Утверждено:

|  |  |
| --- | --- |
| \_\_должность\_\_ \_\_название организации\_\_ \_\_ФИО\_\_ | \_\_дата\_\_ |

**Модель угроз**

Безопасности в \_\_тип системы\_\_

«\_\_название\_системы\_\_»

Принадлежащей

\_\_название организации\_\_

Саратов, \_\_год\_\_

Оглавление

[Список терминов и сокращения 4](#_Toc162130105)

[1. Общие положения 5](#_Toc162130106)

[1.1 Назначение и область действия документа 7](#_Toc162130107)

[1.2 Перечень нормативных и методических документов 7](#_Toc162130108)

[2. Описание системы 8](#_Toc162130109)

[2.1 Характеристики безопасности объектов угроз 8](#_Toc162130110)

[3. Возможные негативные последствия от реализации (возникновения) угроз безопасности информации 8](#_Toc162130111)

[4. Возможные объекты воздействия угроз безопасности информации 9](#_Toc162130112)

[5. Источники угроз безопасности информации 11](#_Toc162130113)

[5.1 Исходные данные для определения возможные актуальных нарушителей 11](#_Toc162130114)

[5.2 Типы и виды нарушителей 12](#_Toc162130115)

[5.3 Потенциал и возможности нарушителей 20](#_Toc162130116)

[6. Способы реализации угроз безопасности информации 21](#_Toc162130117)

Список тегов

* \_\_должность\_\_
* \_\_название организации\_\_
* \_\_ФИО\_\_
* \_\_дата\_\_
* \_\_тип системы\_\_
* \_\_название\_системы\_\_
* \_\_год\_\_
* \_\_описание\_\_системы\_\_
* \_\_название\_нег\_поз\_\_
* \_\_таблица\_нег\_пос\_\_
* \_\_таблица\_виды\_негативного\_воздействия\_\_
* \_\_таблица\_потенциал\_нарушителя\_\_

## Список терминов и сокращения

## Общие положения

Настоящий документ разработан на основе нормативно-методических документов ФСТЭК России, регламентирующих порядок обеспечения безопасности информации.

Настоящая Модель угроз содержит систематизированный перечень угроз безопасности защищаемой информации при их обработке в \_\_тип\_системы\_\_ «\_\_название\_системы\_\_». Эти угрозы обусловлены преднамеренными или непреднамеренными действиями физических лиц или организаций, а также криминальных группировок, создающими условия для нарушения безопасности информации, содержащийся в информационной системе, которые ведут к ущербу жизненно важным интересам личности, общества и государства.

Модель угроз определяет актуальные угрозы для \_\_тип\_системы\_\_ «\_\_название\_системы\_\_».

Модель угроз содержит данные по угрозам безопасности защищаемой информации, обрабатываемой в \_\_тип\_системы\_\_ «\_\_название\_системы\_\_», связанным с:

\_\_название\_нег\_поз\_\_

**Снизу представлен пример потом удалить**

- анализ защищенности ГИС «Название ИС» от угроз безопасности ПДн в ходе организации и выполнения работ по обеспечению безопасности ПДн;

- разработка системы защиты ПДн, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты ПДн, предусмотренных для соответствующего класса ГИС «Название ИС»;

- проведение мероприятий, направленных на предотвращение несанкционированного доступа к ПДн и (или) передачи их лицам, не имеющим права доступа к такой информации;

- недопущение воздействия на технические средства ГИС «Название ИС», в результате которого может быть нарушено их функционирование;

- контроль за обеспечением третьего уровня защищенности персональных данных и третьего класса защищенности ГИС «Название ИС».

В Модели угроз дано обобщенное описание \_\_тип\_системы\_\_ «\_\_название\_системы\_\_», как объекта защиты, возможных источников угроз безопасности, основных классов уязвимостей ИС, возможных видов действий и деструктивных воздействий на ИС а также основных способов их реализации.

Угрозы безопасности, содержащиеся в настоящей Модели угроз, могут уточняться и дополняться по мере выявления новых усточников угроз, развития способов и средств реализации угроз безопасности защищаемой информации в \_\_тип\_системы\_\_ «\_\_название\_системы\_\_». Внесение изменений в Модель угроз осуществляется также в случае внесения новых элемотов в банк данных угроз безопасности информации ФСТЭК России (bdu.fstec.ru) . Кроме того, модель угроз может быть пересмотрена по решению оператора (\_\_название организации\_\_) на основе периодически проводимых им анализа и оценки угроз безопасности защищаемой информации с учётом особенностей и (или) изменений \_\_тип\_системы\_\_ «\_\_название\_системы\_\_», а также по результатам мероприйтий по контролю за выполнением требований к обеспечению безопасности защищаемой информации при обработке оной в ИС.

### 1.1 Назначение и область действия документа

* Настоящая модель угроз безопасности информации (далее – Модель угроз) разработана в целях определения угроз безопасности информации, реализация которых может привести к нарушению безопасности информации \_\_тип системы\_\_.

### 1.2 Перечень нормативных и методических документов

Разработка модели угроз, обрабатываемой в информационной системе \_\_название\_системы\_\_ проведена в соответствии с:

* \_\_список нормативки для соот системы\_\_

**Снизу представлен пример потом удалить**

* Федеральный закон от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
* Федеральным законом «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 N 187-ФЗ;
* Постановлением Правительства РФ от 8 февраля 2018 г. № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений»;
* Приказом ФСТЭК России от 21 декабря 2017 г. N 235 «Об утверждении требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры российской федерации и обеспечению их функционирования»;
* Приказом ФСТЭК России от 25 декабря 2017 г. N 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры российской федерации»;
* Методическим документом ФСТЭК «Методика оценки угроз безопасности информации» от 5 февраля 2021;

## Описание системы

\_\_описание\_\_системы\_\_

**Если описание отсутствует – сохранить текст снизу**

Описание системы можно посмотреть в ТЗ на \_\_тип\_системы\_\_ «\_\_название\_системы\_\_».

### 2.1 Характеристики безопасности объектов угроз

В \_\_тип\_системы\_\_ «\_\_название\_системы\_\_» необходимо обеспечивать целостность, доступность и конфиденциальность защищаемой информации

## Возможные негативные последствия от реализации (возникновения) угроз безопасности информации

Возможные негативные последствия от реализации угроз безопасности информации, обрабатываемой \_\_тип\_системы\_\_ представлены в таблице, приведённой ниже.

**Снизу представлен пример потом удалить**

\_\_таблица\_нег\_пос\_\_

Таблица 1, Возможные негативные последствия

|  |  |
| --- | --- |
| **Вид риска (ущерба)** | **Возможные негативные последствия** |

## Возможные объекты воздействия угроз безопасности информации

Возможные объекты и виды воздействияугроз безопасности информации значимого объекта КИИ представлены в таблице, приведённой ниже.

\_\_таблица\_виды\_негативного\_воздействия\_\_

**Снизу представлен пример потом удалить**

Таблица 2, Виды негативного воздействия

|  |  |  |
| --- | --- | --- |
| Негативные  последствия | Объекты воздействия | Виды воздействия |
| Необходимость дополнительных (незапланированных) затрат на закупку товаров, работ или услуг (в том числе закупка программного обеспечения, технических средств, вышедших из строя, замена, настройка, ремонт указанных средств) (У2) | Проводной канал передачи данных | Отказ в обслуживание компонентов |
| Съемные машинные носители информации | Кража машинного носителя информации |
| Сетевое оборудование | Отказ в обслуживании компонентов |
| Нарушение штатного режима функционирования автоматизированной системы управления и управляемого объекта и/или процесса (У2) | Активное сетевое оборудование | Несанкционированная  модификация (изменение) логики  работы или уставок  коммутатора |
| Снижение показателей государственного оборонного заказа (У3) | Системное и прикладное программное обеспечение | Несанкционированный доступ к компонентам, защищаемой информации, системным, конфигурационным, иным служебным данным |
| Прекращение или нарушение функционирования информационной системы в области обеспечения обороны страны, безопасности государства и правопорядка (У3) | Сетевое оборудование | Отказ в обслуживании компонентов |
| База данных ИС | Несанкционированный доступ к защищаемой информации с целью нарушения целостности или доступности |

## Источники угроз безопасности информации

### 5.1 Исходные данные для определения возможные актуальных нарушителей

* общий перечень угроз безопасности информации, содержащийся в банке данных угроз безопасности информации ФСТЭК России (bdu.fstec.ru), модели угроз безопасности информации, разрабатываемые ФСТЭК России в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. N 1085, а также отраслевые (ведомственные, корпоративные) модели угроз безопасности информации;
* нормативные правовые акты Российской Федерации, в соответствии с которыми создается и функционирует система или сеть, содержащие описание назначения, задач (функций) систем и сетей, состав обрабатываемой информации и ее правовой режим;
* документация на сети и системы (в части сведений о назначении и функциях, составе и архитектуре систем и сетей, о группах пользователей и уровне их полномочий и типах доступа, о внешних и внутренних интерфейсах);
* негативные последствия от реализации (возникновения) угроз безопасности информации, определенные в соответствии с настоящей Методикой;
* объекты воздействия угроз безопасности информации и виды воздействия на них, определенные в соответствии с настоящей Методикой.

### 5.2 Типы и виды нарушителей

В настоящем разделе определяется совокупность условий и факторов, создающих опасность нарушения характеристик безопасности возможных объектов угроз.

В данном разделе под угрозами будут пониматься атаки.

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

* внешние нарушители - нарушители, не имеющие прав доступа в контролируемую (охраняемую) зону (территорию) и (или) полномочий по доступу к информационным ресурсам и компонентам систем и сетей, требующим авторизации;
* внутренние нарушители - нарушители, имеющие права доступа в контролируемую (охраняемую) зону (территорию) и (или) полномочия по автоматизированному доступу к информационным ресурсам и компонентам систем и сетей.

**Внешний нарушитель**

В качестве внешнего нарушителя информационной безопасности, рассматривается нарушитель, который не имеет непосредственного доступа к техническим средствам и ресурсам системы, находящимся в пределах контролируемой зоны.

Предполагается, что внешний нарушитель может воздействовать на защищаемую информацию по техническим каналам утечки и время передачи по каналам связи.

**Внутренний нарушитель**

Возможности внутреннего нарушителя существенным образом зависят от действующих в пределах контролируемой зоны ограничительных факторов, из которых основным является реализация комплекса организационно-технических мер, в том числе по подбору, расстановке и обеспечению высокой профессиональной подготовки кадров, допуску физических лиц внутрь контролируемой зоны и контролю за порядком проведения работ, направленных на предотвращение и пресечение несанкционированного доступа.

Система разграничения доступа ИС обеспечивает разграничение прав пользователей на доступ к информационным, программным, аппаратным и другим ресурсам ИС в соответствии с принятой политикой информационной безопасности.

Внутренний нарушитель может использовать штатные средства*.*

Состав имеющихся у нарушителя средств, которые он может использовать для реализации угроз ИБ, а также возможности по их применению зависят от многих факторов, включая реализованные на объектах конкретные организационные меры, финансовые возможности и компетенцию нарушителей. Поэтому объективно оценить состав имеющихся у нарушителя средств реализации угроз в общем случае практически невозможно.

Поэтому, для создания устойчивой СЗИ предполагается, что вероятный нарушитель имеет все необходимые для реализации угроз средства, возможности которых не превосходят возможности аналогичных средств реализации угроз на информацию, содержащую сведения, не составляющие государственную тайну, и технические и программные средства, обрабатывающие эту информацию.

Предположения об имеющейся у нарушителя информации об объектах реализации угроз.

В качестве основных уровней знаний нарушителей об ИС можно выделить следующие:

* общая информация – информации о назначении и общих характеристиках \_\_тип\_системы\_\_ «\_\_название\_системы\_\_»;
* эксплуатационная информация – информация, полученная из эксплуатационной документации;
* чувствительная информация – информация, дополняющая эксплуатационную информацию об \_\_тип\_системы\_\_ «\_\_название\_системы\_\_» (например, сведения из проектной документации

В частности, нарушитель может иметь:

* данные об организации работы, структуре и используемых технических, программных и программно-технических средствах \_\_тип\_системы\_\_ «\_\_название\_системы\_\_» ;
* сведения об информационных ресурсах \_\_тип\_системы\_\_ «\_\_название\_системы\_\_»: порядок и правила создания, хранения и передачи информации, структура и свойства информационных потоков;
* данные об уязвимостях, включая данные о недокументированных (недекларированных) возможностях технических, программных и программно-технических средств \_\_тип\_системы\_\_ «\_\_название\_системы\_\_» ;
* данные о реализованных в программных средствах защиты информации принципах и алгоритмах;
* исходные тексты программного обеспечения \_\_тип\_системы\_\_ «\_\_название\_системы\_\_» ;
* сведения о возможных каналах реализации угроз;
* информацию о способах реализации угроз.

**Нарушители согласно банку данных угроз ФСТЭК России**

Дополнительно в банке данных угроз ФСТЭК России определены три типа внешних и внутренних нарушителей – с низким потенциалом, со средним потенциалом и с высоким потенциалом.

Нарушители с **низким потенциалом** имеют возможность получить информацию об уязвимостях отдельных компонент информационной системы, опубликованную в общедоступных источниках. Также такие нарушители имеют возможность получить информацию о методах и средствах реализации угроз безопасности информации (компьютерных атак), опубликованных в общедоступных источниках, и (или) самостоятельно осуществляют создание методов и средств реализации атак и реализацию атак на информационную систему.

Нарушители со **средним потенциалом** обладают всеми возможностями нарушителей с низким потенциалом. Имеют осведомленность о мерах защиты информации, применяемых в информационной системе данного типа. Имеют возможность получить информацию об уязвимостях отдельных компонент информационной системы путем проведения, с использованием имеющихся в свободном доступе программных средств, анализа кода прикладного программного обеспечения и отдельных программных компонент общесистемного программного обеспечения. Имеют доступ к сведениям о структурно-функциональных характеристиках и особенностях функционирования информационной системы.

Нарушители с **высоким потенциалом** обладают всеми возможностями нарушителей с низким и средним потенциалами. Имеют возможность осуществлять несанкционированный доступ из выделенных (ведомственных, корпоративных) сетей связи, к которым возможен физический доступ (незащищенных организационными мерами). Имеют возможность получить доступ к программному обеспечению чипсетов (микропрограммам), системному и прикладному программному обеспечению, телекоммуникационному оборудованию и другим программно-техническим средствам информационной системы для преднамеренного внесения в них уязвимостей или программных закладок. Имеют хорошую осведомленность о мерах защиты информации, применяемых в информационной системе, об алгоритмах, аппаратных и программных средствах, используемых в информационной системе. Имеют возможность получить информацию об уязвимостях путем проведения специальных исследований (в том числе с привлечением специализированных научных организаций) и применения специально разработанных средств для анализа программного обеспечения. Имеют возможность создания методов и средств реализации угроз безопасности информации с привлечением специализированных научных организаций и реализации угроз с применением специально разработанных средств, в том числе обеспечивающих скрытное проникновение в информационную систему и воздействие на нее. Имеют возможность создания и применения специальных технических средств для добывания информации (воздействия на информацию или технические средства), распространяющейся в виде физических полей или явлений.

Список рассматриваемых нарушителей представлен в таблице ниже.

\_\_таблица\_нарушители\_\_

**Снизу представлен пример потом удалить**

Таблица 2, Виды нарушителей

| **Вид нарушителя** | **Тип нарушителя** | **Возможные цели (мотивация) реализации угроз безопасности информации** |
| --- | --- | --- |
| Специальные службы иностранных государств | Внешний | На­несе­ние ущер­ба го­сударс­тву в об­ласти обо­роны, бе­зопас­ности и пра­вопо­ряд­ка, а так­же в иных от­дель­ных об­ластях его де­ятель­нос­ти или сек­то­рах эко­номи­ки. |
| Террористические, экстремистские группировки | Внешний | На­несе­ние ущер­ба от­дель­ным сфе­рам де­ятель­нос­ти или сек­то­рам эко­номи­ки го­сударс­тва. |
| Преступные группы (криминальные структуры) | Внешний | Получение финансовой или иной материальной выгоды |
| Отдельные физические лица (хакеры) | Внешний | Получение финансовой или иной материальной выгоды |
| Конкурирующие организации | Внешний | Получение финансовой или иной материальной выгоды |
| Разработчики программных, программно-аппаратных средств | Внутренний | Нарушители данного вида не имеют мотивации по реализации угроз безопасности информации в СЗИ , поскольку используются программно-технические средства производителей, обладающих значительным опытом в сфере информационных технологий |
| Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем | Внешний | Непреднамеренные, неосторожные или неквалифицированные действия |
| Поставщики вычислительных услуг, услуг связи | Внутренний | Непреднамеренные, неосторожные или неквалифицированные действия |
| Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ | Внутренний | Непреднамеренные, неосторожные или неквалифицированные действия |
| Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора (администрация, охрана, уборщики и т.д.) | Внутренний | Непреднамеренные, неосторожные или неквалифицированные действия |
| Авторизованные пользователи систем и сетей | Внутренний | Лю­бопытс­тво или же­лание са­море­али­зации (под­твержде­ние ста­туса);  Неп­редна­мерен­ные, не­ос­то­рож­ные или нек­ва­лифи­циро­ван­ные дей­ствия;  Месть за ра­нее со­вер­шенные дей­ствия. |
| Системные администраторы и администраторы безопасности | Внутренний | Неп­редна­мерен­ные, не­ос­то­рож­ные или нек­ва­лифи­циро­ван­ные дей­ствия. |
| Бывшие работники (пользователи) | Внешний | Получение финансовой или иной материальной выгоды  Месть за ранее совершенные действия |

### 5.3 Потенциал и возможности нарушителей

Нарушители имеют разные уровни компетентности, оснащенности ресурсами и мотивации для реализации угроз безопасности информации. Совокупность данных характеристик определяет уровень возможностей нарушителей по реализации угроз безопасности информации.

В зависимости от уровня возможностей нарушители подразделяются на нарушителей, обладающих:

* базовыми возможностями по реализации угроз безопасности информации (Н1);
* базовыми повышенными возможностями по реализации угроз безопасности информации (Н2);
* средними возможностями по реализации угроз безопасности информации (Н3);
* высокими возможностями по реализации угроз безопасности информации (Н4).

Ниже представлена таблица, сопоставляющая уровень вид нарушителя и его потенциал.

\_\_таблица\_потенциал\_нарушителя\_\_

**Снизу представлен пример потом удалить**

Таблица 3. Потенциал нарушителя

|  |  |  |
| --- | --- | --- |
| **Уровень возможностей** | **Вид нарушителя** | **Потенциал нарушителя** |
| Базовые возможности (Н1) | * Физическое лицо (хакер); | Низкий |
| * Авторизованные пользователи систем и сетей; | Низкий |
| Базовые повышенные возможности (Н2) | * Преступные группы (два лица и более, действующие по единому плану). * Системные администраторы и администраторы безопасности | Средний |
| * Системные администраторы и администраторы безопасности | Средний |
| Средние возможности (Н3) | * Террористические, экстремистские группировки | Средний |
| * Конкурирующие организации | Средний |
| Высокие возможности (Н4) | * Специальные службы иностранных государств | Высокий |

## Способы реализации угроз безопасности информации

Список способов реализации угроз безопасности основывается на:

* объектах воздействия угроз безопасности, ранее определенных в настоящей модели угроз;
* возможностях актуальных нарушителей, ранее определенных в настоящей модели угроз;

Возможными способами реализации угроз безопасности информации для ИС являются:

**ДОПОЛИТЬ ЕСЛИ БУДЕТ ВРЕМЯ И СИЛЫ**

* Эксплуатация уязвимостей
* Внедрение вредоносного программного обеспечения
* Внедрение программных и аппаратных закладок
* Использование недекларированных возможностей
* Реализация социальной инженерии
* Подбор (восстановление) аутентификационной информации
* Использование недостатков механизмов разграничения доступа
* Повреждение данных

## Актуальные угрозы безопасности

В ходе оценки угроз безопасности информации должны быть определены возможные угрозы безопасности информации и оценена их актуальность для систем и сетей – актуальные угрозы безопасности информации.

Исходными данными для оценки актуальности угроз безопасности информации являются:

1. общий перечень угроз безопасности информации, содержащийся в банке данных угроз безопасности информации ФСТЭК России (bdu.fstec.ru)
2. негативные последствия от реализации (возникновения) угроз безопасности информации, определенные в соответствии с настоящей Методикой;
3. объекты воздействия угроз безопасности информации и виды воздействий на них, определенные в соответствии с настоящей Методикой;
4. виды и категории актуальных нарушителей, которые могут реализовывать угрозы безопасности информации, в том числе непреднамеренные угрозы, и их возможности, определенные в соответствии с настоящей Методикой;
5. актуальные способы реализации (возникновения) угроз безопасности информации.

На основе анализа исходных данных определяются возможные для систем и сетей угрозы безопасности информации, к которым относятся осуществляемые нарушителем воздействия на информационные ресурсы и компоненты систем и сетей (объекты воздействия), в результате которых возможно нарушение безопасности информации и (или) нарушение или прекращение функционирования систем и сетей.

Угроза безопасности информации возможна, если имеются нарушитель или иной источник угрозы, объект, на который осуществляются воздействия, способы реализации угрозы безопасности информации, а реализация угрозы может привести к негативным последствиям.

Актуальность возможных угроз безопасности информации определяется наличием сценариев их реализации.

Сценарии реализации угроз безопасности информации должны быть определены для соответствующих способов реализации угроз безопасности информации, определенных в соответствии с настоящей Методикой, и применительно к объектам воздействия и видам воздействия на них.

Определение сценариев предусматривает установление последовательности возможных тактик и соответствующих им техник, применение которых возможно актуальным нарушителем с соответствующим уровнем возможностей, а также доступности интерфейсов для использования соответствующих способов реализации угроз безопасности информации.

На этапе создания систем и сетей должен быть определен хотя бы один сценарий каждого способа реализации возможной угрозы безопасности информации. Сценарий определяется для каждого актуального нарушителя и их уровней возможностей.

При наличии хотя бы одного сценария угрозы безопасности информации такая угроза признается актуальной для системы и сети и включается в модель угроз безопасности систем и сетей для обоснования выбора организационных и технических мер по защите информации (обеспечению безопасности), а также выбора средств защиты информации.

На основание вышеопределенных объектов воздействия и актуальных нарушителях определенных, в настоящей модели угроз, и сценариях реализации угроз, представленных в методическом документе "Методика оценки угроз безопасности информации" (утв. Федеральной службой по техническому и экспортному контролю 5 февраля 2021 г.) составляется перечень актуальных угроз.

\_\_таблица\_актуальных\_угроз\_\_

**Снизу представлен пример потом удалить**

Таблица 5 - Определение актуальности угроз безопасности

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Номер угрозы в системе** | **Наименование угрозы** | **Уязвимость** | **Вектора CAPEC** | **Негативные последствия** | **Объект воздействия** | **ТН** | **Сценарий реализации** | **Актуальность, комментарий** |
| **УБИ.004** | Угроза аппаратного сброса пароля BIOS | Возможность сброса паролей, установленных в BIOS/UEFI без прохождения процедуры авторизации в системе путём обесточивания микросхемы BIOS.  Угроза обусловлена уязвимостями некоторых системных (материнских) плат – наличием механизмов аппаратного сброса паролей, установленных в BIOS/UEFI. | CAPEC-438: Modification During Manufacture  CAPEC-444: Development Alteration  CAPEC-532: Измененный установленный BIOS  Злоумышленник, имеющий доступ к загрузке и обновлению системного программного обеспечения, отправляет злонамеренно измененный BIOS жертве или поставщику/интегратору жертвы, который после установки позволяет использовать его в будущем | Злоумышленник получает доступ к системе в обход механизма аутентификации. | Микропрограммное и аппаратное обеспечение BIOS/UEFI | Н1. нарушитель, обладающий базовыми возможностями. (авторизованные пользователи систем и сетей)  внутренний нарушитель с низким потенциалом | Сценарий реализации отсутствует | **Угроза не актуальна**, так как на материнских платах отсутствует механизм аппаратного сброса пароля |
| Н2. Нарушитель, обладающий базовыми повышенными возможностями. (конкурирующие организации)  Внешний нарушитель со средним потенциалом | Сценарий реализации отсутствует | **Угроза не актуальна**, так как на материнских платах отсутствует механизм аппаратного сброса пароля |
| **УБИ.005** | Угроза внедрения вредоносного кода в BIOS | Возможность заставить BIOS/UEFI выполнять вредоносный код при каждом запуске компьютера, внедрив его в BIOS/UEFI путём замены микросхемы BIOS/UEFI или обновления программного обеспечения BIOS/UEFI на версию, уже содержащую вредоносный код.  Данная угроза обусловлена слабостями технологий контроля за обновлением программного обеспечения BIOS/UEFI и заменой чипсета BIOS/UEFI. | CAPEC-438: Modification During Manufacture  CAPEC-444: Development Alteration  CAPEC-532: Измененный установленный BIOS  Злоумышленник, имеющий доступ к загрузке и обновлению системного программного обеспечения, отправляет злонамеренно измененный BIOS жертве или поставщику/интегратору жертвы, который после установки позволяет использовать его в будущем | Злоумышленник получает возможность запустить вредоносный программный код, что может привести к нарушение работы механизма аутентификации и работоспособности ОС в целом | Микропрограммное и аппаратное обеспечение BIOS/UEFI | Н3. нарушитель, обладающий средними возможностями. (разработчики программных, программно-аппаратных средств).  Внешний нарушитель со средним потенциалом | Т10.6. Несанкционированное воздействие на программный код, конфигурацию и параметры доступа прошивки устройства | **Угроза актуальна,** так как обусловлена слабостями разграничения доступа к управлению BIOS |
| **УБИ.006** | Угроза внедрения кода или данных | Возможность внедрения нарушителем в дискредитируемую информационную систему вредоносного кода, который может быть в дальнейшем запущен «вручную» пользователями, автоматически при выполнении определённого условия а также в возможности несанкционированного внедрения нарушителем некоторых собственных данных для обработки в дискредитируемую информационную систему. | CAPEC-184: Software Integrity Attack  CAPEC-186: Malicious Software Update  CAPEC-533: Вредоносное обновление программного обеспечения вручную  Злоумышленник внедряет вредоносный код в систему жертвы, изменяя полезную нагрузку обновления программного обеспечения, что приводит к дополнительному компрометированию или сбою работы | Подрыв целостности программного кода, структур данных устройства или встроенного ПО устройства, добиваясь изменения целостности объекта для достижения небезопасного состояния | Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение | Н1. нарушитель, обладающий базовыми возможностями. отдельные физические лица (хакеры)  Внешний нарушитель с низким потенциалом | Т3.1. Автоматический запуск скриптов и исполняемых файлов в системе с использованием  пользовательских или системных учетных данных, в том числе с использованием методов  социальной инженерии | **Угроза актуальна,** так как обусловлена слабостями антивирусной системы, низкой степенью осведомлённостью сотрудников в сфере ИБ |
| Н2. Нарушитель, обладающий базовыми повышенными возможностями. (Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ)  Внутренний нарушитель со средним потенциалом | Сценарий реализации отсутствует | **Угроза не актуальна,** так как на предприятие введен контроль пропускной режим, с контролем и учетом переносных носителей информации |