| --- | --- | --- | --- |
| №п/п | Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы) | Актуальностьиспользования(применения)дляпостроенияиреализацииатак | Обоснование отсутствия актуальности угроз |
| 1.1. | Проведение атаки при нахождении в пределахконтролируемой зоны | Неактуально | Проводятся работы по подбору персонала;доступ в контролируемую зону, где располагается СКЗИ, обеспечивается в соответствии с контрольно-пропускным режимом; представители технических, обслуживающих и других вспомогательных служб при работе в помещениях (стойках), где расположены СКЗИ, и сотрудники, не являющиеся пользователями СКЗИ, находятся в этих помещениях только в присутствии сотрудников по эксплуатации; сотрудники, являющиеся пользователями ИСПДн, но не являющиеся пользователями СКЗИ, проинформированы о правилах работы в ИСПДн и ответственности за несоблюдение правил обеспечения безопасности информации;пользователи СКЗИ проинформированы о правилах работы в ИСПДн, правилах работы с СКЗИ и ответственности за несоблюдение правил обеспечения безопасности информации; помещения, в которых располагаются СКЗИ, оснащены входными дверьми с замками, |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  | обеспечивается постоянное закрытие дверей помещений на замок и их открытие только для санкционированного прохода; утверждены правила доступа в помещения, где 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 сПДн; осуществляется контроль целостности средств защиты на АРМах и серверах, на которых установлены СКЗИ: используются сертифицированные средства защиты информации от несанкционированного доступа, используются сертифицированные средства антивирусной защиты |
| 1.2. | Проведение атак на этапе эксплуатации СКЗИ на следующие объекты:* документацию на СКЗИ и компоненты СФ;
* помещения, в которых находится совокупность программных и технических элементов систем обработки данных, способных
 | Неактуально | Проводятся работы по подбору персонала;доступ в контролируемую зону, где располагается СКЗИ, обеспечивается в соответствии с контрольно-пропускным режимом; документация на СКЗИ хранится у ответственного за СКЗИ в металлическом сейфе; помещения, в которых располагаются документация на СКЗИ, СКЗИ и компоненты СФ, оснащены.входными дверьми с замками, обеспечивается постоянное закрытие дверей |

|  |  |  |  |
| --- | --- | --- | --- |
|  | функционировать самостоятельно или в составе других систем (далее -СВТ), на которых реализованы СКЗИ иСФ |  | помещений на замок и их открытие только для санкционированного прохода; утвержден перечень лиц, имеющих право доступа в помещения |
| 1.3. | Получение в рамкахпредоставленныхполномочий, а такжев результатенаблюденийследующейинформации:* сведений о физических мерах защиты объектов, в которых размещены ресурсы информационной системы;
* сведений о мерах по обеспечению контролируемой зоны объектов, в которых размещены ресурсы

информационнойсистемы;сведений о мерах по разграничению доступа в помещения, в которых находятся СВТ, на которых реализованы СКЗИ и СФ | Неактуально | Проводятся работы по подбору персонала;доступ в контролируемую зону и помещения, где располагается ресурсы ИСПДи, обеспечивается в соответствии с контрольно­пропускным режимом; сведения о физических мерах защиты объектов, в которых размещены ИСПДн, доступны ограниченному кругу сотрудников; сотрудники проинформированы об ответственности за несоблюдение правил обеспечения безопасности информации |
| 1.4. | Использование штатных средств ИСПДн, ограниченное мерами,реализованными в информационной | Неактуально | Проводятся работы по подбору персонала; помещения, в которых располагаются -СВТ, на которых располагаются СКЗИ и СФ, оснащены входными дверьми с |

|  |  |  |  |
| --- | --- | --- | --- |
|  | системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий |  | замками, обеспечивается постоянное закрытие дверей помещений на замок и их открытие только для санкционированного прохода;сотрудники проинформированы об ответственности за несоблюдение правил обеспечения безопасности информации;осуществляется разграничение и контроль доступа пользователей к защищаемым ресурсам; осуществляется регистрация и учет действий пользователей; в ИСПДн используются: сертифицированные средства защиты информации от несанкционированного доступа, сертифицированные средства антивирусной защиты |
| 2.1. | Физический доступ к СВТ, на которых реализованы СКЗИ и СФ | Неактуально | Проводятся работы по подбору персонала;доступ в контролируемую зону и помещения, где распола1ается СВТ, на которых реализованы СКЗИ и СФ, обеспечивается в соответствии с контрольно-пропускным режимом;помещения, в которых располагаются СВТ, на которых располагаются СКЗИ и СФ, оснащены входными дверьми с замками, обеспечивается постоянное закрытие дверей помещений на замок и их открытие только для санкционированного прохода |
| 2.2. | Возможность воздействовать на аппаратные компоненты СКЗИ и СФ, ограниченная мерами,реализованными в | Неактуально | Проводятся работы по подбору персонала;доступ в контролируемую зону и помещения, где располагается СВТ, на которых реализованы СКЗИ и СФ, обеспечиваегся в соответствии с контрольно-пропускным |

|  |  |  |  |
| --- | --- | --- | --- |
|  | информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий |  | режимом;помещения, в которых располагаются СКЗИ и СФ, оснащены входными дверьми с замками, обеспечивается постоянное закрытие дверей помещений на замок и их открытие только для санкционированного прохода;представители технических, обслуживающих и других вспомогательных служб при работе в помещениях (стойках), где расположены компоненты СКЗИ и СФ, н сотрудники, не являющиеся пользователями СКЗИ, находятся в этих помещениях только в присутствии сотрудников но эксплуатации |
| 3.1. | Создание способов,подготовка ипроведение атак спривлечениемспециалистов вобласти анализасигналов,сопровождающихфункционированиеСКЗИ и СФ, и вобластииспользованиядля реализацииатакнедокументированных(недекларированных)возможностейприкладногопрограммногообеспечения | Неактуально | Не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности; высокая стоимость и сложность подготовки реализации возможности;проводятся работы по подбору персонала;доступ в контролируемую зону и помещения, где располагается СВТ, на которых реализованы СКЗИ и СФ, обеспечивается в соответствии с контрольно­пропускным режимом; помещения, в которых располагаются СКЗИ и СФ, оснащены входными дверьми с замками, обеспечивается постоянное закрытие дверей помещений на замок и их открытие только для санкционированного прохода; |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  | представители технических, обслуживающих и других вспомогательных служб при работе в помещениях (стойках), где расположены компоненты СКЗИ и СФ, и сотрудники, не являющиеся пользователями СКЗИ, находятся в этих помещениях только в присутствии сотрудников по эксплуатации;осуществляется разграничение и контроль доступа пользователей к защищаемым ресурсам; осуществляется регистрация и учег действий пользователей; на АРМах и серверах, на которых установлены СКЗИ: используются сертифицированные средства защиты информации от несанкционированного доступа, используются сертифицированные |
| 3.2. | Проведениелабораторныхисследований СКЗИ,используемыхвнеконтролируемой 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 |
| 3.3. | Проведение работ по созданию способов и средств атак в научно­исследовательских центрах, | Неактуально | Не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности; |

|  |  |  |  |
| --- | --- | --- | --- |
|  | специализирующихся в области разработки и анализа СКЗИ и СФ, в том числе с использованием исходных текстов входящего в СФ прикладного программного обеспечения, непосредственно использующего вызовы программных функций СКЗИ |  | высокая стоимость и сложность подготовки реализации возможности |
| 4.1. | Создание способов, подготовка и проведение атак с привлечением специалистов в областииспользования дляреализацииатакнедокументированных(недекларированных)возможностейсистемногопрограммногообеспечения | Неактуально | Не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности; высокая стоимость и сложность подготовки реализации возможности;проводятся работы по подбору персонала;доступ в контролируемую зону и помещения, где располагается СВТ, на которых реализованы СКЗИ и СФ, обеспечивается в соответствии с контрольно-пропускным режимом; помещения, в которых располагаются СКЗИ и СФ, оснащены входными дверьми с замками, обеспечивается постоянное закрытие дверей помещений на замок и их открытие только для санкционированного прохода;представители технических, обслуживающих и других вспомогательных служб при работе в помещениях (стойках), где расположены компоненты СКЗИ и |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  | СФ, и сотрудники, не являющиеся пользователями СКЗИ, находятся в этих помещениях только в присутствии сотрудников по эксплуатации;осуществляется раз1раниченис и контроль доступа пользователей к защищаемым ресурсам; осуществляется регистрация и учет действий пользователей; на АРМах и серверах, на которых установлены СКЗИ: используются сертифицированные средства защиты информации от несанкционированного доступа, используются сертифицированные средства антивирусной защиты |
| 4.2. | Возможность располагать сведениями, содержащимися в конструкторской документации на аппаратные и программные компоненты СФ. | Неактуально | Не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности |
| 4.3. | Возможность воздействовать на любые компоненты СКЗИ и СФ. | Неактуально | Не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности |