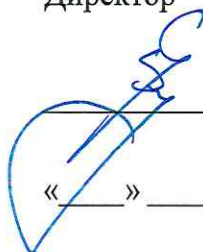


УТВЕРЖДАЮ

Фонд капитального ремонта
многоквартирных домов Вологодской
области

Директор



И.В. Михельсон

« » 2021 года

**МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ
«АСУ ЖКХ Капитальный ремонт»**

Фонда капитального ремонта многоквартирных домов Вологодской области

СОДЕРЖАНИЕ

Термины и определения.....	3
Обозначения и сокращения	5
1. Общие положения	6
1.1. Назначение и область действия документа.....	6
1.2. Источники разработки.....	6
1.3. Обладатель информации	7
1.4. Оператор ИСПДн.....	7
1.5. Ответственные за обеспечение безопасности.....	7
1.6. Разработчик Модели угроз	7
1.7. Экспертная группа для оценки актуальности угроз.....	7
2. Описание и характеристики информационной системы персональных данных.....	9
2.1. Наименование ИСПДн	9
2.2. Уровень защищенности ПДн в ИСПДн.....	9
2.3. Назначение ИСПДн	9
2.4. Состав защищаемой информации	9
2.5. Характеристики ИСПДн	9
3. Возможные негативные последствия от реализации (возникновения) угроз безопасности информации.....	11
3.1. Виды рисков (ущербов), актуальных для оператора ИСПДн	12
3.2. Возможные негативные последствия, наступление которых может привести к возникновению рисков (ущербов)	12
4. Возможные объекты воздействия угроз безопасности информации	16
5. Источники угроз безопасности информации.....	22
6. Способы реализации (возникновения) угроз безопасности информации	38
7. Актуальные угрозы безопасности информации.....	49
7.1. Определение возможных (вероятных) угроз безопасности информации	49
7.2. Определение возможных сценариев реализации угроз безопасности информации.....	52
7.3. Определение актуальности угроз безопасности информации	63
7.4. Выводы об актуальности угроз безопасности информации.....	73
8. Определение актуальности использования СКЗИ для обеспечения безопасности персональных данных и необходимого класса СКЗИ.....	77

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Архитектура систем и сетей – совокупность основных структурно-функциональных характеристик, свойств, компонентов систем и сетей, воплощенных в информационных ресурсах и компонентах, правилах их взаимодействия, режимах обработки информации;

Взаимодействующая (смежная) система – система или сеть, которая в рамках установленных функций имеет взаимодействие посредством сетевых интерфейсов с системой и сетью оператора и не включена им в границу процесса оценки угроз безопасности информации;

Возможности нарушителя – мера усилий нарушителя для реализации угрозы безопасности информации, выраженная в показателях компетентности, оснащенности ресурсами и мотивации нарушителя;

Граница оценки угроз безопасности информации – совокупность информационных ресурсов и компонентов систем и сетей, в пределах которой обеспечивается защита информации (безопасность) в соответствии с едиными правилами и процедурами, а также контроль за реализованными мерами защиты информации (обеспечения безопасности);

Информационные ресурсы – информация, данные, представленные в форме, предназначенной для хранения и обработки в системах и сетях;

Компонент (системы, сети) – программное, программно-аппаратное или техническое средство, входящее в состав систем и сетей;

Обеспечивающие системы – инженерные системы, включающие системы электроснабжения, вентиляции, охлаждения, кондиционирования, охраны и другие инженерные системы, а также средства, каналы и системы, предназначенные для оказания услуг связи, других услуг и сервисов, предоставляемых сторонними организациями, от которых зависит функционирование систем и сетей;

Обладатель информации – лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;

Оператор – лицо, осуществляющее деятельность по эксплуатации систем и сетей, в том числе по обработке содержащейся в них информации;

Основные (критические) процессы (бизнес-процессы) – управленческие, организационные, технологические, производственные, финансово-экономические и иные основные процессы (бизнес-процессы), выполняемые владельцем информации, оператором в рамках реализации функций (полномочий) или осуществления основных видов деятельности, нарушение и (или) прекращение которых может привести к возникновению рисков (ущербу);

Пользователь – лицо, которому разрешено выполнять некоторые действия (операции) по обработке информации в системе или сети и использующее результаты ее функционирования;

Поставщик услуг – лицо, предоставляющее оператору и (или) владельцу на основании договора или ином законном основании услуги по использованию своих вычислительных ресурсов, программного обеспечения, средств хранения или передачи информации;

Программно-аппаратное средство – устройство, состоящее из аппаратного обеспечения и функционирующего на нем программного обеспечения, участвующее в формировании, обработке, передаче или приеме информации;

Угроза безопасности информации – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации;

Уязвимость – недостаток (слабость) программного (программно-технического) средства или системы и сети в целом, который(ая) может быть использован(а) для реализации угроз безопасности информации.

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

АИС	–	автоматизированная информационная система
АРМ	–	автоматизированное рабочее место
АС	–	автоматизированная система
ВИ	–	виртуальная инфраструктура
ЗИ	–	защищаемая информация
ИСПДн	–	информационная система персональных данных
ЛВС	–	локальная вычислительная сеть
НСД	–	несанкционированный доступ
ОС	–	операционная система
ПДн	–	персональные данные
ПО	–	программное обеспечение
ПЭМИН	–	побочные электромагнитные излучения и наводки
СЗИ	–	средства защиты информации
ПСЗИ	–	программные средства защиты
СКЗИ	–	средства криптографической защиты информации
СФ	–	среда функционирования
УБИ	–	угрозы безопасности информации

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Назначение и область действия документа

В соответствии со статьей 19 Федерального закона № 152-ФЗ от 27 июля 2006 г. «О персональных данных», персональные данные должны быть защищены от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения, а также от иных неправомерных действий. Угрозы безопасности ПДн при их обработке в ИСПДн могут быть связаны как с непреднамеренными действиями персонала ИСПДн и (или) потребителей, пользующихся услугами, предоставляемыми ИСПДн в соответствии с ее назначением, так и со специально осуществляемыми неправомерными действиями иностранных государств, криминальных сообществ, отдельных организаций и граждан, а также иными источниками угроз.

Настоящая Модель угроз безопасности информации информационной системы персональных данных «АСУ ЖКХ Капитальный ремонт» (далее – Модель угроз) Фонда капитального ремонта многоквартирных домов Вологодской области (далее – Фонд капитального ремонта МКД ВО) разработана для определения угроз безопасности информации, реализация (возникновение) которых возможна в ИСПДн «АСУ ЖКХ Капитальный ремонт».

При проведении работ по определению актуальных угроз безопасности информации рассмотрен сценарий, при котором отсутствуют организационные и технические меры по защите информации, с целью формирования исходного (проектного) состояния ИСПДн с соответствующим перечнем актуальных угроз. Исходное (проектное) состояние ИСПДн с соответствующим перечнем актуальных угроз позволит правильно определить требования к системе защиты информации ИСПДн «АСУ ЖКХ Капитальный ремонт».

1.2. Источники разработки

При разработке Модели угроз использовались следующие нормативные правовые акты, методические документы и национальные стандарты:

а) Федеральный закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

б) Федеральный закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

в) Постановление Правительства РФ от 01 ноября 2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

г) Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

д) Приказ Федеральной службы безопасности Российской Федерации от 10 июля 2014 г. № 378 г. Москва «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных

Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;

е) Инструкция об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведения, составляющие государственную тайну, утвержденная Приказом ФАПСИ от 13.06.2001 № 152;

ж) Методический документ «Методика оценки угроз безопасности информации» утв. ФСТЭК России 05 февраля 2021 г.;

з) «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» (утверждены руководством 8 Центра ФСБ России 31 марта 2015 года № 149/7/2/6-432);

и) В качестве исходных данных для определения угроз безопасности информации использовался Банк данных угроз безопасности информации (bdu.fstec.ru), ведение которого осуществляется ФСТЭК России;

к) Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утв. зам. директора ФСТЭК России 15 февраля 2008 г.).

1.3. Владелец информации

Владельцем информации, обрабатываемой в ИСПДн «АСУ ЖКХ Капитальный ремонт» является Фонд капитального ремонта МКД ВО.

1.4. Оператор ИСПДн

Оператором ИСПДн «АСУ ЖКХ Капитальный ремонт» является Фонд капитального ремонта МКД ВО.

1.5. Ответственные за обеспечение безопасности

Ответственным лицом за обеспечение безопасности информации в Фонде капитального ремонта МКД ВО является Начальник отдела ИТ и АХО Сугрин Дмитрий Александрович.

1.6. Разработчик Модели угроз

Разработка Модели угроз осуществлялась специалистами Фонда капитального ремонта МКД ВО.

1.7. Экспертная группа для оценки актуальности угроз

Оценка угроз безопасности информации проводится с использованием экспертного метода. С целью оценки негативных последствий от реализации угроз безопасности информации, возможных целей нарушителей, актуальности сценариев реализации угроз безопасности информации ИСПДн «АСУ ЖКХ Капитальный ремонт» из штатных сотрудников Фонда капитального ремонта МКД ВО была сформирована экспертная группа:

Руководитель экспертной группы:

Начальник отдела ИТ и АХО

Сугрин Д.А.

Члены экспертной группы:

Начальник договорного отдела

Узорова О.Г.

Начальник отдела правовой и кадровой работы

Вицина И.М.

2. ОПИСАНИЕ И ХАРАКТЕРИСТИКИ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. Наименование ИСПДн

Настоящая Модель угроз разработана для ИСПДн «АСУ ЖКХ Капитальный ремонт».

2.2. Уровень защищенности ПДн в ИСПДн

В ИСПДн «АСУ ЖКХ Капитальный ремонт» необходимо обеспечение 3 уровня защищенности персональных данных, обрабатываемых в ИСПДн.

2.3. Назначение ИСПДн

ИСПДн «АСУ ЖКХ Капитальный ремонт» предназначена для обработки персональных данных клиентов Фонда капитального ремонта МКД ВО.

2.4. Состав защищаемой информации

В ИСПДн содержится следующая защищаемая информация:

– персональные данные.

В ИСПДн осуществляется обработка информации ограниченного доступа, не содержащая сведений, составляющих государственную тайну.

2.5. Характеристики ИСПДн

Основные характеристики ИСПДн «АСУ ЖКХ Капитальный ремонт» приведены в Таблице №1.

Таблица №1

№ п/п	Характеристики	Описание
Общие характеристики ИСПДн		
1.	Основные процессы, для обеспечения которых функционирует система	Автоматизация работы Фонда капитального ремонта МКД ВО; Автоматизации управления, планирования и контроля над региональной системой капитального ремонта.
2.	Местонахождение ИСПДн	160013, Вологодская область, г. Вологда, ул. Маршала Конева, дом 15
3.	Наличие контролируемой зоны	Контролируемая зона определена приказом. Работники Фонда капитального ремонта МКД ВО ознакомлены с границами контролируемой зоны (под подпись в соответствующем локальном акте). Доступ к ИСПДн имеют только те сотрудники Фонда капитального ремонта МКД ВО, которые определены в соответствующем локальном акте.
4.	Физическая и пожарная защита	В здании, где располагается ИСПДн, ведется видеонаблюдение. Помещения в которых располагается ИСПДн оборудованы дверями с замком. В не рабочее время помещения закрываются. Помещения ИСПДн оснащены охранно-пожарной сигнализацией с выводом на пульт охраны.
5.	Наличие соединения с сетями общего пользования	ИСПДн имеет доступ к информационно-телекоммуникационной сети международного информационного обмена «Интернет».
6.	Взаимосвязи с другими информационными системами	ИСПДн взаимодействует с информационными системами РФ и области.

№ п/п	Характеристики	Описание	
7.	Каналы (линии) связи и меры по ограничению несанкционированного доступа к защищаемой информации	Утверждены ОРД по защите информации, осуществляется контроль за выполнением требований. Осуществляется разграничение доступа к информации, введены меры по идентификации и аутентификации пользователей.	
8.	Внешние интерфейсы сетевого оборудования	Сетевые интерфейсы коммутаторов / маршрутизаторов внутри и (или) на границе ИСПДн	
Технические характеристики серверов			
9.	Общее количество	3 сервера	
10.	Местонахождение серверов	г. Вологда Конева, 15, офис 205	
11.	Программное обеспечение	Лицензионное системное ПО на базе операционных систем Microsoft Windows. АСУ ЖКХ Капитальный ремонт. Свободно распространяемое ПО.	
12.	Средства резервирования	Штатные средства ОС и СУБД	
13.	Доступные внешние интерфейсы	Пользовательский веб-интерфейс доступа к базе данных ИСПДн; Пользовательский интерфейс, используемый для доступа к базе данных ИСПДн; Интерфейс администрирования базы данных ИСПДн; Интерфейс ввода аутентификационной информации; Сетевые интерфейсы сервера ИСПДн; Интерфейсы подключения внешних устройств (USB, COM); Интерфейсы подключения съемных и несъемных машинных носителей информации; Интерфейс локального администрирования сервера ИСПДн; Интерфейс удаленного администрирования сервера ИСПДн	
Технические характеристики рабочих станций			
14.	Местонахождение рабочих станций	Вологодская область, г. Вологда, ул. Маршала Конева, дом 15 Вологодская область, г. Череповец, ул. Metallургов, 42	
15.	Аппаратное обеспечение	IBM-PC-совместимые автоматизированные рабочие места	
16.	Операционные системы	ОС Microsoft Windows	
17.	Программное обеспечение	Лицензионное системное ПО на базе операционных систем Microsoft Windows. Лицензионное прикладное ПО в составе офисного пакета Microsoft Office различных версий. АСУ ЖКХ Капитальный ремонт. Свободно распространяемое ПО.	
18.	Средства резервирования АРМ	Стандартные средства операционной системы.	
19.	Доступные внешние интерфейсы	Интерфейс ввода аутентификационной информации; Сетевой интерфейс АРМ пользователя ИСПДн; Интерфейсы подключения внешних устройств (USB, COM); Интерфейсы подключения съемных и несъемных машинных носителей информации; Сетевой интерфейс удаленного АРМ пользователя ИСПДн; Пользовательский интерфейс прикладного ПО ИСПДн; Интерфейс администрирования прикладного ПО ИСПДн; Пользовательский интерфейс редактирования конфигурационных и информационных файлов; Интерфейс ввода аутентификационной информации электронных почтовых ящиков	
Описание пользователей ИСПДн			
20.	Режим обработки информации	Многопользовательский	
21.	Разграничение доступа к информации	С разграничением доступа к информации	
22.	Группы внутренних пользователей ИСПДн и их уровень доступа	Группа	Уровень доступа
		Администраторы	Полный доступ
		Пользователи	Чтение, запись
23.	Группы внешних пользователей ИСПДн и их уровень доступа	Группа	Уровень доступа
		Внешние пользователи	Только чтение

3. ВОЗМОЖНЫЕ НЕГАТИВНЫЕ ПОСЛЕДСТВИЯ ОТ РЕАЛИЗАЦИИ (ВОЗНИКНОВЕНИЯ) УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

В ходе оценки угроз безопасности информации определяются негативные последствия, которые могут наступить от реализации (возникновения) угроз безопасности информации.

Исходными данными для определения негативных последствий от реализации угроз безопасности информации являются:

- 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. №1085, а также отраслевые (ведомственные, корпоративные) модели угроз безопасности информации;

- нормативные правовые акты Российской Федерации, в соответствии с которыми создается и функционирует ИСПДн, содержащие в том числе описание назначения, задач (функций) ИСПДн, состав обрабатываемой информации и ее правовой режим;

- документация на ИСПДн (в части сведений о назначении и функциях ИСПДн, о составе и архитектуре ИСПДн);

- технологические, производственные карты или иные документы, содержащие описание основных (критических) процессов (бизнес-процессов) обладателя информации, оператора;

- результаты оценки рисков (ущерба), проведенной обладателем информации или оператором.

На основе анализа исходных данных определяются событие или группа событий, наступление которых в результате реализации (возникновения) угроз безопасности информации может привести к:

- нарушению прав граждан;
- возникновению ущерба в области обеспечения обороны страны, безопасности государства и правопорядка, а также в социальной, экономической, политической, экологической сферах деятельности государства;

- возникновению финансовых, производственных, репутационных или иных рисков (видов ущерба) для обладателя информации, оператора.

Событие или группа событий определяются применительно к нарушению основных (критических) процессов (бизнес-процессов), выполнение которых обеспечивает ИСПДн, и применительно к нарушению безопасности информации, содержащейся в ИСПДн.

В случае отсутствия у обладателя информации или оператора результатов оценки рисков (ущерба), возможные негативные последствия от реализации угроз безопасности информации определяются на основе экспертной оценки специалистов, проводящих оценку угроз безопасности информации, на основе информации, представляемой профильными подразделениями или специалистами обладателя информации или оператора.

Определяемые в ходе оценки угроз безопасности информации негативные последствия должны быть конкретизированы применительно к областям и особенностям деятельности обладателя информации или оператора. Для систем и сетей обладателя информации или оператора может быть определено одно или несколько негативных последствий.

3.1. Виды рисков (ущербов), актуальных для оператора ИСПДн

В соответствии с Методическим документом «Методика оценки угроз безопасности информации», утвержденным ФСТЭК России 05.02.2021 г. (далее – Методика), для оператора ИСПДн определяется следующий типовой перечень возможных рисков (ущербов):

- Ущерб физическому лицу;
- Риски юридическому лицу, индивидуальному предпринимателю, связанные с хозяйственной деятельностью;
- Ущерб государству в области обеспечения обороны страны, безопасности государства и правопорядка, а также в социальной, экономической, политической, экологической сферах деятельности.

В соответствии с экспертной оценкой, представителями Фонда капитального ремонта МКД ВО были признаны актуальными следующие типы рисков (ущербов):

- Ущерб физическому лицу;
- Риски юридическому лицу, индивидуальному предпринимателю, связанные с хозяйственной деятельностью.

3.2. Возможные негативные последствия, наступление которых может привести к возникновению рисков (ущербов)

Определение возможных негативных последствий производится экспертным методом экспертной группой, состав которой приведен в Главе 1 настоящей Модели угроз. В ходе работы экспертной группы проводится опрос ее членов с целью определить, возможно ли соответствующее негативное последствие в случае реализации угроз безопасности информации или нет. Оценка производится в 2 раунда. Опрос экспертов включает следующие этапы:

- каждый эксперт проводит оценку возможности негативных последствий по числовой шкале от «1» до «10»;
- в каждом раунде после оценки соответствующего негативного последствия каждым членом экспертной группы отбрасываются минимальные и максимальные оценки;
- определяется среднее значение в каждом раунде;
- определяется итоговое среднее значение по всем раундам.

Негативные последствия считаются актуальными, если итоговое среднее значение больше или равно «7».

Результаты опроса экспертной группы представлены в Таблице №2.

Таблица №2

№ п/п	Раунд 1				Раунд 2				Общий итог	Актуальность
	Сугрин Д.А.	Узорова О.Г.	Вицина И.М.	Итог раунда 1	Сугрин Д.А.	Узорова О.Г.	Вицина И.М.	Итог раунда 2		
Ущерб физическому лицу										
1	Угроза жизни или здоровью									
	1	1	1	1	1	1	1	1	1	нет
2	Унижение достоинства личности									
	1	1	1	1	1	1	1	1	1	нет
3	Нарушение свободы, личной неприкосновенности									
	1	1	1	1	1	1	1	1	1	нет
4	Нарушение неприкосновенности частной жизни									
	1	1	1	1	1	1	1	1	1	нет
5	Нарушение личной, семейной тайны, утрата чести и доброго имени									
	1	1	1	1	1	1	1	1	1	нет
6	Нарушение тайны переписки, телефонных переговоров, иных сообщений									
	1	1	1	1	1	1	1	1	1	нет
7	Нарушение иных прав и свобод гражданина, закрепленных в Конституции Российской Федерации и федеральных законах									
	1	1	1	1	1	1	1	1	1	нет
8	Финансовый, иной материальный ущерб физическому лицу									
	1	1	1	1	1	1	1	1	1	нет
9	Нарушение конфиденциальности (утечка) персональных данных									
	9	9	9	9	10	9	9	9	9	да
10	«Травля» гражданина в сети «Интернет»									
	10	7	10	10	7	10	7	7	8,5	да
11	Разглашение персональных данных граждан									
	9	10	10	10	10	9	9	9	9,5	да
Риски юридическому лицу, индивидуальному предпринимателю, связанные с хозяйственной деятельностью										
12	Нарушение законодательства Российской Федерации									
	8	6	8	8	8	9	8	8	8	да
13	Потеря (хищение) денежных средств									
	1	1	1	1	1	1	1	1	1	нет
14	Недополучение ожидаемой (прогнозируемой) прибыли									
	1	1	1	1	1	1	1	1	1	нет
15	Необходимость дополнительных (незапланированных) затрат на выплаты штрафов (неустоек) или компенсаций									
	9	7	8	8	7	8	7	7	7,5	да
16	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)									
	7	6	7	7	9	9	9	9	8	да

№ п/п	Раунд 1				Раунд 2				Общий итог	Актуальность
	Сугрин Д.А.	Узорова О.Г.	Вицина И.М.	Итог раунда 1	Сугрин Д.А.	Узорова О.Г.	Вицина И.М.	Итог раунда 2		
17	Нарушение штатного режима функционирования автоматизированной системы управления и управляемого объекта и/или процесса									
	1	1	1	1	1	1	1	1	1	нет
18	Срыв запланированной сделки с партнером									
	1	1	1	1	1	1	1	1	1	нет
19	Необходимость дополнительных (незапланированных) затрат на восстановление деятельности									
	9	7	9	9	7	9	9	9	9	да
20	Потеря клиентов, поставщиков									
	1	1	1	1	1	1	1	1	1	нет
21	Потеря конкурентного преимущества									
	1	1	1	1	1	1	1	1	1	нет
22	Невозможность заключения договоров, соглашений									
	1	1	1	1	1	1	1	1	1	нет
23	Нарушение деловой репутации									
	1	1	1	1	1	1	1	1	1	нет
24	Снижение престижа									
	1	1	1	1	1	1	1	1	1	нет
25	Дискредитация работников									
	1	1	1	1	1	1	1	1	1	нет
26	Утрата доверия									
	1	1	1	1	1	1	1	1	1	нет
27	Причинение имущественного ущерба									
	4	3	6	4	2	5	3	3	3,5	нет
28	Неспособность выполнения договорных обязательств									
	1	1	1	1	1	1	1	1	1	нет
29	Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций)									
	8	9	8	8	8	9	9	9	8,5	да
30	Необходимость изменения (перестроения) внутренних процедур для достижения целей, решения задач (реализации функций)									
	3	2	6	3	6	5	3	5	4	нет
31	Принятие неправильных решений									
	1	1	1	1	1	1	1	1	1	нет
32	Простой ИСПДн									
	7	10	7	7	9	9	9	9	8	да
33	Публикация недостоверной информации на веб-ресурсах организации									
	9	10	10	10	10	7	8	8	9	да
34	Использование веб-ресурсов для распространения и управления вредоносным программным обеспечением									
	9	8	10	9	7	9	9	9	9	да

[illegible]

4. ВОЗМОЖНЫЕ ОБЪЕКТЫ ВОЗДЕЙСТВИЯ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

В ходе оценки угроз безопасности информации должны быть определены информационные ресурсы и компоненты ИСПДн, несанкционированный доступ к которым или воздействие на которые в ходе реализации (возникновения) угроз безопасности информации может привести к негативным последствиям – объекты воздействия. Совокупность объектов воздействия и их интерфейсов определяет границы процесса оценки угроз безопасности информации и разработки модели угроз безопасности информации.

Исходными данными для определения возможных объектов воздействия являются:

- общий перечень угроз безопасности информации, содержащейся 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. №1085, а также отраслевые (ведомственные, корпоративные) модели угроз безопасности информации;
- документация на ИСПДн (в части сведений о составе и архитектуре, о группах пользователей и уровне их полномочий и типах доступа, внешних и внутренних интерфейсах);
- договоры, соглашения или иные документы, содержащие условия использования информационно-телекоммуникационной инфраструктуры центра обработки данных или облачной инфраструктуры поставщика услуг (в случае функционирования ИСПДн на базе информационно-телекоммуникационной инфраструктуры центра обработки данных или облачной инфраструктуры);
- негативные последствия от реализации (возникновения) угроз безопасности информации, определенные в Главе 3 настоящей Модели угроз.

Указанные исходные данные могут быть дополнены иными документами и сведениями с учетом особенностей области деятельности, в которой функционирует ИСПДн.

На основе анализа исходных данных и результатов инвентаризации ИСПДн определяются следующие группы информационных ресурсов и компонентов ИСПДн, которые могут являться объектами воздействия:

- информация (данные), содержащаяся в ИСПДн (в том числе защищаемая информация, персональные данные, информация о конфигурации систем и сетей, данные телеметрии, сведения о событиях безопасности и др.);
- программно-аппаратные средства обработки и хранения информации (в том числе автоматизированные рабочие места, серверы, включая промышленные, средства отображения информации, программируемые логические контроллеры, производственное, технологическое оборудование (исполнительные устройства));
- программные средства (в том числе системное и прикладное программное обеспечение, включая серверы приложений, веб-приложений, системы управления базами данных, системы виртуализации);

- машинные носители информации, содержащие как защищаемую информацию, так и аутентификационную информацию;
- телекоммуникационное оборудование (в том числе программное обеспечение для управления телекоммуникационным оборудованием);
- средства защиты информации (в том числе программное обеспечение для централизованного администрирования средств защиты информации);
- привилегированные и непривилегированные пользователи систем и сетей, а также интерфейсы взаимодействия с ними;
- обеспечивающие системы.

На этапе создания ИСПДн объекты воздействия определяются на основе предполагаемых архитектуры и условий функционирования систем и сетей, определенных на основе изучения и анализа исходных данных. В ходе эксплуатации ИСПДн, в том числе при развитии (модернизации) ИСПДн, объекты воздействия определяются для реальных архитектуры и условий функционирования ИСПДн, полученных по результатам анализа исходных данных и инвентаризации ИСПДн. Инвентаризация ИСПДн проводится с использованием автоматизированных средств, которые позволяют определить компоненты ИСПДн, а также внешние и внутренние интерфейсы.

Для определенных информационных ресурсов и компонентов ИСПДн должны быть определены виды воздействия на них, которые могут привести к негативным последствиям. Основными видами таких воздействий являются:

- утечка (перехват) конфиденциальной информации или отдельных данных (нарушение конфиденциальности);
- несанкционированный доступ к компонентам, защищаемой информации, системным, конфигурационным, иным служебным данным;
- отказ в обслуживании компонентов (нарушение доступности);
- несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационных, иных служебных данных (нарушение целостности);
- несанкционированное использование вычислительных ресурсов ИСПДн в интересах решения несвойственных им задач;
- нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передачи и хранения информации.

Объекты воздействия определяются на аппаратном, системном и прикладном уровнях, на уровне сетевой модели взаимодействия, а также на уровне пользователей.

В процессе эксплуатации ИСПДн объекты воздействия и виды воздействия на них могут дополняться и изменяться относительно их состава и видов воздействия, определенных на этапе создания ИСПДн. В этом случае учет изменений должен проводиться в рамках реализации мероприятий по управлению конфигурацией ИСПДн и анализу угроз безопасности информации в ходе ее эксплуатации.

При оценке угроз безопасности информации в ИСПДн, функционирующей на базе информационно-телекоммуникационной инфраструктуры центра обработки данных или облачной инфраструктуры, объекты воздействия определяются с учетом состава и содержания услуг, предоставляемых поставщиком услуг (например, инфраструктура как услуга, платформа как услуга, программное обеспечение как услуга). Арендуемые или

используемые на ином законном основании программно-аппаратные средства и их интерфейсы, каналы связи, программное обеспечение (в том числе программное обеспечение виртуализации и построенных на его базе виртуальных машин, виртуальных серверов, систем управления виртуализацией, виртуальных каналов связи и т.д.) относятся к объектам воздействия, находящимся в границе оценки угроз безопасности информации оператора. В отношении остальной информационно-телекоммуникационной инфраструктуры центра обработки данных или облачной инфраструктуры угрозы безопасности информации оцениваются поставщиком услуг.

Объекты воздействия и виды воздействия на них должны быть конкретизированы применительно к архитектуре и условиям функционирования ИСПДн, а также областям и особенностям деятельности обладателя информации и оператора.

Объекты воздействия угроз безопасности информации ИСПДн «АСУ ЖКХ Капитальный ремонт» и виды воздействия на них, способные привести к определенным в Главе 3 негативным последствиям, представлены в Таблице №3.

Таблица №3

№ п/п	Негативные последствия	Объекты воздействия	Виды воздействия
1.	Нарушение конфиденциальности (утечка) персональных данных (У1)	База данных ИСПДн, содержащая ПДн граждан	Утечка ПДн из базы данных
		АРМ пользователя ИСПДн	Утечка ПДн с АРМ пользователя ИСПДн
		Удаленное АРМ пользователя ИСПДн	Утечка ПДн с АРМ удаленного пользователя ИСПДн
		Сервер ИСПДн	Утечка ПДн с сервера ИСПДн
		Линии связи ИСПДн	Утечка ПДн, передаваемых по линиям связи ИСПДн
		Прикладное ПО ИСПДн, участвующее в обработке ПДн граждан	Несанкционированный доступ к ПДн граждан, обрабатываемом в прикладном ПО ИСПДн
2.	«Травля» гражданина в сети «Интернет» (У1)	База данных ИСПДн, содержащая ПДн граждан	Утечка ПДн из базы данных
		АРМ пользователя ИСПДн	Утечка ПДн с АРМ пользователя ИСПДн
		Удаленное АРМ пользователя ИСПДн	Утечка ПДн с АРМ удаленного пользователя ИСПДн
		Сервер ИСПДн	Утечка ПДн с сервера ИСПДн
		Линии связи ИСПДн	Утечка ПДн, передаваемых по линиям связи ИСПДн
		Прикладное ПО ИСПДн, участвующее в обработке ПДн граждан	Несанкционированный доступ к ПДн граждан, обрабатываемом в прикладном ПО ИСПДн
3.	Разглашение персональных данных граждан (У1)	База данных ИСПДн, содержащая ПДн граждан	Утечка ПДн из базы данных
		АРМ пользователя ИСПДн	Утечка ПДн с АРМ пользователя ИСПДн
		Удаленное АРМ пользователя ИСПДн	Утечка ПДн с АРМ удаленного пользователя ИСПДн
		Сервер ИСПДн	Утечка ПДн с сервера ИСПДн
		Линии связи ИСПДн	Утечка ПДн, передаваемых по линиям связи ИСПДн
		Прикладное ПО ИСПДн, участвующее в обработке ПДн граждан	Несанкционированный доступ к ПДн граждан, обрабатываемом в прикладном ПО ИСПДн
4.	Нарушение	База данных ИСПДн, содержащая	Утечка ПДн из базы данных

№ п/п	Негативные последствия	Объекты воздействия	Виды воздействия
	законодательства Российской Федерации (У2)	ПДн граждан	
		АРМ пользователя ИСПДн	Утечка ПДн с АРМ пользователя ИСПДн
		Удаленное АРМ пользователя ИСПДн	Утечка ПДн с АРМ удаленного пользователя ИСПДн
		Сервер ИСПДн	Утечка ПДн с сервера ИСПДн
		Линии связи ИСПДн	Утечка ПДн, передаваемых по линиям связи ИСПДн
		Прикладное ПО ИСПДн, участвующее в обработке ПДн граждан	Несанкционированный доступ к ПДн граждан, обрабатываемом в прикладном ПО ИСПДн
5.	Необходимость дополнительных (незапланированных) затрат на выплаты штрафов (неустоек) или компенсаций	База данных ИСПДн, содержащая ПДн граждан	Утечка ПДн из базы данных
		АРМ пользователя ИСПДн	Утечка ПДн с АРМ пользователя ИСПДн
		Удаленное АРМ пользователя ИСПДн	Утечка ПДн с АРМ удаленного пользователя ИСПДн
		Сервер ИСПДн	Утечка ПДн с сервера ИСПДн
		Линии связи ИСПДн	Утечка ПДн, передаваемых по линиям связи ИСПДн
		Прикладное ПО ИСПДн, участвующее в обработке ПДн граждан	Несанкционированный доступ к ПДн граждан, обрабатываемом в прикладном ПО ИСПДн
6.	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)	АРМ пользователя ИСПДн	Нарушение функционирования (работоспособности) АРМ пользователя ИСПДн; Отказ в обслуживании
		Удаленное АРМ пользователя ИСПДн	Нарушение функционирования (работоспособности) удаленного АРМ пользователя ИСПДн; Отказ в обслуживании
		Сервер ИСПДн	Нарушение функционирования (работоспособности) сервера ИСПДн; Отказ в обслуживании
7.	Необходимость дополнительных (незапланированных) затрат на восстановление деятельности (У2)	АРМ пользователя ИСПДн	Нарушение функционирования (работоспособности) АРМ пользователя ИСПДн; Отказ в обслуживании
		Удаленное АРМ пользователя ИСПДн	Нарушение функционирования (работоспособности) удаленного АРМ пользователя ИСПДн; Отказ в обслуживании
		Сервер ИСПДн	Нарушение функционирования (работоспособности) сервера ИСПДн; Отказ в обслуживании
8.	Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций) (У2)	АРМ пользователя ИСПДн	Нарушение функционирования (работоспособности) АРМ пользователя ИСПДн; Отказ в обслуживании; Несанкционированное использование вычислительных ресурсов АРМ пользователя ИСПДн в интересах решения несвойственных ему задач
		Удаленное АРМ пользователя ИСПДн	Нарушение функционирования (работоспособности) удаленного

№ п/п	Негативные последствия	Объекты воздействия	Виды воздействия
			АРМ пользователя ИСПДн; Отказ в обслуживании; Несанкционированное использование вычислительных ресурсов удаленного АРМ пользователя ИСПДн в интересах решения несвойственных ему задач
		Сервер ИСПДн	Нарушение функционирования (работоспособности) сервера ИСПДн; Отказ в обслуживании; Несанкционированное использование вычислительных ресурсов сервера ИСПДн в интересах решения несвойственных ему задач
9.	Простой ИСПДн (У2)	АРМ пользователя ИСПДн	Нарушение функционирования (работоспособности) АРМ пользователя ИСПДн; Отказ в обслуживании
		Удаленное АРМ пользователя ИСПДн	Нарушение функционирования (работоспособности) удаленного АРМ пользователя ИСПДн; Отказ в обслуживании
		Сервер ИСПДн	Нарушение функционирования (работоспособности) сервера ИСПДн; Отказ в обслуживании; Несанкционированная модификация системных файлов сервера ИСПДн
10.	Публикация недостоверной информации на веб-ресурсах организации (У2)	Веб-приложение ИСПДн	Несанкционированный доступ к веб-приложению ИСПДн
		Конфигурационные и информационные файлы, используемые веб-приложениями ИСПДн	Несанкционированный доступ к конфигурационным и информационным файлам ИСПДн; Несанкционированная модификация конфигурационных и информационных файлов
11.	Использование веб-ресурсов для распространения и управления вредоносным программным обеспечением (У2)	Сервер ИСПДн	Нарушение функционирования (работоспособности) сервера ИСПДн; Отказ в обслуживании; Несанкционированная модификация системных файлов сервера ИСПДн
		Веб-приложение ИСПДн	Несанкционированный доступ к веб-приложению ИСПДн; Несанкционированная модификация исходного кода веб-приложения, внедрение кода вредоносного ПО
		Конфигурационные и информационные файлы, используемые веб-приложениями ИСПДн	Несанкционированный доступ к конфигурационным и информационным файлам ИСПДн; Несанкционированная модификация конфигурационных и информационных файлов
12.	Рассылка информационных	АРМ пользователя ИСПДн	Несанкционированное использование вычислительных

№ п/п	Негативные последствия	Объекты воздействия	Виды воздействия
	сообщений с использованием вычислительных мощностей оператора и (или) от его имени (У2)		ресурсов АРМ пользователя ИСПДн в интересах решения несвойственных ему задач
		Удаленное АРМ пользователя ИСПДн	Несанкционированное использование вычислительных ресурсов удаленного АРМ пользователя ИСПДн в интересах решения несвойственных ему задач
		Сервер ИСПДн	Несанкционированное использование вычислительных ресурсов сервера ИСПДн в интересах решения несвойственных ему задач
		Учетные записи корпоративных электронных почтовых ящиков	Несанкционированный доступ к аутентификационной информации учетных записей корпоративных электронных почтовых ящиков

5. ИСТОЧНИКИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

В ходе оценки угроз безопасности информации должны быть определены возможные антропогенные источники угроз безопасности информации, к которым относятся лица (группа лиц), осуществляющие реализацию угроз безопасности информации путем несанкционированного доступа и (или) воздействия на информационные ресурсы и (или) компоненты ИСПДн, – актуальные нарушители.

Исходными данными для определения возможных актуальных нарушителей являются:

- 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. №1085, а также отраслевые (ведомственные, корпоративные) модели угроз безопасности информации;

- нормативные правовые акты Российской Федерации, в соответствии с которыми создается и функционирует ИСПДн, содержащие описание назначения, задач (функций) ИСПДн, состав обрабатываемой информации и ее правовой режим;

- документация на ИСПДн (в части сведений о назначении и функциях, составе и архитектуре ИСПДн, о группах пользователей и уровне их полномочий и типах доступа, о внешних и внутренних интерфейсах);

- договоры, соглашения или иные документы, содержащие условия использования информационно-телекоммуникационной инфраструктуры центра обработки данных или облачной инфраструктуры поставщика услуг (в части персонала поставщика услуг, имеющего доступ к этой инфраструктуре, его прав и обязанностей, уровня полномочий и типов доступа);

- результаты оценки ущерба (рисков), определенные в Главе 2 настоящей Модели угроз;

- негативные последствия от реализации (возникновения) угроз безопасности информации, определенные в Главе 3 настоящей Модели угроз;

- объекты воздействия угроз безопасности информации и виды воздействия на них, определенные в Главе 4 настоящей Модели угроз.

Указанные исходные данные могут быть дополнены иными документами и сведениями с учетом особенностей области деятельности, в которой функционируют ИСПДн.

На основе анализа исходных данных, а также результатов оценки возможных целей реализации нарушителями угроз безопасности информации определяются виды нарушителей, актуальных для ИСПДн. Основными видами нарушителей, подлежащих оценке, являются:

- 1) специальные службы иностранных государств;
- 2) террористические, экстремистские группировки;
- 3) преступные группы (криминальные структуры);
- 4) отдельные физические лица (хакеры);

- 5) конкурирующие организации;
- 6) разработчики программных, программно-аппаратных средств;
- 7) лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем;
- 8) поставщики услуг связи, вычислительных услуг;
- 9) лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ;
- 10) лица, обеспечивающие функционирование ИСПДн или обеспечивающих систем оператора (администрация, охрана, уборщики и др.);
- 11) авторизованные пользователи ИСПДн;
- 12) системные администраторы и администраторы безопасности;
- 13) бывшие (уволенные) работники (пользователи).

Указанные виды нарушителей могут быть дополнены иными нарушителями с учетом особенностей области деятельности, в которой функционирует ИСПДн. Для ИСПДн актуальными могут являться нарушители нескольких видов.

Нарушители признаются актуальными для ИСПДн, когда возможные цели реализации ими угроз безопасности информации могут привести к определенным для ИСПДн негативным последствиям и соответствующим рискам (видам ущерба).

Для актуальных нарушителей должны быть определены их категории в зависимости от имеющихся прав и условий по доступу к ИСПДн, обусловленных архитектурой и условиями функционирования ИСПДн, а также от установленных возможностей нарушителей. При этом нарушители подразделяются на две категории:

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

Внутренние нарушители первоначально могут иметь разный уровень прав доступа к информационным ресурсам и компонентам ИСПДн. К внутренним нарушителям относятся пользователи, имеющие как непривилегированные (пользовательские), так и привилегированные (административные) права доступа к информационным ресурсам и компонентам ИСПДн.

Внешние нарушители реализуют угрозы безопасности информации преднамеренно (преднамеренные угрозы безопасности информации) с использованием программных, программно-аппаратных средств или без использования таковых. Внутренние нарушители реализуют угрозы безопасности информации преднамеренно (преднамеренные угрозы безопасности информации) с использованием программных, программно-аппаратных средств или без использования таковых или непреднамеренно (непреднамеренные угрозы безопасности информации) без использования программных, программно-аппаратных средств.

При оценке возможностей нарушителей необходимо исходить из того, что для повышения уровня своих возможностей нарушители 1 вида могут вступать в сговор с нарушителями 5, 6, 7, 8, 9, 10, 11, 12 видов. Нарушители 2 вида могут вступать в сговор с нарушителями 10, 11, 12 видов. Нарушители 3 вида могут вступать в сговор с

нарушителями 10, 11, 12 видов. В случае принятия таких предположений цели и уровни возможностей нарушителей подлежат объединению.

Так как Фонд капитального ремонта МКД ВО является некоммерческой организацией, предполагается, что конкурирующие организации для Фонда капитального ремонта МКД ВО отсутствуют. Соответственно, можно предположить отсутствие целей реализации угроз безопасности информации для данного вида нарушителя.

Предполагается, что разработчики программных, программно-аппаратных средств, применяемых в ИСПДн «АСУ ЖКХ Капитальный ремонт», не заинтересованы в причинении ущерба Фонду капитального ремонта МКД ВО или гражданам, персональные данные которых обрабатываются в ИСПДн «АСУ ЖКХ Капитальный ремонт», вследствие отсутствия объективных мотивов для реализации угроз безопасности информации. Таким образом возможной целью данного вида нарушителя могут быть только непреднамеренные, неосторожные или неквалифицированные действия.

Предполагается, что поставщики услуг связи, вычислительных услуг не заинтересованы в причинении ущерба Фонду капитального ремонта МКД ВО или гражданам, персональные данные которых обрабатываются в ИСПДн «АСУ ЖКХ Капитальный ремонт», вследствие отсутствия объективных мотивов для реализации угроз безопасности информации. Таким образом возможной целью данного вида нарушителя могут быть только непреднамеренные, неосторожные или неквалифицированные действия.

Определение возможных целей потенциальных нарушителей применительно к ИСПДн «АСУ ЖКХ Капитальный ремонт» производится экспертным методом экспертной группой, состав которой приведен в Главе 1 настоящей Модели угроз. В ходе работы экспертной группы проводится опрос ее членов с целью определить, актуальны ли соответствующие цели реализации угроз безопасности информации потенциальными нарушителями или нет. Оценка производится в 2 раунда. Опрос экспертов включает следующие этапы:

- каждый эксперт проводит оценку целей реализации угроз безопасности информации по числовой шкале от «1» до «10»;
- в каждом раунде после оценки соответствующей цели каждым членом экспертной группы отбрасываются минимальные и максимальные оценки;
- определяется среднее значение в каждом раунде;
- определяется итоговое среднее значение по всем раундам.

Негативные последствия считаются актуальными, если итоговое среднее значение больше или равно «7».

Результаты опроса экспертной группы представлены в Таблице №4.

№ п/п	Раунд 1				Раунд 2				Общий итог	Актуальность																																												
	Сугрин Д.А.	Узорова О.Г.	Вицина И.М.	Итог раунда 1	Сугрин Д.А.	Узорова О.Г.	Вицина И.М.	Итог раунда 2																																														
1	Специальные службы иностранных государств Нанесение ущерба государству в области обеспечения обороны, безопасности и правопорядка, а также в иных отдельных областях его деятельности или секторах экономики, в том числе дискредитация или дестабилизация деятельности отдельных органов государственной власти, организаций, получение конкурентных преимуществ на уровне государства, срыв заключения международных договоров, создание внутривластного кризиса <table border="1"> <tr> <td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>нет</td></tr> </table>										1	1	1	1	1	1	1	1	1	1	нет																																	
1	1	1	1	1	1	1	1	1	1	нет																																												
2	Террористические, экстремистские группировки Совершение террористических актов, угроза жизни граждан <table border="1"> <tr> <td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>нет</td></tr> </table> Нанесение ущерба отдельным сферам деятельности или секторам экономики государства <table border="1"> <tr> <td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>нет</td></tr> </table> Дестабилизация общества <table border="1"> <tr> <td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>нет</td></tr> </table> Дестабилизация деятельности органов государственной власти, организаций <table border="1"> <tr> <td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>нет</td></tr> </table>										1	1	1	1	1	1	1	1	1	1	нет	1	1	1	1	1	1	1	1	1	1	нет	1	1	1	1	1	1	1	1	1	1	нет	1	1	1	1	1	1	1	1	1	1	нет
1	1	1	1	1	1	1	1	1	1	нет																																												
1	1	1	1	1	1	1	1	1	1	нет																																												
1	1	1	1	1	1	1	1	1	1	нет																																												
1	1	1	1	1	1	1	1	1	1	нет																																												
3	Преступные группы (криминальные структуры) Получение финансовой или иной материальной выгоды <table border="1"> <tr> <td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>нет</td></tr> </table> Желание самореализации (подтверждение статуса) <table border="1"> <tr> <td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>нет</td></tr> </table>										1	1	1	1	1	1	1	1	1	1	нет	1	1	1	1	1	1	1	1	1	1	нет																						
1	1	1	1	1	1	1	1	1	1	нет																																												
1	1	1	1	1	1	1	1	1	1	нет																																												
4	Отдельные физические лица (хакеры) Получение финансовой или иной материальной выгоды <table border="1"> <tr> <td>9</td><td>10</td><td>10</td><td>7</td><td>10</td><td>8</td><td>8</td><td>9</td><td>9</td><td>9</td><td>да</td></tr> </table> Любопытство или желание самореализации (подтверждение статуса) <table border="1"> <tr> <td>10</td><td>9</td><td>10</td><td>10</td><td>9</td><td>9</td><td>9</td><td>9,5</td><td>9,5</td><td>9,5</td><td>да</td></tr> </table>										9	10	10	7	10	8	8	9	9	9	да	10	9	10	10	9	9	9	9,5	9,5	9,5	да																						
9	10	10	7	10	8	8	9	9	9	да																																												
10	9	10	10	9	9	9	9,5	9,5	9,5	да																																												
5	Конкурирующие организации Получение конкурентных преимуществ <table border="1"> <tr> <td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>нет</td></tr> </table> Получение финансовой или иной материальной выгоды <table border="1"> <tr> <td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>нет</td></tr> </table>										1	1	1	1	1	1	1	1	1	1	нет	1	1	1	1	1	1	1	1	1	1	нет																						
1	1	1	1	1	1	1	1	1	1	нет																																												
1	1	1	1	1	1	1	1	1	1	нет																																												
6	Разработчики программных, программно-аппаратных средств Внедрение дополнительных функциональных возможностей в программные или программно-аппаратные средства на этапе разработки <table border="1"> <tr> <td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>нет</td></tr> </table> Получение конкурентных преимуществ <table border="1"> <tr> <td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>нет</td></tr> </table> Получение финансовой или иной материальной выгоды <table border="1"> <tr> <td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>нет</td></tr> </table>										1	1	1	1	1	1	1	1	1	1	нет	1	1	1	1	1	1	1	1	1	1	нет	1	1	1	1	1	1	1	1	1	1	нет											
1	1	1	1	1	1	1	1	1	1	нет																																												
1	1	1	1	1	1	1	1	1	1	нет																																												
1	1	1	1	1	1	1	1	1	1	нет																																												

№ п/п	Раунд 1				Раунд 2				Общий итог	Актуальность
	Сугрин Д.А.	Узорова О.Г.	Вицина И.М.	Итог раунда 1	Сугрин Д.А.	Узорова О.Г.	Вицина И.М.	Итог раунда 2		
7	1	1	1	1	1	1	1	1	1	нет
	Непреднамеренные, неосторожные или некалфицированные действия									
	6	8	7	7	8	10	9	9	8	да
	Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем									
	Получение финансовой или иной материальной выгоды									
8	7	9	8	8	7	9	9	9	8,5	да
	Непреднамеренные, неосторожные или некалфицированные действия									
	6	8	6	6	9	10	9	9	7,5	да
	Получение конкурентных преимуществ									
	1	1	1	1	1	1	1	1	1	нет
9	Поставщики услуг связи, вычислительных услуг									
	Получение финансовой или иной материальной выгоды									
	1	1	1	1	1	1	1	1	1	нет
	Непреднамеренные, неосторожные или некалфицированные действия									
	10	6	6	6	9	8	8	8	7	да
10	Получение конкурентных преимуществ									
	1	1	1	1	1	1	1	1	1	нет
	Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ									
	Получение финансовой или иной материальной выгоды									
	9	9	9	9	10	8	9	9	9	да
11	Непреднамеренные, неосторожные или некалфицированные действия									
	8	10	10	10	6	10	8	8	9	да
	Получение конкурентных преимуществ									
	1	1	1	1	1	1	1	1	1	нет
	Лица, обеспечивающие функционирование ИСПДн или обеспечивающих систем оператора (администрация, охрана, уборщики и др.)									
11	Получение финансовой или иной материальной выгоды									
	8	9	9	9	9	10	10	10	9,5	да
	Непреднамеренные, неосторожные или некалфицированные действия									
	6	9	9	9	10	8	10	10	9,5	да
	Авторизованные пользователи ИСПДн									
11	Получение финансовой или иной материальной выгоды									
	7	9	8	8	8	8	8	8	8	да
	Лобопытство или желание самореализации (подтверждение статуса)									
	8	7	8	8	6	10	9	9	8,5	да
	Мест за ранее совершенные действия									
	10	8	9	9	10	9	10	10	9,5	да

№ п/п	Раунд 1				Раунд 2				Общий итог	Актуальность
	Сугрин Д.А.	Узорова О.Г.	Вицина И.М.	Итог раунда 1	Сугрин Д.А.	Узорова О.Г.	Вицина И.М.	Итог раунда 2		
12	7	9	7	7	10	10	10	10	8,5	да
	Непреднамеренные, неосторожные или неквалифицированные действия									
	Системные администраторы и администраторы безопасности									
	Получение финансовой или иной материальной выгоды									
	7	10	10	10	9	8	9	9	9,5	да
	Любопытство или желание самореализации (подтверждение статуса)									
13	9	8	9	9	8	10	8	8	8,5	да
	Месть за ранее совершенные действия									
	10	7	10	10	8	10	9	9	9,5	да
	Непреднамеренные, неосторожные или неквалифицированные действия									
	10	10	10	10	9	9	9	9	9,5	да
	Бывшие (увольненные) работники (пользователи)									
	Получение финансовой или иной материальной выгоды									
	9	8	8	8	8	10	8	8	8	да
	Месть за ранее совершенные действия									
	10	10	10	10	6	10	7	7	8,5	да

После определения возможных целей реализации угрозы безопасности информации потенциальными нарушителями, были сопоставлены нарушители, их возможные цели реализации угрозы безопасности информации и возможные негативные последствия и виды рисков (ущерба) от их реализации (возникновения). Результаты сопоставления приведены в Таблице №5.

Таблица №5

Вид нарушителя	Возможные цели реализации угроз безопасности информации			Соответствие целей видам риска (ущерба) и возможным негативным последствиям
	Нанесение ущерба физическому лицу	Нанесение ущерба юридическому лицу, индивидуальному предпринимателю	Нанесение ущерба государству в области обеспечения обороны страны, безопасности государства и правопорядка, а также в социальной, экономической, политической, экологической сферах деятельности	
Специальные службы иностранных государств	Нанесение ущерба отдельному физическому лицу не соответствует предполагаемым целям	Нанесение ущерба юридическому лицу, индивидуальному предпринимателю	Дискредитация или дестабилизация деятельности отдельных органов государственной власти, организаций, получение	Возможные цели реализации угроз безопасности информации не соответствуют определенным видам риска

Вид нарушителя	Возможные цели реализации угроз безопасности информации			Соответствие целей видам риска (ущерба) и возможным негативным последствиям
	Нанесение ущерба физическому лицу	Нанесение ущерба юридическому лицу, индивидуальному предпринимателю	Нанесение ущерба государству в области обеспечения обороны страны, безопасности государства и правопорядка, а также в социальной, экономической, политической, экологической сферах деятельности	
	данного вида нарушителя	соответствует предполагаемым целям данного вида нарушителя	конкурентных преимуществ на уровне государства, срыв заключения международных договоров, создание внутривнутриполитического кризиса	(ущерба) и возможным негативным последствиям
Террористические, экстремистские группировки	Совершение террористических актов, угроза жизни граждан	Дестабилизация деятельности организаций	Нанесение ущерба отдельным сферам деятельности или секторам экономики государства. Дестабилизация общества. Дестабилизация деятельности органов государственной власти	Возможные цели реализации угроз безопасности информации не соответствуют определенным видам риска (ущерба) и возможным негативным последствиям
Преступные группы (криминальные структуры)	Получение финансовой или иной материальной выгоды. Желание самореализации (подтверждение статуса)	Получение финансовой или иной материальной выгоды. Желание самореализации (подтверждение статуса)	Нанесение ущерба государству не соответствует предполагаемым целям данного вида нарушителя	Возможные цели реализации угроз безопасности информации не соответствуют определенным видам риска (ущерба) и возможным негативным последствиям
Отдельные физические лица (хакеры)	Получение финансовой или иной материальной выгоды. Любопытство или желание самореализации (подтверждение статуса)	Получение финансовой или иной материальной выгоды. Любопытство или желание самореализации (подтверждение статуса)	Нанесение ущерба государству не соответствует предполагаемым целям данного вида нарушителя	У1 (Нарушение конфиденциальности (утечка) персональных данных; «Травля» гражданина в сети «Интернет»; Разглашение персональных данных граждан) У2 (Простой ИСПДн; Публикация недостоверной информации на веб-ресурсах организации; Использование веб-ресурсов для распространения и управления вредоносным программным обеспечением; Рассылка информационных сообщений с использованием

Вид нарушителя	Возможные цели реализации угроз безопасности информации			Соответствие целей видам риска (ущерба) и возможным негативным последствиям
	Нанесение ущерба физическому лицу	Нанесение ущерба юридическому лицу, индивидуальному предпринимателю	Нанесение ущерба области обеспечения обороны страны, безопасности государства и правопорядка, а также в социальной, экономической, политической, экологической сферах деятельности	
Конкурирующие организации	Нанесение ущерба отдельному физическому лицу не соответствует предполагаемым целям данного вида нарушителя	Нанесение ущерба юридическому лицу, индивидуальному предпринимателю не соответствует предполагаемым целям данного вида нарушителя	Нанесение ущерба государству не соответствует предполагаемым целям данного вида нарушителя	Возможные цели реализации угроз безопасности информации не соответствуют определенным видам риска (ущерба) и возможным негативным последствиям
Разработчики программных, программно-аппаратных средств	Нанесение ущерба отдельному физическому лицу не соответствует предполагаемым целям данного вида нарушителя	Непреднамеренные, неосторожные или некавалифицированные действия	Непреднамеренные, неосторожные или некавалифицированные действия	Возможные цели реализации угроз безопасности информации не соответствуют определенным видам риска (ущерба) и возможным негативным последствиям
Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем	Нанесение ущерба отдельному физическому лицу не соответствует предполагаемым целям данного вида нарушителя	Получение финансовой или иной материальной выгоды. Непреднамеренные, неосторожные или некавалифицированные действия. Получение конкурентных преимуществ	Непреднамеренные, неосторожные или некавалифицированные действия.	У2 (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); Необходимость дополнительных (незапланированных) затрат на восстановление деятельности; Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации

Вид нарушителя	Возможные цели реализации угроз безопасности информации			Соответствие целей видам риска (ущерба) и возможным негативным последствиям
	Нанесение ущерба физическому лицу	Нанесение ущерба юридическому лицу, индивидуальному предпринимателю	Нанесение ущерба государству в области обеспечения обороны страны, безопасности государства и правопорядка, а также в социальной, экономической, политической, экологической сферах деятельности	
Поставщики услуг связи, вычислительных услуг	Нанесение ущерба отдельному физическому лицу не соответствует предполагаемым целям данного вида нарушителя	Непреднамеренные, неосторожные или некаленифицированные действия.	Непреднамеренные, неосторожные или некаленифицированные действия.	функций); Простой ИСПДн) Возможные цели реализации угроз безопасности информации не соответствуют определенным видам риска (ущерба) и возможным негативным последствиям
Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ	Нанесение ущерба отдельному физическому лицу не соответствует предполагаемым целям данного вида нарушителя	Получение финансовой или иной материальной выгоды. Непреднамеренные, неосторожные или некаленифицированные действия. Получение конкурентных преимуществ	Непреднамеренные, неосторожные или некаленифицированные действия.	У2 (Необходимость дополнительных (незапланированных) затрат на восстановление деятельности; Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций); Простой ИСПДн)
Лица, обеспечивающие функционирование ИСПДн или обеспечивающих систем оператора (администрация, охрана, уборщики и др.)	Получение финансовой или иной материальной выгоды. Непреднамеренные, неосторожные или некаленифицированные действия.	Получение финансовой или иной материальной выгоды. Непреднамеренные, неосторожные или некаленифицированные действия	Непреднамеренные, неосторожные или некаленифицированные действия	У2 (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); Необходимость дополнительных (незапланированных) затрат на восстановление деятельности; Невозможность решения задач (реализации функций) или снижение эффективности

Вид нарушителя	Возможные цели реализации угроз безопасности информации			Соответствие целей видам риска (ущерба) и возможным негативным последствиям
	Нанесение ущерба физическому лицу	Нанесение ущерба юридическому лицу, индивидуальному предпринимателю	Нанесение ущерба государству в области обеспечения обороны страны, безопасности государства и правопорядка, а также в социальной, экономической, политической, экологической сферах деятельности	
Авторизованные пользователи ИСПДн	Получение финансовой или иной материальной выгоды. Любопытство или желание самореализации (подтверждение статуса). Месть за ранее совершенные действия. Непреднамеренные, неосторожные или неквалифицированные действия	Получение финансовой или иной материальной выгоды. Любопытство или желание самореализации (подтверждение статуса). Месть за ранее совершенные действия. Непреднамеренные, неосторожные или неквалифицированные действия	Получение финансовой или иной материальной выгоды. Любопытство или желание самореализации (подтверждение статуса). Месть за ранее совершенные действия. Непреднамеренные, неосторожные или неквалифицированные действия	решения задач (реализации функций); Простой ИСПДн) У1 (Разглашение персональных данных граждан) У2 (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); Необходимость дополнительных (незапланированных) затрат на восстановление деятельности; Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций); Простой ИСПДн; Рассылка информационных сообщений с использованием вычислительных мощностей оператора и (или) от его имени) У1 (Разглашение персональных данных граждан) У2 (Необходимость дополнительных (незапланированных) затрат на закупку товаров, работ или
Системные администраторы и администраторы безопасности	Получение финансовой или иной материальной выгоды. Любопытство или желание самореализации (подтверждение статуса). Месть за ранее совершенные действия	Получение финансовой или иной материальной выгоды. Любопытство или желание самореализации (подтверждение статуса). Месть за ранее совершенные действия	Непреднамеренные, неосторожные или неквалифицированные действия	У1 (Разглашение персональных данных граждан) У2 (Необходимость дополнительных (незапланированных) затрат на закупку товаров, работ или

Вид нарушителя	Возможные цели реализации угроз безопасности информации			Соответствие целей видам риска (ущерба) и возможным негативным последствиям
	Нанесение ущерба физическому лицу	Нанесение ущерба юридическому лицу, индивидуальному предпринимателю	Нанесение ущерба государству в области обеспечения обороны страны, безопасности государства и правопорядка, а также в социальной, экономической, политической, экологической сферах деятельности	
	действия. Непреднамеренные, неосторожные или неквалифицированные действия	действия. Непреднамеренные, неосторожные или неквалифицированные действия		услуг (в том числе закупка программного обеспечения, технических средств, вышедших из строя, замена, настройка, ремонт указанных средств); Необходимость дополнительных (незапланированных) затрат на восстановление деятельности; Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций); Простой ИСПДн; Рассылка информационных сообщений с использованием вычислительных мощностей оператора и (или) от его имени; Публикация недостоверной информации на веб-ресурсах организации; Использование веб-ресурсов для распространения и управления вредоносным программным обеспечением)
Бывшие (уволенные) работники (пользователи)	Получение финансовой или иной материальной выгоды. Месть за ранее совершенные действия	Получение финансовой или иной материальной выгоды. Месть за ранее совершенные действия	Нанесение ущерба государству не соответствует предполагаемым целям данного вида нарушителя	У1 (Нарушение конфиденциальности (утечка) персональных данных; Разглашение персональных данных граждан) У2 (Необходимость дополнительных

Вид нарушителя	Возможные цели реализации угроз безопасности информации			Соответствие целей видам риска (ущерба) и возможным негативным последствиям
	Нанесение ущерба физическому лицу	Нанесение ущерба юридическому лицу, индивидуальному предпринимателю	Нанесение ущерба государству в области обеспечения обороны страны, безопасности государства и правопорядка, а также в социальной, экономической, политической, экологической сферах деятельности	
				(незапланированных) затрат на закупку товаров, работ или услуг (в том числе закупка программного обеспечения, технических средств, вышедших из строя, замена, настройка, ремонт указанных средств); Необходимость дополнительных (незапланированных) затрат на восстановление деятельности; Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций); Простой ИСПДн; Рассылка информационных сообщений с использованием вычислительных мощностей оператора и (или) от его имени)

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;
- базовыми повышенными возможностями по реализации угроз безопасности информации;
- средними возможностями по реализации угроз безопасности информации;
- высокими возможностями по реализации угроз безопасности информации.

Для ИСПДн актуальными могут являться нарушители, имеющие разные уровни возможностей. Уровни возможностей нарушителей по реализации угроз безопасности информации приведены в Таблице №6.

Таблица №6

Уровень возможностей нарушителей	Возможности нарушителей по реализации угроз безопасности информации	Виды нарушителей
Нарушитель, обладающий базовыми возможностями	Имеет возможность при реализации угроз безопасности информации использовать только известные уязвимости, скрипты и инструменты. Имеет возможность использовать средства реализации угроз (инструменты), свободно распространяемые в сети «Интернет» и разработанные другими лицами, имеет минимальные знания механизмов их функционирования, доставки и выполнения вредоносного программного обеспечения, эксплойтов. Обладает базовыми компьютерными знаниями и навыками на уровне пользователя. Имеет возможность реализации угроз за счет физических воздействий на технические средства обработки и хранения информации, линий связи и обеспечивающие системы систем и сетей при наличии физического доступа к ним. Таким образом, нарушители с базовыми возможностями имеют возможность реализовывать только известные угрозы, направленные на известные (документированные) уязвимости, с использованием общедоступных инструментов	Физическое лицо (хакер); Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем; Лица, обеспечивающие функционирование ИСПДн или обеспечивающих систем (администрация, охрана, уборщики и т.д.); Авторизованные пользователи ИСПДн; Бывшие работники (пользователи)
Нарушитель, обладающий базовыми повышенными возможностями	Обладает всеми возможностями нарушителей с базовыми возможностями. Имеет возможность использовать средства реализации угроз (инструменты), свободно распространяемые в сети «Интернет» и разработанные другими лицами, однако хорошо владеет этими средствами и инструментами, понимает, как они работают и может вносить изменения в их функционирование для повышения эффективности реализации угроз. Оснащен и владеет фреймворками и наборами средств, инструментов для реализации угроз безопасности информации и использования уязвимостей. Имеет навыки самостоятельного планирования и реализации сценариев угроз безопасности информации. Обладает практическими знаниями о функционировании ИСПДн, операционных систем, а также имеет знания защитных механизмов, применяемых в программном обеспечении, программно-аппаратных средствах. Таким образом, нарушители с базовыми повышенными возможностями имеют возможность реализовывать угрозы, в том числе направленные на неизвестные (недокументированные) уязвимости, с использованием специально созданных для этого инструментов, свободно распространяемых в сети «Интернет». Не имеют возможностей реализации угроз на физически изолированные сегменты ИСПДн	Преступные группы (два лица и более, действующие по единому плану); Конкурирующие организации; Поставщики вычислительных услуг, услуг связи; Лица, привлекаемые для установок, настройки, испытаний, пуска/наладочных и иных видов работ; Системные администраторы и администраторы безопасности
Нарушитель, обладающий	Обладает всеми возможностями нарушителей с базовыми повышенными возможностями. Имеет возможность приобретать информацию об уязвимостях, размещаемую на специализированных	Террористические, экстремистские группировки;

Уровень возможностей нарушителей	Возможности нарушителей по реализации угроз безопасности информации	Виды нарушителей
средними возможностями	платных ресурсах (биржах уязвимостей). Имеет возможность приобретать дорогостоящие средства и инструменты для реализации угроз, размещаемые на специализированных платных ресурсах (биржах уязвимостей). Имеет возможность самостоятельно разрабатывать средства (инструменты), необходимые для реализации угроз (атак), реализовывать угрозы с использованием данных средств. Имеет возможность получения доступа к встраиваемому программному обеспечению аппаратных платформ, системному и прикладному программному обеспечению, телекоммуникационному оборудованию и другим программно-аппаратным средствам для проведения их анализа. Обладает знаниями и практическими навыками проведения анализа программного кода для получения информации об уязвимостях. Обладает высокими знаниями и практическими навыками о функционировании ИСПДн, операционных систем, а также имеет глубокое понимание защитных механизмов, применяемых в программном обеспечении, программно-аппаратных средствах. Имеет возможность реализовывать угрозы безопасности информации в составе группы лиц. Таким образом, нарушители со средними возможностями имеют возможность реализовывать угрозы, в том числе на выявленные ими неизвестные уязвимости, с использованием самостоятельно разработанных для этого инструментов. Не имеют возможностей реализации угроз на физически изолированные сегменты ИСПДн	Разработчики программных, программно-аппаратных средств
Нарушитель, обладающий высокими возможностями	Обладает всеми возможностями нарушителей со средними возможностями. Имеет возможность получения доступа к исходному коду встраиваемого программного обеспечения аппаратных платформ, системного и прикладного программного обеспечения, телекоммуникационного оборудования и других программно-аппаратных средств для получения сведений об уязвимостях «нулевого дня». Имеет возможность внедрения программных (программно-аппаратных) закладок или уязвимостей на различных этапах поставки программного обеспечения или программно-аппаратных средств. Имеет возможность создания методов и средств реализации угроз с привлечением специализированных научных организаций и реализации угроз с применением специально разработанных средств, в том числе обеспечивающих скрытое проникновение. Имеет возможность реализовывать угрозы с привлечением специалистов, имеющих базовые повышенные, средние и высокие возможности. Имеет возможность создания и применения специальных технических средств для добывания информации (воздействия на информацию или технические средства), распространяющейся в виде физических полей или явлений. Имеет возможность одновременно и незаметно для операторов ИСПДн реализовывать угрозы безопасности информации. Обладает исключительными знаниями и практическими навыками о функционировании ИСПДн, операционных систем, аппаратном обеспечении, а также осведомлен о конкретных защитных механизмах, применяемых в программном обеспечении, программно-аппаратных средствах атакуемой ИСПДн.	Специальные службы иностранных государств

Уровень возможностей нарушителей	Возможности нарушителей по реализации угроз безопасности информации	Виды нарушителей
	Таким образом, нарушители с высокими возможностями имеют практически неограниченные возможности реализовывать угрозы, в том числе с использованием недекларированных возможностей, программных, программно-аппаратных закладок, встроенных в компоненты ИСПДн	

По результатам определения источников угроз безопасности информации определяются:

- виды актуальных нарушителей и возможные цели реализации ими угроз безопасности информации, а также их возможности;
- категории актуальных нарушителей, которые могут реализовывать угрозы безопасности информации, в том числе непреднамеренные угрозы.

При определении источников угроз безопасности информации необходимо исходить из предположения о наличии повышенной мотивации внешних и внутренних нарушителей, преднамеренно реализующих угрозы безопасности информации. Кроме того, необходимо учитывать, что такие виды нарушителей как специальные службы иностранных государств и террористические, экстремистские группировки могут привлекать (входить в сговор) внутренних нарушителей, в том числе обладающих привилегированными правами доступа. В этом случае уровень возможностей актуальных нарушителей определяется совокупностью возможностей нарушителей, входящих в сговор.

Результат определения актуальных нарушителей при реализации угроз безопасности информации и соответствующие им возможности представлен в Таблице №7.

Таблица №7

Вид риска (ущерба)	Возможные негативные последствия	Вид актуального нарушителя	Категория нарушителя	Уровень возможностей нарушителя
Ущерб физическому лицу (У1)	Нарушение конфиденциальности (утечка) персональных данных. «Травля» гражданина в сети «Интернет». Разглашение персональных данных граждан.	Отдельные физические лица (хакеры)	Внешний	Базовый
		Авторизованные пользователи ИСПДн	Внутренний	Базовый
		Системные администраторы и администраторы безопасности	Внутренний	Базовый повышенный
		Бывшие (уволенные) работники (пользователи)	Внешний	Базовый
Риски юридическому лицу, индивидуальному предпринимателю, связанные с	Нарушение законодательства Российской Федерации. Необходимость дополнительных (незапланированных) затрат на выплаты штрафов (неустоек) или компенсаций. Необходимость дополнительных (незапланированных)	Отдельные физические лица (хакеры)	Внешний	Базовый
		Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем	Внешний	Базовый

Вид риска (ущерб)	Возможные негативные последствия	Вид актуального нарушителя	Категория нарушителя	Уровень возможностей нарушителя
хозяйственной деятельностью (У2)	затрат на закупку товаров, работ или услуг (в том числе закупка программного обеспечения, технических средств, вышедших из строя, замена, настройка, ремонт указанных средств). Необходимость дополнительных (незапланированных) затрат на восстановление деятельности. Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций). Простой ИСПДн. Публикация недостоверной информации на веб-ресурсах организации. Использование веб-ресурсов для распространения и управления вредоносным программным обеспечением. Рассылка информационных сообщений с использованием вычислительных мощностей оператора и (или) от его имени.	Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ	Внутренний	Базовый повышенный
		Лица, обеспечивающие функционирование ИСПДн или обеспечивающих систем оператора (администрация, охрана, уборщики и др.)	Внутренний	Базовый
		Авторизованные пользователи ИСПДн	Внутренний	Базовый
		Системные администраторы и администраторы безопасности	Внутренний	Базовый повышенный
		Бывшие (уволненные) работники (пользователи)	Внешний	Базовый

6. СПОСОБЫ РЕАЛИЗАЦИИ (ВОЗНИКНОВЕНИЯ) УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

В ходе оценки угроз безопасности информации должны быть определены возможные способы реализации (возникновения) угроз безопасности информации, за счет использования которых актуальными нарушителями могут быть реализованы угрозы безопасности информации в ИСПДн, – актуальные способы реализации (возникновения) угроз безопасности информации.

Исходными данными для определения актуальных способов реализации (возникновения) угроз безопасности информации являются:

- 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. № 1085, а также отраслевые (ведомственные, корпоративные) модели угроз безопасности информации;

- документация на системы и сети (в части сведений о составе и архитектуре, о группах пользователей и их типах доступа и уровнях полномочий, о внешних и внутренних интерфейсах);

- негативные последствия от реализации (возникновения) угроз безопасности информации, определенные в Главе 3 настоящей Модели угроз;

- объекты воздействия угроз безопасности информации и соответствующие им виды воздействия, определенные в Главе 4 настоящей Модели угроз;

- виды и категории актуальных нарушителей, которые могут реализовывать угрозы безопасности информации, в том числе непреднамеренные угрозы, и их возможности, определенные в Главе 5 настоящей Модели угроз.

Указанные исходные данные могут быть дополнены иными документами и сведениями с учетом особенностей области деятельности, в которой функционирует ИСПДн.

На основе анализа исходных данных, а также возможностей нарушителей определяются способы реализации (возникновения) угроз безопасности информации, актуальные для ИСПДн.

Основными способами реализации (возникновения) угроз безопасности информации являются:

- использование уязвимостей (уязвимостей кода (программного обеспечения), уязвимостей архитектуры и конфигурации ИСПДн, а также организационных и многофакторных уязвимостей);

- внедрение вредоносного программного обеспечения;

- использование недеklarированных возможностей программного обеспечения и (или) программно-аппаратных средств;

- установка программных и (или) программно-аппаратных закладок в программное обеспечение и (или) программно-аппаратные средства;

- формирование и использование скрытых каналов (по времени, по памяти) для передачи конфиденциальных данных;
- перехват (измерение) побочных электромагнитных излучений и наводок (других физических полей) для доступа к конфиденциальной информации, содержащейся в аппаратных средствах аутентификации;
- инвазивные способы доступа к конфиденциальной информации, содержащейся в аппаратных средствах аутентификации;
- нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам (в том числе администрированию, обслуживанию);
- ошибочные действия в ходе создания и эксплуатации ИСПДн, в том числе при установке, настройке программных и программно-аппаратных средств.

Указанные способы реализации (возникновения) угроз безопасности информации могут быть дополнены иными способами с учетом особенностей архитектуры и условий функционирования ИСПДн.

Способы реализации (возникновения) угроз безопасности информации определяются применительно к объектам воздействия, определенным в Главе 4. Способы являются актуальными, когда возможности нарушителя позволяют их использовать для реализации угроз безопасности и имеются или созданы условия, при которых такая возможность может быть реализована в отношении объектов воздействия. Одна угроза безопасности информации может быть реализована несколькими способами.

Условием, позволяющим нарушителям использовать способы реализации угроз безопасности информации, является наличие у них возможности доступа к следующим типам интерфейсов объектов воздействия:

- внешние сетевые интерфейсы, обеспечивающие взаимодействие с сетью «Интернет», смежными (взаимодействующими) информационными системами (проводные, беспроводные, веб-интерфейсы, интерфейсы удаленного доступа и др.);
- внутренние сетевые интерфейсы, обеспечивающие взаимодействие (в том числе через промежуточные компоненты) с компонентами ИСПДн, имеющими внешние сетевые интерфейсы (проводные, беспроводные);
- интерфейсы для пользователей (проводные, беспроводные, веб-интерфейсы, интерфейсы удаленного доступа и др.);
- интерфейсы для использования съемных машинных носителей информации и периферийного оборудования;
- интерфейсы для установки, настройки, испытаний, пусконаладочных работ (в том числе администрирования, управления, обслуживания) обеспечения функционирования компонентов ИСПДн;
- возможность доступа к поставляемым или находящимся на обслуживании, ремонте в сторонних организациях компонентам ИСПДн.

Наличие указанных интерфейсов определяется архитектурой, составом и условиями функционирования ИСПДн, группами пользователей, их типами доступа и уровнями полномочий. В ходе анализа должны быть определены как логические, так и физические интерфейсы объектов воздействия, в том числе требующие физического доступа к ним.

Интерфейсы определяются на аппаратном, системном и прикладном уровнях ИСПДн, а также для телекоммуникационного оборудования. Возможность их использования на указанных уровнях определяется возможностями актуальных нарушителей.

На этапе создания ИСПДн определение интерфейсов объектов воздействия, которые могут использоваться для реализации угроз безопасности, проводится на основе предполагаемой архитектуры и условий функционирования ИСПДн, определенных на основе изучения и анализа исходных данных.

На этапе эксплуатации ИСПДн для определения интерфейсов объектов воздействия, которые могут использоваться для реализации угроз безопасности, дополнительно к документации на ИСПДн используются результаты инвентаризации ИСПДн, проведенной с использованием автоматизированных средств.

По результатам оценки возможных способов реализации угроз безопасности информации определяются:

- виды и категории нарушителей, которые имеют возможность использования актуальных способов;
- актуальные способы реализации угроз безопасности информации и типы интерфейсов объектов воздействия, за счет которых они могут быть реализованы.

Результаты определения актуальных способов реализации угроз безопасности информации и соответствующие им виды нарушителей представлены в Таблице №8.

Таблица №8

№ п/п	Вид нарушителя	Объект воздействия	Доступные интерфейсы	Способы реализации
1.	Отдельные физические лица (хакеры)	АРМ пользователя ИСПДн	Сетевой интерфейс АРМ пользователя ИСПДн	Использование уязвимостей протоколов сетевого взаимодействия; Использование уязвимостей системного программного обеспечения; Использование открытых портов сетевого взаимодействия; Внедрение вредоносного программного обеспечения
		Удаленное АРМ пользователя ИСПДн	Сетевой интерфейс удаленного АРМ пользователя ИСПДн	Использование уязвимостей системного программного обеспечения; Использование уязвимостей протоколов сетевого взаимодействия; Использование открытых портов сетевого взаимодействия; Внедрение вредоносного программного обеспечения
		Сервер ИСПДн	Сетевые интерфейсы сервера ИСПДн	Использование уязвимостей системного программного обеспечения; Использование уязвимостей протоколов сетевого взаимодействия; Использование открытых портов сетевого взаимодействия; Внедрение вредоносного программного обеспечения
		Линии связи ИСПДн	Сетевые интерфейсы коммутаторов / маршрутизаторов внутри и (или) на границе ИСПДн	Использование уязвимостей протоколов сетевого взаимодействия; Использование открытых портов сетевого взаимодействия; Использование уязвимостей сетевого оборудования
		Веб-приложение ИСПДн	Пользовательский интерфейс прикладного ПО ИСПДн	Использование уязвимостей прикладного программного обеспечения; Внедрение вредоносного программного обеспечения; Использование недекларированных возможностей программного обеспечения
		Учетные записи корпоративных электронных почтовых ящиков	Интерфейс администрирования прикладного ПО ИСПДн Интерфейс ввода аутентификационной информации электронных почтовых ящиков	Использование уязвимостей прикладного программного обеспечения; Внедрение вредоносного программного обеспечения; Использование недекларированных возможностей программного обеспечения
2.	Лица, обеспечивающие поставку программных, аппаратных средств, обеспечивающих систем	Прикладное ПО ИСПДн, участвующее в обработке ПДн граждан	Пользовательский интерфейс прикладного ПО ИСПДн	Использование уязвимостей прикладного программного обеспечения; Использование некорректной настройки парольной политики
			Интерфейс администрирования прикладного ПО ИСПДн	Внедрение вредоносного программного обеспечения
		Веб-приложение ИСПДн	Пользовательский интерфейс прикладного ПО ИСПДн	Внедрение вредоносного программного обеспечения
			Интерфейс администрирования	Внедрение вредоносного программного обеспечения

№ п/п	Вид нарушителя	Объект воздействия	Доступные интерфейсы	Способы реализации
3.	Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ	АРМ пользователя ИСПДн	прикладного ПО ИСПДн	Внедрение вредоносного программного обеспечения; Ошибочные действия при настройке
			Сетевой интерфейс АРМ пользователя ИСПДн	
			Интерфейсы подключения внешних устройств (USB, COM)	
			Интерфейсы подключения съемных и несъемных машинных носителей информации	
		Удаленное АРМ пользователя ИСПДн	Сетевой интерфейс удаленного АРМ пользователя ИСПДн	Внедрение вредоносного программного обеспечения; Ошибочные действия при настройке; Программные сбои
			Интерфейсы подключения внешних устройств (USB, COM)	
			Интерфейсы подключения съемных и несъемных машинных носителей информации	
			Сетевые интерфейсы сервера ИСПДн	
		Сервер ИСПДн	Интерфейсы подключения внешних устройств (USB, COM)	Внедрение вредоносного программного обеспечения
			Интерфейсы подключения съемных и несъемных машинных носителей информации	
4.	Лица, обеспечивающие функционирование ИСПДн или	Линии связи ИСПДн	Сетевые интерфейсы коммутаторов / маршрутизаторов внутри и (или) на границе ИСПДн	Ошибочные действия при настройке; Программные сбои
			Интерфейсы подключения внешних устройств (USB, COM)	
		АРМ пользователя ИСПДн	Интерфейсы подключения внешних устройств (USB, COM)	Физический доступ к техническим средствам ИС; Внедрение вредоносного программного обеспечения
			Интерфейсы подключения	

№ п/п	Вид нарушителя	Объект воздействия	Доступные интерфейсы	Способы реализации
5.	обеспечивающих систем оператора (администрация, охрана, уборщики и др.)		съёмных и несъёмных машинных носителей информации	Внедрение вредоносного программного обеспечения
			Интерфейсы подключения внешних устройств (USB, COM)	Физический доступ к техническим средствам ИС; Внедрение вредоносного программного обеспечения
		Сервер ИСПДн	Интерфейсы подключения съёмных и несъёмных машинных носителей информации	Физический доступ к техническим средствам ИС; Внедрение вредоносного программного обеспечения
		База данных ИСПДн, содержащая ПДн граждан	Пользовательский интерфейс, используемый для доступа к базе данных ИСПДн	Использование уязвимостей прикладного программного обеспечения; Внедрение вредоносного программного обеспечения; Использование недеklarированных возможностей программного обеспечения
	Авторизованные пользователи ИСПДн		Интерфейс администрирования базы данных ИСПДн	Использование уязвимостей прикладного программного обеспечения; Внедрение вредоносного программного обеспечения; Использование недеklarированных возможностей программного обеспечения
			Интерфейс ввода аутентификационной информации	Использование уязвимостей прикладного программного обеспечения; Использование уязвимостей системного программного обеспечения; Использование некорректной настройки парольной политики; Программные сбои
		АРМ пользователя ИСПДн	Сетевой интерфейс АРМ пользователя ИСПДн	Использование уязвимостей протоколов сетевого взаимодействия; Использование уязвимостей системного программного обеспечения; Использование открытых портов сетевого взаимодействия; Внедрение вредоносного программного обеспечения
			Интерфейсы подключения внешних устройств (USB, COM)	Физический доступ к техническим средствам ИС; Внедрение вредоносного программного обеспечения
		Удаленное АРМ пользователя ИСПДн	Интерфейсы подключения съёмных и несъёмных машинных носителей информации	Физический доступ к техническим средствам ИС; Внедрение вредоносного программного обеспечения
			Интерфейс ввода аутентификационной информации	Использование уязвимостей прикладного программного обеспечения; Использование уязвимостей системного программного обеспечения; Использование некорректной настройки парольной политики; Программные сбои
			Сетевой интерфейс удаленного АРМ	Использование уязвимостей протоколов сетевого взаимодействия; Использование уязвимостей системного программного обеспечения;

№ п/п	Вид нарушителя	Объект воздействия	Доступные интерфейсы	Способы реализации
			пользователя ИСПДн	Использование открытых портов сетевого взаимодействия; Внедрение вредоносного программного обеспечения
			Интерфейсы подключения внешних устройств (USB, COM)	Физический доступ к техническим средствам ИС; Внедрение вредоносного программного обеспечения
			Интерфейсы подключения съемных и несъемных машинных носителей информации	Физический доступ к техническим средствам ИС; Внедрение вредоносного программного обеспечения
			Интерфейс ввода аутентификационной информации	Использование уязвимостей прикладного программного обеспечения; Использование уязвимостей системного программного обеспечения; Использование некорректной настройки парольной политики; Программные сбои
		Сервер ИСПДн	Сетевые интерфейсы сервера ИСПДн	Использование уязвимостей протоколов сетевого взаимодействия; Использование уязвимостей системного программного обеспечения; Использование открытых портов сетевого взаимодействия; Внедрение вредоносного программного обеспечения
			Интерфейсы подключения внешних устройств (USB, COM)	Физический доступ к техническим средствам ИС; Внедрение вредоносного программного обеспечения
			Интерфейсы подключения съемных и несъемных машинных носителей информации	Физический доступ к техническим средствам ИС; Внедрение вредоносного программного обеспечения
			Сетевые интерфейсы коммутаторов / маршрутизаторов внутри и (или) на границе ИСПДн	Использование уязвимостей протоколов сетевого взаимодействия; Использование открытых портов сетевого взаимодействия; Использование уязвимостей сетевого оборудования
		Линии связи ИСПДн	Пользовательский интерфейс прикладного ПО ИСПДн	Использование уязвимостей прикладного программного обеспечения; Внедрение вредоносного программного обеспечения; Использование недекларированных возможностей программного обеспечения
			Интерфейс администрирования прикладного ПО ИСПДн	Использование уязвимостей прикладного программного обеспечения; Внедрение вредоносного программного обеспечения; Использование недекларированных возможностей программного обеспечения
		Веб-приложение ИСПДн	Пользовательский интерфейс прикладного ПО ИСПДн	Использование уязвимостей прикладного программного обеспечения; Внедрение вредоносного программного обеспечения; Использование недекларированных возможностей программного обеспечения
			Интерфейс	Использование уязвимостей прикладного программного обеспечения;

№ п/п	Вид нарушителя	Объект воздействия	Доступные интерфейсы	Способы реализации
6.	Системные администраторы и администраторы безопасности	Учетные записи корпоративных электронных почтовых ящиков	администрирования прикладного ПО ИСПДн	Внедрение вредоносного программного обеспечения; Использование недеklarированных возможностей программного обеспечения
			Интерфейс ввода аутентификационной информации электронных почтовых ящиков	Использование уязвимостей прикладного программного обеспечения; Использование некорректной настройки парольной политики
		База данных ИСПДн, содержащая ПДн граждан	Пользовательский интерфейс, используемый для доступа к базе данных ИСПДн	Использование уязвимостей прикладного программного обеспечения; Внедрение вредоносного программного обеспечения; Использование недеklarированных возможностей программного обеспечения
			Интерфейс администрирования базы данных ИСПДн	Использование уязвимостей прикладного программного обеспечения; Внедрение вредоносного программного обеспечения; Использование недеklarированных возможностей программного обеспечения
		АРМ пользователя ИСПДн	Интерфейс ввода аутентификационной информации	Использование уязвимостей прикладного программного обеспечения; Использование уязвимостей системного программного обеспечения; Использование некорректной настройки парольной политики; Программные сбои; Ошибочные действия при настройке
			Сетевой интерфейс АРМ пользователя ИСПДн	Использование уязвимостей протоколов сетевого взаимодействия; Использование уязвимостей системного программного обеспечения; Использование открытых портов сетевого взаимодействия; Внедрение вредоносного программного обеспечения; Ошибочные действия при настройке
			Интерфейсы подключения внешних устройств (USB, COM)	Физический доступ к техническим средствам ИС; Внедрение вредоносного программного обеспечения
			Интерфейсы подключения съемных и несъемных машинных носителей информации	Физический доступ к техническим средствам ИС; Внедрение вредоносного программного обеспечения
		Удаленное АРМ пользователя ИСПДн	Интерфейс ввода аутентификационной информации	Использование уязвимостей прикладного программного обеспечения; Использование уязвимостей системного программного обеспечения; Использование некорректной настройки парольной политики; Программные сбои; Ошибочные действия при настройке
			Сетевой интерфейс удаленного АРМ пользователя ИСПДн	Использование уязвимостей протоколов сетевого взаимодействия; Использование уязвимостей системного программного обеспечения; Использование открытых портов сетевого взаимодействия;

№ п/п	Вид нарушителя	Объект воздействия	Доступные интерфейсы	Способы реализации
		Сервер ИСПДн	Интерфейсы подключения внешних устройств (USB, COM)	Внедрение вредоносного программного обеспечения; Ошибочные действия при настройке
			Интерфейсы подключения съемных и несъемных машинных носителей информации	Физический доступ к техническим средствам ИС; Внедрение вредоносного программного обеспечения
			Интерфейс ввода аутентификационной информации	Физический доступ к техническим средствам ИС; Внедрение вредоносного программного обеспечения
			Сетевые интерфейсы сервера ИСПДн	Использование уязвимостей прикладного программного обеспечения; Использование уязвимостей системного программного обеспечения; Использование некорректной настройки парольной политики; Программные сбои; Ошибочные действия при настройке
			Интерфейсы подключения внешних устройств (USB, COM)	Использование уязвимостей протоколов сетевого взаимодействия; Использование уязвимостей системного программного обеспечения; Использование открытых портов сетевого взаимодействия; Внедрение вредоносного программного обеспечения; Ошибочные действия при настройке
			Интерфейсы подключения съемных и несъемных машинных носителей информации	Физический доступ к техническим средствам ИС; Внедрение вредоносного программного обеспечения
			Интерфейс локального администрирования сервера ИСПДн	Использование уязвимостей прикладного программного обеспечения; Использование уязвимостей системного программного обеспечения; Использование некорректной настройки парольной политики; Программные сбои; Ошибочные действия при настройке
			Интерфейс удаленного администрирования сервера ИСПДн	Использование уязвимостей прикладного программного обеспечения; Использование уязвимостей системного программного обеспечения; Использование некорректной настройки парольной политики; Программные сбои; Ошибочные действия при настройке
			Сетевые интерфейсы коммутаторов /	Использование уязвимостей протоколов сетевого взаимодействия; Использование открытых портов сетевого взаимодействия;
		Линии связи ИСПДн		

№ п/п	Вид нарушителя	Объект воздействия	Доступные интерфейсы	Способы реализации
7.	Бывшие (уволненные) работники (пользователи)		маршрутизаторов внутри и (или) на границе ИСПДн	Использование уязвимостей сетевого оборудования; Ошибочные действия при настройке
		Прикладное ПО ИСПДн, участвующее в обработке ПДн граждан	Пользовательский интерфейс прикладного ПО ИСПДн	Использование уязвимостей прикладного программного обеспечения; Внедрение вредоносного программного обеспечения; Использование недекларированных возможностей программного обеспечения
			Интерфейс администрирования прикладного ПО ИСПДн	Использование уязвимостей прикладного программного обеспечения; Внедрение вредоносного программного обеспечения; Использование недекларированных возможностей программного обеспечения
		Веб-приложение ИСПДн	Пользовательский интерфейс прикладного ПО ИСПДн	Использование уязвимостей прикладного программного обеспечения; Внедрение вредоносного программного обеспечения; Использование недекларированных возможностей программного обеспечения
			Интерфейс администрирования прикладного ПО ИСПДн	Использование уязвимостей прикладного программного обеспечения; Внедрение вредоносного программного обеспечения; Использование недекларированных возможностей программного обеспечения
		Конфигурационные и информационные файлы, используемые веб-приложениями ИСПДн	Пользовательский интерфейс редактирования конфигурационных и информационных файлов	Использование уязвимостей прикладного программного обеспечения
		Учетные записи корпоративных электронных почтовых ящиков	Интерфейс ввода аутентификационной информации электронных почтовых ящиков	Ошибочные действия при настройке; Использование некорректной настройки парольной политики
		АРМ пользователя ИСПДн	Сетевой интерфейс АРМ пользователя ИСПДн	Использование уязвимостей протоколов сетевого взаимодействия; Использование уязвимостей системного программного обеспечения; Использование открытых портов сетевого взаимодействия; Внедрение вредоносного программного обеспечения
		Удаленное АРМ пользователя ИСПДн	Сетевой интерфейс удаленного АРМ пользователя ИСПДн	Использование уязвимостей протоколов сетевого взаимодействия; Использование уязвимостей системного программного обеспечения; Использование открытых портов сетевого взаимодействия; Внедрение вредоносного программного обеспечения
		Сервер ИСПДн	Сетевые интерфейсы сервера ИСПДн	Использование уязвимостей протоколов сетевого взаимодействия; Использование уязвимостей системного программного обеспечения; Использование открытых портов сетевого взаимодействия; Внедрение вредоносного программного обеспечения
		Линии связи ИСПДн	Сетевые интерфейсы коммутаторов / маршрутизаторов внутри и	Использование уязвимостей протоколов сетевого взаимодействия; Использование открытых портов сетевого взаимодействия; Использование уязвимостей сетевого оборудования

№ п/п	Вид нарушителя	Объект воздействия	Доступные интерфейсы	Способы реализации
		Веб-приложение ИСПДн	(или) на границе ИСПДн Пользовательский интерфейс прикладного ПО ИСПДн	Использование уязвимостей прикладного программного обеспечения; Внедрение вредоносного программного обеспечения; Использование недекларированных возможностей программного обеспечения
			Интерфейс администрирования прикладного ПО ИСПДн	Использование уязвимостей прикладного программного обеспечения; Внедрение вредоносного программного обеспечения; Использование недекларированных возможностей программного обеспечения
		Учетные записи корпоративных электронных почтовых ящиков	Интерфейс ввода аутентификационной информации электронных почтовых ящиков	Использование уязвимостей прикладного программного обеспечения; Использование некорректной настройки парольной политики

7. АКТУАЛЬНЫЕ УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

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

Исходными данными для оценки актуальности угроз безопасности информации являются:

- 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. № 1085, а также отраслевые (ведомственные, корпоративные) модели угроз безопасности информации;
- негативные последствия от реализации (возникновения) угроз безопасности информации, определенные в Главе 3 настоящей Модели угроз;
- объекты воздействия угроз безопасности информации и виды воздействий на них, определенные в Главе 4 настоящей Модели угроз;
- виды и категории актуальных нарушителей, которые могут реализовывать угрозы безопасности информации, в том числе непреднамеренные угрозы, и их возможности, определенные в Главе 5 настоящей Модели угроз;
- актуальные способы реализации (возникновения) угроз безопасности информации, определенные в Главе 6 настоящей Модели угроз.

7.1. Определение возможных (вероятных) угроз безопасности информации

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

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:

УБИ_і = [нарушитель (источник угрозы); объекты воздействия; способы реализации угроз; негативные последствия].

В качестве источников угроз безопасности информации использовались Банк данных угроз ФСТЭК России (bdu.fstec.ru) и Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утв. зам. директора ФСТЭК России 15.02.2008 г.).

Для формирования перечня возможных (вероятных) угроз безопасности информации из Банка данных угроз и Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных были выделены угрозы, для

которых имеется нарушитель с соответствующим потенциалом, а также объект воздействия, сходный по типу с определенными в Главе 4 настоящей Модели угроз объектами. Так как самый высокий потенциал вероятного внутреннего нарушителя, определенный в настоящей Модели угроз, принимает значение «базовый повышенный», данному потенциалу был сопоставлен «низкий» потенциал из шкалы измерений потенциала нарушителя, принятой в Банке данных угроз. Потенциал вероятного внутреннего нарушителя определен как «базовый», соответственно ему был так же сопоставлен «низкий» потенциал из шкалы измерений Банка данных угроз.

Перечень возможных (вероятных) угроз безопасности информации представлен в Таблице №9.

Таблица №9

№ п/п	Идентификатор УБИ	Название угрозы
Банк данных угроз ФСТЭК России (bdu.fstec.ru)		
1	УБИ.006	Угроза внедрения кода или данных
2	УБИ.008	Угроза восстановления аутентификационной информации
3	УБИ.009	Угроза восстановления предыдущей уязвимой версии BIOS
4	УБИ.012	Угроза деструктивного изменения конфигурации/среды окружения программ
5	УБИ.013	Угроза деструктивного использования декларируемого функционала BIOS
6	УБИ.014	Угроза длительного удержания вычислительных ресурсов пользователями
7	УБИ.015	Угроза доступа к защищаемым файлам с использованием обходного пути
8	УБИ.017	Угроза доступа/перехвата/изменения HTTP cookies
9	УБИ.018	Угроза загрузки нештатной операционной системы
10	УБИ.019	Угроза заражения DNS-кеша
11	УБИ.022	Угроза избыточного выделения оперативной памяти
12	УБИ.023	Угроза изменения компонентов системы
13	УБИ.027	Угроза искажения вводимой и выводимой на периферийные устройства информации
14	УБИ.028	Угроза использования альтернативных путей доступа к ресурсам
15	УБИ.030	Угроза использования информации идентификации/аутентификации, заданной по умолчанию
16	УБИ.031	Угроза использования механизмов авторизации для повышения привилегий
17	УБИ.034	Угроза использования слабостей протоколов сетевого/локального обмена данными
18	УБИ.041	Угроза межсайтового скриптинга
19	УБИ.045	Угроза нарушения изоляции среды исполнения BIOS
20	УБИ.049	Угроза нарушения целостности данных кеша
21	УБИ.051	Угроза невозможности восстановления сессии работы на ПЭВМ при выводе из промежуточных состояний питания
22	УБИ.053	Угроза невозможности управления правами пользователей BIOS
23	УБИ.062	Угроза некорректного использования прозрачного прокси-сервера за счёт плагинов браузера
24	УБИ.067	Угроза неправомерного ознакомления с защищаемой информацией
25	УБИ.069	Угроза неправомерных действий в каналах связи
26	УБИ.071	Угроза несанкционированного восстановления удалённой защищаемой информации
27	УБИ.072	Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS
28	УБИ.074	Угроза несанкционированного доступа к аутентификационной информации
29	УБИ.086	Угроза несанкционированного изменения аутентификационной информации
30	УБИ.087	Угроза несанкционированного использования привилегированных функций BIOS
31	УБИ.088	Угроза несанкционированного копирования защищаемой информации
32	УБИ.089	Угроза несанкционированного редактирования реестра
33	УБИ.090	Угроза несанкционированного создания учётной записи пользователя

№ п/п	Идентификатор УБИ	Название угрозы
34	УБИ.091	Угроза несанкционированного удаления защищаемой информации
35	УБИ.093	Угроза несанкционированного управления буфером
36	УБИ.098	Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб
37	УБИ.099	Угроза обнаружения хостов
38	УБИ.100	Угроза обхода некорректно настроенных механизмов аутентификации
39	УБИ.103	Угроза определения типов объектов защиты
40	УБИ.104	Угроза определения топологии вычислительной сети
41	УБИ.113	Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники
42	УБИ.115	Угроза перехвата вводимой и выводимой на периферийные устройства информации
43	УБИ.116	Угроза перехвата данных, передаваемых по вычислительной сети
44	УБИ.121	Угроза повреждения системного реестра
45	УБИ.124	Угроза подделки записей журнала регистрации событий
46	УБИ.128	Угроза подмены доверенного пользователя
47	УБИ.129	Угроза подмены резервной копии программного обеспечения BIOS
48	УБИ.130	Угроза подмены содержимого сетевых ресурсов
49	УБИ.140	Угроза приведения системы в состояние «отказ в обслуживании»
50	УБИ.145	Угроза пропуска проверки целостности программного обеспечения
51	УБИ.152	Угроза удаления аутентификационной информации
52	УБИ.153	Угроза усиления воздействия на вычислительные ресурсы пользователей при помощи сторонних серверов
53	УБИ.155	Угроза утраты вычислительных ресурсов
54	УБИ.157	Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации
55	УБИ.159	Угроза «форсированного веб-браузинга»
56	УБИ.160	Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации
57	УБИ.162	Угроза эксплуатации цифровой подписи программного кода
58	УБИ.167	Угроза заражения компьютера при посещении неблагонадежных сайтов
59	УБИ.168	Угроза «кражи» учётной записи доступа к сетевым сервисам
60	УБИ.170	Угроза неправомерного шифрования информации
61	УБИ.171	Угроза скрытного включения вычислительного устройства в состав бот-сети
62	УБИ.172	Угроза распространения «почтовых червей»
63	УБИ.173	Угроза «спама» веб-сервера
64	УБИ.174	Угроза «фарминга»
65	УБИ.175	Угроза «фишинга»
66	УБИ.178	Угроза несанкционированного использования системных и сетевых утилит
67	УБИ.179	Угроза несанкционированной модификации защищаемой информации
68	УБИ.180	Угроза отказа подсистемы обеспечения температурного режима
69	УБИ.182	Угроза физического устаревания аппаратных компонентов
70	УБИ.186	Угроза внедрения вредоносного кода через рекламу, сервисы и контент
71	УБИ.191	Угроза внедрения вредоносного кода в дистрибутив программного обеспечения
72	УБИ.192	Угроза использования уязвимых версий программного обеспечения
73	УБИ.208	Угроза нецелевого использования вычислительных ресурсов средства вычислительной техники
74	УБИ.209	Угроза несанкционированного доступа к защищаемой памяти ядра процессора
75	УБИ.211	Угроза использования непроверенных пользовательских данных при формировании конфигурационного файла, используемого программным обеспечением администрирования информационных систем
Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка). ФСТЭК России, 2008 год		
76	-	Угрозы, реализуемые в ходе загрузки операционной системы и направленные на перехват паролей или идентификаторов, модификацию базовой системы ввода/вывода (BIOS), перехват управления загрузкой

№ п/п	Идентификатор УБИ	Название угрозы
77	-	Угрозы, реализуемые после загрузки операционной системы и направленные на выполнение несанкционированного доступа с применением стандартных функций (уничтожение, копирование, перемещение, форматирование носителей информации и т.п.) операционной системы или какой-либо прикладной программы (например, системы управления базами данных), с применением специально созданных для выполнения НСД программ (программ просмотра и модификации реестра, поиска текстов в текстовых файлах и т.п.)
78	-	Угрозы внедрения вредоносных программ
79	-	Угрозы «Анализа сетевого трафика» с перехватом передаваемой по сети информации
80	-	Угрозы «Анализа сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой в ИСПДн из внешних сетей информации
81	-	Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.
82	-	Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях
83	-	Угрозы подмены доверенного объекта
84	-	Угрозы навязывания ложного маршрута путем несанкционированного изменения маршрутно-адресных данных как внутри сети, так и во внешних сетях
85	-	Угрозы выявления паролей
86	-	Угрозы типа «Отказ в обслуживании»
87	-	Угрозы удаленного запуска приложений
88	-	Угрозы внедрения по сети вредоносных программ

7.2. Определение возможных сценариев реализации угроз безопасности информации

Актуальность возможных угроз безопасности информации определяется наличием сценариев их реализации.

Сценарии реализации угроз безопасности информации определяются для соответствующих способов реализации угроз безопасности информации, определенных в Главе 6 настоящей Модели угроз, 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.

Актуальные для ИСПДн «АСУ ЖКХ Капитальный ремонт» нарушители и их условные обозначения представлены в Таблице №10.

Таблица №10

№ п/п	Наименование	Условное обозначение
1.	Отдельные физические лица (хакеры)	Н1
2.	Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем	Н2
3.	Бывшие (уволенные) работники (пользователи)	Н3
4.	Авторизованные пользователи ИСПДн	Н4
5.	Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ	Н5
6.	Лица, обеспечивающие функционирование ИСПДн или обеспечивающих систем	Н6

№ п/п	Наименование	Условное обозначение
	оператора (администрация, охрана, уборщики и др.)	
7.	Системные администраторы и администраторы безопасности	H7

Все возможные способы реализации угроз безопасности информации для ИСПДн «АСУ ЖКХ Капитальный ремонт» и их условные обозначения приведены в Таблице №11.

Таблица №11

№ п/п	Наименование	Условное обозначение
1.	Использование уязвимостей прикладного программного обеспечения	C1
2.	Использование уязвимостей системного программного обеспечения	C2
3.	Внедрение вредоносного программного обеспечения	C3
4.	Использование недеklarированных возможностей программного обеспечения	C4
5.	Использование уязвимостей протоколов сетевого взаимодействия	C5
6.	Использование открытых портов сетевого взаимодействия	C6
7.	Использование некорректной настройки парольной политики	C7
8.	Физический доступ к техническим средствам ИС	C8
9.	Ошибочные действия при настройке	C9
10.	Программные сбои	C10
11.	Использование уязвимостей сетевого оборудования	C11

Для построения сценариев реализации угроз безопасности информации были взяты типовые тактики и соответствующие им техники, приведенные в Методике. Условные обозначения тактик и техник соответствуют таковым в Методике.

Так как при разработке Модели угроз рассматривается исходное (проектное) состояние ИСПДн без учета организационных и технических мер по защите информации, должен быть определен хотя бы один сценарий каждого способа реализации возможной угрозы безопасности информации. Сценарий определяется для каждого актуального нарушителя и их уровней возможностей.

Возможные сценарии реализации угроз представлены в Таблице №12.

Таблица №12

Таблица №12				
№ п/ п	Вероятные нарушители	Способ реализации угрозы	Тактика	Техники
Банк данных угроз ФСТЭК России (bdu.fstec.ru)				
УБИ.006: Угроза внедрения кода или данных				
1	Н1, Н3	С1, С2, С3, С7	Т1	Т1.3, Т1.4, Т1.11
			Т2	Т2.5, Т2.7, Т2.8, Т2.10, Т2.11
			Т3	Т3.1, Т3.7, Т3.14
	Н2	С1, С2, С3, С7	Т1	Т1.3, Т1.4, Т1.11
			Т3	Т3.10
УБИ.008: Угроза восстановления аутентификационной информации				
2	Н4, Н6	С7	Т1	Т1.9, Т1.11, Т1.12
			Т2	Т2.5, Т2.10, Т2.11
	Н5, Н7	С7	Т1	Т1.9, Т1.11, Т1.12
			Т2	Т2.5, Т2.10, Т2.11
	Н1, Н2, Н3	С7	Т1	Т1.6, Т1.11
Т2			Т2.4, Т2.10, Т2.11	
УБИ.009: Угроза восстановления предыдущей уязвимой версии BIOS				
3	Н4, Н6	С8, С10	Т1	Т1.11, Т1.13
			Т2	Т2.5

№ п/ п	Вероятные нарушители	Способ реализации угрозы	Тактика	Техники
	Н5, Н7	С8, С10	Т7	Т7.22
			Т1	Т1.11, Т1.13
			Т2	Т2.5
			Т7	Т7.22
4	УБИ.012: Угроза деструктивного изменения конфигурации/среды окружения программ			
	Н4, Н6	С1	Т1	Т1.3, Т1.11
			Т6	Т6.1, Т6.2
			Т10	Т10.3, Т10.4
	Н5, Н7	С1	Т1	Т1.3, Т1.11
			Т10	Т10.3, Т10.4
5	УБИ.013: Угроза деструктивного использования декларированного функционала BIOS			
	Н4, Н6	С1, С8	Т1	Т1.11
			Т10	Т10.8
	Н5, Н7	С1, С8	Т1	Т1.11
			Т10	Т10.8
6	УБИ.014: Угроза длительного удержания вычислительных ресурсов пользователями			
	Н4, Н6	С1, С2, С3	Т1	Т1.3, Т1.9, Т1.11
			Т6	Т6.1, Т6.2
			Т8	Т8.1, Т8.7
			Т10	Т10.10, Т10.11
	Н5, Н7	С1, С2, С3	Т1	Т1.3, Т1.9, Т1.11
			Т8	Т8.1, Т8.7
			Т10	Т10.10, Т10.11
	Н1, Н2, Н3	С1, С2, С3	Т1	Т1.4, Т1.11, Т1.12
			Т2	Т2.4, Т2.5, Т2.10, Т2.11
			Т6	Т6.1, Т6.2
			Т8	Т8.1, Т8.7
			Т10	Т10.10, Т10.11
7	УБИ.015: Угроза доступа к защищаемым файлам с использованием обходного пути			
	Н4, Н6	С1, С2	Т1	Т1.3, Т1.11
			Т2	Т2.5
			Т10	Т10.1
	Н5, Н7	С1, С2	Т1	Т1.3, Т1.11
			Т2	Т2.5
			Т10	Т10.1
	Н1, Н2, Н3	С1, С2	Т1	Т1.3, Т1.4, Т1.11, Т1.12
			Т2	Т2.4, Т2.5, Т2.10, Т2.11
			Т10	Т10.1
8	УБИ.017: Угроза доступа/перехвата/изменения HTTP cookies			
	Н1, Н2, Н3	С6	Т1	Т1.3, Т1.4
9	УБИ.018: Угроза загрузки нештатной операционной системы			
	Н4, Н6	С8	Т1	Т1.11
			Т2	Т2.5, Т2.8
			Т10	Т10.1, Т10.2
	Н5, Н7	С8	Т1	Т1.11, Т1.16
			Т2	Т2.5, Т2.8
Т10			Т10.1, Т10.2	
10	УБИ.019: Угроза заражения DNS-кеша			
	Н1, Н2, Н3	С5, С11	Т1	Т1.3, Т1.4, Т1.7, Т1.11
			Т7	Т7.21
11	УБИ.022: Угроза избыточного выделения оперативной памяти			
	Н4, Н6	С1, С3	Т1	Т1.11
			Т2	Т2.7
			Т3	Т3.1, Т3.3
			Т10	Т10.10
	Н5, Н7	С1, С3	Т1	Т1.11, Т1.16
			Т2	Т2.7

№ п/ п	Вероятные нарушители	Способ реализации угрозы	Тактика	Техники
	Н1, Н2, Н3	С1, С3	Т3	Т3.1, Т3.3
			Т10	Т10.10
			Т1	Т1.3, Т1.4, Т1.11
			Т2	Т2.8, Т2.10, Т2.11
			Т3	Т3.1, Т3.3
			Т10	Т10.10
12	УБИ.023: Угроза изменения компонентов системы			
	Н4, Н6	С8	Т1	Т1.11
			Т2	Т2.9
			Т4	Т4.4
	Н5, Н7	С8	Т1	Т1.11, Т1.16
			Т2	Т2.9
Т4			Т4.4	
13	УБИ.027: Угроза искажения вводимой и выводимой на периферийные устройства информации			
	Н4, Н6	С1, С2, С3	Т1	Т1.11
			Т3	Т3.1, Т3.3
			Т10	Т10.3, Т10.7
	Н5, Н7	С1, С2, С3	Т1	Т1.11, Т1.16
			Т3	Т3.1, Т3.3
Т10			Т10.3, Т10.7	
14	УБИ.028: Угроза использования альтернативных путей доступа к ресурсам			
	Н4, Н6	С1, С2	Т1	Т1.11
			Т2	Т2.5
			Т6	Т6.1, Т6.2, Т6.3
			Т10	Т10.1
	Н5, Н7	С1, С2	Т1	Т1.11, Т1.16
			Т2	Т2.5
			Т10	Т10.1
	Н1, Н2, Н3	С1, С2	Т1	Т1.3, Т1.4, Т1.11
			Т2	Т2.8, Т2.10, Т2.11
			Т6	Т6.1, Т6.2, Т6.3
			Т10	Т10.1
15	УБИ.030: Угроза использования информации идентификации/аутентификации, заданной по умолчанию			
	Н4, Н6	С1, С2, С7	Т1	Т1.11
			Т2	Т2.10
	Н5, Н7	С1, С2, С7	Т1	Т1.11, Т1.16
Т2			Т2.10	
16	УБИ.031: Угроза использования механизмов авторизации для повышения привилегий			
	Н4, Н6	С1, С2	Т1	Т1.11
			Т6	Т6.3, Т6.6
	Н5, Н7	С1, С2	Т1	Т1.11, Т1.16
			Т6	Т6.3, Т6.6
	Н1, Н2, Н3	С1, С2	Т1	Т1.3, Т1.4, Т1.11
			Т2	Т2.8, Т2.10, Т2.11
Т6			Т6.3, Т6.6	
17	УБИ.034: Угроза использования слабостей протоколов сетевого/локального обмена данными			
	Н4, Н6	С5	Т1	Т1.3, Т1.4, Т1.11
			Т9	Т9.2, Т9.3
	Н5, Н7	С5	Т1	Т1.3, Т1.4, Т1.11, Т1.16
			Т9	Т9.2, Т9.3
	Н1, Н2, Н3	С5	Т1	Т1.3, Т1.4, Т1.11
Т9			Т9.2, Т9.3	
18	УБИ.041: Угроза межсайтового скриптинга			
	Н1, Н2, Н3	С3	Т1	Т1.1, Т1.2, Т1.5, Т1.8
			Т2	Т2.1
Т3			Т3.7	
19	УБИ.045: Угроза нарушения изоляции среды исполнения BIOS			

№ п/ п	Вероятные нарушители	Способ реализации угрозы	Тактика	Техники
	Н4, Н6	С2, С3	T1	T1.3, T1.4, T1.11
			T2	T2.5, T2.8, T2.10, T2.11
			T6	T6.1, T6.2, T6.3
			T7	T7.22
	Н5, Н7	С2, С3	T1	T1.3, T1.4, T1.11
			T2	T2.5, T2.8, T2.10, T2.11
			T6	T6.1, T6.2, T6.3
			T7	T7.22
20	УБИ.049: Угроза нарушения целостности данных кеша			
	Н4, Н6	С1	T1	T1.3, T1.4, T1.11
			T3	T3.1
	Н5, Н7	С1	T1	T1.3, T1.4, T1.11
			T3	T3.1
	Н1, Н2, Н3	С1	T1	T1.3, T1.4, T1.11
			T3	T3.1
	21	УБИ.051: Угроза невозможности восстановления сессии работы на ПЭВМ при выводе из промежуточных состояний питания		
Н4, Н6		С8	T10	T10.10
Н5, Н7		С8	T10	T10.10
22		УБИ.053: Угроза невозможности управления правами пользователей BIOS		
	Н4, Н6	С8	T10	T10.10
	Н5, Н7	С8	T10	T10.10
	23	УБИ.062: Угроза некорректного использования прозрачного прокси-сервера за счёт плагинов браузера		
Н1, Н2, Н3		С3	T1	T1.1, T1.2, T1.5, T1.8
			T2	T2.1
			T3	T3.7
			T5	T5.6
24	УБИ.067: Угроза неправомерного ознакомления с защищаемой информацией			
	Н4, Н6	С7	T10	T10.1
	Н5, Н7	С7	T10	T10.1
	25	УБИ.069: Угроза неправомерных действий в каналах связи		
Н1, Н2, Н3		С5, С11	T1	T1.3, T1.4
			T2	T2.3
26	УБИ.071: Угроза несанкционированного восстановления удалённой защищаемой информации			
	Н4, Н6	С1, С2, С3, С8	T1	T1.3, T1.4, T1.11
			T6	T6.1, T6.2, T6.3
			T10	T10.1
	Н5, Н7	С1, С2, С3, С8	T1	T1.3, T1.4, T1.11
			T6	T6.1, T6.2, T6.3
			T10	T10.1
	Н1, Н2, Н3	С1, С2, С3	T1	T1.3, T1.4, T1.11
			T2	T2.5, T2.8, T2.10, T2.11
			T6	T6.1, T6.2, T6.3
			T10	T10.1
27	УБИ.072: Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS			
	Н4, Н6	С8	T1	T1.3, T1.4, T1.11
			T2	T2.5
			T7	T7.22
	Н5, Н7	С8	T1	T1.3, T1.4, T1.11
			T2	T2.5
			T7	T7.22
28	УБИ.074: Угроза несанкционированного доступа к аутентификационной информации			
	Н4, Н6	С1, С2, С4	T1	T1.9, T1.11, T1.12
	Н5, Н7	С1, С2, С4	T1	T1.9, T1.11, T1.12
	Н1, Н2, Н3	С1, С2, С4	T1	T1.11, T1.12
29	УБИ.086: Угроза несанкционированного изменения аутентификационной информации			
	Н4, Н6	С2	T1	T1.3, T1.4, T1.11

№ п/ п	Вероятные нарушители	Способ реализации угрозы	Тактика	Техники	
	Н5, Н7	С2	Т6	Т6.1, Т6.2, Т6.3	
			Т10	Т10.7	
			Т1	Т1.3, Т1.4, Т1.11	
			Т6	Т6.1, Т6.2, Т6.3	
	Н1, Н2, Н3	С2	Т10	Т10.7	
			Т1	Т1.3, Т1.4, Т1.11	
			Т2	Т2.5, Т2.8, Т2.10, Т2.11	
			Т6	Т6.1, Т6.2, Т6.3	
30	УБИ.087: Угроза несанкционированного использования привилегированных функций BIOS			Т10	
	Н4, Н6	С8	Т1	Т1.11	
			Т10	Т10.10	
	Н5, Н7	С8	Т1	Т1.11	
			Т10	Т10.10	
	31	УБИ.088: Угроза несанкционированного копирования защищаемой информации			
		Н4, Н6	С1, С2, С3	Т1	Т1.3, Т1.4, Т1.11
				Т9	Т9.3, Т9.4, Т9.10
Н5, Н7		С1, С2, С3	Т1	Т1.3, Т1.4, Т1.11	
			Т9	Т9.3, Т9.4, Т9.10	
Н1, Н2, Н3		С1, С2, С3	Т1	Т1.3, Т1.4, Т1.11	
			Т2	Т2.5, Т2.8, Т2.10, Т2.11	
			Т9	Т9.3, Т9.4, Т9.10	
32	УБИ.089: Угроза несанкционированного редактирования реестра				
	Н4, Н6	С1, С2, С3	Т1	Т1.3, Т1.4, Т1.11	
			Т6	Т6.1, Т6.2, Т6.3	
			Т10	Т10.1	
	Н5, Н7	С1, С2, С3	Т1	Т1.3, Т1.4, Т1.11	
			Т6	Т6.1, Т6.2, Т6.3	
			Т10	Т10.1	
	Н1, Н2, Н3	С1, С2, С3	Т1	Т1.3, Т1.4, Т1.11	
			Т2	Т2.5, Т2.8, Т2.10, Т2.11	
			Т6	Т6.1, Т6.2, Т6.3	
			Т10	Т10.1	
33	УБИ.090: Угроза несанкционированного создания учётной записи пользователя				
	Н4, Н6	С1, С2, С3	Т1	Т1.3, Т1.4, Т1.11	
			Т6	Т6.1, Т6.2, Т6.3	
			Т7	Т7.13	
	Н5, Н7	С1, С2, С3	Т1	Т1.3, Т1.4, Т1.11	
			Т6	Т6.1, Т6.2, Т6.3	
			Т7	Т7.13	
	Н1, Н2, Н3	С1, С2, С3	Т1	Т1.3, Т1.4, Т1.11	
			Т2	Т2.5, Т2.8, Т2.10, Т2.11	
			Т6	Т6.1, Т6.2, Т6.3	
Т7			Т7.13		
34	УБИ.091: Угроза несанкционированного удаления защищаемой информации				
	Н4, Н6	С1, С2, С3	Т1	Т1.3, Т1.4, Т1.11	
			Т6	Т6.1, Т6.2, Т6.3	
			Т10	Т10.8	
	Н5, Н7	С1, С2, С3	Т1	Т1.3, Т1.4, Т1.11	
			Т6	Т6.1, Т6.2, Т6.3	
			Т10	Т10.8	
	Н1, Н2, Н3	С1, С2, С3	Т1	Т1.3, Т1.4, Т1.11	
			Т2	Т2.5, Т2.8, Т2.10, Т2.11	
			Т6	Т6.1, Т6.2, Т6.3	
			Т10	Т10.8	
35	УБИ.093: Угроза несанкционированного управления буфером				
	Н4, Н6	С1, С2, С3	Т1	Т1.3, Т1.4, Т1.11	

№ п/ п	Вероятные нарушители	Способ реализации угрозы	Тактика	Техники
	Н5, Н7	С1, С2, С3	Т6	Т6.1, Т6.2, Т6.3
			Т10	Т10.1
			Т1	Т1.3, Т1.4, Т1.11
			Т6	Т6.1, Т6.2, Т6.3
	Н1, Н2, Н3	С1, С2, С3	Т10	Т10.1
			Т1	Т1.3, Т1.4, Т1.11
			Т2	Т2.5, Т2.8, Т2.10, Т2.11
			Т6	Т6.1, Т6.2, Т6.3
Т10	Т10.1			
36	УБИ.098: Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб			
Н1, Н2, Н3	С6	Т1	Т1.3, Т1.4	
37	УБИ.099: Угроза обнаружения хостов			
Н1, Н2, Н3	С6	Т1	Т1.3, Т1.4	
38	УБИ.100: Угроза обхода некорректно настроенных механизмов аутентификации			
	Н4, Н6	С1, С2	Т1	Т1.3, Т1.4, Т1.11
			Т2	Т2.5, Т2.6
	Н5, Н7	С1, С2	Т1	Т1.3, Т1.4, Т1.11
			Т2	Т2.5, Т2.6
	Н1, Н2, Н3	С1, С2	Т1	Т1.3, Т1.4, Т1.11
Т2			Т2.5, Т2.6	
39	УБИ.103: Угроза определения типов объектов защиты			
Н1, Н2, Н3	С6	Т1	Т1.3, Т1.4	
40	УБИ.104: Угроза определения топологии вычислительной сети			
Н1, Н2, Н3	С6	Т1	Т1.3, Т1.4	
41	УБИ.113: Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники			
	Н4, Н6	С8	Т10	Т10.10
	Н5, Н7	С8	Т10	Т10.10
	Н1, Н2, Н3	С2	Т1	Т1.3, Т1.4, Т1.11
			Т2	Т2.5, Т2.8, Т2.10, Т2.11
			Т10	Т10.10
42	УБИ.115: Угроза перехвата вводимой и выводимой на периферийные устройства информации			
	Н4, Н6	С1, С2, С3, С8	Т1	Т1.3, Т1.4, Т1.11
			Т2	Т2.5
			Т10	Т10.1
	Н5, Н7	С1, С2, С3, С8	Т1	Т1.3, Т1.4, Т1.11
			Т2	Т2.5
			Т10	Т10.1
	Н1, Н2, Н3	С1, С2, С3	Т1	Т1.3, Т1.4, Т1.11
			Т2	Т2.5, Т2.10, Т2.11
			Т10	Т10.1
43	УБИ.116: Угроза перехвата данных, передаваемых по вычислительной сети			
Н1, Н2, Н3	С5	Т1	Т1.3, Т1.5	
44	УБИ.121: Угроза повреждения системного реестра			
	Н4, Н6	С1, С2, С3	Т1	Т1.3, Т1.4, Т1.11
			Т2	Т2.5
			Т10	Т10.2, Т10.7
	Н5, Н7	С1, С2, С3	Т1	Т1.3, Т1.4, Т1.11
			Т2	Т2.5
			Т10	Т10.2, Т10.7
	Н1, Н2, Н3	С1, С2, С3	Т1	Т1.3, Т1.4, Т1.11
			Т2	Т2.5, Т2.10, Т2.11
			Т10	Т10.2, Т10.7
45	УБИ.124: Угроза подделки записей журнала регистрации событий			
	Н4, Н6	С1, С2, С3	Т1	Т1.3, Т1.4, Т1.11
			Т7	Т7.2
	Н5, Н7	С1, С2, С3	Т1	Т1.3, Т1.4, Т1.11
			Т7	Т7.2

№ п/ п	Вероятные нарушители	Способ реализации угрозы	Тактика	Техники
	Н1, Н2, Н3	С1, С2, С3	Т1	Т1.3, Т1.4, Т1.11
			Т2	Т2.5, Т2.10, Т2.11
			Т7	Т7.2
46	УБИ.128: Угроза подмены доверенного пользователя			
	Н1, Н2, Н3	С5	Т1	Т1.3, Т1.4, Т1.5, Т1.11
			Т2	Т2.5, Т2.10, Т2.11
47	УБИ.129: Угроза подмены резервной копии программного обеспечения BIOS			
	Н4, Н6	С2, С8	Т1	Т1.11
			Т7	Т7.22
	Н5, Н7	С2, С8	Т1	Т1.11
			Т7	Т7.22
48	УБИ.130: Угроза подмены содержимого сетевых ресурсов			
	Н1, Н2, Н3	С5	Т1	Т1.1, Т1.3, Т1.4, Т1.11
			Т2	Т2.13
			Т10	Т10.7, Т10.9
49	УБИ.140: Угроза приведения системы в состояние «отказ в обслуживании»			
	Н4, Н6	С5, С11	Т1	Т1.3, Т1.4, Т1.11
			Т10	Т10.10
	Н5, Н7	С5, С11	Т1	Т1.3, Т1.4, Т1.11
			Т10	Т10.10
	Н1, Н2, Н3	С5, С11	Т1	Т1.3, Т1.4, Т1.11
Т10			Т10.10	
50	УБИ.145: Угроза пропуска проверки целостности программного обеспечения			
	Н4, Н6	С3	Т1	Т1.3, Т1.4, Т1.11
			Т3	Т3.3, Т3.9
	Н5, Н7	С3	Т1	Т1.3, Т1.4, Т1.11
			Т3	Т3.3, Т3.9
	Н1, Н2, Н3	С3	Т1	Т1.3, Т1.4, Т1.11
Т3			Т3.3, Т3.9	
51	УБИ.152: Угроза удаления аутентификационной информации			
	Н4, Н6	С2, С3	Т1	Т1.3, Т1.4, Т1.11
			Т4	Т4.1
	Н5, Н7	С2, С3	Т1	Т1.3, Т1.4, Т1.11
			Т4	Т4.1
	Н1, Н2, Н3	С2, С3	Т1	Т1.3, Т1.4, Т1.11
Т2			Т2.5, Т2.10, Т2.11	
52	УБИ.153: Угроза усиления воздействия на вычислительные ресурсы пользователей при помощи сторонних серверов			
	Н4, Н6	С5, С6, С11	Т1	Т1.3, Т1.4, Т1.11
			Т10	Т10.10
	Н5, Н7	С5, С6, С11	Т1	Т1.3, Т1.4, Т1.11
			Т10	Т10.10
	Н1, Н2, Н3	С5, С6, С11	Т1	Т1.3, Т1.4, Т1.11
Т10			Т10.10	
53	УБИ.155: Угроза утраты вычислительных ресурсов			
	Н4, Н6	С5, С6, С11	Т1	Т1.3, Т1.4, Т1.11
			Т10	Т10.10
	Н5, Н7	С5, С6, С11	Т1	Т1.3, Т1.4, Т1.11
			Т10	Т10.10
	Н1, Н2, Н3	С5, С6, С11	Т1	Т1.3, Т1.4, Т1.11
Т10			Т10.10	
54	УБИ.157: Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации			
	Н1, Н2, Н3	С8	Т1	Т1.11
			Т10	Т10.8, Т10.10
55	УБИ.159: Угроза «форсированного веб-браузинга»			

№ п/ п	Вероятные нарушители	Способ реализации угрозы	Тактика	Техники
	Н1, Н2, Н3	С1, С2, С3	Т1	Т1.3, Т1.4, Т1.11
			Т2	Т2.5, Т2.10, Т2.11
56	УБИ.160: Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации			
	Н1, Н2, Н3	С8	Т1	Т1.11
Т9			Т9.10	
57	УБИ.162: Угроза эксплуатации цифровой подписи программного кода			
	Н4, Н6	С1, С2, С3	Т1	Т1.3, Т1.4, Т1.11
			Т3	Т3.11
	Н5, Н7	С1, С2, С3	Т1	Т1.3, Т1.4, Т1.11
			Т3	Т3.11
	Н1, Н2, Н3	С1, С2, С3	Т1	Т1.3, Т1.4, Т1.11
			Т2	Т2.5, Т2.10, Т2.11
Т3			Т3.11	
58	УБИ.167: Угроза заражения компьютера при посещении неблагонадёжных сайтов			
	Н4, Н6	С3	Т3	Т3.3
	Н5, Н7	С3	Т3	Т3.3
59	УБИ.168: Угроза «кражи» учётной записи доступа к сетевым сервисам			
	Н1, Н2, Н3	С1, С2, С3, С7	Т1	Т1.1, Т1.5, Т1.11, Т1.12
			Т2	Т2.5, Т2.10, Т2.11
			Т4	Т4.1
60	УБИ.170: Угроза неправомерного шифрования информации			
	Н1, Н2, Н3	С3	Т1	Т1.3, Т1.4, Т1.11
			Т3	Т3.1, Т3.3
61	УБИ.171: Угроза скрытного включения вычислительного устройства в состав бот-сети			
	Н1, Н2, Н3	С3	Т1	Т1.3, Т1.4, Т1.11
			Т3	Т3.1, Т3.3
			Т4	Т4.3
62	УБИ.172: Угроза распространения «почтовых червей»			
	Н1, Н2, Н3	С3	Т1	Т1.3, Т1.4, Т1.11
			Т3	Т3.1, Т3.3
63	УБИ.173: Угроза «спама» веб-сервера			
	Н1, Н2, Н3	С1, С9	Т1	Т1.3, Т1.4, Т1.11
64	УБИ.174: Угроза «фарминга»			
	Н1, Н2, Н3	С5, С6, С9	Т1	Т1.3, Т1.4, Т1.7, Т1.11
			Т2	Т2.3, Т2.4
65	УБИ.175: Угроза «фишинга»			
	Н1, Н2, Н3	С5, С6, С9	Т1	Т1.3, Т1.4, Т1.7, Т1.11
			Т2	Т2.3, Т2.4
66	УБИ.178: Угроза несанкционированного использования системных и сетевых утилит			
	Н4, Н6	С2, С3	Т1	Т1.3, Т1.4, Т1.11
			Т4	Т4.2, Т4.3
	Н5, Н7	С2, С3	Т1	Т1.3, Т1.4, Т1.11
			Т4	Т4.2, Т4.3
	Н1, Н2, Н3	С2, С3	Т1	Т1.3, Т1.4, Т1.11
			Т2	Т2.5, Т2.10, Т2.11
Т4			Т4.2, Т4.3	
67	УБИ.179: Угроза несанкционированной модификации защищаемой информации			
	Н4, Н6	С1, С2, С3, С8	Т1	Т1.3, Т1.4, Т1.11
			Т6	Т6.1, Т6.2, Т6.3
			Т10	Т10.8
	Н5, Н7	С1, С2, С3, С8	Т1	Т1.3, Т1.4, Т1.11
			Т6	Т6.1, Т6.2, Т6.3
			Т10	Т10.8
	Н1, Н2, Н3	С1, С2, С3	Т1	Т1.3, Т1.4, Т1.11
			Т2	Т2.5, Т2.10, Т2.11
			Т6	Т6.1, Т6.2, Т6.3
Т10			Т10.8	

№ п/ п	Вероятные нарушители	Способ реализации угрозы	Тактика	Техники
68	УБИ.180: Угроза отказа подсистемы обеспечения температурного режима			
	Н4, Н6	С8	T1	T1.11
			T10	T10.10
	Н5, Н7	С8	T1	T1.11
T10			T10.10	
69	УБИ.182: Угроза физического устаревания аппаратных компонентов			
	Н4, Н6	С8	T1	T1.11
			T10	T10.10
	Н5, Н7	С8	T1	T1.11
T10			T10.10	
70	УБИ.186: Угроза внедрения вредоносного кода через рекламу, сервисы и контент			
	Н4, Н6	С3	T3	T3.3
	Н5, Н7	С3	T3	T3.3
71	УБИ.191: Угроза внедрения вредоносного кода в дистрибутив программного обеспечения			
	Н4, Н6	С3	T3	T3.10
	Н5, Н7	С3	T3	T3.10
	Н1, Н2, Н3	С3	T1	T1.3, T1.4, T1.11
			T2	T2.5, T2.10, T2.11
T3			T3.10	
72	УБИ.192: Угроза использования уязвимых версий программного обеспечения			
	Н4, Н6	С1, С2	T1	T1.3, T1.4, T1.11
			T2	T2.5
	Н5, Н7	С1, С2	T1	T1.3, T1.4, T1.11
			T2	T2.5
Н1, Н2, Н3	С1, С2	T1	T1.3, T1.4, T1.11	
73	УБИ.208: Угроза нецелевого использования вычислительных ресурсов средства вычислительной техники			
	Н4, Н6	С3	T1	T1.3, T1.4, T1.11
			T10	T10.11
	Н5, Н7	С3	T1	T1.3, T1.4, T1.11
			T10	T10.11
	Н1, Н2, Н3	С3	T1	T1.3, T1.4, T1.11
			T3	T3.1, T3.3
T10			T10.11	
74	УБИ.209: Угроза несанкционированного доступа к защищаемой памяти ядра процессора			
	Н4, Н6	С1, С2	T1	T1.3, T1.4, T1.11
			T2	T2.5
	Н5, Н7	С1, С2	T1	T1.3, T1.4, T1.11
			T2	T2.5
Н1, Н2, Н3	С1, С2	T1	T1.3, T1.4, T1.11	
75	УБИ.211: Угроза использования непроверенных пользовательских данных при формировании конфигурационного файла, используемого программным обеспечением администрирования информационных систем			
	Н4, Н6	С9	T1	T1.3, T1.4, T1.11
			T10	T10.4, T10.5
	Н5, Н7	С9	T1	T1.3, T1.4, T1.11
T10			T10.4, T10.5	
76	Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка). ФСТЭК России, 2008 год			
	Угрозы, реализуемые в ходе загрузки операционной системы и направленные на перехват паролей или идентификаторов, модификацию базовой системы ввода/вывода (BIOS), перехват управления загрузкой			
	Н4, Н6	С2, С8	T1	T1.11, T1.12
			T7	T7.22
T10			T10.1, T10.2, T10.3, T10.4,	

№ п/ п	Вероятные нарушители	Способ реализации угрозы	Тактика	Техники
	Н5, Н7	С2, С8		T10.5, T10.6
			T1	T1.11, T1.12
			T7	T7.22
			T10	T10.1, T10.2, T10.3, T10.4, T10.5, T10.6
77	Угрозы, реализуемые после загрузки операционной системы и направленные на выполнение несанкционированного доступа с применением стандартных функций (уничтожение, копирование, перемещение, форматирование носителей информации и т.п.) операционной системы или какой-либо прикладной программы (например, системы управления базами данных), с применением специально созданных для выполнения НСД программ (программ просмотра и модификации реестра, поиска текстов в текстовых файлах и т.п.)			
	Н4, Н6	С1, С2, С3	T1	T1.11, T1.12
			T2	T2.5, T2.10, T2.11
			T3	T3.1, T3.3
			T10	T10.1
	Н5, Н7	С1, С2, С3	T1	T1.11, T1.12
			T2	T2.5, T2.10, T2.11
			T3	T3.1, T3.3
T10			T10.1	
78	Угрозы внедрения вредоносных программ			
	Н4, Н6	С3	T1	T1.11
			T2	T2.7
			T3	T3.1, T3.3
	Н5, Н7	С3	T1	T1.11
			T2	T2.7
T3			T3.1, T3.3	
79	Угрозы «Анализа сетевого трафика» с перехватом передаваемой по сети информации			
	Н4, Н6	С5, С6	T1	T1.3, T1.4
	Н5, Н7	С5, С6	T1	T1.3, T1.4
	Н1, Н2, Н3	С5, С6	T1	T1.3, T1.4
80	Угрозы «Анализа сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой в ИСПДн из внешних сетей информации			
	Н4, Н6	С5, С6	T1	T1.3, T1.4
	Н5, Н7	С5, С6	T1	T1.3, T1.4
	Н1, Н2, Н3	С5, С6	T1	T1.3, T1.4
81	Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.			
	Н4, Н6	С5, С6	T1	T1.3
	Н5, Н7	С5, С6	T1	T1.3
	Н1, Н2, Н3	С5, С6	T1	T1.3
82	Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях			
	Н4, Н6	С5, С11	T1	T1.3, T1.4, T1.11
			T7	T7.21
	Н5, Н7	С5, С11	T1	T1.3, T1.4, T1.11
			T7	T7.21
	Н1, Н2, Н3	С5, С11	T1	T1.3, T1.4, T1.11
			T2	T2.5, T2.10, T2.11
T7			T7.21	
83	Угрозы подмены доверенного объекта			
	Н4, Н6	С5, С11	T1	T1.3, T1.4, T1.11
			T7	T7.21
	Н5, Н7	С5, С11	T1	T1.3, T1.4, T1.11
			T7	T7.21
	Н1, Н2, Н3	С5, С11	T1	T1.3, T1.4, T1.11
			T2	T2.5, T2.10, T2.11
T7			T7.21	

№ п/ п	Вероятные нарушители	Способ реализации угрозы	Тактика	Техники
84	Угрозы навязывания ложного маршрута путем несанкционированного изменения маршрутно-адресных данных как внутри сети, так и во внешних сетях			
	H4, H6	C5, C11	T1	T1.3, T1.4, T1.11
			T7	T7.21
	H5, H7	C5, C11	T1	T1.3, T1.4, T1.11
			T7	T7.21
	H1, H2, H3	C5, C11	T1	T1.3, T1.4, T1.11
			T2	T2.5, T2.10, T2.11
85	Угрозы выявления паролей			
	H4, H6	C5, C6	T1	T1.3, T1.4, T1.12
	H5, H7	C5, C6	T1	T1.3, T1.4, T1.12
	H1, H2, H3	C5, C6	T1	T1.3, T1.4, T1.12
	Угрозы типа «Отказ в обслуживании»			
86	H4, H6	C1, C2, C3	T1	T1.3, T1.4, T1.11
			T10	T10.10
	H5, H7	C1, C2, C3	T1	T1.3, T1.4, T1.11
			T10	T10.10
	H1, H2, H3	C1, C2, C3	T1	T1.3, T1.4, T1.11
			T2	T2.5, T2.10, T2.11
			T10	T10.10
87	Угрозы удаленного запуска приложений			
	H4, H6	C3	T1	T1.3, T1.4, T1.11
			T3	T3.1, T3.3
			T5	T5.1, T5.2
	H5, H7	C3	T1	T1.3, T1.4, T1.11
			T3	T3.1, T3.3
			T5	T5.1, T5.2
	H1, H2, H3	C3	T1	T1.3, T1.4, T1.11
			T2	T2.5, T2.10, T2.11
			T3	T3.1, T3.3
			T5	T5.1, T5.2
88	Угрозы внедрения по сети вредоносных программ			
	H4, H6	C3	T3	T3.3
	H5, H7	C3	T3	T3.3
	H1, H2, H3	C3	T3	T3.1, T3.3

7.3. Определение актуальности угроз безопасности информации

Определение актуальности угроз безопасности информации производится экспертным методом экспертной группой, состав которой приведен в Главе 1 настоящей Модели угроз. В ходе работы экспертной группы проводится опрос ее членов с целью определить, возможен ли соответствующий сценарий реализации угрозы безопасности информации или нет. Оценка производится в 2 раунда. Опрос экспертов включает следующие этапы:

- каждый эксперт проводит оценку возможности сценария реализации угрозы по числовой шкале от «1» до «10»;
- в каждом раунде после оценки соответствующего сценария каждым членом экспертной группы отбрасываются минимальные и максимальные оценки;
- определяется среднее значение в каждом раунде;
- определяется итоговое среднее значение по всем раундам.

Угроза считается актуальной, если ее итоговое среднее значение больше или равно «7».

Результаты опроса экспертной группы представлены в Таблице №13.

Таблица №13

№ п/п		Сценарий	Раунд 1			Раунд 2			Общий итог	Актуальность		
			Сугрин Д.А.	Узорова О.Г.	Вицина И.М.	Итог раунда 1	Сугрин Д.А.	Узорова О.Г.			Вицина И.М.	Итог раунда 2
Банк данных угроз ФСТЭК России (bdu.fstec.ru)												
1	№1	9	9	9	9	8	8	8	8	8,5	да	
	№2	7	10	7	7	9	8	9	9	8	да	
	УБИ.006: Угроза внедрения кода или данных											
2	№1	8	9	9	9	7	8	8	8	8,5	да	
	№2	10	9	9	9	9	9	9	9	9	да	
	№3	10	8	10	10	9	9	9	9	9,5	да	
3	№1	6	8	6	6	9	10	9	9	9,5	да	
	№2	6	8	8	8	6	9	7	7	7,5	да	
	УБИ.008: Угроза восстановления аутентификационной информации											
4	№1	8	10	10	10	9	10	9	9	9,5	да	
	№2	9	10	9	9	6	9	9	9	9	да	
	УБИ.009: Угроза восстановления предыдущей уязвимой версии BIOS											
5	№1	6	9	7	7	10	9	10	10	8,5	да	
	№2	7	7	7	7	7	8	8	8	7,5	да	
	УБИ.012: Угроза деструктивного изменения конфигурации/среды окружения программ											
6	№1	8	9	8	8	9	9	9	9	8,5	да	
	№2	6	10	10	10	6	9	6	6	8	да	
	№3	7	9	8	8	10	10	10	10	9	да	
7	№1	10	7	7	7	10	9	9	9	9	да	
	№2	7	7	7	7	10	8	9	9	8	да	
	№3	10	7	10	10	8	9	9	9	9,5	да	
8	№1	6	7	7	7	7	9	9	9	8	да	
	№2	8	6	8	8	10	8	8	8	9,5	да	
	УБИ.017: Угроза доступа/перехвата/изменения HTTP cookies											
9	№1	8	6	8	8	10	8	8	8	8	да	
	№2	9	7	7	7	7	10	9	9	8	да	
	УБИ.018: Угроза загрузки нештатной операционной системы											
10	№1	10	10	10	10	7	9	9	9	9,5	да	
	№2	7	6	7	7	8	9	8	8	7,5	да	
	УБИ.019: Угроза заражения DNS-кеша											
11	№1	7	6	7	7	9	10	9	9	9	да	
	№2	7	9	9	9	8	9	8	8	7,5	да	
	УБИ.022: Угроза избыточного выделения оперативной памяти											

№ п/п	Сценарий	Раунд 1				Раунд 2				Общий итог	Актуальность
		Сугрин Д.А.	Узорова О.Г.	Вицина И.М.	Итог раунда 1	Сугрин Д.А.	Узорова О.Г.	Вицина И.М.	Итог раунда 2		
№3		6	7	7	7	8	10	9	9	8	да
УБИ.023: Угроза изменения компонентов системы											
№1		8	8	8	8	8	8	8	8	8	да
№2		9	7	7	7	10	8	9	9	8	да
УБИ.027: Угроза искажения вводимой и выводимой на периферийные устройства информации											
№1		7	6	6	6	8	8	8	8	7	да
№2		7	8	7	7	7	8	7	7	7	да
УБИ.028: Угроза использования альтернативных путей доступа к ресурсам											
№1		10	8	9	9	7	8	8	8	8,5	да
№2		8	9	9	9	9	9	9	9	9	да
№3		9	10	9	9	8	8	8	8	8,5	да
УБИ.030: Угроза использования информации идентификации/аутентификации, заданной по умолчанию											
№1		10	7	8	8	10	9	9	9	8,5	да
№2		8	9	8	8	7	9	8	8	8	да
УБИ.031: Угроза использования механизмов авторизации для повышения привилегий											
№1		8	8	8	8	8	8	8	8	8	да
№2		7	10	8	8	10	10	10	10	9	да
№3		7	6	7	7	10	10	10	10	8,5	да
УБИ.034: Угроза использования слабостей протоколов сетевого/локального обмена данными											
№1		10	8	8	8	8	8	8	8	8	да
№2		6	9	9	9	8	10	8	8	8,5	да
№3		8	6	7	7	8	9	8	8	7,5	да
УБИ.041: Угроза межсайтового скриптинга											
№1		9	9	9	9	10	10	10	10	9,5	да
УБИ.045: Угроза нарушения изоляции среды исполнения BIOS											
№1		8	9	9	9	8	8	8	8	8,5	да
№2		9	9	9	9	7	8	7	7	8	да
УБИ.049: Угроза нарушения целостности данных кеша											
№1		8	8	8	8	6	10	8	8	8	да
№2		7	8	8	8	9	10	10	10	9	да
№3		6	8	7	7	7	8	8	8	7,5	да
УБИ.051: Угроза невозможности восстановления сессии работы на ПК/ВМ при выводе из промежуточных состояний питания											
№1		7	9	8	8	7	8	8	8	8	да
№2		6	9	7	7	10	10	10	10	8,5	да
УБИ.053: Угроза невозможности управления правами пользователей BIOS											
№1		6	9	9	9	9	8	8	8	8,5	да

№ п/п	Сценарий	Раунд 1				Раунд 2				Общий итог	Актуальность
		Сугрин Д.А.	Узорова О.Г.	Вицина И.М.	Итог раунда 1	Сугрин Д.А.	Узорова О.Г.	Вицина И.М.	Итог раунда 2		
23	№2	8	8	8	8	8	10	8	8	8	да
	№1	6	9	9	9	9	9	9	9	9	да
24	№1	7	9	9	9	7	8	7	7	8	да
	№2	9	9	9	9	8	10	10	10	9,5	да
25	№1	10	10	10	10	9	9	9	9	9,5	да
	№1	8	9	9	9	9	9	9	9	9	да
26	№2	9	8	9	9	9	8	9	9	9	да
	№3	8	6	8	8	8	10	10	10	9	да
27	№1	7	9	8	8	6	8	8	8	8	да
	№2	7	6	6	6	8	9	9	9	7,5	да
28	№1	6	10	9	9	8	9	9	9	9	да
	№2	9	8	8	8	6	8	7	7	7,5	да
29	№3	8	9	9	9	6	9	7	7	8	да
	№1	10	6	7	7	8	10	9	9	8	да
30	№2	6	10	9	9	7	9	7	7	8	да
	№3	8	7	7	7	9	9	9	9	8	да
31	№1	9	6	6	6	8	8	8	8	7	да
	№2	6	8	6	6	8	9	8	8	7	да
32	№1	7	8	8	8	9	10	9	9	8,5	да
	№2	6	7	7	7	9	8	9	9	8	да
33	№3	6	10	6	6	8	8	8	8	7	да
	№1	6	9	8	8	10	8	8	8	8	да
33	№2	6	10	8	8	7	10	10	10	9	да
	№3	9	6	8	8	6	8	7	7	7,5	да
33	№1	7	10	9	9	9	8	8	8	8,5	да
	№2	6	10	8	8	7	10	10	10	9	да
33	№3	9	6	8	8	6	8	7	7	7,5	да
	№1	7	10	9	9	9	8	8	8	8,5	да

№ п/п	Сценарий	Раунд 1				Раунд 2				Общий итог	Актуальность
		Сугрин Д.А.	Узорова О.Г.	Вицина И.М.	Итог раунда 1	Сугрин Д.А.	Узорова О.Г.	Вицина И.М.	Итог раунда 2		
	№2	8	10	9	9	9	10	9	9	9	да
	№3	8	10	10	10	8	8	8	8	9	да
34	УБИ.091: Угроза несанкционированного удаления защищаемой информации										
	№1	8	9	9	9	7	10	7	7	8	да
	№2	9	7	7	7	8	9	9	9	8	да
	№3	8	8	8	8	7	9	7	7	7,5	да
35	УБИ.093: Угроза несанкционированного управления буфером										
	№1	10	10	10	10	6	10	9	9	9,5	да
	№2	10	7	10	10	10	8	8	8	9	да
	№3	7	6	7	7	8	10	10	10	8,5	да
36	УБИ.098: Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб										
	№1	6	8	8	8	7	9	9	9	8,5	да
37	УБИ.099: Угроза обнаружения хостов										
	№1	9	8	9	9	8	8	8	8	8,5	да
38	УБИ.100: Угроза обхода некорректно настроенных механизмов аутентификации										
	№1	7	9	9	9	7	8	7	7	8	да
	№2	6	10	10	10	9	9	9	9	9,5	да
	№3	6	7	6	6	8	9	9	9	7,5	да
39	УБИ.103: Угроза определения типов объектов защиты										
	№1	7	10	9	9	7	10	8	8	8,5	да
40	УБИ.104: Угроза определения топологии вычислительной сети										
	№1	7	9	7	7	8	9	8	8	7,5	да
41	УБИ.113: Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники										
	№1	9	10	10	10	7	10	10	10	10	да
	№2	10	8	10	10	6	8	7	7	8,5	да
	№3	10	8	10	10	7	9	8	8	9	да
42	УБИ.115: Угроза перехвата вводимой и выводимой на периферийные устройства информации										
	№1	9	10	10	10	8	8	8	8	9	да
	№2	8	6	6	6	10	8	9	9	7,5	да
	№3	10	7	8	8	6	9	9	9	8,5	да
43	УБИ.116: Угроза перехвата данных, передаваемых по вычислительной сети										
	№1	9	8	8	8	10	8	10	10	9	да
44	УБИ.121: Угроза повреждения системного реестра										
	№1	10	7	7	7	10	9	10	10	8,5	да
	№2	10	10	10	10	8	9	8	8	9	да
	№3	8	6	7	7	7	9	9	9	8	да

№ п/п	Сценарий	Раунд 1			Раунд 2			Общий итог	Актуальность
		Сугрин Д.А.	Узорова О.Г.	Вицина И.М.	Итог раунда 1	Сугрин Д.А.	Узорова О.Г.	Вицина И.М.	Итог раунда 2
45	№1	9	8	8	8	7	10	9	9
	№2	6	7	7	7	8	8	8	8
	№3	8	8	8	8	10	10	10	10
46	№1	8	6	8	8	6	8	6	6
	№2	10	6	9	9	8	8	8	8
	№3	10	7	10	10	8	9	9	9
47	№1	6	8	7	7	7	9	9	9
	№2	6	9	8	8	8	8	8	8
	№3	6	9	8	8	9	10	10	10
48	№1	6	8	7	7	7	9	9	9
	№2	6	9	7	7	7	8	8	8
	№3	6	10	8	8	10	8	8	8
49	№1	6	9	9	9	8	10	10	10
	№2	9	9	9	9	10	9	9	9
	№3	10	7	7	7	8	8	8	8
50	№1	6	9	9	9	8	10	10	10
	№2	9	9	9	9	10	9	9	9
	№3	10	7	7	7	8	8	8	8
51	№1	6	9	8	8	10	9	9	9
	№2	9	7	9	9	10	8	8	8
	№3	9	8	9	9	10	8	8	8
52	№1	7	9	7	7	8	10	10	10
	№2	9	7	8	8	9	10	10	10
	№3	7	9	7	7	8	9	9	9
53	№1	7	8	7	7	8	10	10	10
	№2	8	10	8	8	10	9	9	9
	№3	6	7	6	6	10	10	10	10
54	№1	9	10	10	10	10	10	10	10
	№2	6	10	10	10	9	8	8	8
	№3	6	10	10	10	9	8	8	8
55	№1	6	10	10	10	9	8	8	8
	№2	6	10	10	10	9	8	8	8
	№3	6	10	10	10	9	8	8	8
56	№1	6	10	10	10	9	8	8	8
	№2	6	10	10	10	9	8	8	8
	№3	6	10	10	10	9	8	8	8

№ п/п	Сценарий	Раунд 1				Раунд 2				Общий итог	Актуальность
		Сугрин Д.А.	Узорова О.Г.	Вицина И.М.	Итог раунда 1	Сугрин Д.А.	Узорова О.Г.	Вицина И.М.	Итог раунда 2		
57	№1	6	10	7	7	9	9	9	9	8	да
				УБИ.162: Угроза эксплуатации цифровой подписи программного кода							
	№1	10	8	10	10	10	10	10	10	10	да
	№2	8	8	8	8	6	10	10	10	9	да
58	№3	9	6	8	8	8	10	9	9	8,5	да
				УБИ.167: Угроза заражения компьютера при посещении неблагонадёжных сайтов							
	№1	6	8	6	6	9	10	10	10	8	да
	№2	6	9	8	8	7	9	7	7	7,5	да
59				УБИ.168: Угроза «кражи» учётной записи доступа к сетевым сервисам							
	№1	9	6	9	9	9	9	9	9	9	да
				УБИ.170: Угроза неправомерного шифрования информации							
	№1	9	7	7	7	9	10	9	9	8	да
60				УБИ.171: Угроза скрытного включения вычислительного устройства в состав бот-сети							
	№1	8	7	7	7	7	8	7	7	7	да
				УБИ.172: Угроза распространения «почтовых червей»							
	№1	7	6	6	6	10	10	10	10	8	да
61				УБИ.173: Угроза «спама» веб-сервера							
	№1	6	8	7	7	8	10	9	9	8	да
				УБИ.174: Угроза «фарминга»							
	№1	10	7	8	8	9	8	8	8	8	да
62				УБИ.175: Угроза «фишинга»							
	№1	6	9	9	9	6	8	8	8	8,5	да
				УБИ.178: Угроза несанкционированного использования системных и сетевых утилит							
	№1	7	9	9	9	9	8	9	9	9	да
63	№2	9	10	10	10	9	8	8	8	9	да
	№3	10	6	9	9	7	8	7	7	8	да
				УБИ.179: Угроза несанкционированной модификации защищаемой информации							
	№1	10	10	10	10	6	10	7	7	8,5	да
64	№2	6	8	8	8	9	8	9	9	8,5	да
	№3	9	9	9	9	8	10	8	8	8,5	да
				УБИ.180: Угроза отказа подсистемы обеспечения температурного режима							
	№1	6	10	10	10	9	8	9	9	9,5	да
65	№2	9	9	9	9	10	9	9	9	9	да
				УБИ.182: Угроза физического устаревания аппаратных компонентов							
	№1	10	9	10	10	9	10	10	10	10	да
	№2	9	9	9	9	10	9	9	9	9	да

№ п/п	Сценарий	Раунд 1				Раунд 2				Общий итог	Актуальность
		Сутрин Д.А.	Узорова О.Г.	Вицина И.М.	Итог раунда 1	Сутрин Д.А.	Узорова О.Г.	Вицина И.М.	Итог раунда 2		
70	№1	10	9	10	10	7	10	10	10	10	да
	№2	10	6	9	9	10	8	8	8	8,5	да
71	№1	6	9	8	8	9	8	8	8	8	да
	№2	8	8	8	8	8	8	8	8	8	да
	№3	9	6	7	7	10	10	10	10	10	да
	№1	7	8	8	8	7	8	8	8	8,5	да
72	№2	7	6	7	7	7	10	10	10	10	да
	№3	8	8	8	8	10	10	10	10	10	да
	№1	6	8	6	6	8	9	8	8	7	да
73	№2	8	7	7	7	7	8	8	8	7,5	да
	№3	6	8	6	6	10	8	10	10	8	да
	№1	9	6	9	9	9	9	9	9	9	да
74	№2	9	7	7	7	7	10	10	10	10	да
	№3	8	7	8	8	8	10	10	10	10	да
	№1	10	8	8	8	8	8	8	8	8	да
75	№2	7	9	7	7	10	8	8	8	7,5	да
	№1	10	8	8	8	8	8	8	8	8	да
Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка). ФСТЭК России, 2008 год											
76	Угрозы, реализуемые в ходе загрузки операционной системы и направленные на перехват паролей или идентификацию базовой системы ввода/вывода (BIOS), перехват управления загрузкой	10	10	10	10	10	8	10	10	10	да
	Угрозы, реализуемые после загрузки операционной системы и направленные на выполнение несанкционированного доступа с применением стандартных функций (уничтожение, копирование, перемещение, форматирование носителей информации и т.п.) операционной системы или какой-либо прикладной программы (например, системы управления базами данных), с применением специально созданных для выполнения НСД программ (программ просмотра и модификации реестра, поиска текстов в текстовых файлах и т.п.)	8	6	7	7	8	8	8	8	7,5	да
77	Угрозы, реализуемые после загрузки операционной системы и направленные на выполнение несанкционированного доступа с применением стандартных функций (уничтожение, копирование, перемещение, форматирование носителей информации и т.п.) операционной системы или какой-либо прикладной программы (например, системы управления базами данных), с применением специально созданных для выполнения НСД программ (программ просмотра и модификации реестра, поиска текстов в текстовых файлах и т.п.)	8	6	7	7	8	8	8	8	7	да
	Угрозы внедрения вредоносных программ	6	8	7	7	7	8	7	7	7	да
78	Угрозы внедрения вредоносных программ	8	6	7	7	8	8	8	8	7	да

№ п/п	Сценарий	Раунд 1			Итог раунда 1	Раунд 2			Общий итог	Актуальность
		Сугрин Д.А.	Узорова О.Г.	Вицина И.М.		Сугрин Д.А.	Узорова О.Г.	Вицина И.М.		
	№1	9	10	10	10	7	10	10	10	да
	№2	8	10	10	10	6	8	6	8	да
	Угрозы «Анализа сетевого трафика» с перехватом передаваемой по сети информации									
79	№1	7	6	6	6	10	10	10	8	да
	№2	6	8	6	6	10	10	10	8	да
	№3	7	7	7	7	8	9	8	7,5	да
80	Угрозы «Анализа сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой в ИСПДн из внешних сетей информации									
	№1	8	7	8	8	9	8	9	8,5	да
	№2	7	7	7	7	9	9	9	8	да
	№3	7	7	7	7	7	8	7	7	да
	Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.									
	81	№1	7	9	9	9	7	9	9	9
	№2	6	10	9	9	10	8	8	8,5	да
	№3	10	7	7	7	8	10	8	7,5	да
	Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях									
82	№1	6	7	6	6	8	8	8	7	да
	№2	9	10	9	9	9	8	9	9	да
	№3	6	7	7	7	10	10	10	8,5	да
	Угрозы подмены доверенного объекта									
	№1	7	9	9	9	8	9	8	8,5	да
	№2	8	6	7	7	10	10	10	8,5	да
83	№3	9	7	7	7	9	10	10	8,5	да
	Угрозы навязывания ложного маршрута путем несанкционированного изменения маршрутно-адресных данных как внутри сети, так и во внешних сетях									
	84	№1	9	8	9	9	6	8	7	8
	№2	7	9	7	7	7	8	8	7,5	да
	№3	6	9	6	6	10	9	10	8	да
	Угрозы выявления паролей									
85	№1	6	10	10	10	8	8	8	9	да
	№2	6	7	6	6	9	8	9	7,5	да
	№3	6	7	6	6	10	8	9	7,5	да
	Угрозы типа «Отказ в обслуживании»									
	№1	10	9	9	9	7	9	7	8	да
	86	№2	7	9	9	9	7	8	7	8
	№3	7	6	6	6	10	10	10	8	да
	Угрозы удаленного запуска приложений									
	87									

№ п/п	Сценарий	Раунд 1				Раунд 2				Общий итог	Актуальность
		Сугрин Д.А.	Узорова О.Г.	Вицина И.М.	Итог раунда 1	Сугрин Д.А.	Узорова О.Г.	Вицина И.М.	Итог раунда 2		
88	№1	6	8	7	7	9	9	9	9	8	да
	№2	8	10	10	10	8	10	8	8	9	да
	№3	6	10	8	8	6	10	9	9	8,5	да
	№1	8	6	7	7	8	9	8	8	7,5	да
	№2	7	7	7	7	7	10	10	10	8,5	да
	№3	6	7	7	7	9	9	9	9	8	да
	Угрозы внедрения по сети вредоносных программ										
	Угроза восстановления аутентификационной информации										
	Угроза восстановления предыдущей уязвимой версии BIOS										

7.4. Выводы об актуальности угроз безопасности информации

Для ИСПДн «АСУ ЖКХ Капитальный ремонт» определены актуальные угрозы, представленные в Таблице №14.

№ п/п	Идентификатор УБИ	Название угрозы
Банк данных угроз ФСТЭК России (bdu.fstec.ru)		
1	УБИ.006	Угроза внедрения кода или данных
2	УБИ.008	Угроза восстановления аутентификационной информации
3	УБИ.009	Угроза восстановления предыдущей уязвимой версии BIOS
4	УБИ.012	Угроза деструктивного изменения конфигурации/среды окружения программ
5	УБИ.013	Угроза деструктивного использования декларированного функционала BIOS
6	УБИ.014	Угроза длительного использования вычислительных ресурсов пользователями
7	УБИ.015	Угроза доступа к защищаемым файлам с использованием обходного пути
8	УБИ.017	Угроза доступа/перехвата/изменения HTTP cookies
9	УБИ.018	Угроза загрузки нештатной операционной системы
10	УБИ.019	Угроза заражения DNS-кеша
11	УБИ.022	Угроза избыточного выделения оперативной памяти
12	УБИ.023	Угроза изменения компонентов системы
13	УБИ.027	Угроза искажения вводимой и выводимой на периферийные устройства информации
14	УБИ.028	Угроза использования альтернативных путей доступа к ресурсам
15	УБИ.030	Угроза использования информации идентификации/аутентификации, заданной по умолчанию
16	УБИ.031	Угроза использования механизмов авторизации для повышения привилегий
17	УБИ.034	Угроза использования слабостей протоколов сетевого/локального обмена данными
18	УБИ.041	Угроза межсайтового скриптинга
19	УБИ.045	Угроза нарушения изоляции среды исполнения BIOS

Таблица №14

№ п/п	Идентификатор УБИ	Название угрозы
20	УБИ.049	Угроза нарушения целостности данных кеша
21	УБИ.051	Угроза невозможности восстановления сессии работы на ПЭВМ при выводе из промежуточных состояний питания
22	УБИ.053	Угроза невозможности управления правами пользователей BIOS
23	УБИ.062	Угроза некорректного использования прозрачного прокси-сервера за счёт плагинов браузера
24	УБИ.067	Угроза неправомерного ознакомления с защищаемой информацией
25	УБИ.069	Угроза неправомерных действий в каналах связи
26	УБИ.071	Угроза несанкционированного восстановления удалённой защищаемой информации
27	УБИ.072	Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS
28	УБИ.074	Угроза несанкционированного доступа к аутентификационной информации
29	УБИ.086	Угроза несанкционированного изменения аутентификационной информации
30	УБИ.087	Угроза несанкционированного использования привилегированных функций BIOS
31	УБИ.088	Угроза несанкционированного копирования защищаемой информации
32	УБИ.089	Угроза несанкционированного редактирования реестра
33	УБИ.090	Угроза несанкционированного создания учётной записи пользователя
34	УБИ.091	Угроза несанкционированного удаления защищаемой информации
35	УБИ.093	Угроза несанкционированного управления буфером
36	УБИ.098	Угроза несанкционированного открытия портов и идентификации привязанных к нему сетевых служб
37	УБИ.099	Угроза обнаружения хостов
38	УБИ.100	Угроза обхода некорректно настроенных механизмов аутентификации
39	УБИ.103	Угроза определения типов объектов защиты
40	УБИ.104	Угроза определения топологии вычислительной сети
41	УБИ.113	Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники
42	УБИ.115	Угроза перехвата вводимой и выводимой на периферийные устройства информации
43	УБИ.116	Угроза перехвата данных, передаваемых по вычислительной сети
44	УБИ.121	Угроза повреждения системного реестра
45	УБИ.124	Угроза подделки записей журнала регистрации событий
46	УБИ.128	Угроза подмены доверенного пользователя
47	УБИ.129	Угроза подмены резервной копии программного обеспечения BIOS
48	УБИ.130	Угроза подмены содержимого сетевых ресурсов
49	УБИ.140	Угроза приведения системы в состояние «отказ в обслуживании»
50	УБИ.145	Угроза пропуска проверки целостности программного обеспечения
51	УБИ.152	Угроза удаления аутентификационной информации
52	УБИ.153	Угроза усиления воздействия на вычислительные ресурсы пользователей при помощи сторонних серверов
53	УБИ.155	Угроза утраты вычислительных ресурсов
54	УБИ.157	Угроза физического вывода из строя средств хранения, обработки и (или) ввода/вывода/передачи информации
55	УБИ.159	Угроза «форсированного веб-браузинга»
56	УБИ.160	Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации

№ п/п	Идентификатор УБИ	Название угрозы
57	УБИ.162	Угроза эксплуатации цифровой подписи программного кода
58	УБИ.167	Угроза заражения компьютера при посещении ненадежных сайтов
59	УБИ.168	Угроза «кражи» учётной записи доступа к сетевым сервисам
60	УБИ.170	Угроза неправомерного шифрования информации
61	УБИ.171	Угроза скрытного включения вычислительного устройства в состав бот-сети
62	УБИ.172	Угроза распространения «почтовых червей»
63	УБИ.173	Угроза «спама» веб-сервера
64	УБИ.174	Угроза «фарминга»
65	УБИ.175	Угроза «фишинга»
66	УБИ.178	Угроза несанкционированного использования системных и сетевых утилит
67	УБИ.179	Угроза несанкционированной модификации защищаемой информации
68	УБИ.180	Угроза отказа подсистемы обеспечения температурного режима
69	УБИ.182	Угроза физического устаревания аппаратных компонентов
70	УБИ.186	Угроза внедрения вредоносного кода через рекламу, сервисы и контент
71	УБИ.191	Угроза внедрения вредоносного кода в дистрибутив программного обеспечения
72	УБИ.192	Угроза использования уязвимых версий программного обеспечения
73	УБИ.208	Угроза нецелевого использования вычислительных ресурсов средства вычислительной техники
74	УБИ.209	Угроза несанкционированного доступа к защищаемой памяти ядра процессора
75	УБИ.211	Угроза использования непроверенных пользовательских данных при формировании конфигурационного файла, используемого программным обеспечением администрирования информационных систем
Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка). ФСТЭК России, 2008 год		
76	-	Угрозы, реализуемые в ходе загрузки операционной системы и направленные на перехват паролей или идентификаторов, модификацию базовой системы ввода/вывода (BIOS), перехват управления загрузкой
77	-	Угрозы, реализуемые после загрузки операционной системы и направленные на выполнение несанкционированного доступа с применением стандартных функций (уничтожение, копирование, перемещение, форматирование носителей информации и т.п.) операционной системы или какой-либо прикладной программы (например, системы управления базами данных), с применением специально созданных для выполнения НСД программ (программ просмотра и модификации реестра, поиска текстов в текстовых файлах и т.п.)
78	-	Угрозы внедрения вредоносных программ
79	-	Угрозы «Анализа сетевого трафика» с перехватом передаваемой по сети информации
80	-	Угрозы «Анализа сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой в ИСПДн из внешних сетей информации
81	-	Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.
82	-	Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях
83	-	Угрозы подмены доверенного объекта

№ п/п	Идентификатор УБИ	Название угрозы
84	-	Угрозы навязывания ложного маршрута путем несанкционированного изменения маршрутно-адресных данных как внутри сети, так и во внешних сетях
85	-	Угрозы выявления паролей
86	-	Угрозы типа «Отказ в обслуживании»
87	-	Угрозы удаленного запуска приложений
88	-	Угрозы внедрения по сети вредоносных программ

8. ОПРЕДЕЛЕНИЕ АКТУАЛЬНОСТИ ИСПОЛЬЗОВАНИЯ СКЗИ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ И НЕОБХОДИМОГО КЛАССА СКЗИ

Использование СКЗИ для обеспечения безопасности персональных данных необходимо в следующих случаях:

- если персональные данные подлежат криптографической защите в соответствии с законодательством Российской Федерации;
- если в информационной системе существуют угрозы, которые могут быть нейтрализованы только с помощью СКЗИ.

Кроме того, решение о необходимости криптографической защиты персональных данных может быть принято конкретным оператором на основании технико-экономического сравнения альтернативных вариантов обеспечения требуемых характеристик безопасности информации, содержащей, в том числе, персональные данные.

К случаям, когда угрозы могут быть нейтрализованы только с помощью СКЗИ, относятся:

- передача персональных данных по каналам связи, не защищенным от перехвата нарушителем передаваемой по ним информации или от несанкционированных воздействий на эту информацию (например, при передаче персональных данных по информационно-телекоммуникационным сетям общего пользования);
- хранение персональных данных на носителях информации, несанкционированный доступ к которым со стороны нарушителя не может быть исключен с помощью некриптографических методов и способов.

Оператором осуществляется передача персональных данных по информационно-телекоммуникационным сетям общего пользования.

Оператором не осуществляется хранение персональных данных на носителях информации, несанкционированный доступ к которым со стороны нарушителя не может быть исключен с помощью некриптографических методов и способов.

Таким образом, необходимо использование средств криптографической защиты информации.

Дополнительные характеристики ИСПДн «АСУ ЖКХ Капитальный ремонт» при использовании СКЗИ представлены в Таблице №15.

Таблица №15

№ п/п	Характеристики	Описание
1.	Меры по разграничению доступа в помещения, в которых размещены ресурсы информационной системы, имеющие отношение к криптографической защите персональных данных	Доступ в помещения, где располагаются СКЗИ, обеспечивается в соответствии с порядком доступа в помещения, в рабочее и нерабочее время, а также в нестандартных ситуациях. Утверждены перечни лиц, имеющих право доступа в помещения, где располагаются СКЗИ (сотрудники по эксплуатации). Помещения, в которых располагаются СКЗИ, оснащены входными дверями с замками, обеспечивается постоянное закрытие дверей помещений на замки и их открытие только для санкционированного прохода.

№ п/п	Характеристики	Описание
		Представители технических, обслуживающих и других вспомогательных служб при работе в помещениях, где расположены СКЗИ, и сотрудники Оператора, не входящие в перечень лиц, имеющих право доступа в помещение с СКЗИ, находятся в этом помещении только в присутствии сотрудников по эксплуатации. Ведется учет доступа в помещения с СКЗИ.
2.	Информационные технологии, базы данных, технические средства, программное обеспечение, используемые в информационной системе для обработки персональных данных и имеющие отношение к криптографической защите персональных данных	Автоматизированные рабочие места; Операционная система Microsoft Windows;
3.	Отчуждаемые носители защищаемой информации, в информационной системе, для которых несанкционированный доступ к хранимой на них информации не может быть исключен без использования криптографических методов и способов	Отсутствуют, не предусмотрены технологией обработки информации.
4.	Область применения СКЗИ в информационной системе	Взаимодействие (обмен данными) с информационными системами РФ и области.
5.	Цели применения СКЗИ в информационной системе	Проверка авторства (ЭП) полученных данных. Подписание ЭП отправляемых данных.

При использовании оператором СКЗИ, к объектам защиты, кроме персональных данных, относятся:

- СКЗИ;
- среда функционирования СКЗИ;
- информация, относящаяся к криптографической защите персональных данных, включая ключевую, парольную и аутентифицирующую информацию СКЗИ;
- документы, дела, журналы, картотеки, издания, технические документы, видео-, кино- и фотоматериалы, рабочие материалы и т.д., в которых отражена защищаемая информация, относящаяся к информационным системам персональным данным и их криптографической защите, включая документацию на СКЗИ и на технические и программные компоненты СФ;
- носители защищаемой информации, используемые в информационной системе и 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.

Согласно требованиям методического документа «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 года №149/7/2/6-432) описывается фактическое состояние ИСПДн и обобщенный состав внедренных организационно-технических мер защиты для корректного формирования актуальных угроз безопасности персональных данных при использовании СКЗИ и определения класса применяемых СКЗИ.

На основании исходных данных об информационных системах, объектах защиты и источниках атак выделены обобщенные возможности источников атак, представленные в Таблице №16.

Таблица №16

№	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 (далее – АС), 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 АС, на которых реализованы СКЗИ и среда их функционирования	Нет
4.	Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области анализа сигналов линейной передачи и сигналов побочного электромагнитного излучения и наводок СКЗИ)	Нет
5.	Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области использования для реализации атак недокументированных возможностей прикладного программного обеспечения)	Нет
6.	Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области использования для реализации атак недокументированных возможностей аппаратного и программного компонентов среды функционирования СКЗИ)	Нет

В зависимости от положительных ответов заполняется Таблица №17. В соответствии с определенными обобщенными возможностями источниками атак определяются уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы).

Таблица №17

№	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
1.1.	Проведение атаки при нахождении в пределах контролируемой зоны	Не актуально	– Проводятся работы под подбору персонала; – доступ в контролируемую зону, где располагается СКЗИ, обеспечивается в соответствии с порядком доступа в помещения; – представители технических, обслуживающих и других вспомогательных служб при работе в помещениях, 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;

№	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
			– 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, обеспечения постоянного закрытия дверей помещений на замок и их открытия только для санкционированного прохода; – утверждена 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;
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 функционировать самостоятельно или в составе других систем (далее - СВТ), на которых реализованы СКЗИ и СФ	Не актуально	– Проводятся работы по подбору персонала; – доступ в контролируемую зону, где располагается СКЗИ, обеспечивается в соответствии с порядком доступа в помещения; – документация на СКЗИ хранится у ответственного за СКЗИ в металлическом сейфе; – помещения, в которых располагаются СКЗИ, оснащены входными дверьми с замками, обеспечения постоянного закрытия дверей помещений на замок и их открытия только для санкционированного прохода; – утвержден перечень лиц, имеющих право доступа в помещения, где располагаются СКЗИ;
1.3.	Получение в рамках предоставленных полномочий, а также в результате наблюдений следующей информации: – сведений о физических мерах защиты объектов, в которых размещены ресурсы информационной системы; – сведений о мерах по обеспечению контролируемой зоны объектов, в которых размещены ресурсы информационной системы; – сведений о мерах по разграничению доступа в Помещения, в которых находятся СВТ, на которых реализованы СКЗИ и СФ	Не актуально	– Проводятся работы под подбору персонала; – доступ в контролируемую зону, где располагается СКЗИ, обеспечивается в соответствии с порядком доступа в помещения; – 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	Не актуально	– Проводятся работы под подбору персонала; – помещения, в которых располагаются СКЗИ, оснащены входными дверьми с замками, обеспечения постоянного закрытия дверей

№	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий		помещений на замок и их открытия 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;
2.1.	Физический доступ к СВТ, на которых реализованы СКЗИ и СФ	Не актуально	– Проводятся работы под подбору персонала; – доступ в контролируемую зону, где располагается СКЗИ, обеспечивается в соответствии с порядком доступа в помещения; – помещения, в которых располагаются СКЗИ, оснащены входными дверьми с замками, обеспечения постоянного закрытия дверей помещений на замок и их открытия только для санкционированного прохода;
2.2.	Возможность воздействовать на аппаратные компоненты СКЗИ и СФ, ограниченная мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий	Не актуально	– Проводятся работы под подбору персонала; – доступ в контролируемую зону, где располагается СКЗИ, обеспечивается в соответствии с порядком доступа в помещения; – помещения, в которых располагаются СКЗИ, оснащены входными дверьми с замками, обеспечения постоянного закрытия дверей помещений на замок и их открытия только для санкционированного прохода; – представители технических, обслуживающих и других вспомогательных служб при работе в помещениях, где расположены СКЗИ, и сотрудники, не являющиеся пользователями СКЗИ, находятся в этих помещениях только в присутствии сотрудников по эксплуатации;
3.1.	Создание способов, подготовка и проведение атак с привлечением специалистов в области анализа сигналов, сопровождающих функционирование СКЗИ и СФ, и в области использования для реализации атак недокументированных (недекларированных) возможностей прикладного ПО	Не актуально	– 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 под подбору персонала; – доступ в контролируемую зону, где располагается СКЗИ, обеспечивается в соответствии с порядком доступа в помещения; – помещения, в которых располагаются СКЗИ, оснащены входными дверьми с замками, обеспечения постоянного закрытия дверей помещений на замок и их открытия только для санкционированного прохода; – представители технических, обслуживающих и других вспомогательных служб при работе в помещениях, где расположены СКЗИ, 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;

№	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
			– осуществляется регистрация и учет действий пользователей;
3.2.	Проведение лабораторных исследований СКЗИ, используемых вне контролируемой зоны, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий	Не актуально	– 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 научно-исследовательских центрах, специализирующихся в области разработки и анализа СКЗИ и СФ, в том числе с использованием исходных текстов входящего в СФ прикладного ПО, непосредственно использующего вызовы программных функций СКЗИ	Не актуально	– 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;
4.1.	Создание способов, подготовка и проведение атак с привлечением специалистов в области использования для реализации атак недокументированных (недекларированных) возможностей системного ПО	Не актуально	– 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 под подбору персонала; – доступ в контролируемую зону, где располагается СКЗИ, обеспечивается в соответствии с порядком доступа в помещения; – помещения, в которых располагаются СКЗИ, оснащены входными дверями с замками, обеспечения постоянного закрытия дверей помещений на замок и их открытия только для санкционированного прохода; – представители технических, обслуживающих и других вспомогательных служб при работе в помещениях, где расположены СКЗИ, и сотрудники, не являющиеся пользователями СКЗИ, находятся в этих помещениях только в присутствии сотрудников по эксплуатации; – осуществляется разграничение и контроль доступа пользователей к защищаемым ресурсам; – осуществляется регистрация и учет действий пользователей;
4.2.	Возможность располагать	Не актуально	– Не осуществляется обработка сведений,

№	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	сведениями, содержащимися в конструкторской документации на аппаратные и программные компоненты СФ		составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности;
4.3.	Возможность воздействовать на любые компоненты СКЗИ и СФ	Не актуально	– Не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности

Уровень криптографической защиты персональных данных, обеспечиваемой СКЗИ, определяется путем отнесения нарушителя, действиям которого должно противостоять СКЗИ, к конкретному типу, и базируется на подходах, описанных в «Методических рекомендациях 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» № 149/7/2/6-432 от 31.03.2015 г. и приказе ФСБ от 10 июля 2014 года № 378 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

Исходя из анализа исходных данных, приведенных в Таблице №17, можно сделать вывод, что у нарушителя есть возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак только за пределами контролируемой зоны.

Для нейтрализации атак, при создании способов, подготовке и проведении которых используются актуальные уточненные возможности нарушителей и направления атак должно применяться СКЗИ класса КС1 и выше.

СОСТАВЛЕНО ЭКСПЕРТНОЙ ГРУППОЙ

Наименование организации	Должность	Фамилия, Имя, Отчество	Подпись	Дата
Фонд капитального ремонта МКД ВО	Системный администратор	Сугрин Д.А.		
Фонд капитального ремонта МКД ВО	Начальник договорного отдела	Узорова О.Г.		
Фонд капитального ремонта МКД ВО	Начальник отдела правовой и кадровой работы	Вицина И.М.	