ПРИНЯТО
Решением Ученого совета ГБОУ ВО МО «Технологический университет»
Протокол № 8
«06» июня 2017 г.

УТВЕРЖДАЮ
Ректор ГБОУ ВО МО «Технологический университет»
Т.Е. Старцева
«06» июня 2017 г.

СИСТЕМА МЕНЕДЖМЕНТА КАЧЕСТВА

МОДЕЛЬ УГРОЗ
безопасности персональных данных при их обработке в информационных системах персональных данных Государственного бюджетного образовательного учреждения высшего образования Московской области «Технологический университет»

СМК-П-3.2-03-17

Дата введения: «06» июня 2017 г.

Королев, 2017

СОДЕРЖАНИЕ

Термины и определения

Информационная система персональных данных	Совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств
Контролируемая зона	Пространство, в котором исключено неконтролируемое пребывание сотрудников и посетителей оператора и посторонних транспортных, технических и иных материальных средств
Недекларированные возможности	Функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации
Несанкционированный доступ (несанкционированные действия)	Доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по своим функциональному предназначению и техническим характеристикам
Обработка персональных данных	Любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных
Персональные данные	Любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)

Побочные электромагнитные излучения и наводки	Электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания
Нарушитель безопасности персональных данных	Физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных
Технические средства информационной системы персональных данных	Средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации
Угрозы безопасности персональных данных	Совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных
Целостность информации	Состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право

СОКРАЩЕНИЯ

АРМ	Автоматизированное рабочее место
ИСПДн	Информационная система персональных данных
КЗ	Контролируемая зона
НСД	Несанкционированный доступ (несанкционированные действия)
ПДн	Персональные данные
ПО	Программное обеспечение
ПЭМИН	Побочные электромагнитные излучения и наводки
СЗИ	Средство защиты информации
УБПДн	Угрозы безопасности персональных данных

1. ОБЩИЕ СВЕДЕНИЯ

Современная система обеспечения безопасности при их обработке в информационных системах персональных данных должна строиться на основе комплексирования разнообразных мер защиты и опираться на современные методы прогнозирования, анализа и моделирования возможных угроз безопасности информации и последствий их реализации. При этом необходимо придерживаться следующего правила: стоимость реализуемой системы защиты информации не должна превышать величину ущерба, который может быть нанесён собственнику ИСПДн.

Настоящая Модель угроз безопасности персональных данных(далее – Модель угроз) при их обработке в информационных системах персональных данных ***«Кадры», «Бухгалтерия», «Спрут»*** определяет подход в Государственном бюджетном образовательном учреждении высшего образования Московской области «Технологический университет» (далее - «МГОТУ») к определению актуальных угроз и категорий нарушителей безопасности персональных данных при их обработке с использованием средств автоматизации.

Модель угроз предназначена для определения требований к системе защиты персональных данных ИСПДн.

Модель угроз разработана на основании следующих нормативно-методических документов:

- Федерального закона от 27.07.2006 года № 152-ФЗ «О персональных данных»;
- Постановления Правительства Российской Федерации от 01.11.2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Методики определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных утвержденной заместителем директора ФСТЭК России 14.02.2008 года;
- Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной заместителем директора ФСТЭК России 15.02. 2008 года.

Угрозы безопасности ПДн, обрабатываемых в ИСПДн, и категории нарушителей, содержащиеся в настоящей Модели угроз, могут уточняться и дополняться по мере выявления новых источников угроз, развития способов и средств реализации угроз безопасности персональных данных в ИСПДн, изменения законодательства в области обработки и защиты персональных данных.

Внесение изменений в Модель угроз осуществляется также в случае изменения основных характеристик ИСПДн, указанных в разделе 2.

2. ОПИСАНИЕ ИСПДн

2.1. Общие сведения

ИСПДн по структуре являются комплексом автоматизированных рабочих мест, объединенных в единую информационную систему средствами связи без подключения к сети «Интернет» и иным информационным системам (локальная вычислительная сеть);

ИСПДн по режиму обработки ПДн относятся к многопользовательским системам с разграничением прав доступа пользователей.

ИСПДн являются информационными системами, обрабатывающими не только персональные данные сотрудников «МГОТУ», но и персональные данные учащихся.

Объем обрабатываемых персональных данных ИСПДн имеет значение менее чем 100 000 записей.

Все технические средства ИСПДн находятся в пределах Российской Федерации.

2.2. Определение степени исходной защищенности

Под уровнем исходной защищенности ИСПДн понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПДн. Технические и эксплуатационные характеристики ИСПДн, определяющие степень исходной защищённости, приведены в табл. 1.

Таблица 1.

Технические и эксплуатационные характеристики ИСПДн	**Уровень защищенности**		
	высокий	**средний**	**низкий**
1. По территориальному размещению:			
локальная (кампусная) ИСПДн, развернутая в пределах нескольких близко расположенных зданий		+	
локальная ИСПДн, развернутая в пределах одного здания	+		
2. По наличию соединения с сетями общего пользования:			
ИСПДн, физически отделённая от сети общего пользования	+		
3. По встроенным (легальным) операциям с записями баз персональных данных:			
модификация, передача			+
4. По разграничению доступа к персональным данным:			
ИСПДн, к которой имеют доступ определенные перечнем сотрудники организации, являющейся владельцем ИСПДн, либо субъект ПДн;		+	

5. По наличию соединений с другими базами ПДн иных ИСПДн:			
ИСПДн, в которой используется одна база ПДн, принадлежащая организации – владельцу данной ИСПДн	+		
6. По уровню обобщения (обезличивания) ПДн:			
ИСПДн, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта ПДн)			+
7. По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки:			
ИСПДн, не предоставляющая никакой информации	+		

Для ИСПДн не менее 70% характеристик соответствуют среднему и высокому уровню защищенности, а остальные — низкому уровню защищённости. Таким образом, информационные системы имеют среднюю степень исходной защищенности (числовой показатель - Y_1=5).

3. МОДЕЛЬ НАРУШИТЕЛЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Методика формирования модели нарушителя

Для определения перечня актуальных нарушителей безопасности ПДн и их возможностей выполняется:

– классификация потенциальных нарушителей;

– определение перечня доверенных лиц;

– определение перечня актуальных нарушителей из числа потенциальных нарушителей;

– определение возможностей актуальных нарушителей.

3.2. Классификация потенциальных нарушителей

При определении потенциальных нарушителей безопасности все физические лица классифицируются по следующим признакам:

– наличие санкционированного (не санкционированного) физического доступа к техническим средствам ИСПДн;

– наличие санкционированного (не санкционированного) логического доступа к ИСПДн;

Таким образом, выделяются четыре основных типа потенциальных нарушителей (Н.1.1—Н.2.2), представленных в табл. 2.

Таблица 2.

		Логический доступ	
		санкционирован	**не санкционирован**
Физический доступ	**санкционирован**	**Н.1.1** Администратор ИСПДн Администратор СЗПДн Пользователь ИСПДн	**Н.1.2** Охрана Персонал обслуживающих организаций Работники «МГОТУ», не допущенные к ПДн
	не санкционирован	**Н.2.1** Персонал поставщика услуг аутсорсинга	**Н.2.2** Посетитель Внешний нарушитель (имеет доступ к Интернет)

3.3. Доверенные лица

С целью обеспечения доверия к физическим лицам и внешним организациям, на которых возложена ответственность за сопровождение технических или программных средств, либо ответственность за обеспечение информационной или физической безопасности, проводятся дополнительные мероприятия:

- проверка благонадежности и наличия необходимой квалификации;

- непрерывный контроль деятельности;

- ознакомление с документами, регламентирующими порядок обеспечения информационной безопасности и объектового режима;

- информирование об ответственности за нарушения в области информационной безопасности;

- подписание соглашений о неразглашении информации ограниченного распространения.

Выполнение указанного комплекса мероприятий позволяет отнести к доверенным следующие категории лиц:

- администраторы ИСПДн (Н.1.1.1);

- сотрудники охраны (Н.1.2.1);

- сотрудники организаций, осуществляющих техническое сопровождение и гарантийный ремонт технических средств ИСПДн (Н.1.2.2, Н.2.1.2).

3.4. Оценка актуальности нарушителей

Исходя из перечня доверенных лиц, технических особенностей ИСПДн, организационно-штатной структуры «МГОТУ» и характера взаимоотношений с внешними структурами проведена оценка актуальности категорий потенциальных нарушителей. Результаты оценки приведены в табл. 3.

Таблица 3.

Индекс	Категория нарушителя	Оценка актуальности категории нарушителя
Н.1.1	**Лица, имеющие санкционированный физический и логический доступ к техническим средствам ИСПДн**	
Н.1.1.1	Администраторы ИСПДн	Данная категория **не является актуальной**. Администраторы ИСПДн относятся к доверенным лицам.
Н.1.1.2	Администраторы СЗПДн ИСПДн	Данная категория **не является актуальной** по причине отсутствия Администраторов СЗПДн ИСПДн.

Индекс	Категория нарушителя	Оценка актуальности категории нарушителя
Н.1.1.3	Сотрудники, допущенные к обработке ПДн в ИСПДн (внутренние пользователи ИСПДн)	Данная категория является **актуальной**. В ИСПДн имеются внутренние пользователи.
	Зарегистрированные пользователи ИСПДн, осуществляющие удалённый доступ к ИСПДн с помощью технических средств, не входящих в состав ИСПДн	Данная категория **не является актуальной**. Удаленный доступ к ИСПДн запрещён.
Н.1.2	**Лица, имеющие санкционированный физический доступ к ИСПДн, но не имеющие логического доступа.**	
Н.1.2.1	Сотрудники подразделений физической охраны и представители внешних охранных предприятий, действующих на основании договора	Данная категория **не является актуальной**. Сотрудники подразделений физической охраны и внешних охранных предприятий, оказывающих услуги на основании договора, являются доверенными лицами.
Н.1.2.2	Представители организаций, осуществляющих техническую поддержку ИСПДн на основании договора, прибывшие на объект с целью исполнения договорных обязательств	Данная категория **не является актуальной**, т.к. поддержка ИСПДн осуществляется исключительно силами собственных сотрудников.

Индекс	Категория нарушителя	Оценка актуальности категории нарушителя
	Производители и поставщики технических средств ИСПДн, имеющие полный физический доступ к компонентам технических средств ИСПДн до момента поставки оборудования в ИСПДн	Данная категория **не является актуальной** по причине отсутствия у производителей и поставщиков технических средств информации, в составе каких конкретно систем будет использоваться поставляемое оборудование.
	Представители внешних организаций, которым предоставлен доступ к ИСПДн на основании договора или партнёрского соглашения, прибывшие на объект в деловых целях	Данная категория **не является актуальной**, т.к. представителям внешних организаций не предоставляется доступ к ИСПДн.
Н.1.2.3	Работники «МГОТУ», не допущенные к обработке ПДн, технический и обслуживающий персонал, в том числе работники хозяйственных служб, сотрудники, обслуживающие системы вентиляции, электроснабжения, пожаротушения и др.	Данная категория является **актуальной**.
Н.2.1	**Лица, имеющие санкционированный логический доступ к ИСПДн, но не имеющие физического доступа к ИСПДн.**	
Н.2.1.1	Незарегистрированные (анонимные) пользователи ИСПДн, осуществляющие удалённый доступ к не требующим аутентификации областям ИСПДн с помощью технических средств, не входящих в состав ИСПДн.	Данная категория **не является актуальной**. Области ИСПДн, доступ к которым выполняется без использования средств аутентификации, отсутствуют.

Индекс	Категория нарушителя	Оценка актуальности категории нарушителя
Н.2.1.2	Представители внешних организаций, выполняющих работы по технической поддержке ИСПДн на основании договора, осуществляющие удалённый доступ к ИСПДн с помощью технических средств, не входящих в состав ИСПДн.	Данная категория **не является актуальной** по причине отсутствия технической поддержки ИСПДн посредством удаленного доступа.
Н.2.2	**Лица, не имеющие санкционированного физического и логического доступа к ИСПДн.**	
Н.2.2.1	Посетители, в том числе представители внешних организаций, прибывшие на объект для проведения переговоров, частные лица, соискатели вакантных должностей, курьеры и др.	Данная категория является **актуальной**.
Н.2.2.2	Представители внешних организаций, предоставляющих услуги связи, имеющие доступ к используемым в ИСПДн каналам передачи данных	Данная категория является **актуальной**.
Н.2.2.3	Посторонние лица, имеющие доступ к сетям связи общего пользования и каналам передачи данных за пределами контролируемой зоны	Данная категория является **актуальной**.
Н.2.2.4	Посторонние лица, имеющие возможность удаленного съема информации с технических средств ИСПДн по каналам ПЭМИН из-за пределов контролируемой зоны.	Данная категория **не является актуальной**. Меры физической безопасности на объекте исключают возможность съёма информации по техническим каналам.

Индекс	Категория нарушителя	Оценка актуальности категории нарушителя
Н.2.2.5	Разработчики программного обеспечения ИСПДн, имеющие полный логический доступ к разрабатываемым программным компонентам до момента его поставки в «МГОТУ» и в процессе его обновления.	Данная категория **не является актуальной** по причине отсутствия интереса к защищаемой информация у лиц, имеющих возможность внедрения программных закладок на этапах разработки, поставки и обновления программного обеспечения.

3.5. Возможности актуальных категорий нарушителей

При оценке возможностей нарушителя определяется уровень информированности нарушителя, имеющиеся в его распоряжении средства атаки и доступные нарушителю каналы атаки исходя из приведенного ниже перечня.

1. Нарушитель может обладать следующей информацией:

- о технических средствах ИСПДн;
- о каналах связи, используемых «МГОТУ»;
- о системном и прикладном ПО на АРМ ИСПДн;
- об алгоритмах обработки информации в ИСПДн;
- о применяемых «МГОТУ» СЗИ;
- необходимой для доступа к ИСПДн (ключевой, аутентифицирующей и парольной информацией);
- о ПДн, к обработке которых в ИСПДн он допущен;
- об имеющихся недокументированных (недекларированных) возможностях системного и/или прикладного ПО.

2. Нарушитель может воспользоваться следующими средствами и каналами атаки:

-ПО (свободно распространяемым, доступным в свободной продаже или специально разработанным);

- оборудованием (доступными в свободной продаже или специально разработанными);

- средствами съема информации по техническим каналам утечки;

- возможностью доступа и/или изменения конфигурации технических средств ИСПДн;

- возможностью доступа и/или изменения конфигурации системного и прикладного ПО ИСПДн;

- возможностью доступа и/или изменения конфигурации СЗИ;

- возможностью доступа и/или изменения обрабатываемых в ИСПДн ПДн;

- возможностью доступа к информации, передаваемой в открытом виде по каналам связи в пределах и/или за пределами КЗ;

- возможностью внесения аппаратных закладок;

- возможностью внесения недекларированных (недокументированных) возможностей в системное или прикладное ПО ИСПДн;

- возможностью внесения (внедрения) вредоносных программ.

Описание возможностей актуальных категорий нарушителей представлено в табл. 4.

Таблица 4

Индекс	**Актуальная Категория нарушителей**	**Предположение о возможностях нарушителя**
Н.1.1.3	Сотрудники, допущенные к обработке ПДн в ИСПДн (внутренние пользователи ИСПДн)	Обладают следующей информацией: - информацией о части технических средств ИСПДн; - информацией о системном и прикладном ПО ИСПДн; - информацией об алгоритмах обработки информации в ИСПДн; - информацией о части применяемых «МГОТУ» СЗИ;

Индекс	Актуальная Категория нарушителей	Предположение о возможностях нарушителя
		- ключевой, аутентифицирующей и парольной информацией, необходимой для доступа к ИСПДн; - защищаемыми ПДн, к обработке которых в ИСПДн он допущен. Обладает средствами и каналами атаки: - ПО (свободно распространяемым, доступным в свободной продаже или специально разработанным); - оборудованием (доступным в свободной продаже или специально разработанным); - возможностью доступа к части технических средств ИСПДн; - возможностью доступа к системному и прикладному ПО ИСПДн; - возможностью доступа к части СЗИ, используемых в ИСПДн; - возможностью доступа и/или изменения обрабатываемых в ИСПДн ПДн; - возможностью доступа к информации, передаваемой в открытом виде по каналам связи в пределах КЗ; - возможностью внедрения вредоносных программ.
Н.1.2.3	Работники «МГОТУ», не допущенные к обработке персональных данных, технический и обслуживающий	Обладают следующей информацией: - информацией о части технических средств ИСПДн; - информацией о системном и прикладном ПО ИСПДн. Обладает средствами и каналами атаки:

Индекс	Актуальная Категория нарушителей	Предположение о возможностях нарушителя
	персонал, в том числе работники хозяйственных служб, сотрудники, обслуживающие системы вентиляции, электроснабжения, пожаротушения и др.	- ПО (свободно распространяемым, доступным в свободной продаже или специально разработанным); - оборудованием (доступным в свободной продаже или специально разработанными); - возможностью доступа к части технических средств ИСПДн; - возможностью доступа к информации, передаваемой в открытом виде по каналам связи в пределах КЗ.
Н.2.2.1	Посетители, в том числе представители внешних организаций, прибывшие на объект для проведения переговоров, частные лица, устраивающиеся на работу, курьеры и др.	Обладают следующей информацией: - информацией о части технических средств ИСПДн; - информацией о системном и прикладном ПО ИСПДн. Обладает средствами и каналами атаки: - ПО (свободно распространяемым, доступным в свободной продаже или специально разработанным); - оборудованием (доступным в свободной продаже или специально разработанным); - возможностью доступа к части технических средств ИСПДн.
Н.2.2.2	Представители организаций, предоставляющих услуги связи, имеющие доступ к используемым в ИСПДн каналам передачи данных	Обладают следующей информацией: - информацией о части технических средств ИСПДн; - информацией о системном и прикладном ПО ИСПДн; - информацией о части каналов связи, используемых «МГОТУ»;

Индекс	Актуальная Категория нарушителей	Предположение о возможностях нарушителя
		- информацией о части применяемых «МГОТУ» СЗИ. Обладает средствами и каналами атаки: - ПО (свободно распространяемым, доступным в свободной продаже или специально разработанным); - оборудованием (доступным в свободной продаже или специально разработанным); - возможностью доступа к части технических средств ИСПДн; - возможностью внедрения вредоносных программ по сети.
Н.2.2.3	Посторонние лица, имеющие доступ к сетям связи общего пользования и каналам передачи данных за пределами контролируемой зоны	Обладают следующей информацией: - информацией о части технических средств ИСПДн; - информацией о системном и прикладном ПО ИСПДн. Обладает средствами и каналами атаки: - ПО (свободно распространяемым, доступным в свободной продаже или специально разработанным); - оборудованием (доступным в свободной продаже или специально разработанным); - возможностью внесения вредоносных программ по сети.

4. УГРОЗЫ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Классификация угроз

При обработке ПДн в ИСПДн возможна реализация следующих угроз, приводящих к нарушению **конфиденциальности, целостности и доступности** информации:

– угрозы несанкционированного, в том числе случайного, доступа к информации, обрабатываемой в ИСПДн (У.1);

– угрозы утечки информации по техническим каналам (У.2);

– угрозы, обусловленные наличием недекларированных возможностей в прикладном или системном ПО (У.3);

– угрозы не антропогенного характера (У.4).

4.2. Перечень и описание угроз

Перечень рассматриваемых угроз безопасности персональных данных и их описание приведены в таб. 5.

Таблица 5.

Индекс угрозы	Наименование угрозы	Описание угрозы
У.1	**Угрозы несанкционированного доступа к информации, обрабатываемой в ИСПДн** *(связаны с действиями нарушителей, включая пользователей ИСПДн)*	
У.1.1	Уничтожение, хищение аппаратных средств ИСПДн, машинных носителей информации путем физического доступа к элементам ИСПДн.	Кража компьютеров, машинных носителей информации, паролей и атрибутов доступа, модификация и уничтожение информации, вывод из строя узлов компьютера, каналов связи, несанкционированное отключение средств защиты. Реализация угрозы обусловлена халатностью персонала, недостаточностью принятых мер физической охраны помещений ИСПДн, а также нарушениями требований организационно-распорядительной документации, либо отсутствием документированных требований.

Индекс угрозы	Наименование угрозы	Описание угрозы
У.1.2	Утеря машинных носителей информации	Потеря пользователем ИСПДн машинных носителей информации, в том числе идентификатора для доступа к системе защиты ИСПДн, обусловленная его халатностью.
У.1.3	Угрозы, реализуемые в ходе загрузки операционной системы (далее - ОС) на АРМ, в частности при получении доступа к ИСПДн ввиду оставленных без присмотра АРМ.	Перехват паролей или идентификаторов, модификация базовой системы ввода / вывода, перехват управления загрузкой ОС. Реализация угрозы обусловлена халатностью персонала, несоблюдением требований организационно-распорядительной документации либо отсутствием документированных требований, недостаточностью принятых мер по физической охране помещений, где размещены технические средства ИСПДн.
У.1.4	Угрозы, реализуемые после загрузки ОС.	НСД к информации с применением стандартных функций ОС (уничтожение, копирование, перемещение, форматирование носителей информации и т.п.) или с применением специально созданных для выполнения НСД программ (программ просмотра и модификации реестра, поиска текстов в текстовых файлах т.п.). Реализация угрозы обусловлена халатностью персонала, несоблюдением требований организационно-распорядительной документации либо отсутствием документированных требований, недостаточностью принятых мер по физической охране помещений, где размещены технические средства ИСПДн.

Индекс угрозы	Наименование угрозы	Описание угрозы
У.1.5	Внедрение аппаратных закладок	Угрозы хищения, несанкционированной модификации или блокирования информации за счёт применения аппаратных закладок. Реализация угрозы обусловлена халатностью персонала, несоблюдением требований организационно-распорядительной документации либо отсутствием документированных требований, недостаточностью принятых мер по физической охране помещений, где размещены технические средства ИСПДн.
У.2	**Угрозы утечки информации по техническим каналам**	
У.2.1	Угрозы утечки акустической (речевой) информации.	Возникновение угроз утечки акустической (речевой) информации, содержащейся непосредственно в произносимой речи пользователя ИСПДн, возможно при наличии функций голосового ввода ПДн в ИСПДн или функций воспроизведения ПДн акустическими средствами ИСПДн. В ИСПДн не реализованы функции голосового ввода ПДн в ИСПДн. Акустические средства воспроизведения ПДн в ИСПДн не предусмотрены. **Поэтому рассмотрение угроз утечки акустической (речевой) информации нецелесообразно в связи с отсутствием предпосылок возникновения угроз.**

Индекс угрозы	Наименование угрозы	Описание угрозы
У.2.2	Угрозы утечки видовой информации.	Реализация угрозы утечки видовой информации возможна за счет просмотра информации с помощью оптических (оптико-электронных) средств с экранов дисплеев и других средств отображения информации, входящих в состав ИСПДн.
У.2.3	Угрозы утечки информации по каналу ПЭМИН	Угрозы утечки информации по каналу ПЭМИН возможны из-за наличия электромагнитных излучений, в основном, монитора и системного блока компьютера.
У.3	**Угрозы, обусловленные наличием недекларированных возможностей в прикладном или системном ПО**	
У.3.1	Угрозы, связанные с наличием недекларированных возможностей в системном ПО	Инициируют выполнение не описанных в документации функций ПО, приводящих к нарушению конфиденциальности, доступности или целостности обрабатываемой информации.
У.3.2	Угрозы, связанные с наличием недекларированных возможностей в прикладном ПО	
У.4	**Угрозы не антропогенного характера**	
У.4.1	Природные угрозы	Данные угрозы обусловлены стихийными бедствиями. Возникновение подобных событий трудно спрогнозировать и им тяжело противодействовать.
У.4.2	Техногенные угрозы	Угрозы выхода из строя технических средств ИСПДн в результате аварий, неприемлемых параметров питающей энергосети, взрывов.

5. ОПРЕДЕЛЕНИЕ АКТУАЛЬНЫХ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. Оценка вероятности реализации угрозы

Под вероятностью реализации угрозы понимается определяемый экспертным путем показатель (коэффициент Y_2), характеризующий, насколько вероятным является реализация конкретной угрозы безопасности ПДн для данной ИСПДн в складывающихся условиях обстановки.

Вводятся четыре вербальных градации этого показателя и соответствующий числовой коэффициент Y_2 (табл. 6).

Таблица 6

Градация	Описание	Y2
маловероятно	отсутствуют объективные предпосылки для осуществления угрозы	**0**
низкая вероятность	объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию	**2**
средняя вероятность	объектные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны	**5**
высокая вероятность	объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности ПДн не приняты	**10**

С учетом исходного уровня защищённости ИСПДн в целом (коэффициент Y_1) и вышеизложенного коэффициент реализуемости угрозы (Y) будет определяться по формуле:

$$Y = (Y_1 + Y_2) / 20 = (5 + Y_2) / 20,$$

Возможность реализации угрозы определяется исходя из значения коэффициента Y следующим образом:

Значение Y	Возможность реализации угрозы
$0 \leq Y \leq 0,3$	Низкая
$0,3 \leq Y \leq 0,6$	Средняя
$0,6 \leq Y \leq 0,8$	Высокая
$Y > 0,8$	Очень высокая

Результаты расчета возможности реализации угрозы приводится в табл. 7.

5.2. Опасность угрозы

Под опасностью угрозы понимают степень тяжести последствий реализации угрозы для субъекта персональных данных. Вводятся три вербальных градации этого показателя:

а) **Низкая опасность** – если реализация угрозы может привести к незначительным негативным последствиям для субъектов персональных данных;

б) **Средняя опасность** – если реализация угрозы может привести к негативным последствиям для субъектов персональных данных;

в) **Высокая опасность** – если реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных.

Исходя из оценки вреда, который может быть причинен субъектам, при обработке их персональных данных, категории и объемов, обрабатываемых в ИСПДн персональных данных, установлено, что реализация угроз безопасности персональных данных в ИСПДн может привести к незначительным негативным последствиям для субъектов персональных данных (**низкая опасность**).

Показатели опасности реализации угроз приводятся в табл. 7.

5.3. Оценка актуальности угроз

Актуальность угрозы определяется исходя из возможности реализации угрозы и ее опасности следующим образом:

Возможность реализации угрозы	**Опасность угрозы**		
	Низкая	**Средняя**	**Высокая**
Низкая	неактуальная	неактуальная	**актуальная**
Средняя	неактуальная	**актуальная**	**актуальная**
Высокая	**актуальная**	**актуальная**	**актуальная**
Очень высокая	**актуальная**	**актуальная**	**актуальная**

Итоговая оценка актуальности угроз безопасности персональных данных в ИСПДн приведена в табл. 7.

Таблица 7

Индекс угрозы	**Наименование угрозы**	**Оценка вероятности реализации**	**Актуальные нарушители**	**Возможность реализации**	**Опасность угрозы**	**Показатель актуальности угрозы**
У.1	**Угрозы несанкционированного доступа к информации, обусловленные наличием физического доступа к техническим средствам ИСПДн**					
У.1.1	Уничтожение, хищение аппаратных средств ИСПДн, машинных носителей информации путем физического доступа к элементам ИСПДн.	В «МГОТУ» введен пропускной и внутри объектовый режим. Вероятность реализации угроз определена как **маловероятная** в связи с тем, что отсутствуют объективные предпосылки для осуществления угрозы.	–	Низкая (Y=0,25)	Низкая	Неактуальна

Индекс угрозы	Наименование угрозы	Оценка вероятности реализации	Актуальные нарушители	Возможность реализации	Опасность угрозы	Показатель актуальности угрозы
У.1.2	Утеря машинных носителей информации	Вероятность реализации угроз определена как **маловероятная** в связи с тем, что отсутствуют объективные предпосылки для осуществления угрозы. Кроме того, идентификация и аутентификация пользователей производится по логину и паролю (без использования аппаратных персональных идентификаторов).	–	Низкая (Y=0,25)	Низкая	Неактуальна
У.1.3	Угрозы, реализуемые в ходе загрузки ОС на АРМ, в частности при получении доступа к ИСПДн ввиду оставленных без присмотра АРМ	Вероятность реализации угроз определена как **средняя** в связи с тем, что существуют объективные предпосылки для реализации угрозы и принятые меры обеспечения безопасности ПДн недостаточны.	Н.1.1.3 Н.1.2.3 Н.2.2.1	Средняя (Y=0,5)	Средняя	Актуальная
У.1.4	Угрозы, реализуемые после загрузки ОС.	Вероятность реализации угроз определена как **низкая** в связи с тем, что существуют объективные предпосылки для реализации угрозы, но принятые меры существенно затрудняют их реализацию.	Н.1.1.3	Низкая (Y=0,25)	Средняя	Неактуальна

Индекс угрозы	Наименование угрозы	Оценка вероятности реализации	Актуальные нарушители	Возможность реализации	Опасность угрозы	Показатель актуальности угрозы
У.1.5	Угроза внедрения аппаратных закладок	Вероятность реализации угроз определена как **маловероятная** в связи с тем, что отсутствуют объективные предпосылки для осуществления угрозы (отсутствуют нарушители, обладающие возможностью внедрения аппаратных закладок).	–	Низкая (Y=0,25)	Низкая	Неактуальна
У.2	**Угрозы утечки информации по техническим каналам**					
У.2.2	Угрозы утечки видовой информации.	В «МГОТУ» введен пропускной и внутриобъектовый режим. Неконтролируемое пребывание посторонних лиц в помещениях, в которых ведется обработка ПДн, не допускается. Вероятность реализации угроз определена как **низкая** в связи с тем, что существуют объективные предпосылки для реализации угрозы, но принятые меры существенно затрудняют их реализацию.	Н.1.2.3	Средняя (Y=0,5)	Низкая	Неактуальна

Индекс угрозы	Наименование угрозы	Оценка вероятности реализации	Актуальные нарушители	Возможность реализации	Опасность угрозы	Показатель актуальности угрозы
У.2.3	Угрозы утечки информации по каналу ПЭМИН	Предполагается, что объем и ценность обрабатываемых в ИСПДн персональных данных являются недостаточными для мотивации нарушителей к осуществлению действий, направленных на съем информации по каналам ПЭМИН. Вероятность реализации угроз определена как **маловероятная** в связи с тем, что отсутствуют объективные предпосылки для осуществления угрозы (отсутствуют нарушители, обладающие возможностью съема информации по каналу ПЭМИН).	–	Низкая (Y=0,25)	Низкая	Неактуальна
У.3	**Угрозы, обусловленные наличием недекларированных возможностей в прикладном или системном ПО**					
У.3.1	Угрозы, связанные с наличием недекларированных возможностей в системном ПО	Разработчик системного ПО не рассматривается как возможный нарушитель. Вероятность реализации угроз определена как **маловероятная** в связи с тем, что отсутствуют объективные	–	Низкая (Y=0,25)	Низкая	Неактуальна

Индекс угрозы	Наименование угрозы	Оценка вероятности реализации	Актуальные нарушители	Возможность реализации	Опасность угрозы	Показатель актуальности угрозы
		предпосылки для осуществления угрозы.				
У.3.2	Угрозы, связанные с наличием недекларированных возможностей в прикладном ПО	Разработчик прикладного ПО не рассматривается как возможный нарушитель. Вероятность реализации угроз определена как **маловероятная** в связи с тем, что отсутствуют объективные предпосылки для осуществления угрозы.	–	Низкая (Y=0,25)	Низкая	Неактуальна
У.6	**Угрозы не антропогенного характера**					
У.6.1	Природные угрозы	Исходя из территориального размещения ИСПДн, основной природной угрозой является угроза возникновения пожара. В помещениях, в которых располагаются технические средства ИСПДн, установлена пожарная сигнализация. Работники проинструктированы о действиях в случае возникновения внештатных ситуаций. Вероятность реализации угроз определена	–	Средняя (Y=0,5)	Низкая	Неактуальна

Индекс угрозы	Наименование угрозы	Оценка вероятности реализации	Актуальные нарушители	Возможность реализации	Опасность угрозы	Показатель актуальности угрозы
		как **низкая** в связи с тем, что существуют объективные предпосылки для реализации угрозы, но принятые меры существенно затрудняют их реализацию.				
У.6.2	Техногенные угрозы	Вероятность реализации угроз определена как **низкая** в связи с тем, что существуют объективные предпосылки для реализации угрозы, но принятые меры существенно затрудняют их реализацию.	–	Средняя (Y=0,5)	Низкая	Неактуальна

6. ЗАКЛЮЧЕНИЕ

Для информационных систем персональных данных «Кадры», «Бухгалтерия», «Спрут» в Государственном бюджетном образовательном учреждении высшего образования Московской области «Технологический университет», неимеющих подключений к сети «Интернет», **актуальными являются только угрозы НСД**, а именно:

- угрозы, реализуемые в ходе загрузки ОС на АРМ, в частности при получении доступа к ИСПДн ввиду оставленных без присмотра АРМ (У.1.3);

Данный вид угроз в соответствии с Постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении Требований к защите

персональных данных при их обработке в информационных системах персональных данных» **относится** к **угрозам 3-го типа.**

Исходя из перечня актуальных угроз информационной безопасности ИСПДн, рекомендуется применение следующих организационных, технических и программных мер защиты информации:

1. Разработка и внедрение организационных мер защиты информации включающие в себя:

- внедрение в «МГОТУ» пропускного и внутри объектового режима;
- осуществление уборки помещений, где расположена ИСПДн, в присутствии сотрудников соответствующих подразделений;
- создание перечня лиц, допущенных до обработки информации в ИСПДн;
- внедрение разрешительной системы доступа пользователя к защищаемым ресурсам ИСПДн;
- назначение лица, ответственного за эксплуатацию ИСПДн и защиту информации, обрабатываемую в ней;
- создание и внедрение инструкции Администратору ИСПДн;
- создание и внедрение инструкции пользователю ИСПДн;
- ведение журнала паролей;
- ведение журнала учёта машинных носителей информации (CD-дисков, флеш-носителей и т.д.).

2. Внедрение следующих программно-технических средств защиты информации:

- применение сертифицированных по требованиям безопасности информации СЗИ от НСД;
- применение антивирусного ПО.

3. Внедрение следующих организационно-технических мер защиты информации:

- замена устаревших технических средств ИСПДн;
- подключение АРМ к источникам бесперебойного питания;

- закрепление за ИСПДн машинных носителей информации для хранения резервных копий документов;
- размещение технических средств просмотра информации и технических средств выдачи информации на твердую копию должно обеспечивать невозможность её просмотра лицами, до неё не допущенными, а так же через окна кабинетов с помощью специальных оптических устройств;
- оборудование помещений, где расположены технические средства ИСПДн надежными замками.

Проректор по безопасности и режиму А.П. Федоров

7. Лист согласования

СОГЛАСОВАНО:

Первым проректором	«24» 04 2017 г.	О.В. Ковальской
Проректором по качеству и дистанционному обучению	«24» 04 2017 г.	В.В. Нефедьевым
Проректором по информационным технологиям	«24» 04 2017 г.	А.Ю. Щикановым
Начальником управления по персоналу и общим вопросам	«24» 04 2017 г.	С.Н. Панфёровой
Начальником юридического отдела	«24» 04 2017 г.	Г.А. Прокоповичем

8. Лист регистрации изменений

Номер изменения	Номер листа			Дата внесения изменения	Основание для введения изменения	Всего листов в документе	Подпись ответственного за внесение изменений
	измененного	нового	изъятого				