Содержание

Введение

Большинство систем персональных данных нуждаются в программно-аппаратных средствах защиты информации. Для каждой конкретной организации необходимо построение системы защиты, что на начальном этапе предполагает анализ информационной системы специалистом в области безопасности, её классификации по определенным критериям защиты, построение модели угроз и формирование частного технического задания для информационной системы защиты.

Автоматизация процессов анализа позволит значительно упростить и ускорить процесс построения системы защиты, уменьшится объем изучения нормативных актов и иных документов для формирования модели угроз, сократятся материальные затраты и возможные случайные ошибки.

В результате работы должна быть получена автоматизированная компьютерная среда, в которой оператор персональных данных (уполномоченное физическое лицо), указав технические и эксплуатационные характеристики системы тип обрабатываемых данных, получает построенную модель угроз и сформированное частное техническое задание для построения системы защиты.

Постановка задачи

Цель работы:

Главной задачей данной работы является создание приложения, автоматизирующего процесс формирования документов, отражающих требования к системе защиты информационной системы, обрабатывающей персональные данные. Решение должно содержать два документа: модель угроз и техническое задание для конкретной ИСПДн.

Задачи, подлежащие решению для достижения цели:

1) Изучение нормативно-правовой базы, а именно законов, приказов, актов, постановлений правительства РФ по регулированию процесса обеспечения безопасности персональных данных, обрабатывающихся в ИСПДн.
2) Разработка приложения, позволяющего автоматизировать процесс анализа и формирования требований к системе защиты ИСПДн.
3) Проверка актуальности результатов посредством сравнения сформированных документов с существующими работающими техническими заданиями и моделями угроз.
4) Тестирование приложения на конкретной информационной системе.

Анализ нормативно-правовой базы

Основа нормативно-правовой базы работы Федеральный Закон №152 “О персональных данных”.[1]

Вступивший в силу в 2007 году закон в настоящий момент в него внесено 11 изменений (на 27.04.2014) федеральными законами разного уровня и разной значимости.

Возможно, это связанно с новизной и отсутствием наработок в данной сфере в нашей стране.

Особенно трудную задачу приходится решать операторам, вынужденным обрабатывать большие количества персональных данных, например, нотариальные конторы, школы, вузы, которые в силу их правового статуса не имеют подразделений, ответственных за защиту персональных данных, и из-за отсутствия материальным возможностей не могут позволить себе

возложить эту ответственность на другое юридическое лицо. Определить актуальные угрозы безопасности – сложная задача.

ФЗ №152 подразумевает большое количество нормативных документов, которые должны приниматься ФСБ и ФСТЭК как уполномоченными на федеральном уровне принимать решения в области информационной безопасности, а также постановлений правительства, например, постановления правительства № 512,687,221,940,1119.

В соответствии с ФЗ № 152 статья 19 существуют меры, которые независимо от уровня защищенности системы должен выполнить каждый оператор, первая мера говорит о том, что модель угроз обязательна при построении системы защиты. [1]

Полный список документов для реализации поставленной задачи расположен в *Приложении 1.*

Большинство этих документов рассмотрены в процессе описания алгоритма.

Отдельно стоит отметить постановление правительства № 211 в соответствии, с которым существует список документов, который операторы обязаны разработать, утвердить. Данный список может составить уполномоченное лицо организации, в которой осуществляется обработка персональных данных. Данные из этих документов используются для работы с разработанным приложением, для построения модели угроз и технического задания, например, “Перечень персональных данных”.

Также стоит отметить, что используемые на сегодняшний момент документы ФСТЭК: базовая модель угроз и методика актуализации угроз сохраняют свой правовой статус, несмотря на то, что методика актуализации принята на основании постановления правительства № 781, которое было признано утратившим силу 1 ноября 2012 года, она не базируется на понятии класса информационной системы персональных данных и не было принято решения, что она не подлежит применению.

Учитывая требования, заложенные в федеральном законе, и методологию, заложенную в документах ФСБ и ФСТЭК, проектирование и реализация системы защиты должны состоять из следующих этапов (рисунок.)

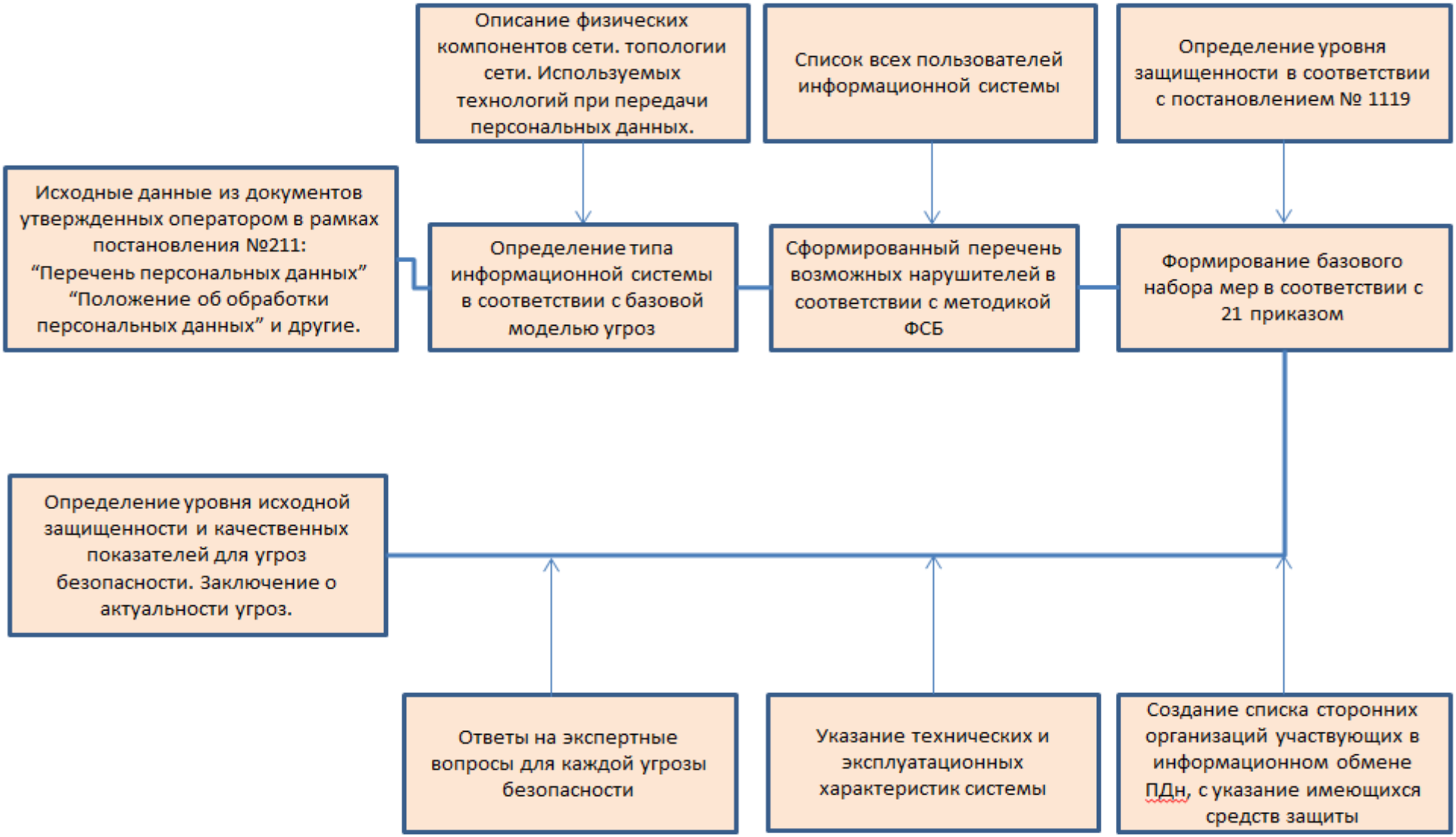
Описание физических компонентов сети. топологии сети. Используемых технологий при передачи персональных данных.
Список всех пользователей информационной системы
Определение уровня защищенности в соответствии с постановлением № 1119
Исходные данные из документов утвержденных оператором в рамках постановления №211: “Перечень персональных данных” “Положение об обработки персональных данных” и другие.
Определение типа информационной системы в соответствии с базовой моделью угроз
Сформированный перечень возможных нарушителей в соответствии с методикой ФСБ
Формирование базового набора мер в соответствии с 21 приказом
Определение уровня исходной защищенности и качественных показателей для угроз безопасности. Заключение о актуальности угроз.
Ответы на экспертные вопросы для каждой угрозы безопасности
Указание технических и эксплуатационных характеристик системы
Создание списка сторонних организаций участвующих в информационном обмене ПДн, с указание имеющихся средств защиты

Рисунок 1

Описание алгоритма

Физическая структура ИСПДн, компоненты сети

Определить названия существующей ИСПДн, список серверов, функционирующих в ИСПДн, и решаемые на этих серверах задачи, связанные с обработкой ПДн, указав местоположение(фактический адрес) серверов.

Под задачами понимается перечень действий (операций) связанный с обработкой персональных, определенный в ФЗ от 27.07.2006 N 152-ФЗ (ред. от 21.12.2013) "О персональных данных", глава 1, статья 3, пункт 3: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Согласно статье 6 ФЗ № 152 в договоре на обработку указывается перечень операций, который может совершаться с персональными данными, данные из перечня вносятся модель угроз ИСПДн.

Далее необходимо указать топологию сети и используемые технологии при передаче данных, а также количество физических компонентов сети, в том числе количество узлов, доступных из интернет. Теперь, учитывая физическое расположение компонентов сети, можно классифицировать ИСПДн в рамках типовой модели угроз безопасности в ИСПДн [2] по структуре информационной системы как автоматизированное рабочее место, локальную информационную систему или распределенную информационную систему и наличию подключений к сетям общего пользования как систему, имеющую подключения или не имеющую подключений.

Необходимо указать операционную систему для каждого из серверов, выбрав из приведенного в приложении списка операционных систем или добавить новую.

Определение характеристик безопасности

Далее необходимо указать требуемые характеристики безопасности персональных данных для конкретной информационной системы – определить модель угроз верхнего уровня. [3]

Под моделью угроз верхнего уровня понимается перечень всех характеристик безопасности.

Под характеристикой безопасности понимается требование выполнение которого необходимо для обеспечения защищенности персональных данных.

Основными характеристиками безопасности являются конфиденциальность, целостность и доступность.

Также могут рассматриваться дополнительные характеристики безопасности. Например, неотказуемость, учетность, аутентичность ,адекватность.

Как правило, условия создания и существования реальных объектов достаточно сложны и, как следствие, к ним можно предъявить достаточно много самых различных требований.

Так как угроза безопасности объекта – возможное нарушение характеристики безопасности объекта, то перечень всех характеристик безопасности для всех возможных объектов угроз, по сути, определяет модель угроз верхнего уровня. [3]

Конфиденциальность— состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на неё право;

Целостность — избежание несанкционированной модификации информации;

Доступность — избежание временного или постоянного сокрытия информации от пользователей, получивших права доступа.

Неотказуемость – способность доказать, что действие или событие произошло таким образом, что факт действия или события не может быть опровергнут (ИСО 7498–2:99 и ИСО 13888–1:2004).

Учетность – свойство, обеспечивающее однозначное отслеживание собственных действий любого логического объекта;

Аутентичность– свойство обеспечения идентичности субъекта или ресурса заявленной идентичности. Аутентичность применяется к таким субъектам как пользователи, процессы, системы и информация (ISO/IEC 13335–1:2004);

Идентичность – объекта тому, что заявлено.

Адекватность – свойство соответствия преднамеренному поведению и результатам (ISO/IEC 13335–1:2004).

Список прикладного программного обеспечения

Необходимо указать все операционные системы, установленные на рабочих местах, а также привести примерный список прикладного программного обеспечения, используемого на рабочих местах.

Примерный список прикладного обеспечения представлен в программе.

Средства защиты используемые в ИСПДн

Определим группы средств СЗИ:

1) Средства резервного копирования
2) Межсетевые экраны
3) Системы обнаружения/предотвращения вторжений
4) Средства криптографической защиты
5) Средства защиты от НСД
6) Антивирусные программы
7) Защита от ПЭМИН

Затем необходимо указать перечень технических и программных средств по обеспечению информационной безопасности в ИСПДн, для каждой группы средств.

В программе приведен список наиболее часто используемых средств. В случае отсутствия СЗИ в списке можно добавить новое средство для каждой группы.

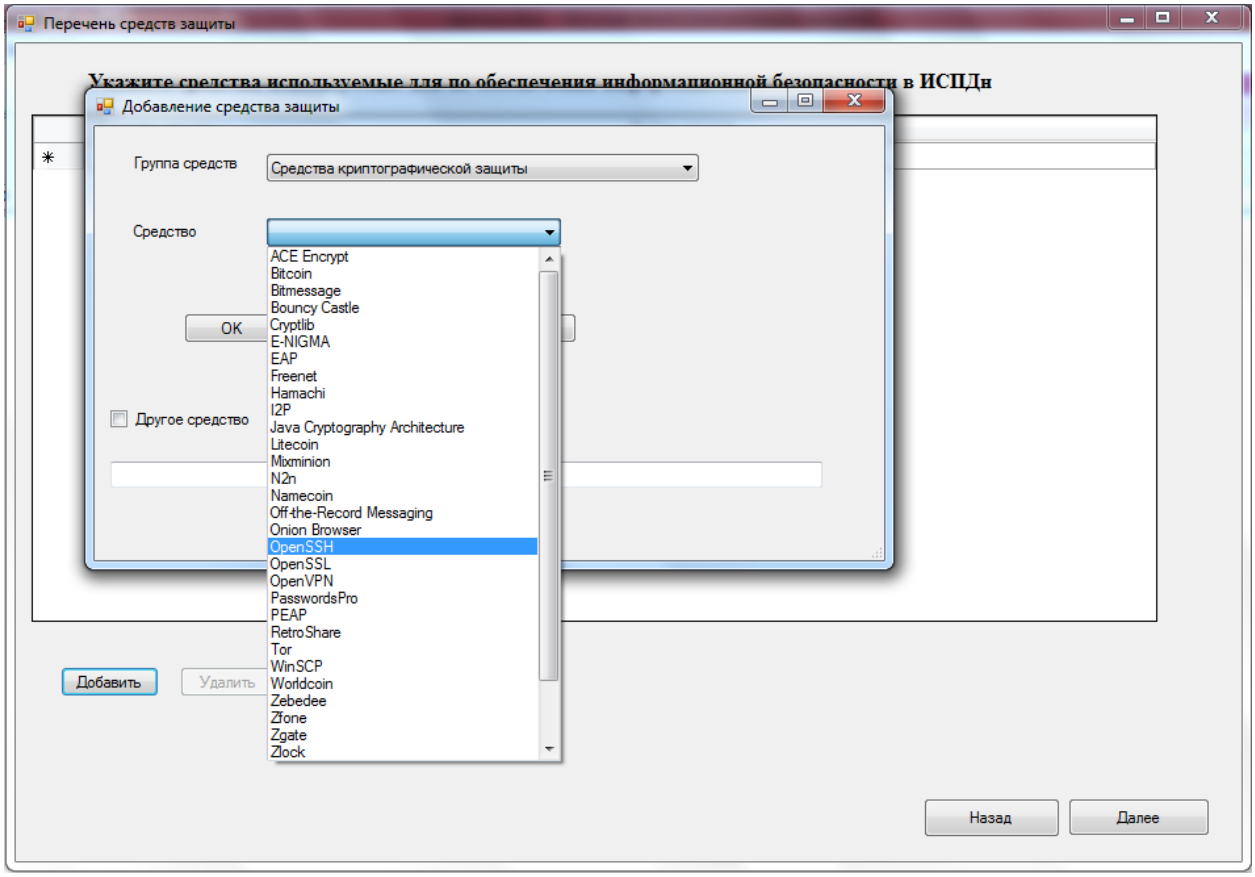

Рисунок 2

Большинство ИСПДн участвуют в информационном обмене со сторонними организациями.

Требуется указать документы, дающие основания для информационного обмена (например, трудовой кодекс РФ). И средства защиты для всех существующих информационных потоков передачи ПДн между организациями, из составленного выше перечня средств защиты, либо добавить неуказанное средство защиты.

Постановление правительства 1119

Необходимо определить требования к защите персональных данных, руководствуясь постановлением правительства 1119. [5]

Процесс формирования требований 1119 постановления состоит из следующих задач:

1) Определение категории персональных данных, обрабатываемых в информационной системе.
2) Определение актуальных угроз безопасности
3) Определение уровня защищенности исходя из категории ПДн(пункт 1), актуальных угроз(пункт 2) и количества субъектов персональных данных в информационной системе.

Постановление 1119 вводит 4 группы систем персональных данных в зависимости от категории обрабатываемых ПДн категория определяется исходя из анализа документа составленного на основании постановления правительства № 211 - “ Перечень персональных данных”.

Понятия актуальных угроз и категорий ПДн приводятся в 1119 постановлении, также пункте 7 постановления 1119 говорится, что тип актуальных угроз безопасности ПДн, определяется на основе оценки возможного вреда, который в свою очередь определяется оператором персональных данных.

Согласно статье 18.1 ФЗ № 152 в обязанности оператора входит оценка вреда, который может быть нанесет субъектам персональных данных. Вопрос оценки вреда связанный с нарушением законных прав субъекта (гражданина) методологически непроработанная задача с точки зрения юриспруденции и судебного производства.

Критериев для оценки вреда в постановлении не приводится. На сегодняшний день отсутствует утвержденная методика, позволяющая произвести оценку возможного вреда.

Исходя из того, обоснование выбора типа актуальных угроз не регламентировано, оно может быть любым, способ определения типа актуальных угроз остается на усмотрение оператора. По умолчанию выставлен третий тип актуальных угроз, так как он предполагает установление третьего или четвертого уровня защищенности и существенное снижение ответственности оператора перед субъектами персональных данных и органами исполнительной власти. Второй уровень защищенности при наличии третьего типа актуальных угроз может быть установлен только при обработке специальной категории персональных данных более чем 100000 субъектов, что видно из таблицы.

Таблица 1

Тип ИСПДн	Сотрудники оператора	Количество субъектов персональных данных	Тип актуальных угроз		
			1	2	3
Специальные	Нет	> 100000	УЗ-1	УЗ-1	УЗ-2
	Нет	< 100000	УЗ-1	УЗ-2	УЗ-3
	Да				
Биометрические			УЗ-1	УЗ-2	УЗ-3
Иные	Нет	> 100000	УЗ-1	УЗ-2	УЗ-3
	Нет	< 100000	УЗ-2	УЗ-3	УЗ-4
	Да				
Общедоступные	Нет	> 100000	УЗ-2	УЗ-2	УЗ-4
	Нет	< 100000	УЗ-2	УЗ-3	УЗ-4
	Да				

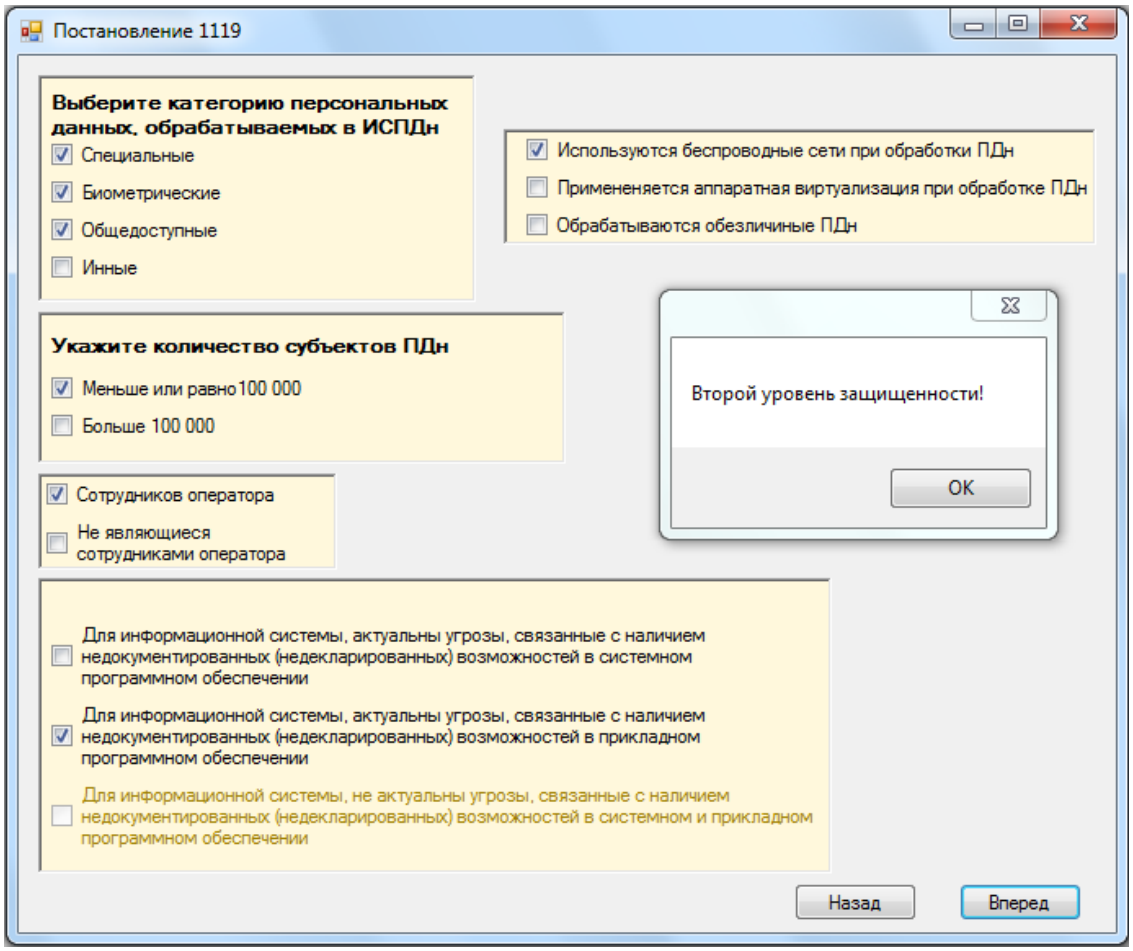

Рисунок 3

После определения уровня защищенности руководствуясь постановлением Правительства РФ от 01.11.2012 N 1119 можно определить **требования** для уровня защищенности персональных данных.

Контроль, за выполнением требований постановления 1119 проводится оператором самостоятельно или с привлечением юридического лица, имеющего лицензию минимум раз в три года. Оператору не требуется лицензия, в случае если он не оказывает никому услуг и действует в собственных интересах, однако не исключено, что организация, самостоятельно занимающая технической защитой и не имеющая лицензии, будет привлечена к ответственности. Вопрос лицензирования до конца не регламентирован, поэтому оператор, не имеющий лицензии, рискует.

Выбор мер для определенного уровня защищенности

Далее, зная уровень защищенности информационной системы, можно определить список мер, согласно Приказу 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”.

Начальный базовый список мер определяется в соответствии с классом защищенности информационной системы.

Затем исходя из структуры информационной систем, базовый список мер подлежит адаптации, которая заключается в исключении мер из базового набора, не связанных с данной технологиям и (или) характеристиками информационной системой.

Далее адаптированный список мер подлежит процедуре уточнения, которая заключается в дополнении списка мер мерами из приложения к 21 приказу, для обеспечения блокирования всех угроз безопасности.[4]

Уточненный адаптированный список мер подлежит процедуре дополнения для выполнения иных нормативных актов по обеспечения защиты информационной системы.

У оператора есть возможность заменить меры из полученного списка на компенсирующие меры, обосновав при этом необходимость замены. Обоснование должно включать причины исключения меры. В программе приведены 3 наиболее частых причины исключения:

1) Мера экономически не целесообразна
2) Технологии, связанные с мерой, не используются
3) Нет возможности технической реализации меры

Есть возможность указать другую причину исключения меры. Также необходимо описать содержание компенсирующей меры, аргументировав адекватное блокирование угрозы безопасности.

Согласно статье 19 ФЗ № 152 оператор обязан обеспечить организационные и технические меры по информационной безопасности ИСПДн.

Необходимо описать организационные меры по обеспечению информационной безопасности, указать организацию, осуществляющую охрану контролируемой зоны или ее отсутствие, а также ответить на вопросы отражающие наличие организационных мер (рисунок).

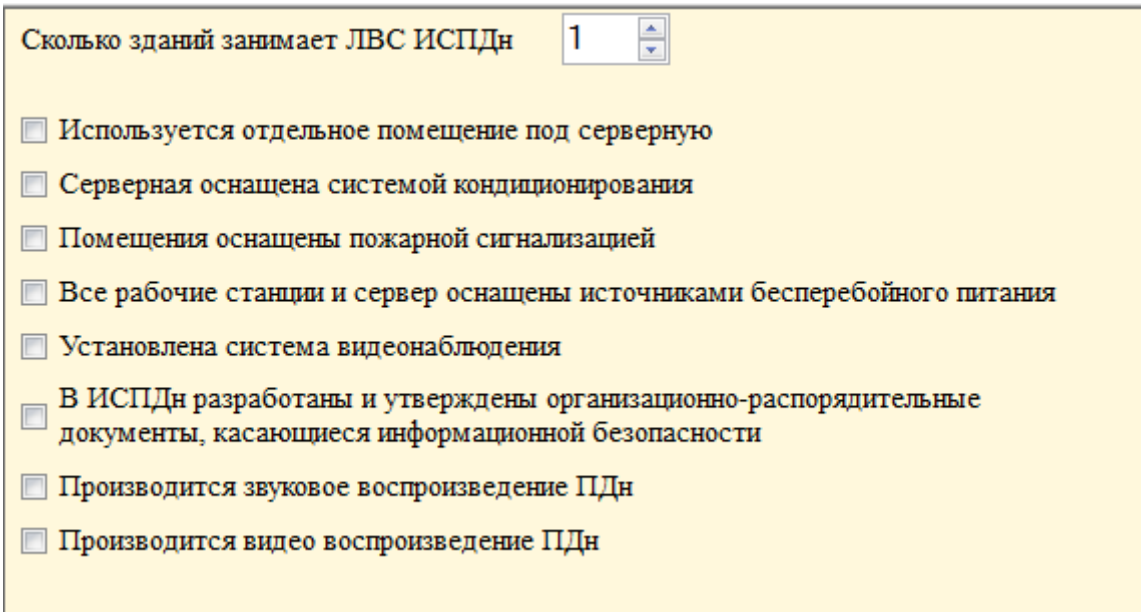

Рисунок 4

Построение модели нарушителя

Построение модели нарушителя регламентировано методикой ФСБ России. В приложении алгоритм построения модели нарушителя следующий:

Рассматриваются все пользователи информационной системы, при этом определяется возможность доступа в контролируемую зону для каждого пользователя, а также степень его привилегированности. Привилегированные пользователи не рассматриваются в качестве потенциальных нарушителей (они могут “законно” получить доступ к персональным данным).

Далее необходимо рассмотреть возможности всех пользователей по характеристикам: доступной информации об объекте атаки, возможных средствах атаки, доступных каналах атаки, путем высказывания предположения об этих критерия сотрудником организации, в задачи которого входит формирование модели угроз.

Тип нарушителя в приложении формируется исходя из полученных характеристик и возможностей нарушителя.

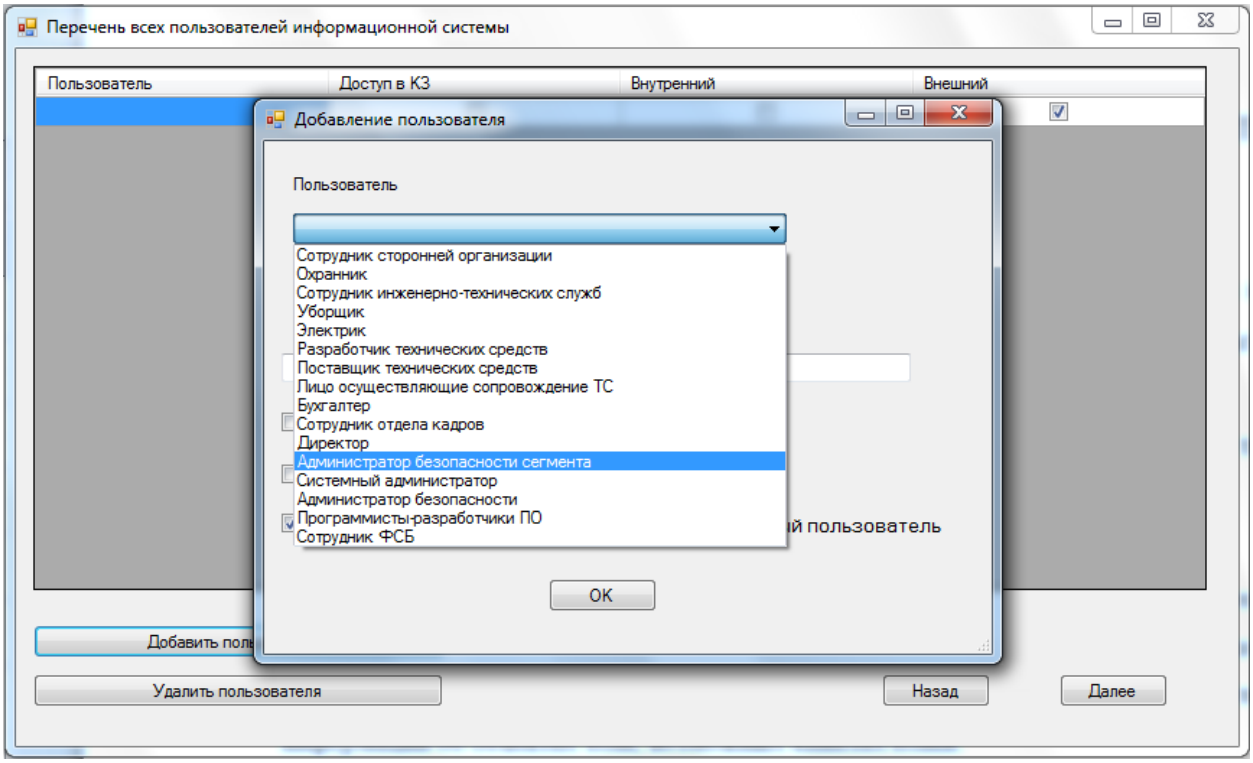

Рисунок 5

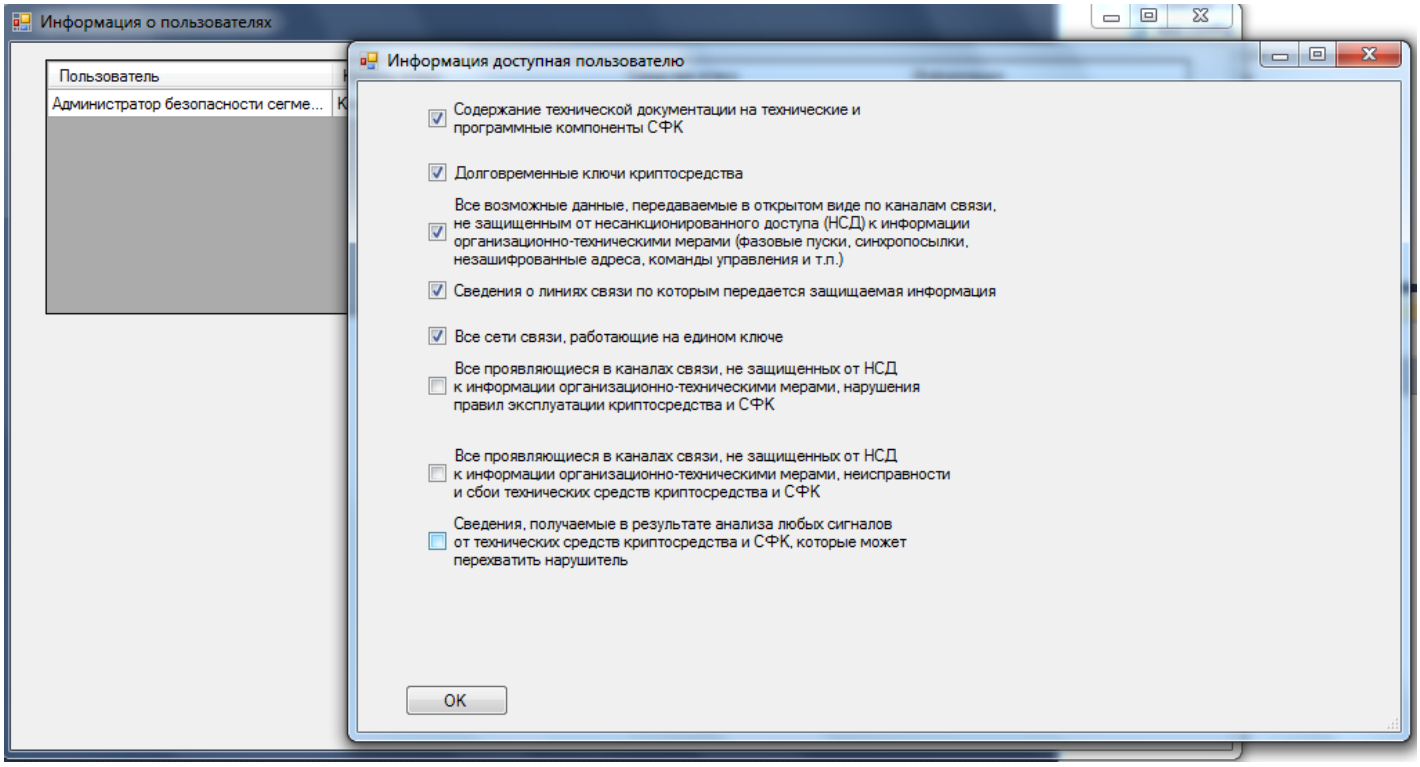

Рисунок 6

Зная тип нарушителя и руководствуясь методикой ФСБ России, однозначно определяются уровни защиты от ПЭМИН, криптографической защиты, а также требования, позволяющие контролировать внедрение криптосредства.

Характеристики информационной системы

В соответствии с базовой моделью ФСТЭК существует 6 типовых модели угроз безопасности в зависимости от характеристик информационной системы. Искомые характеристики может однозначно определить сотрудник информационной системы.

1) Режим, в котором обрабатываются персональные данные: однопользовательский или многопользовательский.
2) Разграничение прав доступа для пользователей: с разграничением или без разграничения.
3) Местонахождение физических компонентов информационной системы: на территории Российской федерации, либо частично или полностью за границей Российской Федерации.
4) Подключение к сетям общего использования: присутствует или отсутствует подключение.
5) В целом по структуре: распределенные системы, локальные информационные системы, автоматизированные рабочие места.

После определения можно сделать вывод о типе ИСПДн, руководствуясь методикой ФСБ[].

Далее необходимо перечислить все персональные данные, подлежащие защите, в соответствии с документом “Перечень ПДн подлежащих защите”, разработанным во исполнение 152 ФЗ “О персональных данных”.

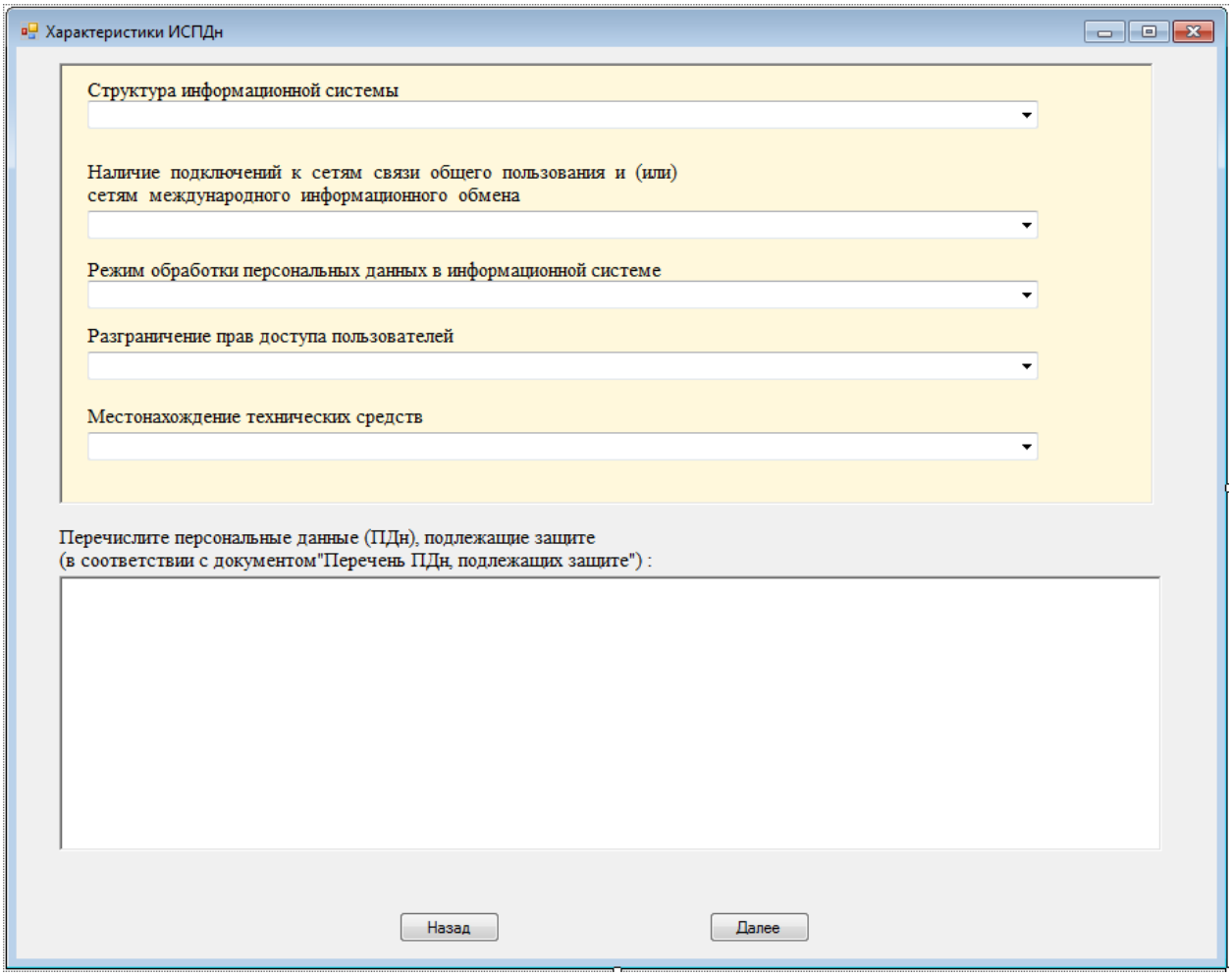

Рисунок 7

Определение актуальных угроз

На заключительном этапе формирования модели угроз, необходимо сформировать перечень актуальных угроз безопасности персональных данных в ИСПДн.

Перечень возможных угроз формируется исходя из базовой модели угроз ФСТЭК.

Согласно методике определения актуальных угроз ФСТЭК для определения актуальности угрозы безопасности персональных данных, обрабатываемых в ИСПДн, необходимо рассчитать уровень исходной защищенности системы и определить вербальные (качественные) показатели для конкретной угрозы – опасность и вероятность реализации угрозы.

Показатель исходной защищенности рассчитывается исходя из характеристик системы. В нормативных документах ФСТЭК предложен ряд вопросов, позволяющих оценить уровень защищенности системы – один вопрос по каждой характеристике.

В исходной программе после ответа сотрудника на указанные вопросы рассчитывается уровень исходной защищенности, в соответствии с методикой определения актуальных угроз в зависимости от процентов полученных значений, при ответах на вопросы.

Возможные значения уровня защищенности регламентированы ФСТЭК России: высокий (70% характеристик имеют высокий уровень защищенности), средний (не менее 70% характеристик соответствуют уровням: средний и высокий), низкий (менее 70% характеристик соответствуют уровням: средний и высокий).

Качественные показатели угроз безопасности должны определяться на основе субъективных мнений экспертов по информационной безопасности, привлеченных для этой задачи.

Рассмотрим, способ реализации экспертных оценок защищенности информационной системы персональных данных для последующего применения показателей при построении системы защиты, используемый в приложении.

Предлагается рассчитывать вербальный показатель, на основе анализа оценок, полученных от сотрудника организации, которому будет предложен ряд вопросов заранее “взвешенных” по важности экспертами.

Имея набор входных данных, характеризующих конкретную информационную систему, полученных от уполномоченного лица предприятия, можно сформировать модель угроз и техническое задание соответствующие стандартам установленным регуляторами в области информационной безопасности (Росскомнадзор, ФСТЭК, ФСБ) и отражающие специфические требования предприятия.

На этапе оценивания актуальности угроз необходимо учитывать вербальные (качественные) показатели, определяемые только экспертным путем. Например, экспертом определяется показатель “вероятность реализации угрозы”, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности персональных данных (ПДн) для данной информационной системы персональных данных (ИСПДн) в складывающихся условиях обстановки.

Понятно, что вербальные показатели рассчитываются преимущественно на основе субъективных мнений экспертов в области безопасности, руководства организации или других лиц, выполняющих оценку. Следовательно, данные показатели – качественные характеристики угроз. Как правило, качественный анализ выполняется путем заполнения опросных листов и проведения совместных обсуждений с участием представителей различных групп организации, таких как упомянутые выше эксперты по информационной безопасности, менеджеры и

сотрудники ИТ-подразделений. Задача – получить актуальные показатели без привлечения экспертов со стороны.

Предлагается рассчитывать вербальный показатель, на основе оценок, полученных от сотрудника (уполномоченного лица), которому будет предложен ряд вопросов заранее “взвешенных” по важности экспертами, где важность (мнение эксперта) будет отражена в матрице оценок. А собственный вектор этой матрицы будет отражать коэффициенты важности (приоритеты) для каждого вопроса. После ответа тестируемого на заданные вопросы и получения вектора приоритетов необходимо провести построение функций принадлежности ответов к нечеткому терм-множеству, учитывая полученные приоритеты, где термы – значения искомых вербальных показателей [6].

Введем лингвистические переменные [7] для каждого вербального показателя – “Опасность” и “Вероятность”, базовые терм-множества которых представим нечеткими термами T = {T1, .., TL}, имеющих названия введенные методикой определения актуальных угроз[6]:

Опасность: “Низкая”, “Средняя”, “Высокая ”.

Вероятность: “Маловероятно”, “Низкая”, “Средняя”, “Высокая ”.

Определим числовое универсальное множество $U = [1, L-1]$,

где L – количество термов.

Для построения показателя тестируемый (сотрудник) должен ответить на n вопросов по N-балльной шкале, причем значение N может быть различным для каждого вопроса.

После чего, имея набор ответов в баллах, отобразим диапазон изменения параметра X_j (количества баллов по каждому вопросу), $J = 1..n$ на универсальное множество $U = [1, L-1]$. Пересчет фиксированного значения X_j в соответствующий элемент $U_j \in [1, L-1]$ выполним по следующей формуле[15]:

$$U_j = (L-1)\frac{X_j - \underline{X}_j}{\overline{X}_j - \underline{X}_j},$$

где $\underline{X}_j = 0$, $\overline{X}_j = N_j$ -изменения параметра X_j по каждому вопросу.

Построим функции принадлежности $\mu_i(X_j)$ ответа X_j терму T_i.

Имеем L термов T_i на универсальном множестве $U = [1, L-1]$

Функции принадлежности $\mu_i(X_j)$, составляющие количественный смысл термов для введенной ЛП, должны удовлетворять следующим условиям, которые исходят из дальнейшего алгоритма нахождения решения (максиминный принцип) и теории построения функций принадлежности [9].

А именно:

1) Ограниченность. Универсальное множество U должно быть ограничено, т.к. понятие, описываемое с помощью ЛП, имеет ограниченный набор значений.

$$\forall i = 1..n : 0 < \sum_{U} \mu_{T_i}(u) < +\infty$$

Следует из общих принципов построения функции принадлежности [7].

2) Симметричность μ_i.

Теперь можно приступить к подбору функции принадлежности, удовлетворяющей этим условиям.

Колоколообразная функция принадлежности вида:

$$\mu_B(x) = \frac{1}{1+\left[\frac{x-\alpha}{c}\right]^2}$$

,где нечеткое число B с колоколообразной функцией принадлежности задается парой чисел $B = (a, c)$, где а α – центр, c – величина характеризующая ширину функции.

Данная функция удовлетворяет перечисленным требованиям, является гладкой на всей области определения и принимает ненулевые значения. Для построения такой функции необходим довольно большой набор данных, график колоколообразной функции симметричен относительно своей моды (центра).

Функции принадлежности нечеткого терма с номером i определим следующим образом [10]:

$$\mu_i^j(U_j) = \left[\frac{1}{1+(U_j - i + 1)^2}\right]^{PN_j},$$

Где PN_j, $j = 1..n$ – коэффициенты важности, определенные экспертом по каждому вопросу.

Рассмотрим вариант применения метода анализа иерархий для задачи – получения коэффициентов важности (приоритетов) для вопросов.

Метод анализа иерархий состоит в декомпозиции проблемы на более простые составляющие части и дальнейшей обработке последовательности суждений лицом принимающим решение, например на основе метода парных сравнений[11]. Эти суждения затем выражаются численно.

Если рассматривать какой-либо качественный *показатель* угрозы безопасности системы обработки персональных данных – как объект иерархии, а вопросы задаваемые экспертам – как объект иерархии следующего (дочернего) уровня, то веса вопросов $\omega_1, \dots, \omega_n$ являются приоритетами для *показателя*. Основным инструментом будет матрица чисел, представляющая суждения о парных сравнениях вопросов. Для представления приоритетов выбран собственный вектор, соответствующий наибольшему собственному значению. [11]

Пусть имеем:

$i = 1,2..n$ угроз безопасности

$j = 1,2..m$ вопросов для каждой угрозы, характеризующих вербальный показатель (Опасность угрозы или вероятность угрозы)

Глобальные приоритеты - приоритеты альтернатив относительно цели (качественный *показатель*), которые вычисляются на заключительном этапе метода путем линейной свертки локальных приоритетов всех элементов.

В нашем случае все приоритеты глобальные т.к. иерархия состоит из двух уровней.

Значения приоритетов нормализуем: $\sum_1^m \text{Приоритет}_m = 1$.

В таком случае сравнив вопросы методом парных сравнений, мы получим значения глобальных приоритетов для цели “важность j-го вопроса для показателя i - ой угрозы”.

В основе метода парных сравнений лежит процедура обработки результатов опроса экспертов в виде упомянутой выше матрицы оценок A.

$A = (a_{ij}), (i, j = 1,2, \dots, n)$

$$A = \begin{bmatrix} 1 & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ 1/a_{1n} & \cdots & 1 \end{bmatrix}$$

После представления количественных суждений a_{ij} о важности вопросов, необходимо поставить в соответствие множество весов ω_n соответствующих суждениям a_{ij}.

$$\frac{\omega_i}{\omega_j} = a_{ij}, \text{ (для } i, j = 1,2, \dots, n)$$

$$A = \begin{bmatrix} \frac{\omega_1}{\omega_1} & \cdots & \frac{\omega_i}{\omega_1} \\ \vdots & \ddots & \vdots \\ \frac{\omega_n}{\omega_1} & \cdots & \frac{\omega_n}{\omega_n} \end{bmatrix}$$

Далее обработка заключается в оценке максимального собственного значения указанной матрицы. Вектор приоритетов вопросов — собственный вектор матрицы оценок. Поэтому для нахождения вектора приоритетов необходимо найти вектор удовлетворяющий уравнению[11]:

$$A\omega = \lambda_{max}\omega$$

Для уменьшения числа сравнений и обеспечения согласованности суждений, сами сравнения достаточно производить только в одном направлении. Например, если величине ω_{ij} присвоено значение k, то величина ω_{ij} автоматически принимает значение $1/k$. Экспертам необходимо произвести $n(n-1)/2$ сравнений важности вопросов относительно друг друга. Затем вычисляется собственный вектор матрицы парных сравнений, для представления приоритетов вопросов.

Корректность применения метода получения из количественных суждений группы (т. е. из относительных величин, ассоциируемых с парами объектов (вопросов)) множества весов, ассоциируемых с отдельными объектами (вопросами) и более подробное обоснование использования метода можно найти в работах Т. Саати, например[7]

Нашей модели присуще требование транзитивности. Однако в [12] исследовано предположение, что нетранзитивность предпочтений может быть естественным явлением, а не следствием ошибки в суждениях или заблуждением. Сделано заключение, что в ряде случаев нетранзитивность является естественной и ее нельзя избежать.

Все оценки парных сравнений подвержены погрешностям, которые могут привести к несогласованным выводам. Степень согласованности суждений экспертов оценивается показателями согласованности.

Связь вектора приоритетов с согласованностью показывается с помощью вычисления индекса согласованности, ИС: $((\lambda_{max}) - n)/(n-1)$, где λ_{max} – наибольшее собственное значение

n – количество элементов квадратной матрицы сравнений

В общем случае,

Если $\text{ИС} \leq 0{,}1$, мы можем быть удовлетворены суждениями.

ИС - это количественная оценка противоречивости результатов сравнений. Затем вычисляется относительная согласованность, ОС (отношение индекса согласованности к среднестатистическому значению индекса согласованности(СС), СС получено Т.Саати методом генерации ИС случайным образом по шкале от 1 до 9 обратно-симметричной матрицы).

Величина ОС должна быть порядка 10% или менее, чтобы быть приемлемой. В некоторых случаях можно допустить 20%, но не более. Если ОС выходит из этих пределов, то участникам нужно исследовать задачу и проверить свои суждения.[13]

Значение качественного показателя для угрозы , определим используя свертку на основе пересечения нечетких множеств, на основании следующего нечеткого логического выражения [14]:

$$\mu_S(X_j) = \bigvee_{i=1}^{L} \bigwedge_{j=1}^{n} \mu_i^j$$

Где $i = 1..L$ – номер терма из базового терм-множества T а $j = 1..n$ – номер вопроса.

Покажем используемый способ на конкретном примере, для угрозы удаленного запуска приложений.

- **Тип угрозы:** Несанкционированный доступ к информации и аппаратным средствам ИСПДн, реализуемый внешними нарушителями
- **Угроза:** Удаленный запуск приложений

Таблица 2

U_j	Значения функций принадлежности ответов к термам				Ответы в баллах	Веса вопросов	Результат
1,2	0,987589679	0,99945106	0,99309818	0,97997925	4	0,014	
1,8	0,911692926	0,96883539	0,99749302	0,94451107	6	0,064	
2,4	0,843596451	0,90793558	0,98687748	0,97300492	8	0,089	
2,7	0,417481254	0,57062503	0,84815274	0,96503454	9	0,413	
0,6	0,945865658	0,97349361	0,82166767	0,70758668	2	0,181	
1,2	0,959798502	0,99819747	0,97750094	0,93570978	4	0,046	
1,2	0,963229173	0,99835409	0,97943712	0,9411322	4	0,042	
2,4	0,750771876	0,84977949	0,97798299	0,95492478	8	0,15	
	0,417481254	**0,57062503**	**0,82166767**	**0,70758668**			**0,8216677**
	Маловероятно	Низкая вероятность	Средняя вероятность	Высокая вероятность			

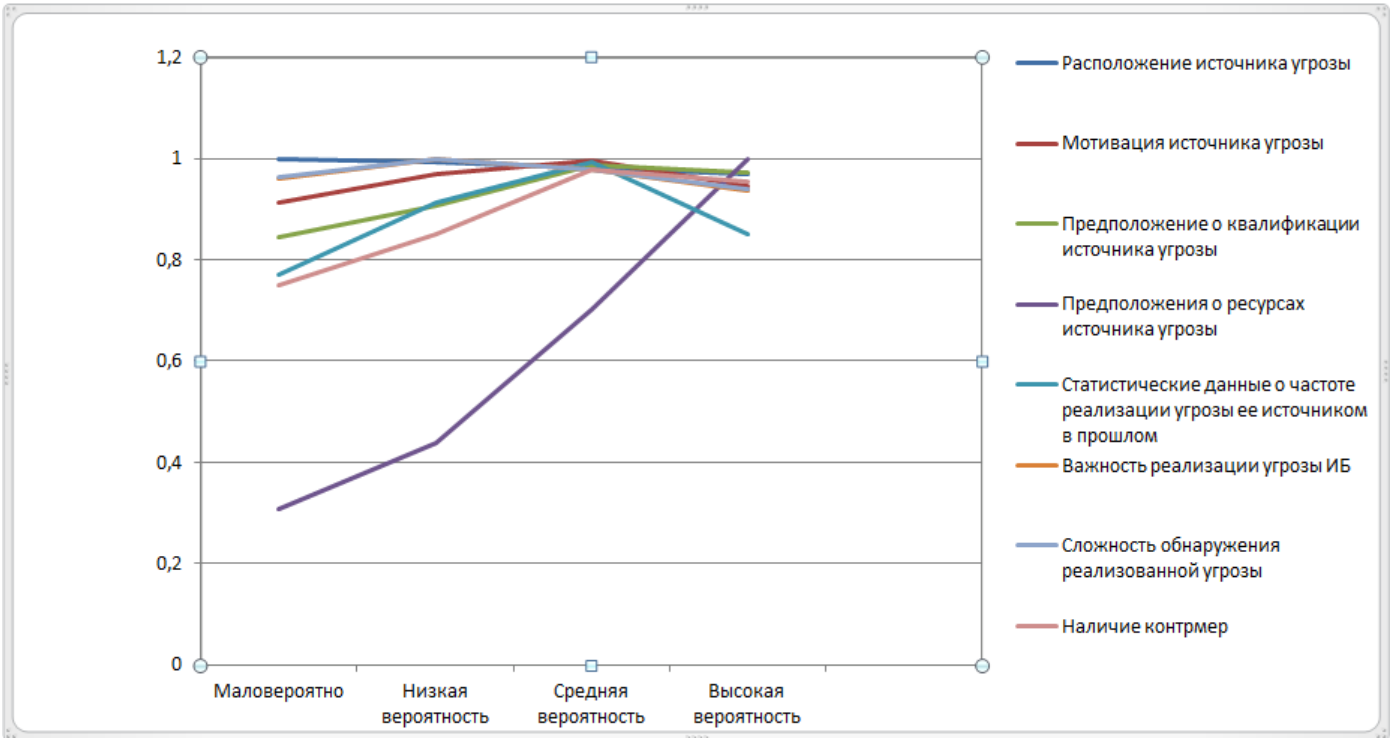

Рисунок 9

Далее, исходя из определенной вероятности угрозы и уровня исходной защищенности, автоматически рассчитывается возможность реализации для конкретной угрозы безопасности, по формуле, предложенной ФСТЭК России. Возможные значения также регламентированы: низкая, средняя, высокая, очень высокая.

Зная возможность реализации и опасность, можно рассчитать актуальность для конкретной угрозы безопасности в соответствие с таблицей, приведенной в методике определения актуальных угроз.

Написание приложения

Среда разработки

Для написания приложения использовалась интегрированная среда разработки программного обеспечения **Microsoft Visual Studio** обеспечивающая поддержку языка C# и .NET Framework 4.0, которая позволяет разрабатывать приложения используя технологию Windows Forms, обеспечивающую создание удобного пользовательского инерфейса.

Технология Windows Forms использует событийно ориентированную парадигму. Выполнение программы задается действиями пользователя, событиями операционной системы и других программ. В настоящем приложении пользователю предлагается выполнить последовательное заполнение форм для последующего формирования документов.

Общие сведения об объектной модели Word

В Word существует множество объектов для взаимодействия. Все объекты Word представляются в иерархии, вверху которой находится объект Application, который представляет текущий экземпляр Word. Объект Application является родителем для следующих объектов: Range, Selection, Document, Bookmark. Каждый из объектов имеет набор методов и свойств, через которые можно получить доступ для управления и взаимодействия с объектом.

На рисунке показано множество объектов в иерархии объектной модели Word[16]:

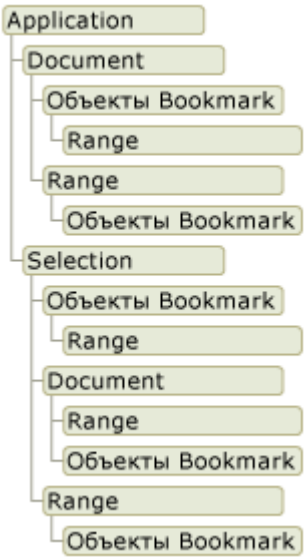

Рисунок 10

Объекты Document и Selection содержат объекты Range и Bookmark, объект Bookmark в свою очередь содержит объект Range. Перекрытие существует, поскольку существует множество способов доступа к одному и тому же типу объекта. Например, форматирование применяется к объекту Range; но может понадобиться получить доступ к объектам в диапазоне текущего выбора, конкретного параграфа, раздела или всего документа.

Для решаемой программной задачи, в основе которой лежит задача формирования документа на основе шаблона, рассмотрим объекты верхнего уровня и способы их взаимодействия друг с другом. Это следующие пять объектов:

- объект приложения; (Application)
- объект документа; (Document)
- объект выделенной области; (Selection)
- объект диапазона; (Range)
- объект закладки. (Bookmark)

Объект приложения

Объект Application представляет приложение Word и является родительским для всех других объектов. Создать объект Application – значит запустить Word. Его свойства и методы можно использовать для управления средой Word. Для запуска Word необходимо добавить ссылку на библиотеку Microsoft Word 11.0 Object Library в проект.

При создании объекта Application word запускается в скрытом режиме (невидимом окне) и закрывается после завершения процедуры его создания.

Объект документа

Объект Microsoft.Office.Interop.Word.Document является наследником объекта Application и основой для программирования в Word. Он представляет документ и все его содержимое. При открытии документа или создании нового документа создается новый объект Microsoft.Office.Interop.Word.Document, который добавляется в коллекцию Documents объекта Application. Документ, в котором находится фокус, называется активным документом. Он представляется свойством ActiveDocument объекта Application.

Создание, открытие, сохранение и другие операции осуществляются с помощью объекта Document.

Объект выбора

После того, как приложение запущено, открыт документ, обычно выполняется редактирование документа в нужном месте. Для этого используются объекты Selection, Range и Bookmark.

Объект Selection представляет область, выбранную в текущий момент, данный объект в документе может быть только один. Объект создается автоматически при запуске Word. Если ничего не выделено, то объект представляет область в которой находится указатель(точку вставки).

При выполнении операции в пользовательском интерфейсе машинного слова, как bolding текст выбран или выделите текст, а затем примените форматирование. Объект Selection всегда присутствует в документе. Кроме того, объект выбор может охватывать несколько разделенных блоков текста.

Объект Range

Объект Range представляет непрерывную область документа и задается положениями начального и конечного символов. Нет ограничения на количество объектов Range. Можно задавать несколько объектов Range в одном документе. Объект Range имеет следующие характеристики:

- Объект диапазона может представлять собой одну точку вставки, диапазон текста или весь документ.
- Он может включать непечатные символы, например пробелы, символы табуляции и метки параграфов.
- Он может представлять собой область текущего выделения или область за пределами текущего выделения.
- Этот объект невидим в документе, в отличие от выделения, которое видимо всегда.

- Он не сохраняется вместе с документом и существует только во время выполнения кода.
- Диапазон можно задать только программно (в отличие от объека Selection, который может быть задан с помощью пользовательского интерфейса).

При вставке текста в конец диапазона Word автоматически расширяет диапазон на размер вставленного текста.

Объект закладки

Объект Microsoft.Office.Interop.Word.Bookmark представляет непрерывную область документа с начальной и конечной позициями. Закладки можно использовать для отметки некоего расположения в документе или в качестве контейнера для текста в документе. Объект Microsoft.Office.Interop.Word.Bookmark может состоять из одной точки вставки или быть размером в весь документ. Объект Microsoft.Office.Interop.Word.Bookmark имеет следующие характеристики, отличающие его от объекта Range:

- Имена закладкам можно давать во время разработки.
- Объекты Microsoft.Office.Interop.Word.Bookmark сохраняются с документом, т.е. они не удаляются при остановке выполнения кода или при закрытии документа.
- Закладки можно скрывать или делать видимыми, устанавливая для свойства ShowBookmarks объекта View соответствующее значение **false** или **true**.

Основные алгоритмы

Для построения программы используется объекты класса Form.

Пространство имен: System.Windows.Forms

Сборка**:** System.Windows.Forms (в System.Windows.Forms.dll)

```
[ComVisibleAttribute(true)]
[ClassInterfaceAttribute(ClassInterfaceType.AutoDispatch)]
public class Form : ContainerControl
```

Каждый объект представляет окно или диалоговое окно, которое составляет пользовательский интерфейс приложения.

Программа представляет из себя совокупность объектов класса Form.

В процессе разработки приложения предполагает добавление множества элементов управления на формы, обеспечивающие графический интерфейс пользователя

Элементы управления — это объекты, которые находятся внутри объектов формы. Каждый тип элемента управления имеет собственный набор свойств, методов и событий, соответствующих определенному назначению. С элементами управления можно работать в конструкторе или добавлять их динамически во время выполнения с помощью кода.

Рассмотрим свойство Tag класса Forms, которое получает или задает объект содержащий данные элемента управления

Свойству Tag можно назначить любой тип, производный от класса Object. Если свойство Tag настроено с помощью конструктора Windows Forms, то можно назначить только текст.

В разработанной программной среде свойство Tag каждого объекта Form позволяет однозначно идентифицировать объект и используется для взаимодействия объектов в ходе выполнения программы.

В программе свойству Tag каждого объекта Form присваивается целочисленное значение служащие идентификатором объекта.

Объекты класса Form образуют древовидную структуру. Корневой элемент – форма First, с которой начитается выполнение программы.

Для навигации по формам и организации информационных потоков между элементами управления форм разработан *класс навигации.*

В *классе навигации* реализованы два метода *Search* и *FindRoot.*

FindRoot – метод, нахождения корня дерева из любого узла.

Search – метод, осуществляющий поиск в глубину по дереву элементов класса Form, из корневого элемента.

static public Form search(Form root, Int32 key)

root – Узел дерева для начала поиска в глубину

key – целочисленный параметр, идентификатор искомого узла

static public Form *FindRoot* (Form node)

node – любой узел дерева

Интерфейс программы для конечного пользователя представлен в виде анкеты. После заполнения которой формируются документы в формате DOCX для хранения электронных документов пакетов офисных приложений — в данном случае, Microsoft Office Word.

Word запускается отдельным приложением, которое должно быть установелено на компьютере, класс просто управляет им через интерфейс Word Interoperability, в проекте должна быть ссылка на Microsoft.Office.Interop.Word, соотвествующая библиотека .dll должна быть в папке с программой, - класс позволяет создать новый документ по шаблону, произвести поиск и замену строк (одно вхождение или все), изменить видимость документа, закрыть документ

Два реализованных в программе класса - WordDocument и WordSelection (просто часть документа, обертка над Range), реализующие описанные приемы, эти классы используют шаблон Фасад.

Итак, задача получить документ Word с добавлением данных из кода C#.

Шаблоны

Шаблоны Word — это файлы, содержащие стили, структуру, параметры страниц и др., на основе которых можно создавать новые документы.

Соответственно большую часть сложного оформления можно вынести в шаблоны и из кода открывать шаблон и вставлять данные в нужные места. Шаблон в формате dot создается заранее в Microsoft Office Word.

Для связи с ним используется механизм COM Interoperability (сокращенно Interop), то есть запускается отдельный exe-процесс для Microsoft Office Word и управляется через интерфейсы, находящиеся в библиотеках, поставляемых вместе с Microsoft Office.

При разработке решений Word в Visual Studio выполняется взаимодействие с объектной моделью Word. Эта объектная модель состоит из классов и интерфейсов, которые предоставляются в основной сборке взаимодействия для Word и задаются в пространстве имен Microsoft.Office.Interop.Word.

Укажем ссылки на соответствующие библиотеки:

```
using Word = Microsoft.Office.Interop.Word;
using System.Reflection;
```

Рассмотрим два объекта объектной модели Word: Application и Document. Переменные для них объявим через интерфейсы.

```
Word._Application application;
Word._Document document;
```

Почти все функции Word требуют объектных параметров, заранее создадим несколько оберток

```
Object missingObj = System.Reflection.Missing.Value;
Object trueObj = true;
Object falseObj = false;
```

Запустим Word и откроем в нем шаблон, по известному пути:

```
public WordDocument(string templatePath, bool startVisible)
    {
            //создание объекта приложения
        _application = new Word.Application();
        // по имени файла создается путь к файлу
        _templatePathObj = templatePath;
        try
        {
           _document = _application.Documents.Add(ref  _templatePathObj, ref _missingObj, ref _missingObj, ref _missingObj);
        }
```

```
        catch (Exception error)
        {
            this.Close();
            throw error;
        }
        Visible = startVisible;
        // устанавливаем текущую позицию в начало документа
        SetSelectionToBegin();
    }
```

Удобный способ вставить текст в нужную часть Word-шаблона - использовать закладки. Закладки не надо искать, они невидимы и всегда имеют уникальное имя. Имея открытый документ Word можно получить диапазон-Range для закладки (bookmark).

```
Word.Range bookmarkRange = _document.Bookmarks.get_Item(ref bookmarkNameObj).Range;
```

Работа с таблицами.

Выбрать уже существующую таблицу внутри документа можно по ее порядковому номеру (начиная с 1 и начала документа) можно через интерфейс Tables. При этом мы получим объект типа Table.

```
Word.Table _table = _document.Tables[tableNumber];
```

Новая вставляется методом Tables.Add (предполагается что уже получен диапазон Range того места в документе, куда будет произведена вставка таблицы):

```
_table = _document.Tables.Add(_currentRange, numRows, numColumns, ref _missingObj, ref _missingObj);
```

Добавление строк к таблице:

```
_table.Rows.Add(ref _missingObj);
```

Имея таблицу мы можем получить диапазон для конкретной ячейки по номеру строки/колонки через интерфейс Cell:

```
_currentRange = _table.Cell(rowIndex, columnIndex).Range;
```

Заключение

В результате выполнения поставленных задач было разработано приложение, позволяющие сформировать модель угроз и техническое задание для информационной системы, обрабатывающей персональные данные. Предложена реализация метода нахождения качественных характеристик безопасности для угроз информационной системы. Тестирование программы показало значительное совпадение сформированных документов с уже имеющимися и работающими техническими заданиями и моделями угроз. Работа имеет внедрение в рамках задачи построения системы защиты персональных данных для Конструкторско-технологический института вычислительной техники Сибирского отделения Российской академии наук, сотрудники которого были привлечены для работы с разработанным приложением. Для указанного института были сформированы документы, отражающие требования для построения системы защиты.

Список сокращений и условных обозначений

ИСПДн	Информационная система персональных данных
ОС	Операционная система
ПДн	Персональные данные
СЗИ	Система защиты информации
ФСТЭК	Федеральная служба по техническому и экспортному контролю

Список использованных источников и литературы

1) Федеральный закон Российской Федерации от 27 июля 2006 г. №152-ФЗ «О персональных данных».
2) «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных». Утверждена Заместителем директора ФСТЭК России 15 февраля 2008 года.
3) «Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации». Утверждена руководством 8 Центра ФСБ России 21 февраля 2008 года. № 149/54-144.
4) Приказ 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.
5) Постановление Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных";
6) Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России, 2008 год Режим доступа: http://fstec.ru/normativnye-i-metodicheskie-dokumenty-tzi/114-deyatelnost/tekushchaya/tekhnicheskaya-zashchita-informatsii/normativnye-i-metodicheskie-dokumenty/spetsialnye-normativnye-dokumenty/380-metodika-opredeleniya-aktualnykh-ugroz-bezopasnosti-personalnykh-dannykh-pri-ikh-obrabotke-v-informatsionnykh-sistemakh-personalnykh-dannykh-fstek-rossii-2008-god (дата обращения 07.04.2014).
7) Т. Саати Принятие решений. Метод анализа иерархий. М.: Радио и Связь, 1993.
8) Попов, Э.В. Экспертные системы: Решение неформализованных задач в диалоге с ЭВМ; М.: Наука - Москва, 1987. - 288 с
9) Кофман А. Введение в теорию нечётких множеств. – М., Радио и связь, 1982, 432 с
10) Борисов А.Н., Крумберг О.А., Федоров И.П. Принятие решений на основе нечетких моделей. Примеры использования (1990), 184 с

11) Базы данных интеллектуальная обработка информации 2-е издание/ В.В. Корнеев, А.Ф. Гареев, С.В. Васюткин, В.В. Райх, 2-е изд., М.:Молгачева С.В., Издательство Нолидж, 2001. - 496 с
12) May, Kenneth Q.: Intransitivity, Utility, and the Aggregation of Preference Patterns, Econometrica, vol. 22, no. 1, January 1954.
13) Грибунин В. Г. Комплексная система защиты информации на предприятии: учеб.пособие для студ. высш. учеб. заведений /В. Г. Грибунин, В.В.Чудовский. — М. : Издательский центр≪Академия≫, 2009. — 416 с
14) Функция принадлежности и методы ее построения [Электронный ресурс].Режим доступа:http://fuzzy-group.narod.ru/files/Fuzzy_Modeling/Lection03.The.membership.function.pdf(дата обращения 07.04.2014).
15) Ротштейн А. П. Медицинская диагностика на нечеткой логике. – Винница: Континент-Прим, 1996, 132 с.
16) Word Object Model Overview. [Электронный ресурс]. Режим доступа:http://msdn.microsoft.com/ru-ru/library/kw65a0we.aspx

Приложение 1.

1) Федеральный закон Российской Федерации от 27 июля 2006 г. №152-ФЗ «О персональных данных».
2) «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных». Утверждена Заместителем директора ФСТЭК России 14 февраля 2008 года.
3) «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных». Утверждена Заместителем директора ФСТЭК России 15 февраля 2008 года.
4) «Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации». Утверждена руководством 8 Центра ФСБ России 21 февраля 2008 года. № 149/54-144.
5) «Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных», ФСБ России, № 149/6/6-622, 2008.
6) Постановление Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных";
7) Методический документ “Меры защиты информации в государственных информационных системах” (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.)
8) Приказ 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.
9) Постановление Правительства РФ от 21.03.2012 N 211 (ред. от 20.07.2013) "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами".