УТВЕРЖДАЮ
Ректор ФГБОУ ВПО
«Казанский государственный
энергетический университет»
_____ Э.Ю. Абдуллазянов
«___» _____ 2015 г.

ЧАСТНАЯ МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННОЙ СИСТЕМЕ ПЕРСОНАЛЬНЫХ ДАННЫХ ФГБОУ ВПО «КАЗАНСКИЙ ГОСУДАРСТВЕННЫЙ ЭНЕРГЕТИЧЕСКИЙ УНИВЕРСИТЕТ»

г. Казань
2015

Сокращения

VPN	Virtual Private Network (виртуальная частная сеть)
АРМ	Автоматизированное рабочее место
АС	Автоматизированная система
ИСПДн	Информационная система персональных данных
КЗ	Контролируемая зона
ЛВС	Локальная вычислительная сеть
МЭ	Межсетевой экран
НСД	Несанкционированный доступ
ОС	Операционная система
ПДн	Персональные данные
ПО	Программное обеспечение
ПЭМИН	Побочные электромагнитные излучения и наводки
СКЗИ	Средство криптографической защиты информации
ТС	Техническое средство
ЭВТ	Электронно-вычислительная техника
ЭМ	Электромагнитный

1. Общие положения.

Частная модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных ФГБОУ ВПО «Казанский государственный энергетический университет» (далее по тексту – Модель) разработана в целях определения основных исходных положений для разработки и задания требований по защите информации в них.

Модель, учитывая особенности функционирования ИСПДн в ФГБОУ ВПО «Казанский государственный энергетический университет», используемые технические средства и технологический процесс обработки информации, позволяет определить конкретные условия эксплуатации, защищаемые активы, дать описания нарушителя и угроз безопасности информации, необходимые для выработки основных подходов по защите информации.

Разработка Модели велась на основании анализа исходных данных о ИСПДн ФГБОУ ВПО «Казанский государственный энергетический университет», с учётом требований следующих нормативных документов:

- Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных»;
- Постановления Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Приказа Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утверждённой заместителем директора ФСТЭК России 15 февраля 2008 года;
- Методики определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утверждённой заместителем директора ФСТЭК России 14 февраля 2008 года.

Средства защиты информации, а также мероприятия по обеспечению безопасности информационных и технических ресурсов ИСПДн ФГБОУ ВПО «Казанский государственный энергетический университет», определяемые на основе Модели, должны осуществлять защиту от влияния как преднамеренных, так и случайных событий, процессов или явлений, приводящих к НСД к информации, её искажению, уничтожению, блокированию доступа к ней, нарушению свойств аутентичности, а также возможности воздействия на ИСПДн, приводящие к сбою их функционирования и возникновению указанных негативных последствий в отношении обрабатываемой в них информации.

2. Исходные данные по объекту информатизации

2.1. Общая характеристика объекта информатизации

В ФГБОУ ВПО «Казанский государственный энергетический университет» функционирует 1 ИСПДн. Перечень ИСПДн с указанием их месторасположения приведён в Таблице 1.

Таблица 1. Перечень ИСПДн

№ п/п	Наименование ИСПДн	Местонахождение
1.	Федеральная информационная система обеспечения проведения государственной итоговой аттестации	420066, Республика Татарстан, г. Казань, ул. Красносельская, 51.

2.2. Состав информации, обрабатываемых в ИСПДн

В ИСПДн ФГБОУ ВПО «Казанский государственный энергетический университет» не обрабатываются специальные категории персональных данных.

2.3. Категории пользователей ИСПДн

Все пользователи ИСПДн относятся к одной из следующих категорий, описание которых приведено в Таблице 2.

Таблица 2. Характеристики категорий пользователей ИСПДн

Категория пользователей	Описание
Оператор ИСПДн	Персонал, выполняющий функции по обработке ПДн с использованием ТС ИСПДн.
Ответственное лицо за ИСПДн	Персонал, выполняющий технологические функции по обеспечению функционирования системы, конфигурацию и настройку сетевого оборудования, в том числе и МЭ.
Ответственное лицо по защите информации	Персонал, выполняющий функции по управлению и конфигурации СЗИ, а так же контролю выполнения организационных мер, направленных на защиту информации.

3. Модель нарушителя безопасности ПДн

3.1. Общие положения

Одним из основных источников угроз НСД в ИСПДн является нарушитель.

По наличию права постоянного или разового доступа к ИСПДн нарушители подразделяются на два типа: внешние и внутренние.

Внутренние нарушители – нарушители, имеющие доступ к ИСПДн, включая пользователей ИСПДн, реализующие угрозы непосредственно в ИСПДн.

Внешние нарушители – нарушители, не имеющие доступа к ИСПДн, реализующие угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена.

3.2. Типы нарушителя

Все возможные типы нарушителя безопасности ПДн, приведённые в Таблице 3.

Таблица 3. Нарушители безопасности ПДн

Категория	Нарушитель
Внутренние (потенциальные) нарушители	
КН1	Лица, имеющие санкционированный доступ к ИСПДн, но не имеющие доступа

Категория	Нарушитель
	обеспечивающие нормальное функционирование ИСПДн и пользователи ЛВС, не являющиеся легальными пользователями ИСПДн.
КН2	Зарегистрированные пользователи ИСПДн, осуществляющие ограниченный доступ к ресурсам ИСПДн с рабочего места.
КН3	Зарегистрированные пользователи ИСПДн, осуществляющие удаленный доступ к ПДн по локальным и (или) распределенным информационным системам.
КН4	Зарегистрированные пользователи ИСПДн с полномочиями администратора безопасности сегмента (фрагмента) ИСПДн.
КН5	Зарегистрированные пользователи с полномочиями системного администратора ИСПДн.
КН6	Зарегистрированные пользователи с полномочиями администратора безопасности ИСПДн.
КН7	Программисты-разработчики (поставщики) прикладного программного обеспечения и лица, обеспечивающие его сопровождение на защищаемом объекте.
КН8	Разработчики и лица, обеспечивающие поставку, сопровождение и ремонт технических средств на ИСПДн.
Внешние потенциальные нарушители	
КН9	Посторонние лица (посетители, конкуренты, недобросовестные партнеры, внешние субъекты (физические лица)).

3.3. Модель вероятного нарушителя

На основании анализа архитектур рассматриваемых ИСПДн, организационных мер, а также организационно-штатной структуры ФГБОУ ВПО «Казанский государственный энергетический университет», можно сделать следующие выводы:

1. К лицам категорий КН4, КН5 и КН6, ввиду их исключительной роли в ИСПДн, должен применяться комплекс особых организационных мер по их подбору, принятию, назначению на должность и контролю выполнения функциональных обязанностей. В число лиц категорий КН4, КН5 и КН6 включаются только доверенные лица и поэтому указанные лица исключаются из числа вероятных нарушителей.

2. Лица категории КН1 могут являться пользователями сети, не являющимися легальными пользователями ИСПДн. Лица, обеспечивающие нормальное функционирование ИСПДн, могут выполнять работы только в присутствии и под контролем ответственных сотрудников ФГБОУ ВПО «Казанский государственный энергетический университет» (далее по тексту – сотрудники ФГБОУ ВПО «Казанский государственный энергетический университет»). В силу указанных причин лиц данной категории можно исключить из числа вероятных нарушителей. Пользователи сети, не являющиеся легальными пользователями ИСПДн могут являться потенциальными нарушителями.

3. Остальные категории потенциально также могут являться нарушителями безопасности ПДн и реализовывать различные угрозы в их отношении.

Таким образом, к возможным нарушителям безопасности ПДн относятся категории КН1 (пользователи сети), КН2, КН3, КН7, КН8 и КН9.

Предполагается, что в случае сговора внешних и внутренних нарушителей возможности внешнего нарушителя не превысят возможности внутреннего.

4. Модель угроз безопасности персональных данных

Модель разрабатывается в соответствии с методологией ФСТЭК России, определенной в документе «Методика определения актуальных угроз безопасности

Модель разрабатывается в соответствии с методологией ФСТЭК России, определенной в документе «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденной заместителем директора ФСТЭК России 14 февраля 2008 года.

Для каждой ИСПДн определен перечень актуальных угроз безопасности персональных данных.

Следует учесть, что в описанных ниже моделях угроз, исключены угрозы, создаваемые лицами категорий КН4, КН5 и КН6.

4.1. Перечень основных угроз

Основываясь на информации, содержащийся в построенной модели нарушителя, требуемых характеристиках безопасности, особенностях функционирования оборудования системы, а также на документе ФСТЭК России «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных», можно определить следующий перечень угроз, характерных для ИСПДн ФГБОУ ВПО «Казанский государственный энергетический университет».

4.1.1. Угрозы утечки по техническим каналам за счёт ПЭМИН

Возникновение угрозы по каналам ПЭМИН возможно за счёт перехвата техническими средствами побочных (не связанных с прямым функциональным значением элементов системы) информативных электромагнитных полей и электрических сигналов, возникающих при обработке защищаемой информации техническими средствами.

Для регистрации ПЭМИН используется аппаратура в составе радиоприемных устройств и оконечных устройств восстановления информации.

Утечка информации по каналам ПЭМИН может быть осуществлена:

- за счёт побочных ЭМ излучений ЭВТ;
- за счёт радиоизлучений от внедренных в ТС и выделенные помещения специальных электронных устройств перехвата информации («закладок»);
- за счёт изменения тока потребления, обусловленного обрабатываемыми ТС информационными сигналами;
- за счёт наводок по цепям питания;
- за счёт радиоизлучений, модулированных информационным сигналом.

Утечка информации от компонентов ИСПДн ФГБОУ ВПО «Казанский государственный энергетический университет» по каналам ПЭМИН маловероятна из-за большой сложности регистрации ПЭМИН, а также несоответствия стоимости средств съёма информации и ценности полученной в результате информации. Стоимость оборудования получения информации по каналам ПЭМИН составляет порядка нескольких сотен тысяч долларов и больше, а сами работы являются достаточно трудоёмкими и требуют высокой квалификации специалиста, проводящего такие работы. С другой стороны, результатом перехвата будут данные, которые могут быть получены менее затратными средствами.

4.1.2. Угрозы утечки акустической (речевой) информации

Возникновение угроз утечки акустической (речевой) информации, содержащейся непосредственно в произносимой речи, при обработке информации в системе, обусловлено наличием функций голосового ввода или функций воспроизведения информации акустическими средствами.

В ИСПДн не реализованы функции голосового ввода-вывода информации.

4.1.3. Угрозы утечки видовой информации

Угрозы утечки видовой информации реализуются за счёт просмотра защищаемой информации с помощью оптических (оптикоэлектронных) средств с экранов дисплеев и других средств отображения ЭВТ, информационно-вычислительных комплексов, ТС обработки графической, видео- и буквенно-цифровой информации, входящих в состав системы. Кроме этого просмотр (регистрация) информаций возможна с использованием специальных электронных устройств съёма, внедрённых в служебных помещениях или скрытно используемых физическими лицами при посещении ими служебных помещений.

При работе с ИСПДн отсутствует возможность неконтролируемого пребывания физических лиц в помещениях, в которых размещается оборудование ИСПДн. Возможность удалённого просмотра информации должна исключаться за счёт реализованных организационно-технических мер физической безопасности.

4.1.4. Угрозы НСД к информации

В качестве угроз НСД рассматриваются следующие угрозы:

угрозы НСД за счёт непосредственного физического доступа:

- недоверенная загрузка операционной системы (изменение параметров BIOS, нештатный носитель), позволяющая получить доступ к информации на жёстких носителях системы в обход системы разграничения доступа;
- подключение к каналу связи с целью съёма (копирования) или модификации передаваемой информации;
- хищение элементов ИСПДн (системных блоков или жёстких дисков), содержащих ПДн;
- хищение отчуждаемых носителей информации, содержащих ПДн;
- вывод из строя элементов ИСПДн;
- внедрение в ИСПДн аппаратных закладок;
- угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и средств защиты ПДн;
- утрата паролей доступа к ИСПДн (просмотр набора пароля пользователем, пароль записанный на бумажном носителе и размещённый возле АРМ).

угрозы НСД с применением программно-аппаратных или программных средств:

- установка и запуск шпионских программ, в целях получения паролей или информации вводимой пользователем при работе на АРМ;
- НСД с помощью чужого сеанса доступа (оставленное без присмотра АРМ);
- установка или запуск постороннего ПО, полученного из недостоверного источника, которое может привести к заражению системы вредоносным ПО;
- вызов штатных программ ОС ИСПДн или запуск специально разработанных программ, реализующих НСД к ИСПДн в обход основного способа обработки информации;
- удалённое программное воздействие на ТС с целью несанкционированного получения или повышения привилегий пользователя ТС, за счёт эксплуатации уязвимостей системного и прикладного ПО системы;
- перехват аутентификационной информации или подбор, получение или сброс пароля к системе (прикладному ПО);
- внесение несанкционированных деструктивных изменений непосредственно в код приложений;
- НСД за счёт подбора пароля пользователя ТС ИСПДн с использованием программного интерфейса (пароль входа в операционную систему);
- использование остаточной информации на носителях.

прочие угрозы:

- искажение или уничтожение информации в результате ошибок пользователя;

- выход из строя аппаратно-программных средств ИСПДн;
- сбой системы электроснабжения ИСПДн;
- уничтожение данных в ИСПДн или блокирование доступа к ИСПДн, вызванное стихийными бедствиями или техногенными катастрофами;
- угрозы социально–политического характера, сопровождаемые нападением на объекты, в которых размещаются ресурсы ИСПДн.

4.2. Актуальность угроз безопасности персональных данных в соответствии с «Методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных»

В соответствии с «Методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» для оценки возможности реализации угрозы применяются два показателя: уровень исходной защищённости ИСПДн и частота (вероятность) реализации рассматриваемой угрозы.

Под **уровнем исходной защищённости ИСПДн** понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПДн.

Под **частотой (вероятностью) реализации угрозы** понимается определяемый экспертным путём показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности ПДн для данной ИСПДн в реальных условиях эксплуатации, а также реализованных в системе функций безопасности.

Используются четыре вербальных градации этого показателя и соответствующий им коэффициент Y2:

Маловероятно – отсутствуют объективные предпосылки для осуществления угрозы (Y2=0);

низкая вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (Y2=2);

средняя вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности информации недостаточны (Y2=5);

высокая вероятность – объективные предпосылки для реализации угрозы существуют, и меры по обеспечению безопасности информации не приняты (Y2=10).

Реализуемость угрозы определяется значением коэффициента $Y=(Y1+Y2)/20$. При этом используется следующая вербальная интерпретация коэффициента реализуемости:

- если, $0 < Y < 0,3$ то возможность реализации угрозы признается низкой:
- если, $0,3 < Y < 0,6$ то возможность реализации угрозы признается средней;
- если, $0,6 < Y < 0,8$ то возможность реализации угрозы признается высокой;
- если, $0,8 < Y$ то возможность реализации угрозы признается очень высокой.

По результатам оценки показателей будет проведена оценка опасности каждой угрозы. При оценке опасности на основе опроса эксперта (специалистов в области защиты информации) определялся вербальный показатель опасности для системы.

Этот показатель имеет три значения:

низкая опасность – если реализация угрозы может привести к незначительным негативным последствиям;

средняя опасность – если реализация угрозы может привести к негативным последствиям;

высокая опасность – если реализация угрозы может привести к значительным негативным последствиям.

Далее, будет осуществлен выбор из общего (предварительного) перечня угроз безопасности тех, которые относятся к актуальным для данной ИСПДн, в соответствии с правилами, показанными в Таблице 4.

Таблица 4. Правила отнесения угрозы безопасности ПДн к актуальной

Возможность реализации угрозы	Показатель опасности угрозы		
	Низкая	Средняя	Высокая
Низкая	Неактуальная	Неактуальная	Актуальная
Средняя	Неактуальная	Актуальная	Актуальная
Высокая	Актуальная	Актуальная	Актуальная
Очень высокая	Актуальная	Актуальная	Актуальная

Таким образом, для каждой ИСПДн в рамках определения актуальных угроз безопасности ПДн, будут определены следующие показатели:

- уровень исходной защищённости;
- вероятность реализации угроз;
- вербальный показатель опасности.

4.3. Определение актуальных угроз безопасности ПДн при их обработке в ИСПДн

4.3.1. *Модель угроз безопасности персональных данных для ИСПДн «Федеральная информационная система обеспечения проведения государственной итоговой аттестации»*

Описание ИСПДн «Федеральная информационная система обеспечения проведения государственной итоговой аттестации».

ИСПДн «Федеральная информационная система обеспечения проведения государственной итоговой аттестации» предназначена для обеспечения проверки результатов государственной итоговой аттестации обучающихся, освоивших основные образовательные программы основного общего и среднего общего образования.

Пользователем системы являются сотрудники ФГБОУ ВПО «Казанский государственный энергетический университет». Все пользователи ИСПДн относятся к категориям пользователей, определённым в таблице 2 Модели.

Характеристики для ИСПДн «Федеральная информационная система обеспечения проведения государственной итоговой аттестации» определены в Таблице 5.

Таблица 5. Характеристики ИСПДн «Федеральная информационная система обеспечения проведения государственной итоговой аттестации»

Местонахождение технических средств информационной системы персональных данных	420066, Республика Татарстан, г. Казань, ул. Красносельская, 51.
Уровень значимости информации	Информация имеет минимальный уровень значимости (УЗ 4), если обладателем информации (заказчиком) и (или) оператором степень ущерба от нарушения свойств безопасности информации (конфиденциальности, целостности, доступности) не может быть определена, но при этом информация подлежит защите в соответствии с законодательством Российской Федерации.
Масштаб	Объектовый (функционирует на объектах одного федерального

	органа государственной власти, органа государственной власти субъекта Российской Федерации, муниципального образования и (или) организации и не имеет сегментов в территориальных органах, представительствах, филиалах, подведомственных и иных организациях).

Режим обработки данных: Многопользовательский, с разграничением прав доступа.

Основными операциями являются сбор, запись, систематизация, накопление, хранение, извлечение, использование, а также уточнение (обновление, изменение) данных в системе.

Информационный обмен с другими ИСПДн не производится.

Основными составляющими ИСПДн являются:

– АРМы сотрудников ФГБОУ ВПО «Казанский государственный энергетический университет» с базой данных информационной системы «Федеральная информационная система обеспечения проведения государственной итоговой аттестации».

Основное общесистемное программное обеспечение:

– Операционная система Microsoft Windows 7.

Порядок резервного копирования определяется отдельным нормативным правовым актом ФГБОУ ВПО «Казанский государственный энергетический университет» о резервном копировании и восстановлении информации, содержащей персональные данные, обрабатываемой с использованием средств вычислительной техники.

Администрирование ИСПДн осуществляется лицом, назначенным приказом ректора ФГБОУ ВПО «Казанский государственный энергетический университет».

Определение уровня исходной защищённости ИСПДн «Федеральная информационная система обеспечения проведения государственной итоговой аттестации» в соответствии с «Методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных»

В соответствии с «Методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» ИСПДн «Федеральная информационная система обеспечения проведения государственной итоговой аттестации» обладает следующими показателями исходной защищённости, которые указаны в Таблице 6.

Таблица 6. Показатели исходной защищённости ИСПДн «Федеральная информационная система обеспечения проведения государственной итоговой аттестации»

Технические и эксплуатационные характеристики	Уровень защищённости
По территориальному размещению: локальная ИСПДн, развернутая в пределах одного здания.	Высокий
По наличию соединения с сетями общего пользования: ИСПДн, имеющая одноточечный выход в сеть общего пользования.	Средний
По встроенным (легальным) операциям с информацией: модификация, передача.	Низкий
По разграничению доступа к данным: ИСПДн, к которой имеет доступ определённый перечень сотрудников организации.	Средний
По наличию соединений с другими системами: ИСПДн в которой используется одна база ПДн, принадлежащая организации.	Высокий
По уровню обобщения (обезличивания) данных: ИСПДн, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта ПДн).	Низкий
По объёму данных, которые предоставляются сторонним пользователям без предварительной обработки: ИСПДн, предоставляющая всю базу данных с ПДн.	Низкий

Уровень «высокий» имеют 29% характеристик системы, что меньше значения 70%. Уровень не ниже «средний» имеют 57% характеристик системы, что меньше значения 70%. Таким образом, исходная защищенность системы определяется как «низкая» и числовой коэффициент Y1 устанавливается равным десяти (Y1 = 10).

Определение актуальности угроз

Данные по определению актуальности угроз в отношении ИСПДн «Федеральная информационная система обеспечения проведения государственной итоговой аттестации» приведены в Таблице 7.

Таблица 7. Актуальность угроз

Наименование угрозы	Категория нарушителя	Вероятность реализации угрозы (Y_2)	Возможность реализации угрозы (Y)	Опасность угрозы	Актуальность угрозы
1. Угрозы от утечки по техническим каналам					
1.1. Угрозы утечки акустической информации					
Перехват акустической (речевой) информации с использованием направленных микрофонов	КН9	Маловероятная	Средняя	Низкая	Неактуальная
Перехват акустической (речевой) информации с использованием ненаправленных микрофонов	КН9	Маловероятная	Средняя	Низкая	Неактуальная
Перехват акустической (речевой) информации с использованием вибродатчиков («контактных микрофонов»)	КН1, КН7, КН8, КН9	Маловероятная	Средняя	Низкая	Неактуальная
Перехват акустической (речевой) информации с использованием «оптических микрофонов» (в поле акустического сигнала)	КН9	Маловероятная	Средняя	Низкая	Неактуальная
Перехват акустической (речевой) информации с использованием «лазерных микрофонов»	КН9	Маловероятная	Средняя	Низкая	Неактуальная
Перехват акустической (речевой) информации с использованием электрических сигналов, возникающих в результате «микрофонного эффекта» в технических средствах обработки ПДн и ВТСС и распространяющихся по проводам и линиям за пределы служебных помещений, ВЧ-навязывания	КН8, КН9	Маловероятная	Средняя	Низкая	Неактуальная

Наименование угрозы	Категория нарушителя	Вероятность реализации угрозы (Y_2)	Возможность реализации угрозы (Y)	Опасность угрозы	Актуальность угрозы
Перехват акустической (речевой) информации с использованием радиоизлучений, модулированных информативным сигналом, возникающих при ВЧ-облучении технических средств обработки ПДн и ВТСС	КН8, КН9	Маловероятная	Средняя	Низкая	Неактуальная
Перехват акустической (речевой) информации с использованием специальных электронных устройств съёма речевой информации («аппаратурные закладки»)	КН1, КН2, КН7, КН8, КН9	Маловероятная	Средняя	Низкая	Неактуальная
1.2. Угрозы утечки видовой информации					
Просмотр информации на дисплее сотрудниками, не допущенными к обработке ПДн	КН1, КН2, КН7, КН8	Низкая	Средняя	Средняя	Актуальная
Просмотр информации на дисплее посторонними лицами, находящимися в помещении, в котором ведётся обработка ПДн	КН9	Маловероятная	Средняя	Низкая	Неактуальная
Просмотр информации на дисплее посторонними лицами, находящимися за пределами помещения, в котором ведётся обработка ПДн	КН9	Маловероятная	Средняя	Низкая	Неактуальная
Просмотр информации с помощью специальных электронных устройств внедрённых в помещении, в котором ведётся обработка ПДн	КН1, КН2, КН7, КН8, КН9	Маловероятная	Средняя	Низкая	Неактуальная

Наименование угрозы	Категория нарушителя	Вероятность реализации угрозы (Y_2)	Возможность реализации угрозы (Y)	Опасность угрозы	Актуальность угрозы
1.3. Угрозы утечки информации по каналам ПЭМИН					
Перехват техническими средствами побочных электромагнитных излучений информативных сигналов от технических средств и линий передачи информации	КН8, КН9	Маловероятная	Средняя	Низкая	Неактуальная
Перехват техническими средствами наводок информативного сигнала, обрабатываемого техническими средствами, на цепи электропитания, заземления, линии связи и коммуникации, выходящие за пределы служебных помещений	КН8, КН9	Маловероятная	Средняя	Низкая	Неактуальная
Перехват техническими средствами радиоизлучений, модулированных информативным сигналом, возникающих в результате работы различных генераторов в составе ИСПДн или в результате паразитной генерации в узлах (элементах) технических средств	КН8, КН9	Маловероятная	Средняя	Низкая	Неактуальная
Перехват техническими средствами радиоизлучений, формируемых за счёт высокочастотного облучения технических средств ИСПДн	КН8, КН9	Маловероятная	Средняя	Низкая	Неактуальная
Перехват техническими средствами оптического излучения с боковой поверхности оптического волокна в волоконно-оптической системе передачи данных	КН8, КН9	Маловероятная	Средняя	Низкая	Неактуальная

Наименование угрозы	Категория нарушителя	Вероятность реализации угрозы (Y_2)	Возможность реализации угрозы (Y)	Опасность угрозы	Актуальность угрозы
Применение электронных устройств перехвата информации, подключенных к каналам связи или техническим средствам обработки ПДн («аппаратурные закладки»)	КН8, КН9	Маловероятная	Средняя	Низкая	Неактуальная
2. Угрозы несанкционированного доступа к информации					
2.1. Угрозы непосредственного доступа к ИСПДн					
2.1.1. Угрозы, реализуемые в ходе загрузки операционной системы					
Угрозы направленные на перехват паролей или идентификаторов	КН1, КН2, КН7	Низкая	Средняя	Низкая	Неактуальная
Угрозы направленные на модификацию базовой системы ввода/вывода (BIOS)	КН7, КН8	Низкая	Средняя	Низкая	Неактуальная
Угрозы направленные на перехват управления загрузкой с изменением необходимой технологической информации для получения НСД в операционную среду ИСПДн	КН7, КН8	Низкая	Средняя	Низкая	Неактуальная
2.1.2. Угрозы, реализуемые после загрузки операционной системы					
Угрозы направленные на выполнение НСД с применением стандартных функций (уничтожение, копирование, перемещение, форматирование носителей информации и т.п.) операционной системы или какой-либо прикладной программы	КН1, КН2, КН7	Низкая	Средняя	Низкая	Неактуальная

Наименование угрозы	Категория нарушителя	Вероятность реализации угрозы (Y_2)	Возможность реализации угрозы (Y)	Опасность угрозы	Актуальность угрозы
Угрозы направленные на выполнение НСД с применением специально созданных для выполнения НСД программ (программ просмотра и модификации реестра, поиска текстов в текстовых файлах и т.п.)	КН1, КН2, КН7	Низкая	Средняя	Средняя	Актуальная
2.1.3. Угрозы внедрения вредоносных программ	КН1, КН2, КН7	Средняя	Высокая	Средняя	Актуальная
2.2. Угрозы уничтожения, хищения технических средств ИСПДн, носителей информации путём физического доступа к элементам ИСПДн					
Кража ПЭВМ	КН8	Маловероятная	Средняя	Низкая	Неактуальная
Кража носителей информации	КН1, КН2, КН, КН8	Низкая	Средняя	Низкая	Неактуальная
Кража ключей доступа	КН1, КН2, КН7	Низкая	Средняя	Низкая	Неактуальная
Модификация, уничтожение информации	КН1, КН2, КН7	Низкая	Средняя	Низкая	Неактуальная
Вывод из строя узлов ПЭВМ, каналов связи	КН1, КН2, КН7, КН8, КН9	Низкая	Средняя	Низкая	Неактуальная
НСД к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	КН8	Низкая	Средняя	Низкая	Неактуальная

Наименование угрозы	Категория нарушителя	Вероятность реализации угрозы (Y_2)	Возможность реализации угрозы (Y)	Опасность угрозы	Актуальность угрозы
Несанкционированное отключение средств защиты	КН1, КН2, КН7, КН8	Низкая	Средняя	Низкая	Неактуальная
2.3. Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера					
Утрата ключей и атрибутов доступа	КН1, КН2	Низкая	Средняя	Средняя	Актуальная
Непреднамеренная модификация (уничтожение) информации сотрудниками	КН1, КН2	Средняя	Высокая	Средняя	Актуальная
Непреднамеренное отключение средств защиты	КН1, КН2, КН7, КН8	Низкая	Средняя	Низкая	Неактуальная
Выход из строя программно-аппаратных средств		Низкая	Средняя	Низкая	Неактуальная
Сбой системы электроснабжения, заземления	КН9	Низкая	Средняя	Средняя	Актуальная
Угрозы природного характера (стихийные бедствия и природные явления)		Низкая	Средняя	Низкая	Неактуальная
Угрозы социально–политического характера, сопровождаемые нападением на объекты, в которых размещаются ресурсы ИСПДн		Низкая	Средняя	Низкая	Неактуальная

Наименование угрозы	Категория нарушителя	Вероятность реализации угрозы (Y_2)	Возможность реализации угрозы (Y)	Опасность угрозы	Актуальность угрозы
2.4. Угрозы хищения, несанкционированной модификации или блокирования информации за счёт НСД с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий)					
Действия вредоносных программ (вирусов)	КН1, КН2, КН7	Средняя	Высокая	Средняя	Актуальная
Недекларированные возможности системного ПО и ПО для обработки персональных данных	КН7	Низкая	Средняя	Низкая	Неактуальная
Установка ПО не связанного с исполнением служебных обязанностей	КН1, КН2, КН7	Низкая	Средняя	Низкая	Нектуальная
Наличие аппаратных закладок в приобретаемых ПЭВМ	КН8	Низкая	Средняя	Низкая	Неактуальная
Внедрение аппаратных закладок сотрудниками	КН1	Низкая	Средняя	Низкая	Неактуальная
Внедрение аппаратных закладок обслуживающим персоналом (ремонтными организациями)	КН1, КН8	Низкая	Средняя	Низкая	Неактуальная
Внедрение аппаратных закладок посторонними лицами после начала эксплуатации ИСПДн	КН7, КН8	Низкая	Средняя	Низкая	Неактуальная
Угроза создания нештатного режима работы (программно – аппаратных) средств за счёт преднамеренных изменений служебных данных	КН7, КН8	Низкая	Средняя	Низкая	Неактуальная
Использование остаточной информации на носителях	КН1, КН2, КН7	Низкая	Средняя	Низкая	Неактуальная

Наименование угрозы	Категория нарушителя	Вероятность реализации угрозы (Y_2)	Возможность реализации угрозы (Y)	Опасность угрозы	Актуальность угрозы
2.5. Угрозы несанкционированного доступа по каналам связи					
Угрозы «анализа сетевого трафика» с перехватом информации, передаваемой по локальной сети, а также во внешние сети и принимаемой из внешних сетей	КН1, КН2, КН7	Низкая	Средняя	Низкая	Неактуальная
Угрозы типа «отказ в обслуживании»	КН7	Низкая	Средняя	Низкая	Неактуальная
Угрозы выявления паролей по сети	КН1, КН2, КН7	Низкая	Средняя	Низкая	Неактуальная
Угрозы удалённого запуска приложений	КН7	Низкая	Средняя	Низкая	Неактуальная
Угрозы сканирования, направленные на выявление сетевых адресов рабочих станций, типа операционной системы АРМ, открытых портов и служб, открытых соединений и др.	КН7	Низкая	Средняя	Низкая	Неактуальная
Угрозы навязывания ложного маршрута путём несанкционированного изменения маршрутно-адресных данных	КН7, КН8	Низкая	Средняя	Низкая	Неактуальная
Угрозы получения НСД путём подмены доверенного объекта	КН7	Низкая	Средняя	Низкая	Неактуальная
Угрозы внедрения ложного объекта сети	КН1, КН7	Низкая	Средняя	Низкая	Неактуальная
Угрозы внедрения по сети вредоносных программ	КН1, КН2, КН7	Низкая	Средняя	Средняя	Актуальная

Наименование угрозы	Категория нарушителя	Вероятность реализации угрозы (Y_2)	Возможность реализации угрозы (Y)	Опасность угрозы	Актуальность угрозы
2.6. Угрозы преднамеренных действий внутренних нарушителей					
Доступ к ИСПДн, модификация, уничтожение сотрудниками не допущенными к ее обработке	КН1, КН2	Низкая	Средняя	Низкая	Неактуальная
Разглашение информации, модификация, уничтожение сотрудниками допущенными к ее обработке	КН1, КН2	Низкая	Средняя	Низкая	Неактуальная

5. Выводы

Разработанные модели нарушителя и угроз в отношении ИСПДн, функционирующих в ФГБОУ ВПО «Казанский государственный энергетический университет», определяют угрозы безопасности, для противодействия которым необходимо применять следующие меры безопасности:

1. Атаки внешнего нарушителя, направленные на каналы связи посредством перехвата информации и последующего её анализа, уничтожения, модификации и блокирования информации, реализация попыток преодоления системы защиты, с использованием, в том числе, уязвимостей программной среды, а также утечка информации по техническим каналам нейтрализуются организационными и режимными мероприятиями.

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

Представленная модель угроз с описанием вероятного нарушителя для существующих ИСПДн должна использоваться при формировании обоснованных требований безопасности и проектировании средств защиты ИСПДн.

Проректор по информатизации  Ю.Н. Смирнов