## 1. Общие положения

Модель угроз безопасности информации при её обработке в {Название ИС} разработана на основании обследования информационной системы.

Модель угроз содержит описание процесса определения актуальных угроз безопасности информации, реализуемых за счёт:

* несанкционированного доступа к информации в информационных системах;
* утечки информации по техническим каналам в информационных системах;
* воздействия на информационные системы различных техногенных факторов;
* использования в информационных системах СКЗИ для обеспечения безопасности информации конфиденциального характера.

В Модели содержится описание информационной системы, особенностей ее функционирования и структурно-функциональных характеристик, а также описание угроз безопасности информации, включающее описание возможностей нарушителей, возможных способов реализации угроз, и уязвимостей, которые могут быть использованы для их реализации, и последствий от нарушения свойств безопасности информации.

Настоящая модель угроз разработана в соответствии со следующими нормативно-техническими документами, стандартами и информационными ресурсами:

* + - Приказ об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, от 11 февраля 2013 г. № 17;
    - ГОСТ Р 56546-2015 «Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем»;
    - Банк данных угроз безопасности информации ФСТЭК России;
    - Банк уязвимостей ФСТЭК России;
    - Международный стандарт BS ISO/IEC 27005:2011 ISO/IEC 27005 (BS 7799) (SE) «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности»;
    - ГОСТ Р ИСО/МЭК 16085-2007 «Менеджмент риска. Применение в процессах жизненного цикла систем и программного обеспечения»;
    - ГОСТ Р ИСО/МЭК 31010-2011 «Менеджмент риска. Методы оценки риска»;
    - Методические рекомендации 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, утвержденные руководством 8 Центра ФСБ России 31 марта 2015 г.

Настоящая Модель определяет актуальные угрозы безопасности информации при её обработке в и используется при определении состава и содержания организационных и технических мер по обеспечению безопасности информации в информационной системе.

## 2. Описание информационной системы и особенностей ее функционирования

## 3 Модель нарушителя

В данном разделе содержится описание типов, видов, потенциала и мотивации нарушителей, от которых необходимо обеспечить защиту информации при её обработке в {Название ИС}, а также предположения об имеющихся у нарушителей способах и средствах реализации угроз.

## 3.1 Типы нарушителей

В зависимости от имеющихся прав доступа нарушители могут иметь легитимный физический (непосредственный) и (или) логический доступ к компонентам информационной системы и (или) содержащейся в них информации или не иметь такого доступа. С учетом этого нарушители подразделяются на два типа:

* внешние нарушители – лица, не имеющие права доступа к информационной системе, ее отдельным компонентам и реализующие угрозы безопасности информации из-за границ информационной системы;
* внутренние нарушители – лица, имеющие право постоянного или разового доступа к информационной системе, ее отдельным компонентам.

## 3.1.1 Внешние нарушители

Внешнего нарушителя необходимо рассматривать в качестве актуального во всех случаях, когда имеются подключения информационной системы к внешним информационно-телекоммуникационным сетям и (или) имеются линии связи, выходящие за пределы контролируемой зоны, используемые для иных подключений.

Внешний нарушитель может:

* + - осуществлять несанкционированный доступ к каналам связи, выходящим за пределы служебных помещений;
    - осуществлять несанкционированный доступ через автоматизированные рабочие места, подключенные к сетям связи общего пользования и (или) сетям международного информационного обмена;
    - осуществлять несанкционированные доступ через элементы информационной инфраструктуры ИС, которые в процессе своего жизненного цикла (модернизация, сопровождение, ремонт, утилизация) оказываются за пределами контролируемой зоны;
    - осуществлять несанкционированные доступ через информационные системы взаимодействующих ведомств, организаций и учреждений при их подключении к ИС.

К нарушителям внешнего типа относят:

* специальные службы иностранных государств (блоков государств);
* террористические, экстремистские группировки;
* преступные группы (криминальные структуры);
* внешние субъекты (физические лица);
* конкурирующие организации;
* разработчики, производители, поставщики программных, технических и программно-технических средств;
* бывшие работники (пользователи).

## 3.1.2 Внутренние нарушители

Нарушители данного типа обладают наибольшими возможностями по реализации угроз безопасности. При оценке возможностей внутренних нарушителей необходимо учитывать принимаемые оператором организационные меры по допуску субъектов к работе в информационной системе. Возможности внутреннего нарушителя существенным образом зависят от установленного порядка допуска физических лиц к информационной системе и ее компонентам, а также мер по контролю за доступом и работой этих лиц.

К внутренним нарушителям относятся:

* специальные службы иностранных государств (блоков государств);
* пользователи информационной системы;
* лица, привлекаемые для установки, наладки, монтажа, пусконаладочных и иных видов работ;
* администраторы информационной системы и администраторы безопасности.

## 3.2 Определение видов и потенциала нарушителей

Степень информированности нарушителя первой категории зависит от многих факторов, включая реализованные в {Название ИС} конкретные организационные меры и компетенцию нарушителей, поэтому однозначно оценить объем знаний вероятного нарушителя в общем случае практически невозможно.

Возможности каждого вида нарушителя по реализации угроз безопасности информации характеризуются его потенциалом. Потенциал нарушителя определяется компетентностью, ресурсами и мотивацией, требуемыми для реализации угроз безопасности информации в информационной системе с заданными структурно-функциональными характеристиками и особенностями функционирования.

В зависимости от потенциала, требуемого для реализации угроз безопасности информации, нарушители подразделяются на:

* нарушителей, обладающих базовым (низким) потенциалом нападения при реализации угроз безопасности информации в информационной системе;
* нарушителей, обладающих базовым повышенным (средним) потенциалом нападения при реализации угроз безопасности информации в информационной системе;
* нарушителей, обладающих высоким потенциалом нападения при реализации угроз безопасности информации в информационной системе.

Согласно Проекту Методики определения угроз безопасности информации в информационных системах каждому виду нарушителя ставятся в соответстевие его возможности по реализации УБИ и потенциал.

С учетом заданных структурно-функциональных характеристик, особенностей функционирования и организационно-технических мер защиты, реализованных в ней, а также предположений о возможных целях (мотивации) реализации УБИ нарушителями, в результате проведения группой экспертов из состава специалистов органа по аттестации объектов информатизации Федерального государственного бюджетного образовательного высшего образования «Дальневосточный государственный университет путей сообщения» экспертных оценок было определено, что для данной ИС характерны виды нарушителей, представленные в таблице № .

Таблица № – Виды, типы и потенциал нарушителей, характерные для {Название ИС}

{Intruder\_Table}

На основании данных о возможностях нарушителей, полученных в результате аудита информационной системы, было установлено, что для в результате будут характерны:

{Intruder\_List}

Перечень угроз, которые способен реализовать определенный для {Название ИС} нарушитель, представлен в таблице № (Банк данных угроз безопасности информации ФСТЭК России [www.bdu.fstec.ru/](http://www.bdu.fstec.ru/)).

Таблица № – Перечень УБИ, выбранных в соответствии с нарушителем, определённым для информационной системы

{NSD\_Filter\_1\_Intruder}

## 3.3 Анализ возможных уязвимостей {Название ИС}

На этапе обследования информационной системы были определены её структурно-функциональные характеристики, условия функционирования и расположения относительно границ КЗ, а также ряд реализованных в ней организационных и технических мер защиты. Экспертной группой в информационной системе рассматривались и определялись возможные уязвимости по следующим их видам:

* технологические или архитектурные – отсутствие определенных механизмов, технологий обеспечения информационной безопасности;
* организационные – отсутствие документированных требований, процессов обеспечения информационной безопасности;
* эксплуатационные – уязвимости, связанные с недостатками в существующих компонентах ИТ-инфраструктуры.

Также учитывались положения национального стандарта ГОСТ P 56546—2015 «Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем» по классификации уязвимостей в ИС и были использованы следующие классификационные признаки:

* область происхождения уязвимостей ИС;
* типы недостатков ИС;
* место возникновения (проявления) уязвимостей ИС.

В качестве уязвимых компонентов {Название ИС} рассматривались: общесистемное (общее), прикладное, специальное программное обеспечение, технические средства обработки информации, сетевое (коммуникационное, телекоммуникационное) оборудование, средства защиты информации.

В процессе анализа и определения возможных эксплуатационных уязвимостей в {Название ИС} установлено:

* …

В процессе алализа и определения организационных уязвимостей в {Название ИС} установлено:

* …

В результате анализа возможных уязвимостей с учетом классификации, данной в ГОСТ P 56546 – 2015 «Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем» были выявлены следующие виды уязвимостей, характерных для :

{Vulnerabilities}

В соответствии с исходным перечнем возможных уязвимостей были выбраны угрозы, при реализации которых они могут быть использованы (таблица № ).

Таблица № – Перечень угроз безопасности информации, выбранных в соответствии с возможными уязвимостями, существующими в {Название ИС}

{NSD\_Filter\_2\_Vuls}

## 3.4 Предположения о возможных способах реализации угроз безопасности информации нарушителем в {Название ИС}

Целью определения возможных способов реализации угроз безопасности информации является формирование предположений о возможных сценариях реализации угроз безопасности информации, описывающих последовательность (алгоритмы) действий отдельных видов нарушителей или групп нарушителей и применяемые ими методы и средства для реализации угроз безопасности информации.

С учетом структурно-функциональных характеристик, особенностей функционирования и данных о её возможных нарушителях группой экспертов из состава специалистов органа по аттестации Федерального государственного бюджетного образовательного высшего образования «Дальневосточный государственный университет путей сообщения» были определены следующие возможныеспособы реализации УБИ в {Название ИС}:

{Implement\_List}

Также предполагается, что при возможных способах реализации угроз безопасности в нарушитель может действовать один или в составе группы нарушителей и в отношении информационной системы.

Таким образом, были отобраны угрозы, соответствующие определенным возможным способам реализации УБИ (Таблица №).

Таблица № – Перечень УБИ, выбранных в соответствии с возможными способами их реализации

{NSD\_Filter\_3\_Implement}

## 4 Оценка уровня проектной защищенности информационной системы

Под уровнем проектной защищенности (Y1П) понимается исходная защищенность информационной системы, обусловленная заданными при проектировании структурно-функциональными характеристиками и условиями ее функционирования. Уровень проектной защищенности (Y1П) {Название ИС} определяется на основе анализа проектных структурно-функциональных характеристик, приведенных в таблице №.

Таблица № – Показатели проектной защищенности

| Структурно-функциональные характеристики ИС, условия ее эксплуатации | Уровень проектной защищенности ИС (Y1П) | | |
| --- | --- | --- | --- |
| Высокий | Средний | Низкий |
| По структуре ИС: |  |  |  |
| * автономное автоматизированное рабочее место; |  |  |  |
| * локальная ИС; |  |  |  |
| * распределенная ИС |  |  |  |
| По используемым информационным технологиям: |  |  |  |
| * системы на основе виртуализации; |  |  |  |
| * системы, реализующие «облачные вычисления»; |  |  |  |
| * системы с мобильными устройствами; |  |  |  |
| * системы с технологиями беспроводного доступа; |  |  |  |
| * грид-системы; |  |  |  |
| * суперкомпьютерные системы |  |  |  |
| По архитектуре информационной системы: |  |  |  |
| * системы на основе «тонкого клиента»; |  |  |  |
| * системы на основе одноранговой сети; |  |  |  |
| * файл-серверные системы; |  |  |  |
| * центры обработки данных; |  |  |  |
| * системы с удаленным доступом пользователей; |  |  |  |
| * использование разных типов операционных систем (гетерогенность среды); |  |  |  |
| * использование прикладных программ, независимых от операционных систем; |  |  |  |
| * использование выделенных каналов связи |  |  |  |
| По наличию (отсутствию) взаимосвязей с иными информационными системами: |  |  |  |
| * взаимодействующая с системами; |  |  |  |
| * невзаимодействующая с системами |  |  |  |
| По наличию (отсутствию) взаимосвязей (подключений) к сетям связи общего пользования: |  |  |  |
| * подключенная; |  |  |  |
| * подключенная через выделенную инфраструктуру (gov.ru или иную); |  |  |  |
| * неподключенная |  |  |  |
| По размещению технических средств: |  |  |  |
| * расположенные в пределах одной контролируемой зоны; |  |  |  |
| * расположенные в пределах нескольких контролируемых зон; |  |  |  |
| * расположенные вне контролируемой зоны |  |  |  |
| По режимам обработки информации в ИС: |  |  |  |
| * многопользовательский; |  |  |  |
| * однопользовательский |  |  |  |
| По режимам разграничения прав доступа: |  |  |  |
| * без разграничения; |  |  |  |
| * с разграничением |  |  |  |
| По режимам разделения функций по управлению информационной системой: |  |  |  |
| * без разделения; |  |  |  |
| * выделение рабочих мест для администрирования в отдельный домен; |  |  |  |
| * использование различных сетевых адресов; |  |  |  |
| * использование выделенных каналов для администрирования |  |  |  |
| По подходам к сегментированию ИС: |  |  |  |
| * без сегментирования; |  |  |  |
| * с сегментированием |  |  |  |
| Общее количество решений | 5 | 14 | 16 |
| Величина в % одного положительного решения | 20% | 7,14% | 6,25% |
| Процент характеристик, соответствующих уровню «высокий» |  |  |  |
| Процент характеристик, соответствующих уровню «средний» |  |  |  |
| Процент характеристик, соответствующих уровню «низкий» |  |  |  |

По результатам анализа структурно-функциональных характеристик {Название ИС} был присвоен **«****{Project\_Security}»** уровень проектной защищённости.

Угрозы безопасности информации, не связанные с информационными технологиями, применяемыми в {Название ИС}, будут неактуальны для данной информационной системы, таким образом, перечень угроз, выбранных в соответствии с определенными нарушителями и возможным способам реализации, был изменен с учетом информационных технологий и структурно-функциональных характеристик . В таблице № приведено описание УБИ из итогового перечня.

Таблица № – Перечень УБИ, выбранных в соответствии с информационными технологиями и структурно-функциональными характеристиками {Название ИС}

{NSD\_Filter\_4\_SFH}

## 5 Определение актуальных угроз безопасности информации

## 5.1 Определение актуальных угроз, реализуемых за счёт НСД к информации, обрабатываемой в {Название ИС}

В качестве исходных данных об угрозах безопасности информации и их характеристиках используется банк данных угроз безопасности информации, сформированный и поддерживаемый ФСТЭК России ([www.bdu.fstec.ru/](http://www.bdu.fstec.ru/)), а также базовые и типовые модели угроз безопасности информации, разрабатываемые ФСТЭК России для различных классов и типов информационных систем.

## 5.1.1 Возможность реализации угроз безопасности информации в информационной системе

Возможность реализации j – ой угрозы безопасности информации (Yj) оценивается, исходя из уровня проектной защищенности информационной системы (Y1П) и потенциала нарушителя (Y2), необходимого для реализации этой угрозы безопасности информации в информационной системе с заданными структурно-функциональными характеристиками и особенностями функционирования:

**Yj = [уровень проектной защищенности (Y1П); потенциал нарушителя (Y2)].**

Возможность реализации определяется для угроз из банка данных угроз безопасности информации, выбранных оператором в соответствии с потенциалом нарушителя, возможными способами их реализации, возможными уязвимостями, а также информационными технологиями, применяемыми в информационной системе. Решение о возможности реализации каждой j – ой угрозы принимается в соответствии с таблицей №.

Таблица № – Определение возможности реализации УБИ

|  |  |  |  |
| --- | --- | --- | --- |
| Уровень защищенности  (Y1П)  потенциал  нарушителя (Y2) | Высокий | Средний | Низкий |
| Базовый (низкий) | Низкая | Средняя | Высокая |
| Базовый повышенный (средний) | Средняя | Высокая | Высокая |
| Высокий | Высокая | Высокая | Высокая |

Результаты определения возможностей реализации УБИ представлены в таблице №.

Таблица № – Перечень угроз безопасности информации и возможности их реализации в {Название ИС}

{Feasibility}

## 5.1.2 Оценка степени возможного ущерба от реализации угроз безопасности информации в {Название ИС}

Для оценки степени возможного ущерба от реализации УБИ определяются:

* + возможный результат реализации УБИ в ИС;
  + вид ущерба, к которому может привести реализация УБИ;
  + степень последствия от реализации УБИ для каждого вида ущерба

В качестве результата реализации угрозы безопасности информации рассматриваются непосредственное или опосредованное воздействие на конфиденциальность, целостность, доступность информации, содержащейся в информационной системе. Результат реализации угрозы безопасности информации определяется воздействием угрозы на каждое свойство безопасности информации (конфиденциальность, целостность, доступность) в отдельности.

При обработке в информационной системе двух и более видов информации воздействие на конфиденциальность, целостность, доступность определяется отдельно для каждого вида информации (k, …, m), содержащейся в ИС.

Степень возможного ущерба от реализации угрозы безопасности информации определяется степенью негативных последствий от нарушения конфиденциальности, целостности или доступности каждого вида информации, содержащейся в информационной системе.

Степень негативных последствий от нарушения конфиденциальности, целостности или доступности информации определяется для каждого вида ущерба, зависит от целей и задач, решаемых информационной системой, и может иметь разные значения для разных обладателей информации и операторов. В качестве единой шкалы измерения степени негативных последствий принимаются значения «незначительные», «умеренные» и «существенные» негативные последствия, в свою очередь степень ущерба определяется как «высокая», «средняя» или «низкая» в зависимости от показателей степени негативных последствий.

По результатам оценок экспертов были определены степени возможного ущерба, который может наступить в результате реализации выявленных угроз безопасности информации в {Название ИС} (таблица №).

Таблица № – Степень возможного ущерба от реализации угроз безопасности информации в {Название ИС}

| № п/п | Идентификатор и название УБИ | Степень ущерба в результате нарушения каждого свойства безопасности относительно всех видов ущерба | Итоговая степень ущерба |
| --- | --- | --- | --- |
|  |

## 5.1.3 Актуальность угроз безопасности информации, реализуемых за счет НСД к информации, обрабатываемой в {Название ИС}

Решение об актуальности угрозы безопасности информации относительно информационной системы с заданными структурно-функциональными характеристиками и условиями функционирования принимается в соответствии с таблицей №.

Таблица № – Определение актуальности угроз безопасности информации

|  |  |  |  |
| --- | --- | --- | --- |
| Возможность реализации угрозы (Yj) | Степень возможного ущерба (Хj) | | |
| Низкая | Средняя | Высокая |
| Низкая | неактуальная | неактуальная | актуальная |
| Средняя | неактуальная | актуальная | актуальная |
| Высокая | актуальная | актуальная | актуальная |

Результат определения актуальности угроз безопасности информации для {Название ИС} представлена в таблице №.

Таблица № – Актуальность угроз безопасности информации для {Название ИС}

{ACT\_NSD}