МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение высшего образования

«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Кафедра Информационных технологий и систем безопасности

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

(дипломная работа)

На тему «Разработка программного средства для автоматизированного создания частной модели угроз в ИСПДн»

Исполнитель Абрамов Виктор Александрович
(фамилия, имя, отчество)

Руководитель Богданов Павел Юрьевич
(фамилия, имя, отчество)

«К защите допускаю»

Заведующий кафедрой

(подпись)

доктор технических наук, профессор,
(ученая степень, ученое звание)

Бурлов Вячеслав Георгиевич
(фамилия, имя, отчество)

«17» февраля 2017 г.

Санкт–Петербург

2017

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение высшего образования

«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Кафедра Информационных технологий и систем безопасности

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

(дипломная работа)

На тему«Разработка программного средства для автоматизированного создания частной модели угроз в ИСПДн»

Исполнитель Абрамов Виктор Александрович
(фамилия,имя,отчество)

Руководитель Богданов Павел Юрьевич
(фамилия, имя, отчество)

«Кзащитедопускаю»

Заведующийкафедрой_____

(подпись)

доктор технических наук, профессор,
(ученаястепень,ученое звание)

Бурлов Вячеслав Георгиевич
(фамилия,имя,отчество)

««»20г.

Санкт–Петербург

2017

РЕФЕРАТ

Дипломная работа: 82с., 17 рис., 2 табл., 2 приложения, 30 источников литературы.

ЧАСТНАЯ МОДЕЛЬ УГРОЗ, ПЕРСОНАЛЬНЫЕ ДАННЫЕ, ИНФОРМАЦИОННАЯ СИСТЕМА ПЕРСОНАЛЬНЫХ ДАННЫХ, АЛГОРИТМ СОЗДАНИЯ МОДЕЛИ УГРОЗ, РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, АВТОМАТИЗАЦИЯ.

Объект исследования: частная модель угроз

Предмет исследования: автоматизация создания частных моделей угроз

Цель работы: автоматизация процесса создания частной модели угроз и минимизация ошибок, связанных с человеческим фактором.

В дипломной работе проводится анализ руководящих документов по созданию моделей угроз и исследования алгоритма их разработки. Выделяются особенности каждого этапа, и модернизируется алгоритм для использования в программном обеспечении.

Разработано программное обеспечение на языке программирования Delphi.

Внесено определенное количество подготовленных ответов для снижения человеческих ошибок при создании частных моделей угроз. Создан автозаполняющийся шаблон результирующих документов.

Представленое в данной работе программное обеспечение позволяет сократить временные затраты на создание частных моделей угроз и сократить недочеты при разработке и оформлении итоговых документов.

«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

КафедраИнформационных технологий и систем безопасности

«УТВЕРЖДАЮ»
Заведующий кафедрой
_____ Бурлов Вячеслав Георгиевич
(подпись) (фамилия, имя,отчество)

« _ »_____2017 года

Задание
на выпускную квалификационную работу

студенту Абрамову Виктору Александровичу
(фамилия, имя, отчество)

1. ТемаРазработка программного средства для автоматизированного создания частной модели угроз в ИСПДн
закреплена приказом ректора Университета от «___» _____2017 года,№ ____
2. Срок сдачи законченной работы «___» _____2017 года

3.Исходные данные к выпускной квалификационнойработе:
«Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных»
«Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных»
«Положение о методах и способах защиты информации в информационных системах персональных данных»

3. Перечень вопросов, подлежащих разработке (краткое содержание работы(проекта):
— Введение. Актуальность темы, цели и задачи выпускной квалификационнойработы.
— Глава1.Анализ руководящих документов
(наименование главы)
— Глава2.Исследование и модификация алгоритма создания частной модели угроз в ИСПДн
(наименование главы)
— Глава3.Разработка программного средства на базе алгоритма для автоматизированного создания частной модели угроз
— Глава4.Безопасность жизнедеятельности
(наименование главы)
— Заключение. Выводы по работе. Практическиерекомендации.

4.Перечень материалов, представляемых кзащите:

— Пояснительнаязаписка;

5.Дата выдачизадания:«_____»_____2017 года
Руководитель выпускной квалификационной работы
старший преподаватель Богданов Павел Юрьевич _____
(должность, ученая степень, ученое звание, фамилия,имя,отчество) (подпись)
Задание принял кисполнению «_____»_____2017 года

СтудентАбрамов Виктор Александрович, ИБ-С11-2 _____
(фамилия, имя, отчество,учебнаягруппа) (подпись)

Оглавление:

Сокращения

АРМ – автоматизированное рабочее место;

АС – автоматизированная система;

АВС – антивирусные средства;

ВП – выделенное помещение;

ВТСС– вспомогательные технические средства и системы;

ИСПДн - информационная система персональных данных;

КЗ – контролируемая зона;

МУ –модель угроз;

НДВ – недекларированные возможности;

НСД – несанкционированный доступ;

ОС – операционная система;

ПДн – персональные данные;

ПМВ – программно-математическое воздействие;

ПО – программное обеспечение;

ПЭВМ– персональная электронно-вычислительная машина;

САЗ – система анализа защищенности;

СВТ – средства вычислительной техники;

СЗИ – средства защиты информации;

СЗПДн– система (подсистема) защиты персональных данных:

СОВ – система обнаружения вторжений;

СУБД– система управления базами данных;

УБПДн– угрозы безопасности персональным данным.

Введение.

В настоящее время информация представляет собой очень ценный ресурс. Миллионы гигабайт данных каждый день обрабатываются всевозможными ИС, в том числе и персональные данные людей. В повседневной жизни человека сохранность информации об его жизни зависит от него самого. Но совсем другая ситуация, когда мы обязаны предоставить данные о себе в соответствии с законом третьему лицу. Тогда вся защита персональных данных кладется уже на владельца ИСПДн, вследствие чего защита информации в процессе ее сбора, хранения, обработки и передачи приобретает исключительное значение. Безопасность информации – состояние защищенности информации при ее получении, обработке, хранении, передаче и использовании от различного вида угроз. Но для того, чтобы обеспечить должный уровень защиты, необходимо обладать необходимыми данными о возможностях ИСПДн и возможных угрозах. Именно для этого и создается частная модель угроз.Без частной модели угроз невозможно построить адекватную систему защиты информации, обеспечивающую безопасность персональных данных. В ходе разработки частной модели, к сожалению, возникает множество проблем и ошибок, связанных с человеческим фактором:

— отсутствие необходимых для проектирования выводов.

— отсутствие понимания структуры документа;

— рассматриваются не все угрозы, связанные с особенностями используемых технологий.

— отсутствие перечней нормативных правовых актов

— использование при моделировании угроз безопасности информации устаревшей нормативной правовой базы.

Именно поэтому целью данной выпускной квалификационной работы является автоматизация процесса создания частной модели угроз и минимизация ошибок, связанных с человеческим фактором. Для достижения

поставленной цели было решено разработать программное средство для автоматизированного создания частной модели угроз в ИСПДн.

Разрабатываемое программное средство должно решить данные проблемы и уменьшить временные затраты на разработку частной модели угроз за счет автоматизации процессов. Для достижения заданной цели, были поставлены следующие задачи:

— Анализ руководящих документов

— Исследование и реализация алгоритма создания частной модели угроз в ИСПДн

— Разработка программного средства на базе алгоритма для автоматизированного создания частной модели угроз.

Структура данной работы определена целью и задачами разработки программного обеспечения. Работа состоит из введения, четырех глав, заключения, списка литературы и приложения. Во введение раскрыта актуальность и цель данной работы, поставлены задачи для решения существующих проблем в сфере персональных данных.

В первой главе рассматривается анализ предметной области и руководящих документов. Во второй главе подробно разобран алгоритм создания частной модели угроз, и проанализирована модификация его для использования в ПО. Третья глава посвящена техническому аспекту - описание разработанного приложения, анализ аналогов и рассмотрение возможностей ПО. В четвертой главе уделяется внимание анализу и рекомендациям по безопасному использованию программно-аппаратных комплексов.

В заключении подводятся итоги по данной выпускной квалификационной работе, формируются выводы и рекомендации. В приложении размещены листинги всех исполняемых модулей разработанного программного обеспечения.

1. Анализ руководящих документов

1.1Системный анализ предметной области

В Законе №152-ФЗ "О персональных данных" указано, что к персональным данным относится любая информация, при использовании которой можно достоверно определить физическое лицо (субъект ПДн), Этими сведениями являются, как и паспортные данные, медицинские, экономические, так и любая другая информация, владение которой может помочь установить личность человека.

Обеспечение защиты персональных данных является важной проблемой общества. Информация о личности всегда имела большую цену, но затем превратилась в один из самых дорогих товаров. Сведения о личности в руках злоумышленника может сильно навредить, как и организации, хранящей эти данные, так и самому человеку, которому они принадлежат. Именно поэтому так важно правильно и надежно хранить персональные данные.

Необходимость повышать защищенность персональных данных в первую очередь связана с увеличением технических возможностей по получению и передачи сведений о человеке. Степень развития информационных технологий дошла уже до того уровня, что самозащита личных данных самим человеком не способна обеспечить должный уровень сохранности при покушении на частную информацию. В текущее время, неподготовленный человек не может самостоятельно защитить себя от огромного количества всевозможных следящих приборов и технических устройств, которые круглосуточно собирают информацию.

В последнее время возросло количество инцидентов и правонарушений, связанных с распространением и незаконным использованием персональных данных. В первую очередь это связано с тем, что ежегодно разрабатывается множество средств для ускорения сбора сведений о людях и для всевозможной интеграции в массовых коммуникациях и социальные сети. Также обеспечивать максимальную защиту мешает то, что не все сведения о себе человек считает

важными, но для злоумышленника любые данные о конкретной личности могут стать очень ценными.

В наше время практически не существует какой-либо компании без обработки данных о пользователях или сотрудниках. Кража, продажа или даже просто потеря персональных данных приводит к огромному материальному ущербу, а иногда и к полному прекращению функционирования компании.

Так как сведения о человеке обладают особой ценностью и значимостью, а также заботясь о соблюдении конституционных прав человека, государство имеет право требовать от компаний и юридических лиц устанавливать защиту на данные, полученными или обрабатываемыми этими организациями[1]. Обеспечение безопасности личных данных человека основывается на Конституции РФ, Федерального закона РФ N 152-ФЗ «О персональных данных» и других федеральных законов, содержащих руководство по обеспечению защищенности персональных данных.

Если после обработки и модернизации персональные данные очень сложно определить, какому именно конкретному лицу они соответствуют, то тогда данные принимают статус обезличенных. Такие данные не требуют специальных мер и действий в обеспечении безопасности, так как уже не принадлежат определенному лицу. Также человек имеет право сделать свои данные общедоступными - это данные, которые обычно используются для адресных книг, энциклопедий и справочников. Для этого необходимо письменное соглашение и затем личные данные владельца попадают в категорию данных, которые могут свободно распространяться.

Оператор персональных данных - это государственная организация, компания, или человек, обрабатывающий персональные данные, и также определяющий условия и цель обработки[2]. Следуя из этого, оператор обязан обеспечивать защищенность персональных данных.

Для этого необходимо:

— устраивать мероприятия, необходимые для профилактики и предупреждения возможные опасностей, связанных с несанкционированным доступом;

— своевременно обнаруживать инциденты НСД к персональным сведениям;

— не допускать вредоносных влияний и воздействий на систему обработки и хранения ПДн;

— своевременно восстанавливать и модернизировать данные в случае получения к ним несанкционированного доступа;

— обеспечивать постоянный контроль над работоспособностью и защищенностью информационной системы обработки ПДн.

Информационные системы персональных данных представляют собой совокупность программных и информационных систем, основными из которых являются:

— ПДн, содержащиеся в базах данных, как совокупность информации и ее источников, используемых в информационных системах;

— информационные технологии, как совокупность приемов, способов и методов применения средств вычислительной техники при обработке ПДн;

— технические средства, осуществляющие обработку ПДн, под которыми понимаются средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (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, прикладное программное обеспечение и т.п.);

— средства защиты информации;

— вспомогательные технические средства и системы, к которым относятся средства и системы коммуникации, не предназначенные для обработки ПДн, но размещенные в помещениях, в которых расположены ИСПДн.

Для основных типов информационных систем созданы типовые модели угроз безопасности ПДн, описывающие последствия и реализации угроз. Всего таких моделей существует шесть вариантов, и все они описаны в документе ФСТЭК «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных»:

— типовая модель угроз безопасности ПДн, обрабатываемых в автоматизированных рабочих местах, не имеющих подключения к сетям общего пользования и (или) сетям международного информационного обмена;

— типовая модель угроз безопасности ПДн, обрабатываемых в автоматизированных рабочих местах, имеющих подключения к сетям общего пользования и (или) сетям международного информационного обмена;

— типовая модель угроз безопасности ПДн, обрабатываемых в локальных ИСПДн, не имеющих подключения к сетям общего пользования и (или) сетям международного информационного обмена;

— типовая модель угроз безопасности ПДн, обрабатываемых в локальных ИСПДн, имеющих подключения к сетям общего пользования и (или) сетям международного информационного обмена;

— типовая модель угроз безопасности ПДн, обрабатываемых в распределенных ИСПДн, не имеющих подключения к сетям общего пользования и (или) сетям международного информационного обмена;

— типовая модель угроз безопасности ПДн, обрабатываемых в распределенных ИСПДн, имеющих подключения к сетям общего пользования и (или) сетям международного информационного обмена.

На основе базовой модели угроз и в соответствии с нормативным документом ФСТЭК «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», создаются частные модели угроз в отношении конкретных ИСПДн. В ходе такой разработки составляется список реальных угроз в отношении конкретных информационных систем.Используя составленный перечень актуальных угроз и уровень исходной защищенности, формулируются конкретные организационно- технические требования по защите информационных систем от утечки данных по техническим каналам, от несанкционированного доступа [3]. Также осуществляется выбор программных и технических средств защиты информации, которые могут быть использованы при создании и дальнейшей эксплуатации ИСПДн.

Модель угроз информационной безопасности – это описание существующих угроз ИБ, их актуальности, возможности реализации и последствий[4].Стандарт СТО БР ИББС – 1.0-2010 определяет модель угроз информационной безопасности следующим образом: это «описание источников угроз ИБ; методов реализации угроз ИБ; объектов, пригодных для реализации угроз ИБ; уязвимостей, используемых источниками угроз ИБ; типов возможных потерь (например, нарушение доступности, целостности или конфиденциальности информационных активов); масштабов потенциального ущерба».

Адекватные модели угроз информационной безопасности служат для выявления существующих угроз, разработки мер противодействия угрозам информационной безопасности, и оптимизации затрат на защиту (с акцентом на её текущие угрозы):

Рисунок 1 – Меры защиты от угроз

В модели должны учитываться все актуальные угрозы на всех стадиях их жизненного цикла.(Рисунок 1)

Типовая модель угроз базируется на четырех аспектах информационной безопасности[5]:

— Безопасность персональных данных при их обработке в ИСПДн контролируется и регулируется системой защиты информации.

— При формировании модели угроз учитываются как угрозы, реализация которых нарушает безопасность персональных данных (прямая угроза), так и угрозы создания условий для возникновения прямых и/или косвенных угроз (косвенные угрозы).

— Личные данные обрабатываются и хранятся в информационной системе с использованием специфических информационных технологий и средств генерации различных уровней объектов защиты, атаки на которые создают прямые или косвенные угрозы для защищенной информации.

— Системы защиты персональных данных не могут обеспечить защиту информации от ведения деятельности, осуществляемой в рамках полномочий,

предоставленных субъекту действия (например, системы защиты персональных данных не могут защитить информацию от разглашения лицами, которым были предоставлено право доступа к этой информации).

Различные информационные системы, а также объекты единой информационной системы могут иметь разные диапазоны угроз, определяемые особенностями конкретной информационной системы и ее объектов, а также характером возможных действий источником угрозы.Модели угроз основаны на постоянно изменяющихся данных, и поэтому их следует регулярно пересматривать и обновлять.Модель угроз безопасности персональных данных необходима для определения требований к системе защиты. Без модели угроз невозможно построить адекватную (с точки зрения денежных затрат) систему защиты информации, которая обеспечивает безопасность персональных данных.

Система безопасности включает в себя защиту информации только для актуальных угроз.В соответствии с пунктом 2 статьи 19ФЗ «О персональных данных» обеспечение безопасности персональных данных достигается, в частности определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных, т.е. разработкой модели угроз.Безопасность персональных данных при их обработке в информационных системах обеспечивается системой защиты персональных данных, которая включает в себя меры для измерения и защиты средств информации, а также используемые в информационной системе информационные технологии. Технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации[6].

В соответствии с определением необходимым условием разработки системы защиты персональных данных является формирование модели угроз безопасности персональных данных.Модель угроз формируется и утверждается

оператором в соответствии с методическими документами, разработанными в соответствии с пунктом 2 постановления Правительства Российской Федерации от 17 ноября 2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных».

Модель угроз может быть пересмотрена:

— по решению оператора на основе их периодического обзора и оценки угроз безопасности персональных данных с учетом характеристик и (или) изменения в той или иной информационной системы;

— по результатам мероприятий по контролю за выполнением требований к обеспечению безопасности персональных данных при их обработке в информационной системе.

1.2Руководящие документы

В начале любого исследования необходимо правильно выбрать опорные данные и руководящие документы для решения поставленных задач.В настоящее время ФСТЭК предоставляет несколько документов связанных с обработкой ПД. Из них было выбрано:

— «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных»

— «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных»

— «Положение о методах и способах защиты информации в информационных системах персональных данных»

Данные документы находятся в свободном доступе на официальном портале ФСТЭК России.В «Методике определения актуальных угроз» главным образом рассматривается подход к рассмотрению угроз безопасности персональных данных и созданию частных моделей угроз.Следовательно, «Методика» должна использоваться для определения угроз персональных

данных в государственных структурах, а также всеми организациями, осуществляющих защиту персональных данных. Единственное ограничение – невозможность использования для оценки угроз безопасности информации, являющейся государственной тайной. В «Методике определения угроз» также не рассматриваются вопросы обеспечения защиты данных, располагающихся за контуром информационной системы защиты (личные АРМ, телефоны, коммуникаторы)

Одним из главных положений является указание уделять особое внимание оценке антропогенных угроз, связанных с НСД к объектам обработки персональных данных, а также воздействиям вредоносных средств на систему обработки и защиты ПДн. Из нововведений в «Методике» стоит отметить размещения требований по оценке способностей нарушителя и внешних угроз – конкурирующие организации, внешние субъекты, спец. службы иных государств.

В «Положение о методах и способах защиты информации в информационных системах персональных данных» указаны сведения и рекомендации о возможностях защиты информации в ИСПДн. Среди них можно выделить следующие методы:

— система допуска лиц к информационным ресурсам
— регистрация и контроль действий пользователей
— контроль и защита носителей персональных данных
— ограничения доступа в помещения с техническими ресурсами ИСПДн.

«Базовая модель угроз безопасности персональных данных» содержит обобщенный список угроз безопасности персональных данных при их обработке в ИСПДн. Угрозы, приведенные в базовой модели, устарели и далеки от совершенства. Тем не менее, за неимением лучшего документа приходится пользоваться текущей версией «Базовой модели».

Разработка модели угроз по данным документам может производиться сотрудниками, ответственными за защиту ПД в компании, а при необходимости возможно использование сторонних организаций, специализирующихся на осуществлении защиты персональных данных[7]. Чаще всего, для соблюдения экономических и организационных составляющих, руководство компании настаивает на согласовании разработанной модели угроз в ФСТЭК. Но не стоит забывать, что согласование моделей угроз - процедура необязательная. На данный момент, в П.7 ст.19 152-ФЗ сообщается, что частные МУ нужно согласовывать, если в них имеются «дополнительные угрозы безопасности», которые рассматриваются в Постановлении Правительства от 18.10.2012 №940. Но если опираться на статистику ответов ФСТЭК и их публичные доклады, даже при согласовании моделей, большая часть МУ содержит множество ошибок, связанных с непониманием и некомпетентностью сотрудников, выполняющих разработку модели угроз.

Типичные ошибки при согласовании моделей угроз в ФСТЭК:

1. Отсутствие описание структурно-функциональных характеристик информационной системы. ФСТЭК хочет убедиться, что учтены все особенности защищаемой системы. Для решения этой проблемы необходимо прикладывать паспорт (описание) информационной системы, состоящий из:
    а. структуры ИС
    б. состава ИС
    в. взаимосвязи между сегментами ИС
    г. взаимосвязи с другими ИС и ИТКС
    д. условий функционирования ИС.

2. Рассмотрение не всех угроз, связанных с особенностями используемых технологий.

3. Неверное определениеобъектов и методов защиты.

Следующие четыре ошибки связаны с терминологией “угроза”:

4. Не проводится анализ возможных источников угроз (внешние злоумышленники, закладное оборудование).

5. Не составляется модель нарушителя, при явных угрозах извне.

6. Не учитываются уязвимости, присутствующие в системе.

7. Неверное определение способов реализации угроз.

Остальные ошибки связаны с несоблюдением мер по контролю и разработке модели угроз:

8. При изменении компонентов ИС не производится пересмотр модели угроз.

9. Использование при моделировании угроз безопасности устаревшей нормативной правовой базы.

10. Отсутствиеперечня технического и правовы актов о составе ИСПДн и её компонентов.

11. Отсутствие единого перечня технической терминологии

Возможно, часть ошибок зависит от того, что имеется большая трудоемкость при применении методики определения угроз, и если раньше актуальность угроз напрямую зависела от исходно принятых мер защиты, то теперь исходные меры защиты влияют на потенциал нарушителя, который потом уже влияет на актуальность угрозы.В связи с этим расчеты моделей стали достаточно сложными для анализа оператором вручную, что становится фактически нереальным, либо нерентабельным экономически. Для решения этой проблемы было предложено разработать средство автоматизированного создания частной модели угроз в ИСПДн.

1.3Классификация угроз безопасности персональных данных

Угрозы безопасности - это сумма всех условий и факторов, создающих риск умышленного или случайного доступа к персональным данным, который в итоге может привести к разрушению, модификации, блокирование, копирование, распространение персональных данных, а также другая

незаконная деятельность при их обработке в информационной базе персональных данных[8].Возникновение таких угроз может быть связано со специальной деятельностью злоумышленников, так и с непреднамеренными действиями операторов ИСПДн. Угрозы безопасности реализуются двумя способами:

— через технические каналы утечки;

— путем несанкционированного доступа.

Обобщенная схема реализации канала угроз ПД показана на рисунке 2.

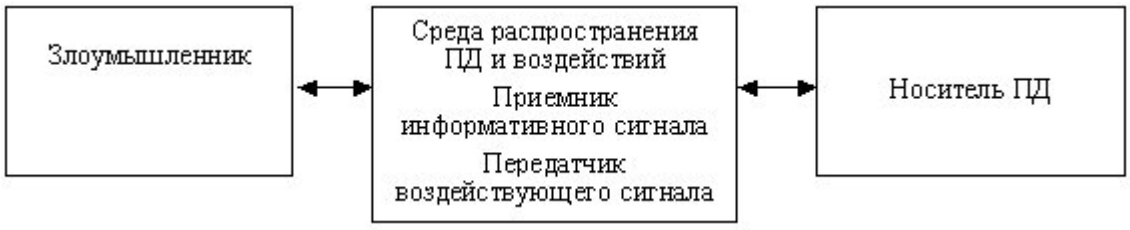


Рисунок 2 - Схема реализации канала угроз ПД.

Как правило, выделяют следующие угрозы за счет реализации технических каналов утечки[9]:

— угроза утечки речевой информации. На самом деле, злоумышленник перехватывает информации с использованием специальной аппаратуры в виде акустических, виброакустических волн и электромагнитного излучения, модулированный звуковой сигнал. Эти средства могут быть использованы в качестве различных видов электронных устройств, подключенных к каналам коммуникации или технических средств.

— угроза утечки видовой информации. В этом случае речь идет о прямом просмотре ПД в присутствии линии прямой видимости между средствами наблюдения и ПД носителя. В качестве средства мониторинга выступают системы с использованием оптических средств и видеозакладок;

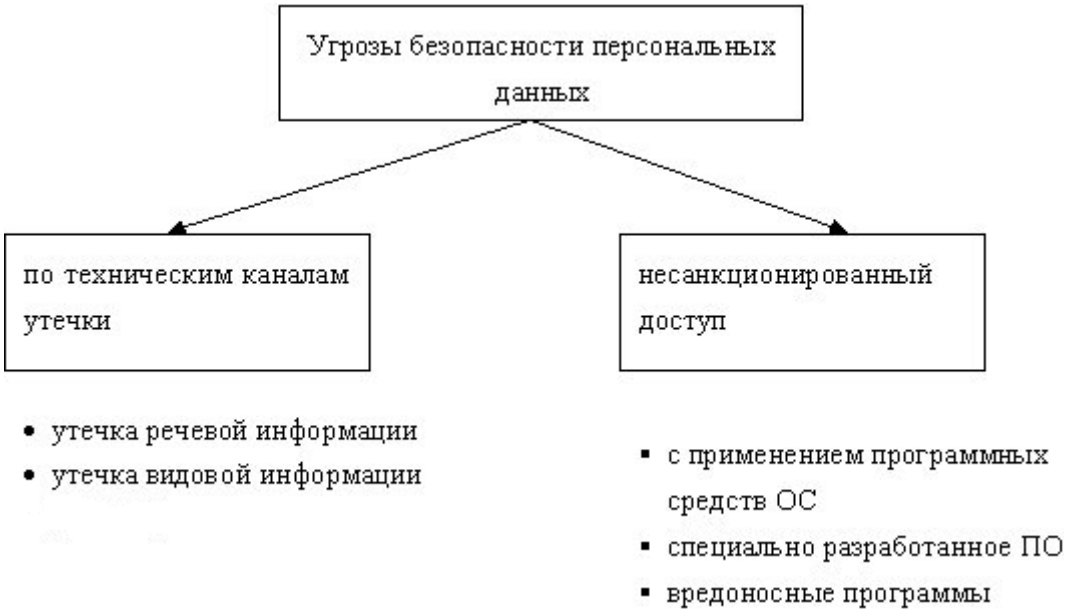


Рисунок 3 - Классификация угроз безопасности.

1.4Вывод по главе

В данной главе был выявлен перечень персональной информации, обрабатываемый в системе и критерии ИСПДн. Такжепроанализированы основные документы, связанные с обеспечением безопасности персональных данных. Были выбраны три руководящих документа для создания частной модели угроз ПДн и приведена их организационная структура. Также были рассмотрены наиболее частые ошибки при согласовании МУ в ФСТЭК, для того, чтобы при разработке программного обеспечения. Обозначена используемая классификация угроз безопасности.

2. Исследование и модификация алгоритма создания частной модели угроз в ИСПДн

2.1Алгоритм создания частной модели угроз

Изучив руководящие документы, был составлен общий алгоритм разработки частной модели угроз. Для корректого создания МУ необходимо выявление актуальных угроз, так как именно они будут влиять на устанавливаемые средства защиты информации. Алгоритм состоит из пяти пунктов:

— Определение исходной защищенности ИСПДн

— Получение списка всех возможных угроз

— Определение вероятности каждой угрозы

— Определение опасности каждой угрозы

— Определение актуальных угроз

Актуальной считается угроза, которая может быть реализована в ИСПДн и представляет опасность для ПДн. Для оценки возможности реализации угрозы применяются два показателя: уровень исходной защищенности ИСПДн и частота (вероятность) реализации рассматриваемой угрозы. Необходимо углубленный разбор каждого из пунктов алгоритма с целью их дальнейшего использования в программном обеспечении.Затем данный алгоритм будет модернизирован для использования в программном обеспечении для автоматизации создания частной модели.

2.1.1Определение исходной защищенности ИСПДн

Под уровнем исходной защищенности ИСПДн понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПДн, приведенных в таблице 1.

Таблица 1

Показатели исходной защищенности ИСПДн

Технические и эксплуатационные характеристики ИСПДн	Уровень защищенности		
	Высокий	Средний	Низкий
1. По территориальному размещению:			
распределеннаяИСПДн, которая охватывает несколько областей, краев, округов или государство в целом;	–	–	+
городскаяИСПДн, охватывающая не более одного населенного пункта (города, поселка);	–	–	+
корпоративная распределенная ИСПДн, охватывающая многие подразделения одной организации;	–	+	–
локальная (кампусная) ИСПДн, развернутая в пределах нескольких близко расположенных зданий;	–	+	–
локальнаяИСПДн, развернутая в пределах одного здания	+	–	–
2. По наличию соединения с сетями общего пользования:			
ИСПДн, имеющая многоточечный выход в сеть общего пользования;	–	–	+
ИСПДн, имеющая одноточечный выход в сеть общего пользования;	–	+	–
ИСПДн, физически отделенная от сети общего пользования	+	–	–

3. По встроенным (легальным) операциям с записями баз персональных данных:			
чтение, поиск;	+	–	–
запись, удаление, сортировка;	–	+	–
модификация, передача	–	–	+
4.По разграничению доступа к персональным данным:			
ИСПДн, к которой имеют доступ определенные перечнем сотрудники организации, являющейся владельцем ИСПДн, либо субъект ПДн;	–	+	–
ИСПДн, к которой имеют доступ все сотрудники организации, являющейся владельцем ИСПДн;	–	–	+
ИСПДн с открытым доступом	–	–	+
5. По наличию соединений с другими базами ПДн иных ИСПДн:			
интегрированная ИСПДн (организация использует несколько баз ПДнИСПДн, при этом организация не является владельцем всех используемых баз ПДн);	–	–	+
ИСПДн, в которой используется одна база ПДн, принадлежащая организации – владельцу данной ИСПДн	+	–	–
6. По уровню обобщения (обезличивания) ПДн:			
ИСПДн, в которой предоставляемые пользователю данные являются обезличенными (на уровне организации, отрасли, области,	+	–	–

региона и т.д.);			
ИСПДн, в которой данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации;	–	+	–
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, предоставляющая всю базу данныхсПДн;	–	–	+
ИСПДн, предоставляющая часть ПДн;	–	+	–
ИСПДн, не предоставляющая никакой информации.	+	–	–

Исходная степень защищенности определяется следующим образом:

— ИСПДн назначается высокий уровень, если не менее семидесяти процентов положительных решений по первой колонке (соответствуют уровню «высокий»), а также остальное - положительное решение по второй колонке (средний уровень защиты).

— ИСПДн назначается средний уровень, если не выполняются условия по первому пункту и не менее семидесяти процентов положительных решений соответствуют уровню, не ниже «среднего» (первая и вторая колонка), а остальные – низкому уровню защищенности(третья колонка).

— ИСПДн присваивается низкий уровень, если требования первого и второго пункта не выполняются,

При составлении перечня актуальных угроз безопасности ПДн каждой степени исходной защищенности ставится в соответствие числовой коэффициентY1, а именно:

0 – для высокой степени исходной защищенности;

5 – для средней степени исходной защищенности;

10 – для низкой степени исходной защищенности.

2.1.2Получение списка всех возможных угроз

В «Методике определения актуальных угроз» имеется пункт – «Наличие источника угрозы и уязвимого звена, которое может быть использовано для реализации угрозы, свидетельствует о наличии данной угрозы»[5] В связи с этим, сотрудники организации могут попадать под определение «внутренних нарушителей», а теоретическое наличие уязвимостей ПО может рассматриваться как целый класс угроз[10]. Следовательно, необходимо указать практически все возможные угрозы, связанные с обеспечением персональных данных. Этот пункт полностью кладется на оператора ПД.

2.1.3Определение вероятности каждой угрозы

Угрозы утечки акустической (речевой) информации

Для возникновения угрозы утечки речевой информации необходимо наличие функции голосового ввода или управления при обработке данных в ИСПДн.

Если в ИСПДнорганизации функции голосового ввода ПДн или функции воспроизведения ПДн акустическими средствами отсутствуют, то вероятность угрозы для всех типов ИСПДн - маловероятна.

Угрозы утечки видовой информации

Появление угрозы утечки видовой информации возможно при наличии возможности считывания информации с помощью оптических или электронных приборов с экранов мониторов и других средств воспроизведения видовой информации, входящих в состав ИСПДн[11].

Если в организации имеется контроль доступа в охраняемую зону, места операторов расположены таким образом, что практически устранен визуальный доступ к мониторам, а на окнах установлены средства защиты, то для всех типов ИСПДн вероятность угрозы – маловероятна. Средства защиты от утечки видовой информации необходимо установить, если в организации отсутствуют вышеуказанные меры защиты.

Угрозы несанкционированного доступа к информации

При возникновении угроз несанкционированного доступа к информации нарушается ее безопасность, а именно:

- конфиденциальность (копирование, неправомерное распространение);
- целостность (уничтожение, изменение);
- доступность (блокирование).

Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн

Кража ПЭВМ.

Кража подразумевает собой незаконное изъятие ПЭВМ путем неправомерного доступа внешними и внутренними злоумышленниками в контролируемую зону, где расположены элементы ИСПДн.

Если в организации введена защита доступа посторонних лиц в охраняемую зону, установлена система оповещения о нелегальном вторжении, установлены запирающие механизмы на первых и последних этажах здания, то для всех типов ИСПДн вероятность реализации угрозы – маловероятна.

Если у вас есть свободный доступ к контролируемой зоне посторонних лиц, вероятность угрозы должна быть пересмотрена или при необходимости должны быть приняты меры для предотвращения несанкционированного доступа посторонних лиц к контролируемой зоне.

Кража носителей информации

Угроза осуществляется путем НСД злоумышленниками к носителям персональных данных.

Если в организации введен контроль доступа в охраняемую зону, существует система контроля количества и состояния носителей в сейфе, то для всех типов ИСПДн вероятность реализации угрозы – маловероятна.

Если имеется свободный доступ к контролируемой зоне посторонних лиц, вероятность угрозы должна быть пересмотрена или при необходимости должны быть приняты меры для предотвращения несанкционированного доступа посторонних лиц к контролируемой зоне[12].

Кража ключей и атрибутов доступа

Угроза осуществляется путем неправомерного доступа нарушителями в помещения, отведенных для работы пользователей.

Если в компании имеется контроль доступа в охраняемую зону, установлена охранная система сигнализирования, двери оборудованы запирающими механизмами, установлены решетки на первых и последних этажах здания, организовано хранение ключей доступа в сейфе и введена политика «чистого стола», то для всех типов ИСПДн вероятность реализации угрозы – маловероятна

Если имеется неконтролируемый доступ к охраняемой зоне незарегистрированных лиц, оценка угрозы должна быть рассчитана, включая этот факт, или при необходимости должны быть приняты меры для

предотвращения несанкционированного доступа посторонних лиц к контролируемой зоне и получению ключей и атрибутов для входа.

Вывод из строя узлов ПЭВМ, каналов связи

Угроза осуществляется путем неконтролируемого доступа посторонних лиц в помещения, где расположены элементы ИСПДн и находятся каналы, обеспечивающие связь программно-аппаратных комплексов.

Если в организации введен контроль доступа в охраняемую зону, установлена охранная сигнализация, двери оборудованы запирающими механизмами, то для всех типов ИСПДн вероятность реализации угрозы – маловероятна.

При наличии свободного доступа в контролируемую зону посторонних лиц вероятность реализации угрозы должна быть пересмотрена или необходимо принять меры по пресечению НСД в контролируемую зону[13].

Несанкционированное отключение средств защиты

Угроза осуществляется путем доступа нарушителями в помещения, где расположены средства защиты ИСПДн.

Если в организации введен контроль доступа в контролируемую зону, установлена охранная сигнализация, двери и окна оборудованы запирающими механизмами, пользователи ИСПДн обладают информацией о правильном использовании системы обработки ПДн, то для всех типов ИСПДн вероятность реализации угрозы –маловероятна[14].

При наличии свободного доступа в охраняемую зону посторонних лиц вероятность угрозы должна учитывать этот факт, или необходимо принять меры по пресечению доступа в охраняемую зону и информированию пользователей о порядке работы в ИСПДн.

Недекларированныевозможности системного ПО для обработки персональных данных.

Недекларированные возможности – функциональность компьютерного оборудования, не указанная в соответствующей документации, использование которой приводит к нарушению конфиденциальности, целостности или доступности обрабатываемой информации[14].

Вероятность реализации угрозы повышается при:

— добавлении новых компонент в ИСПДн

— увеличение количества функциональных связей

— подключение к общей сети и/или внешней сети обмена.

В том случае, если в обработке персональных данных участвует программное обеспечение собственной разработки или стандартное программное обеспечение, модифицированное для нужд организации, необходимо увеличить значение вероятности угрозы[15]:

— для всех типов ИСПДн, кромеАвтономная ИС I типа, на порядок;

— для Распределенной ИС II типа на два порядка.

Для снижения вероятности угрозы необходимо получение сертификата на ПО собственной разработки в соответствии со стандартом сертификации программного обеспечения[16].

Угрозы преднамеренных действий внутренних нарушителей

Одной из угроз этого типа является вероятность доступа или модификация незарегистрированных лиц или операторов к персональным данным.

Угроза реализуется путем неправомерного доступа злоумышленников в помещения, где установлены элементыИСПДн и средства ее защиты, а такжеогранизована работа с ИСПДн операторов.

При наличии в организации системы контроля над помещением, охранной сигнализации, запорных механизмов на дверях и окнах, установленных ставнях на оконных проемах на этажах здания, то для всех типов ИСПДн вероятность реализации угрозы – маловероятна.

При наличии неправомерного доступа в охраняемую зону незарегистрированных лиц, вероятность реализации угрозы должна учитывать этот факт или же необходимо принять меры по пресечению несанкционированного доступа в охраняемую зону[17].

Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке.

Данная угроза реализуетсяиз-заошибок человеческого фактора пользователей ИСПДн, которые нарушают протоколы о неразглашении обрабатываемых персональных данных или не уведомлены о них[18].

В организации, где операторы осведомлены о порядке обработки персональных данных, а также подписано положение о конфиденциальности, вероятность угрозы для всех типов ИСПДн – низкая

Если пользователи не знакомы с положением о конфиденциальности или же на территории организации оно вовсе не подписано, то вероятность угрозы существенно возрастает. Необходимо принимать меры по снижению вероятности угрозы и срочному заполнению соответствующих документов

Угрозы несанкционированного доступа по каналам связи

В регламенте в «Типовой модели угроз безопасности персональных данных», к угрозам, реализуемым при использовании протоколов межсетевого взаимодействия, следует отнести:

— угроза «Анализ сетевого трафика» с перехватом исходящей из ИСПДн во внешние сети информации;

— угрозы сканирования, направленные на выявление типа или типов используемых операционных систем,открытых портов и служб, топологии сети, сетевых адресов рабочих станций ИСПДн, открытых соединений и др.;

— угрозы для обнаружения сетевых паролей;

— угрозы введения ложной маршрутной сети;

— угрозы подмены доверенного объекта в сети;

— угрозы введения ложного объекта в ИСПДн и внешние сети;

— угрозы типа «отказ в обслуживании»;

— угрозы для запуска удаленных приложений;

— угрозы внедрения по сети вредоносных программ.

— угроза «анализ сетевого трафика»

Эта угроза реализуется с помощью специальных программных приложений - анализаторов(sniffer), перехватывающей все пакеты на сетевом сегменте, и выделяющей среди них те, в которых передаются сведения, с помощью которых злоумышленник может заполучить данные операторов(идентификаторы, пароли)[19]. В ходе угрозы злоумышленник:

— изучает логику работы ИСПДн – целью является выявить однозначное соответствие событий, происходящих в системе, и команд, выполняемых операторов ИС, в момент возникновения этих событий. В будущем это может позволить злоумышленнику на основании соответствующих должностных инструкций получить преимущественные права на действия в системе или расширить свои полномочия в ней;

— захватывает поток передаваемых данных между компонентами сетевой операционной системы, с целью получения или генерации конфиденциальной или идентификационной информации (например, статических паролей пользователей для доступа удаленным серверам через FTP и протоколы TELNET, которые не предусматривают шифрование), ее замену, модификации и т. п.

Перехват за пределами контролируемой зоны

Если в организации обрабатываемые ПДн не передаются по сетям общего пользования и внешнего обмена, то вероятность реализации угрозы – маловероятна.

Во всех остальных случаях следует оценивать вероятность угрозы.

Перехват в пределах контролируемой зоны внешними нарушителями

Если в организации введен контроль доступа в охраняемую зону, установлена охранная сигнализация, двери оборудованы запирающими механизмами, установлены решетки на первых и последних этажах здания, то для всех типов ИСПДн вероятность реализации угрозы – маловероятна.

Если имеется вероятность проникновения в охраняемую зону незарегистрированных лиц, то вероятность угрозы должна быть перерассчитана или при необходимости нужно провести мероприятия, исключающие эту возможность[20].

Угроза «сканирование сети»

Суть процесса реализации угрозы заключается в передаче запросов сетевых сервисов хостам ИСПДн и анализ ответов от них. Цель – определение используемых служб, доступности сетевых портов и протоколов связи, законов формирования идентификатора соединения, идентификации активных сетевых услуг, выбора идентификаторов и паролей.

Если в организации обрабатываемые ПДн не отправляются по сетям общего пользования и внешнего обмена, то вероятность реализации угрозы – маловероятна.

Во всех других случаях должна быть оценена вероятность реализации угрозы.

Под вероятностью реализации угрозы понимается получаемый аналитическим методом показатель, указывающий вероятность реализации определенных угроз безопасности ПДн для данной ИСПДн в текущих условиях обстановки. Вводятся четыре словесные градации этого показателя:

маловероятно – нет никаких объективных предпосылок для реализации угрозы (например, угроза хищения носителей информации лицами, не имеющими законного доступа в помещение, где последние хранятся);

низкая вероятность – существуют предпосылки для реализации угроз, но принятые меры существенно препятствуют ее реализации (например, использованы необходимые средства защиты персональных данных);

средняя вероятность - объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны;

высокая вероятность - объективные предпосылки для реализации угрозы существуют, и меры по обеспечению безопасности ПДн не приняты.

При составлении перечня актуальных угроз безопасности ПДн каждой градации вероятности возникновения угрозы ставится в соответствие числовой коэффициентY2, а именно:

0 – для маловероятной угрозы;

2 – для низкой вероятности угрозы;

5 – для средней вероятности угрозы;

10 – для высокой вероятности угрозы.

С учетом изложенного, коэффициент реализуемости угрозы Y будет определяться соотношением(1), где Y_1 – коэффициент исходной защищенности, а Y_2–коэффициент вероятности возникновения угрозы.

$$Y= (Y_1+Y_2)/20 \quad (1)$$

По значению коэффициента реализуемости угрозы Y формируется вербальная интерпретация реализуемости угрозы следующим образом:

— если $0 \leq Y \leq 0,3$, то возможность реализации угрозы считается низкой;

— если $0,3 < Y \leq 0,6$, то возможность реализации угрозы считается средней;

— если $0,6 < Y \leq 0,8$, то возможность реализации угрозы считается высокой;

— если $Y > 0,8$, то возможность реализации угрозы - очень высокая.

2.1.4 Определение опасности каждой угрозы

На следующем этапе необходимо определить опасность каждой угрозы. Для этого вводится вербальный показатель опасности для рассматриваемой ИСПДн. Этот показатель имеет три значения:

— низкая опасность – реализация угрозы приведет к незначительным отрицательным последствиям для субъектов ПД;

— средняя опасность – реализация угрозы приведет к негативным последствиям для субъектов ПД;

— высокая опасность – реализация угрозы приведет к значительным негативным последствиям для субъектов ПД.

Показатель опасности определяется аналитическим методом оператором ИСПДн или специалистом по защите информации и зависит от экономического, технического и правового состояния организации.

2.1.5 Определение актуальных угроз

Затем осуществляется выбор из общего (предварительного) перечня угроз безопасности тех, которые относятся к актуальным для данной ИСПДн, в соответствии с правилами, приведенными в таблице 2.

Таблица 2

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

С использованием сведений об уровне исходной защищенности ИСПДн и составленного перечня актуальных угроз формулируются конкретные требования по организационной и технической защите ИСПДн от утечки информации по техническим каналам, от несанкционированного доступа и выбираются компоненты физической и технической защиты, которые могут быть использованы при создании и дальнейшей эксплуатации ИСПДн.

2.2Модификация алгоритма для разработки программного средства

В данном разделе разобран модифицированный алгоритм, необходимый для реализации программного обеспечения (Рисунок 4).

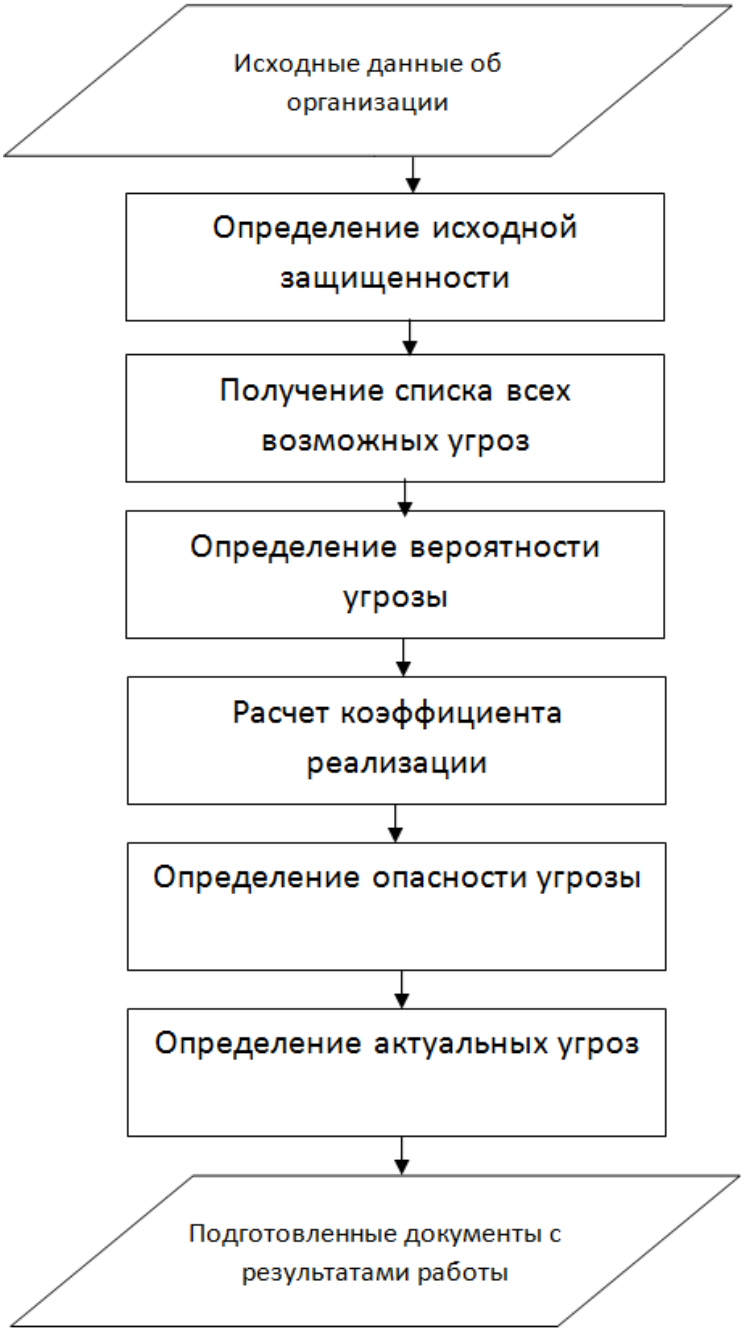


Рисунок 4 – Модифицированный алгоритм создания модели угроз.

Подробно рассмотрим каждый из пунктов алгоритма для уточнения операций, выполняемых в них. Были добавлены три блока в отличие от стандартного алгоритма.

1. Задание исходных данных об организации

Первый блок – ввод информации об организации – название, юридический адрес, сведения о руководящем составе. Это необходимо для последующего составления документов, подтверждающих разработку частной модели угроз и проведения мероприятий для получения остальных необходимых данных. Впоследствии, в результате работы программного обеспечения, возможно редактирование полученных документов из-за опечатки оператора или при изменении каких-либо параметров. Это позволяет, с одной стороны, добиться снижения срока проведения работ по оформлению и подготовки документов, и также сохраняется возможность их редактирования после тестирования.

2. Определение исходной защищенности

В этом блоке оператор вносит технические характеристики информационной системы обработки персональных данных, с помощью которых программное обеспечение автоматически расчитывает исходную защищенность ИСПДн. Приложение использует вариант расчета, приведенный в “Методике определения актуальных угроз”, где на основании указанных данных, рассчитывается обобщенный показатель и системе присваивается числовой коэффициент защищенности. Данный коэффициент не выводится оператору, а предоставляется вербальный показатель. Вся информация в блоках полностью соответствует всем возможным вариантам реализации ИСПДн, и позволяет максимально возможным способом определить уровень исходной защищенности.

3. Получение списка всех возможных угроз

В текущем блоке оператор выбирает из предложенных характеристик информационной системы и возможностей нарушителя пункты, соответствующие данному оцениваемому объекту для составления списка всех возможных угроз. Непредвиденные обстоятельства не подлежат

прогнозированию, поэтому они не включены в данный список. После определения технических характеристик, не включенных в определение исходной защищенности, оператор имеет возможность получить частный список угроз для тестируемой системы. Так как данный список является обобщением возможных угроз, и не может включить в себя полный список всех существующих угроз, то по окончанию заполнения и переходу к следующему пункту, оператор имеет возможность отдельно указать дополнительные угрозы, присущие конкретной ИСПДн.

4. Определение вероятности угрозы

Далее из списка данных, введенных в предыдущем пункте, оператору необходимо определить вероятность возможных угроз. В этом пункте используется вербальный показатель, рассматриваемый выше. Оператору необходимо руководствоваться логическим мышлением и руководящими документами. Данный пункт обладает очень большой вариативностью, из-за неявного описания метода определения вероятности. Поэтому при получении неправдоподобных результатов, необходимо очень тщательно пересмотреть определение вероятности угроз. Остается надежда на то, что вскоре все-таки будет разработан документ, который позволит обойти данное ограничение, и определить технические параметры для выявления вероятности угрозы безопасности в ИСПДн.

5. Определение коэффициента реализации

В данном блоке, программа автоматически рассчитывает коэффициент реализации, используя данные, введенные оператором ранее, а именно коэффициент исходной защищенности и коэффициент вероятности угрозы. Этот коэффициент зависит от того, насколько высок шанс вероятности данной угрозы в условиях текущей защищенности системы. Он позволяет выделить угрозы, к которым система обработки ПД в данный момент наиболее уязвима, и

направить разработку системы защиты ИСПДн в нужном направлении и наилучшим образом распределить технические возможности.

6. Определение опасности угрозы

Затем, оператор должен указать опасность указанных угроз. Эти данные могут быть получены только аналитическим способом, так как каждая организация имеет уникальный спектр свойств и возможностей. На данном этапе оператор, руководствуясь текущим экономическим и техническим состоянием организации, определяет степень влияния угрозы, в случае ее реализации, на последствия ее влияние на систему обработки персональных данных. Этими последствиями могут быть, к примеру, нарушение режима функционирования ИСПДн, несанкционированное разглашение и ознакомление с личными данными пользователей, финансовые потери организации, получение данных о техническом состоянии защищенности ИСПДн.

7. Определение актуальных угроз

В этом блоке производится расчет актуальных угроз для конкретной организации. Это происходит на основании таблицы актуальности в «Методике определения актуальных угроз». В данном блоке программное обеспечение устанавливает зависимости между опасностью угрозы и возможностью ее реализации, и затем, присваивает данному типу угроз необходимый уровень актуальности. В дальнейшем, будут рассмотрены только угрозы с уровнем “актуальна”. Это позволит направить ресурсы системы защиты информации на обеспечение защищенности объекта от актуальных угроз, вследствии чего, достигается определенный уровень защиты системы. Это решает одну из поставленных задач - возможность экономически выгодно рассчитать направленность системы защиты ПД во время их обработки и хранения в ИСПДн[20].

8. Вывод подготовленных документов.

На данном этапе оператор имеет возможность вывести на печать или сохранить автоматически составленные документы с результатами операций, проведенных ранее. Это позволит существенно сократить время на подготовку материалов по окончанию составления модели угроз ИСПДн. Документы содержат необходимые сведения о заключении тестирования, акт о прохождении анализа исходной защищенности, а также заполненный шаблон частной модели угроз.

Данный алгоритм позволяет оценить всю разработку частной модели угроз и перенести его в функции и модули программного обеспечения. Следующая глава будет посвещена непосредственно решению задачи по переносу данного алгоритма в тело программы для дальшейшего применения в качестве ПОс целью автоматизации создания частной модели угроз.

2.3Вывод по главе

В данной главе был изучен алгоритм создания частной модели угроз. Были подробно разобраны все пять этапов построения и выделены основные операции. Часть операция все же остается за оператором, остальные будут реализированы в теле разрабатываемой программы. Затем данный алгоритм был модифицирован для дальнейшего использования в программном обеспечении. Были введены несколько блоков для корректного взаимодействия с пользователем.

3. Разработка программного средства на базе алгоритма для автоматизированного создания частной модели угроз.

3.1 Обзор аналогов и актуальность задачи

Разрабатываемый программный продукт не является уникальной разработкой на данный момент времени. Проблема автоматизации при составлении частных моделей угроз рассматривается уже несколько лет. Рассмотрим имеющиеся аналоги на рынке информационной безопасности, связанные с возможностями для построения моделей угроз. Некоторые из них используются в процессе разработки программного обеспечения и для других задач неприменимы, какие-то являются внутренними решениями, какие-то ориентированы на отдельные отрасли или вертикали. Далее мной были рассмотрены наиболее близкие по техническим особенностям и популярные продукты на рынке информационной безопасности. В ходе разработки ПОдля автоматизации создания частной модели угроз необходимо учитывать имеющиеся аналоги с целью улучшения уже имеющихся модулей и разработки функционала, отсутствующего у аналогичных программ.

1. ADTool

ADTool(Attack-Defense Tree Tool).Создан как программное обеспечение для подготовки модели распространения атак и защитных мер. ADTool, доступный в исходных кодах, используется только как инструмент для визуализации данных и автоматизации некоторых действий (Рисунок 5).Также сильно сказывается отсутствие встроенных библиотек или шаблонов. Имеется тольконесколько готовых частных моделей угроз на сайте разработчика.

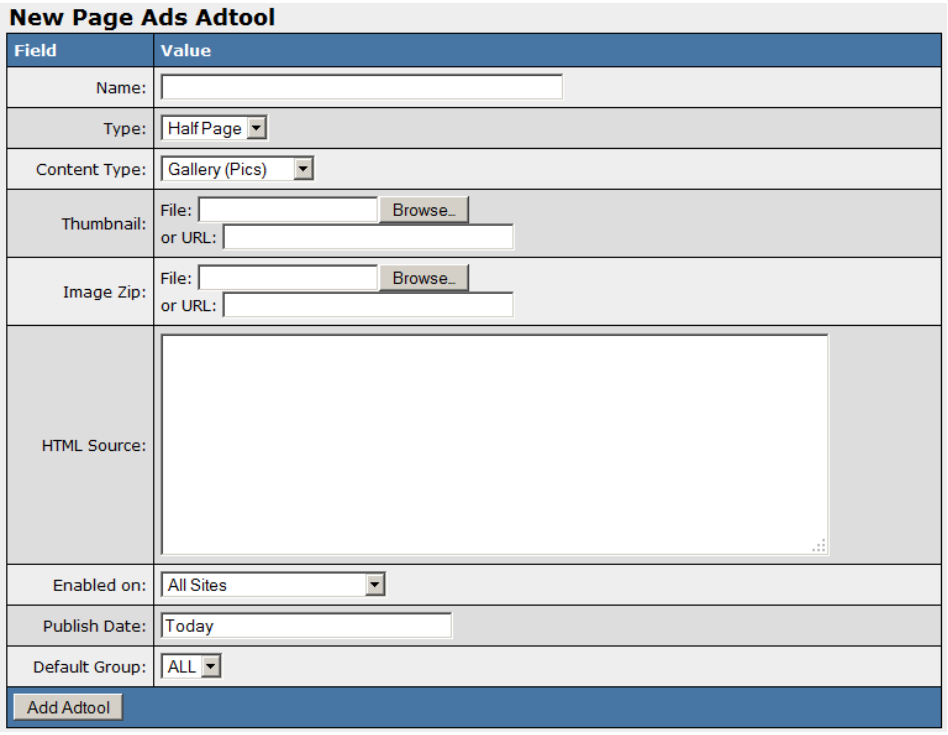


Рисунок 5 – Одно из окон ADTool

2. Trike.

В 2006-м году стартовал проект Trike , который включает разработку методологий и инструментов для создания моделей угроз. Сам метод был разработан еще в 2003-2005-м годах, но оформилась в открытый проект она чуть позже. Реализация Trike доступна в двух вариантах. Первый - обычная табличка вMicrosoftExcel(Рисунок 6)

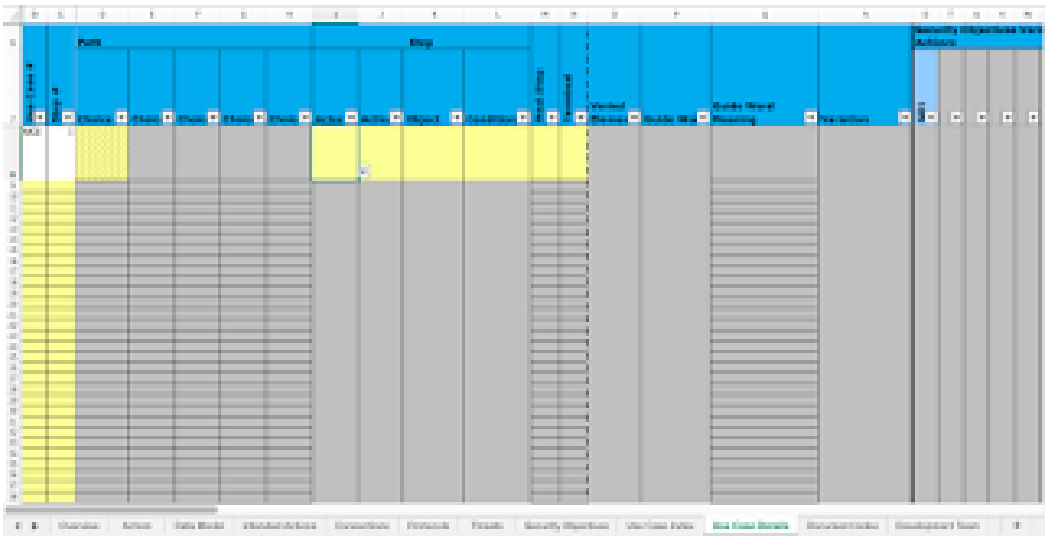
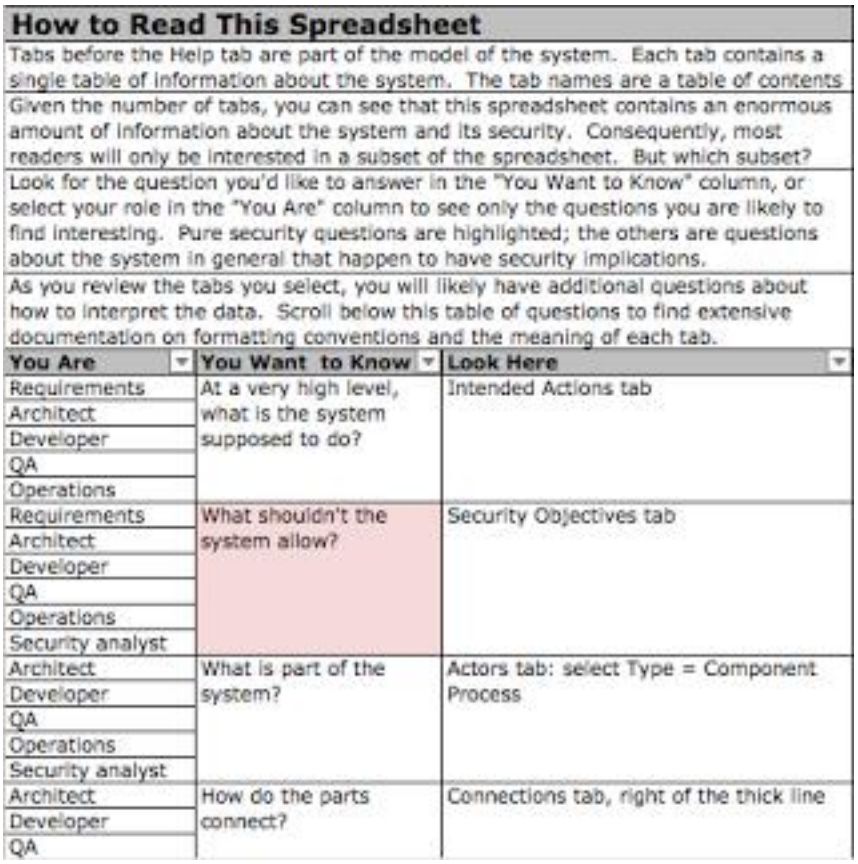


Рисунок 6 – Электронная таблица Trike

К таблице прилагается подробная подсказка, ориентированная на разные целевые аудитории - разработчики, тестировщики, архитекторы и т.п. Второй вариант представляет собой отдельное приложение, написанное на Smalltalk (Рисунок 7).



How to Read This Spreadsheet

Tabs before the Help tab are part of the model of the system. Each tab contains a single table of information about the system. The tab names are a table of contents

Given the number of tabs, you can see that this spreadsheet contains an enormous amount of information about the system and its security. Consequently, most readers will only be interested in a subset of the spreadsheet. But which subset?

Look for the question you'd like to answer in the "You Want to Know" column, or select your role in the "You Are" column to see only the questions you are likely to find interesting. Pure security questions are highlighted; the others are questions about the system in general that happen to have security implications.

As you review the tabs you select, you will likely have additional questions about how to interpret the data. Scroll below this table of questions to find extensive documentation on formatting conventions and the meaning of each tab.

You Are	You Want to Know	Look Here
Requirements Architect Developer QA Operations	At a very high level, what is the system supposed to do?	Intended Actions tab
Requirements Architect Developer QA Operations Security analyst	What shouldn't the system allow?	Security Objectives tab
Architect Developer QA Operations Security analyst	What is part of the system?	Actors tab: select Type = Component Process
Architect Developer QA	How do the parts connect?	Connections tab, right of the thick line

Рисунок 7 – Trike(Smalltalk)

3. MS ThreatModelingTool 2016

Компания Microsoft давно заявила себя как организация с собственным подходом к безопасной разработке, так что неудивительно, что она также имеет инструмент для создания моделей угроз с их техникой, описанной в книге бывшего сотрудника Microsoft Адама Шостака. Решение Microsoft бесплатно и предназначен для разработчиков программного обеспечения. Она свободно интегрируется в большинство комплексов, используемых для отслеживания ошибок и других проблем в программном обеспечении, что делает этот продукт

лидером среди подобных программных решений, доступных на рынке. Системаоснащенашаблонамипроблемпометоду STRIDE (spoofing identity, tampering of data, repudation, information disclosure, denial of service, elevation of privelege).

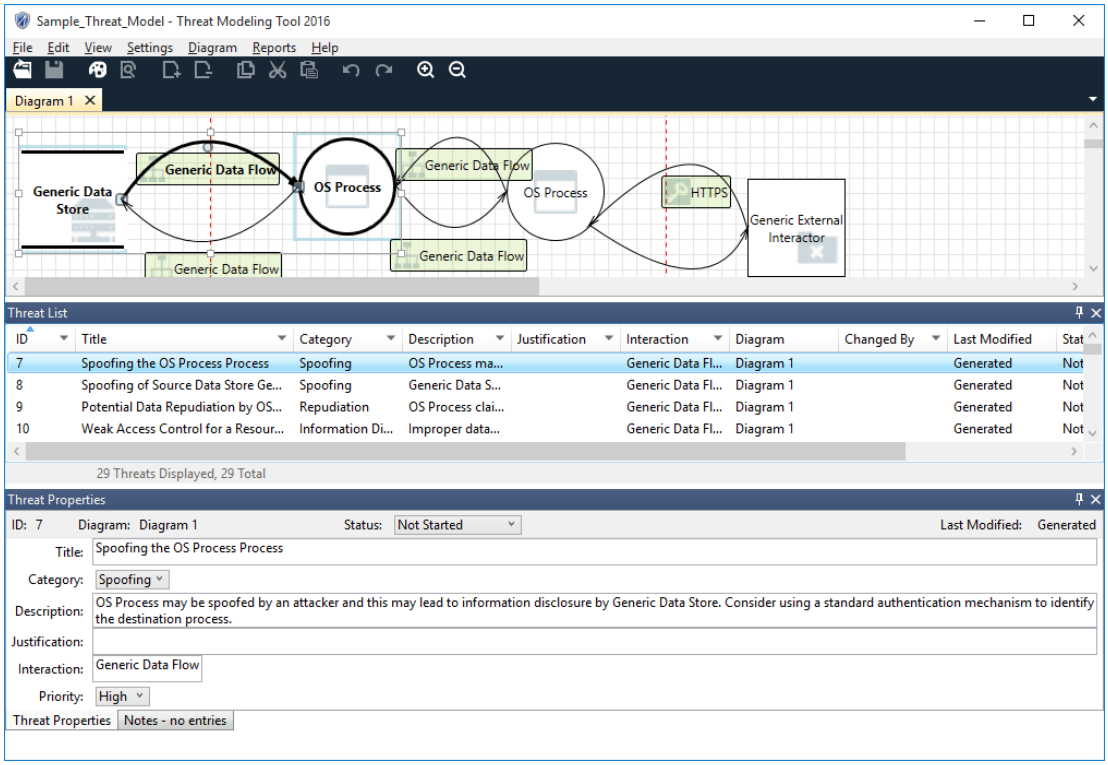


Рисунок 8 – MSModelingTool с отображением диаграммы данных.

Также в MS ThreatModelingTool встроена подсистема визуализации информационных потоков (Рисунок 8) и системе генерации отчетов, что делает это решение очень простым и надежным в использовании.

4. R-Vision.

В тоже время развивается другая отечественная компания - R-Vision , которая разработала систему обеспечения безопасности по модульному методу. Продукт носит название фирмы-разработчика - R-Vision. Среди прочих есть у R-Vision и модуль "Риски" (RiskManager), который также содержит в себе подмодуль для создания моделей угроз собственных активов предприятия.Идентифицируются виды, источники и способы реализации угроз (Рисунок 9).

Но, к сожалению, полным инструментом для создания угроз решение от R-Vision назвать никак нельзя - эта задача там лишь часть из многих.

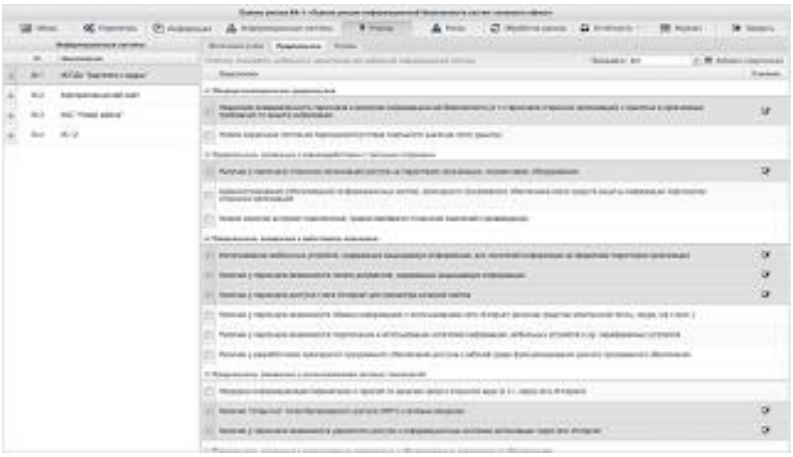


Рисунок 9 – R-Vision и модуль «Риски»

5. WingDoc ПД.

НТЦ "Сфера" - одна из первых разработала в России средство по автоматизации процесса создания моделей угроз по документам ФСБ и ФСТЭК. Но, к сожалению, на данный момент компания больше не существует - их веб-сайт больше не поддерживается, а продукты не обновляются.

Программный комплекс предприятия НТЦ “Сфера” чаще всего приобретался организациями, чей профиль включал в себя обеспечение информационной безопасностиили же оказание соответствующих услуги, или организациями, чья основная деятельность связана с обработкой персональных данных.Программа состояла из нескольких модулей, были варианты для физических и юридических лиц. Также была возможность создания технического задания.

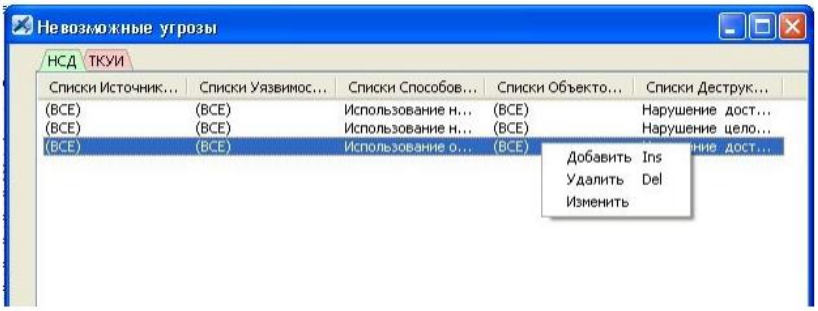


Рисунок 10 – WingDocПД. Модуль невозможных угроз.

В заключение, можно сказать, что у каждого из описанного выше инструментов есть свой диапазон применения и определенная задача. Однозначно применить их для моделирования угроз по методике ФСТЭК не получится, однако облегчить жизнь разработчикам, консультантам или архитекторам они могут.

3.2 Анализ вариантов реализации системы

Методология проектирования соединяет в себе предметное разложение, методы представления физической, логической, а также динамической и статической моделей системы.

Типовой проект включает в себя следующие этапы разработки программного обеспечения:

— определение требований заказчика;

— анализ и проектирование ПО;

— реализация и кодирование программных модулей;

— сборка и тестирование системы;

— внедрение и сопровождение.

Определение требований заказчика

На данном этапе важно сформулировать цели проекта, а также подчеркнуть фундаментальные отношения в системе. То есть, создается основа для последующего проектирования системы.

В рамках данной стадии необходимо зафиксировать требования заказчика, и провести их формирование – подобрать наилучшее решение их проблем, определить необходимую степень автоматизации, выявить наиболее важные для разработки бизнес-процессы.

На этапе анализа также подготавливаются заранее сроки сдачи и оценочная стоимость программного обеспечения, формируется и подписывается техническое задание на разработку ПО.

Проектирование

На основании предыдущей стадии осуществляется проектирование системы. Эта методология проектирования сочетает в себе разложение объекта, методы представления физических, логических, а также стационарных и динамических моделей систем.

На этой стадии разрабатываются проектные решения по выбору платформы, на которую разместится система языка или языков реализации, устанавливаются требования к рабочему интерфейсу, определяется наиболее подходящая база данных. Обрабатывается функциональная спецификация ПО: происходит выбор архитектуры системы, обсуждаются требования к аппаратному обеспечению, составляется список организационных мер, которые необходимы для внедрения ПО, а также перечень документов, которые регламентируют его применение.

Реализация

Эта стадия разработки программного обеспечения соответствует моделям эволюции жизненного цикла ПО. При разработке применяются прикладные методы экспериментов и анализ, строятся прототипы частей и комплексной системы. Прототипы позволяют понять возможные проблемы еще на ранних этапах проектирования и принять все необходимые проектные решения еще до момента тестирования и внедрения. Такие решения задействуют разные части системы: внутреннюю организацию, технический интерфейс, системы контроля доступа и т.д. В итоге на стадии реализации осуществляется сборка и проверкарабочай версии продукта.

Тестирование продукта

Тестирование тесно связано с предыдущими этапами разработки программного обеспечения, такими, как проектирование и реализация. На данном этапе создаются специальные механизмы и условия, позволяющие провести тестирования системы на соблюдение требований, предъявляемым к ним, проверить наличие необходимой специальной документации пакета.

Результатом тестирования является заблаговременное устранение всех ошибок и проблем системы и получение сведений о ее качестве.

Внедрение и поддержка

Внедрения системы обычно состоит из трех пунктов:

— установка системы,
— обучение пользователей,
— эксплуатация.

Любая разработка содержит полный пакет документации, в который включается техническое описание системы, руководства пользователей и специальные алгоритмы работы.В дальнейшем осуществляется прямая и косвенная поддержка пользователей, своевременное исправления выявленных со временем ошибок в программное коде, и замена аппаратных частей, по мере снижения их надеждости и прочих параметров.

3.3 Выбор технологии реализации

Для реализации данного проекта был выбран язык Delphi (ранее имел название ObjectPascal).Рассмотрим его подробнее со стороны встроенных объектов и возможностей системы. Средой разработки является BorlandDelphi 7.

Delphi – это среда разработки программных приложений, в которой в качестве языка программирования используется ObjectPascal. В основе системы

программ (RAD – система, RapidApplicationDevelopment – среда быстрой разработки приложений) лежит технология визуального проектирования и событийного программирования, суть которого заключается в том, что среда разработки генерирует большую часть общего кода программы, оставляя программисту только работу по созданию новых диалоговых окон и функций обработки событий, написанных на языке ObjectPascal, являющимся расширением языка программирования Паскаль[21].

При запуске Delphiотображается главное окно,окно редактора, окно просмотра списка объектов, окно инспектора объектов,кода окно формы.

Основными компонентами страницы являются:

— Label (надпись),
— Button (настраиваемая клавиша),
— Edit (редактируемое поле),
— MEMO (многострочный текстовый редактор),
— Panel (панель для разделения компонентов на группы).

Со страницы Additional: в первую очередь, компонент BitBtn (клавиша с надписью и пиктограммой) и компонент StaticText(надпись с эффектами выделения поля). Перечисленные компонентыможноиспользовать для создания пользовательского интерфейса при написании простейших программных приложений[22]. Далее рассмотрим преимущества и недостатки Delphi.

Достоинства Delphi:

— максимизация простой обработки, ясность и удобство при разработке элементов технического интерфейса – готовые компоненты из библиотеки визуальных компонентов (VCL) выполняют практически уже всю готовую работу;

— возможность тонкой настройки и универсальность при работе ссистема управления базами данных: поддерживаются практически все

новейшие технологии; одни и те же компоненты позволяют получить доступ к различным базам данных;

— быстрый компилятор: можно проверять внесенных в программу исправлений практически без задержек;

— мощные средства отладки приложений;

— хорошая справочная система;

— все библиотеки Delphi (как стандартные, так и VCL) приведены с исходным кодом, что позволяет изучить внутреннее устройство Delphi;

— имеется возможность создания своих собственных компонентов «с нуля» или на основе компонентов, уже содержащихся в самой среде Delphi;

— возможно создание приложений на различные платформы (для Windows и Linux), с помощью библиотеки компонентов CLX – аналог библиотеки VCL.

Недостатки Delphi:

— большой объем выходных exe-файлов по сравнению с другими системами разработки, так как они содержат уже встроенные компоненты VCL;

— сложность при использовании Windows API, которая возникает при преобразовании между типами данных языков C и Pascal (особенно при использовании строк и указателей);

Имеющиеся недостатки в рамках поставленной задачи несущественны, вследствие чего и была выбрана данная среда разработки. Также интегрируя ведущие приложения разработки в единый и легкий в использовании пакет, Delphi 7 существенно уменьшает жизненный цикл разработки приложений и ускоряет вывод создаваемых с его помощью продуктов на рынок ПО[23].

3.4 Описание интерфейсов системы

Для решения поставленной задачи было разработано программное обеспечение - “Автоматизированная система создания частной модели угроз в

ИСПДн”. Программное обеспечение разработано для использования оператором ИСПДн или же специалиста по защите информации. Программа выполнена в виде мастера, где на каждом этапе необходимо указывать данные об исследуемом объекте. Для неопытных пользователей работа с программой может ограничиваться ответами на вопросы. По результатам работы с программным обеспечением определяется исходная защищенность объекта информатизации, актуальные угрозы. Также на выходе программы имеется возможность сформировать отчеты о принятых мероприятиях и заключения об определении актуальных угроз с последующим выводом на печать; отчет создается в формате DOC.Также предлагается вывести подготовленные документы, а именно:

— Положение об обработке персональных данных работников;

— Приказ о создании комиссии для определения уровня защищенности;

— Акт установления уровня защищенности персональных данных;

— Частная модель угроз безопасности персональных данных

— Состав и содержание организационных и технических мер.

ПО состоит из одного главного и 6 диалоговых окон. На рисунке 11 изображено главное окно, с указанием названия продукта, автора и года разработки программного обеспечения. При графической составляющей программного обеспечения использовались общепринятые стандарты размещения компонентов и их порядок. За основу были приняты аналоги прототипов, успешно себя зарекомендовавших(1С, TotalCommander, Dev-C++)[24]

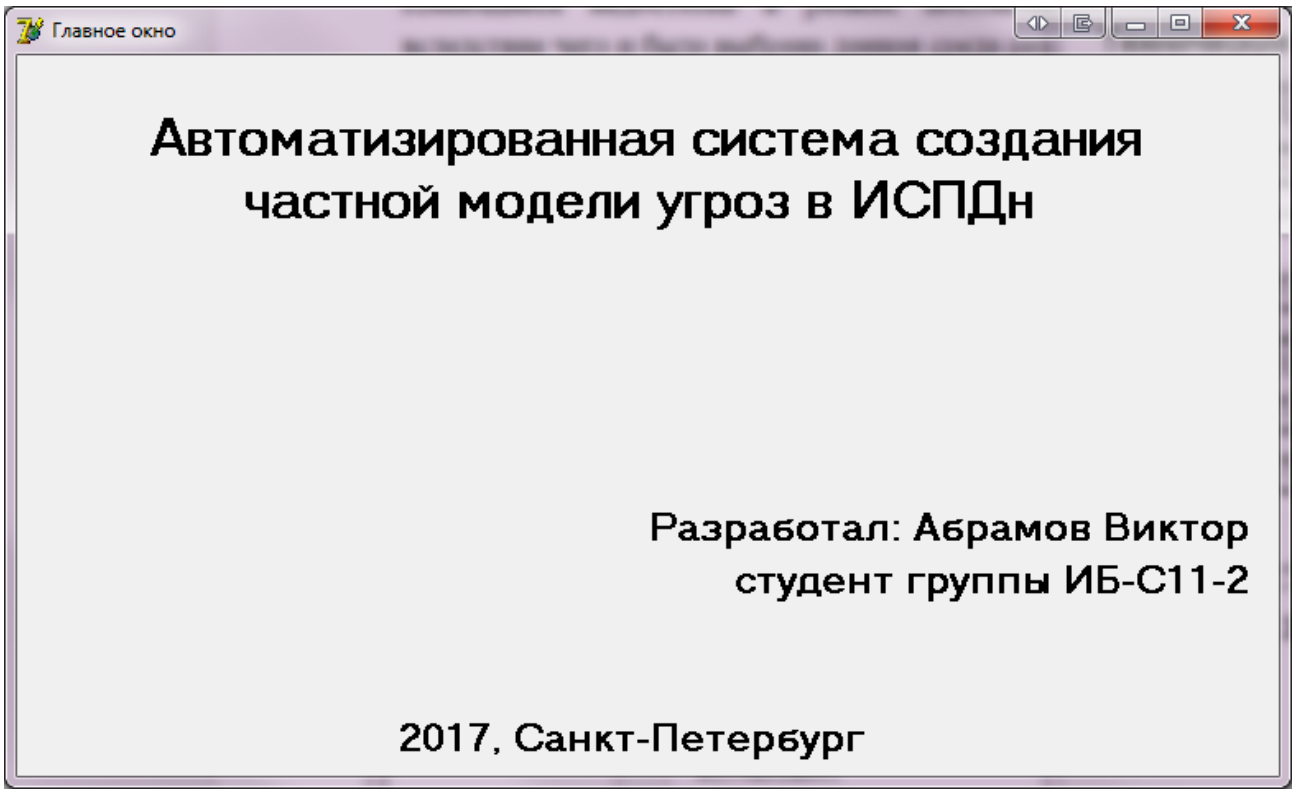


Рисунок 11 - Главное окно программы

Дизайн приложения был подобран таким образом, чтобы гарантировать быструю адаптацию оператора к интерфейсу программного обеспечения.

Следующее окно открывается при нажатии в любом месте на главное окно(Рисунок 12). В нем необходимо указать данные об организации для последующего использования их в документах.

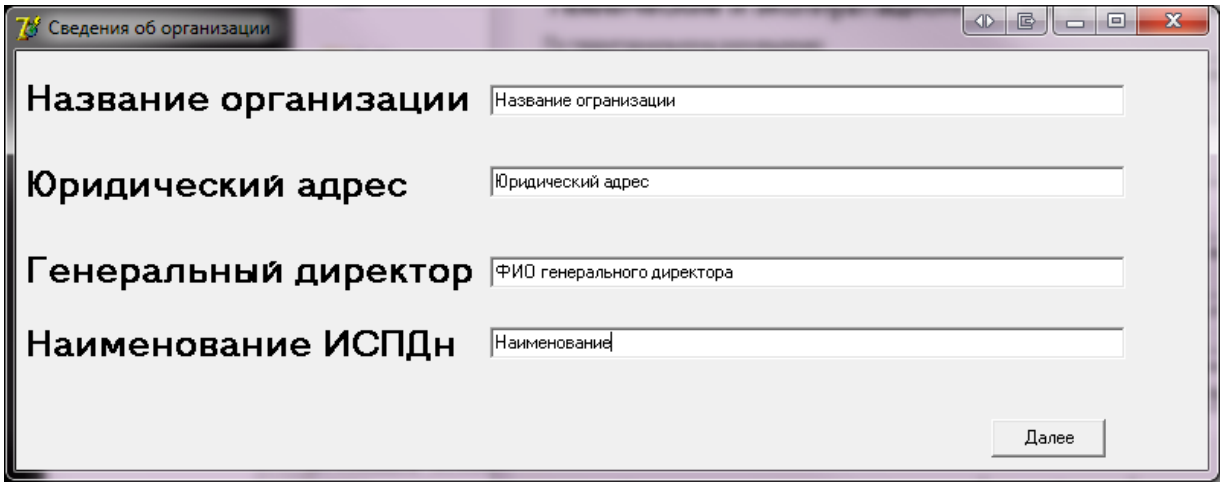


Рисунок 12 - Окно со сведениями об организации

В этом пункте оператор указывает сведения о компании, которой принадлежит исследуемая ИСПДн. По окончанию имеется возможность изменить введенные данные. Затем, при нажатии кнопки “Далее” оператор попадает на следующий этап - Определение исходной защищенности ИСПДн (Рисунок 13).Он представляет собой специализированный тест с вариантами выбора из выпадающих списков. Оператору необходимо выбрать данные, соответствующие конкретной информационной системе обработке персональных данных. Затем программа, используя указания из “Методики определения актуальных угроз”, рассчитывает исходную защищенность ИСПДн и выводит это на данном диалоговом окне. Затем необходимо перейти на следующее окно, нажав кнопку “Далее”.

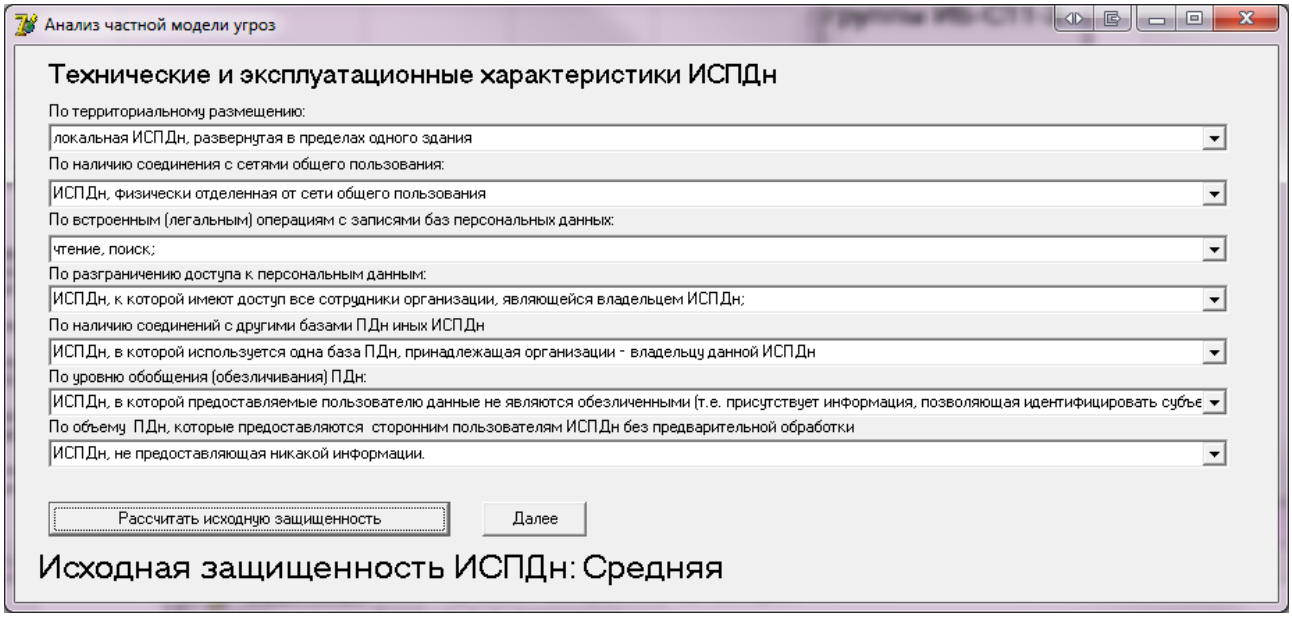


Рисунок 13 - Диалоговое окно определения исходной защищенности

Затем, нажав кнопку “Далее” оператор попадает на диалоговое окно получения списка возможных угроз(Рисунок 14). Оно также выполнено в виде тестирования. Необходимо указать технические особенности системы, не связанные с определением исходной защищенности. По ним система определит список возможных угроз, и наличие принятых мер по устранению

существующих угроз.После указания ответа на все заданные вопросы, оператор переходит на следующее окно.

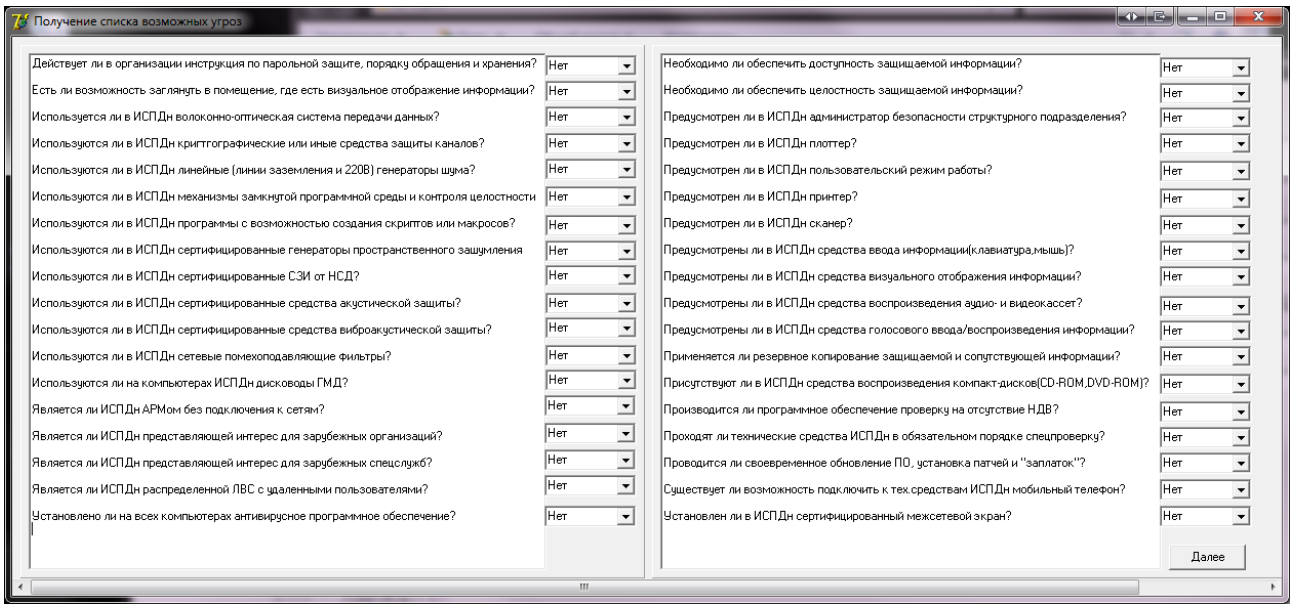


Рисунок 14 - Диалоговое окно составления списка возможных угроз

Следующим пунктом алгоритма является определение вероятностей угрозы (Рисунок 15). На данном окне представлен список возможных угроз и каждому из них соответствует поле выбора значения вероятности с категориями:

— маловероятно

— низкая вероятность

— средняя вероятность

— высокая вероятность

После заполнения всех полей, переход на следующий этап осуществляется при нажатии кнопки “Далее”.

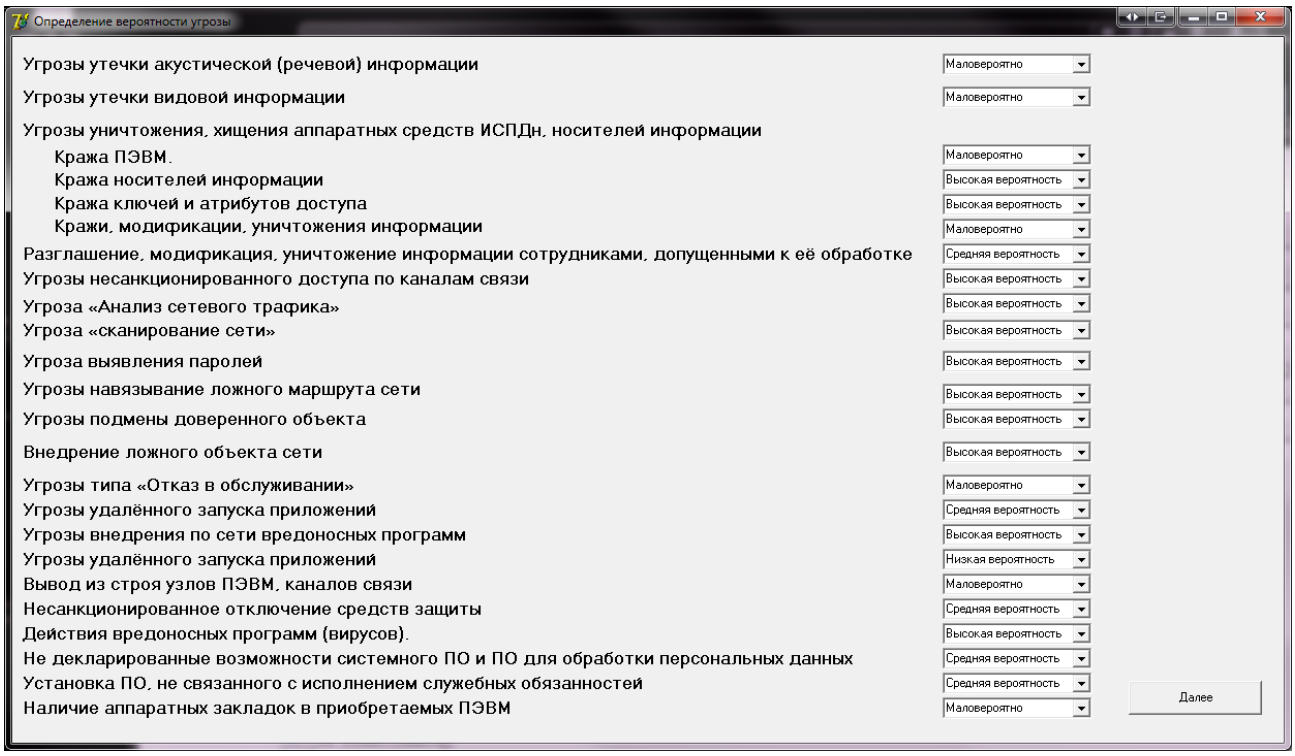


Рисунок 15 - Диалоговое окно определения вероятности угрозы

На следующем шаге реализовано определение опасности угроз. Данное окно выполнено по аналогии с предыдущим, только теперь при выборе необходимо указать возможную опасность угрозы (Рисунок 16). Возможные варианты в данном случае:

— низкая опасность

— средняя опасность

— высокая опасность

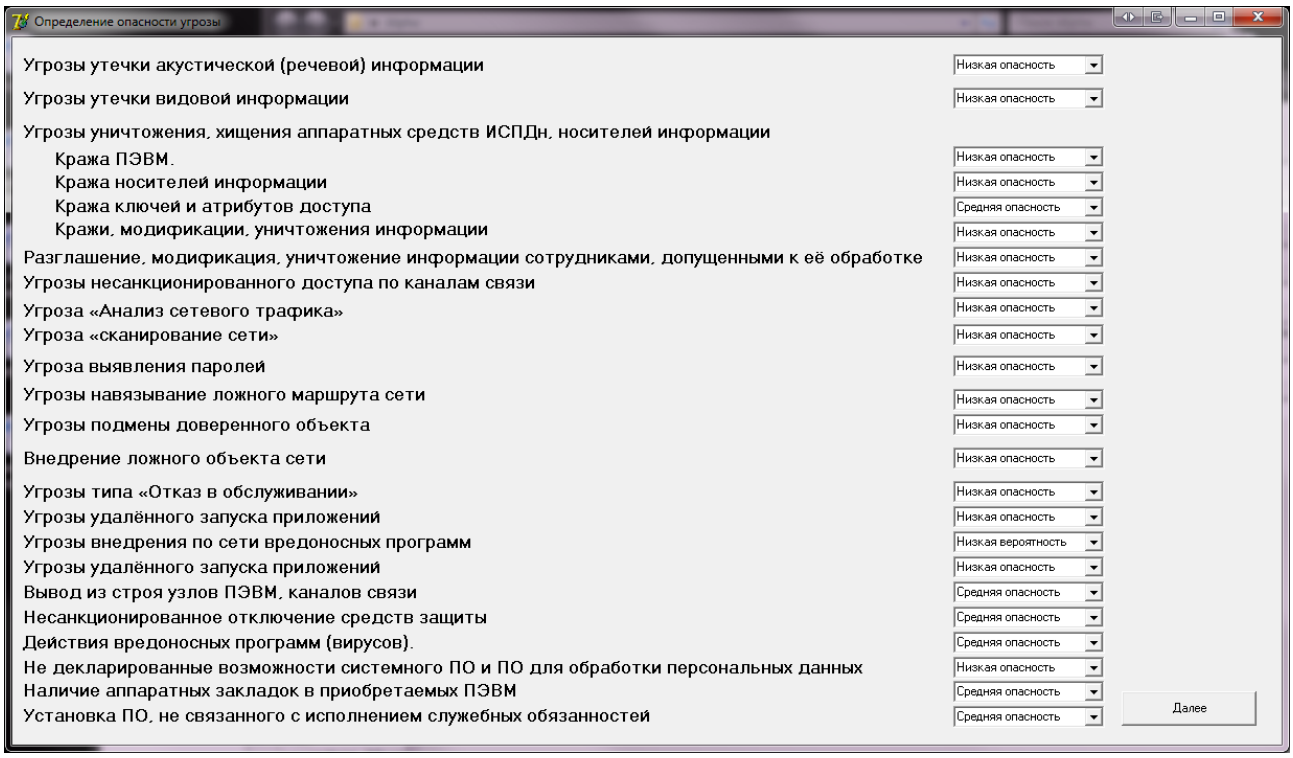


Рисунок 16 - Диалоговое окно определения опасности угрозы

При нажатии кнопки “Далее” оператор попадает на последнее окно программы (Рисунок 17). На нем представлен большой объем информации. Первое - это заключительная таблица с результатами проведенных тестов. В ней указаны все полученные данные в ходе работы, такие как:

— множество угроз

— предпосылки

— меры

— коэффициент Y1

— возможность реализации угрозы

— коэффициент Y2

— опасность угрозы

— актуальность

Актуальность в результате получена на основании таблицы актуальности в «Методике определения актуальных угроз». Программное обеспечение устанавливает зависимости между опасностью угрозы и возможностью ее

реализации, и затем, присваивает данному типу угроз необходимый уровень актуальности. В левой части окна также представлена расшифровка всего множества угроз по пунктам. Также имеются кнопки для получения автоматически подготовленных документов.

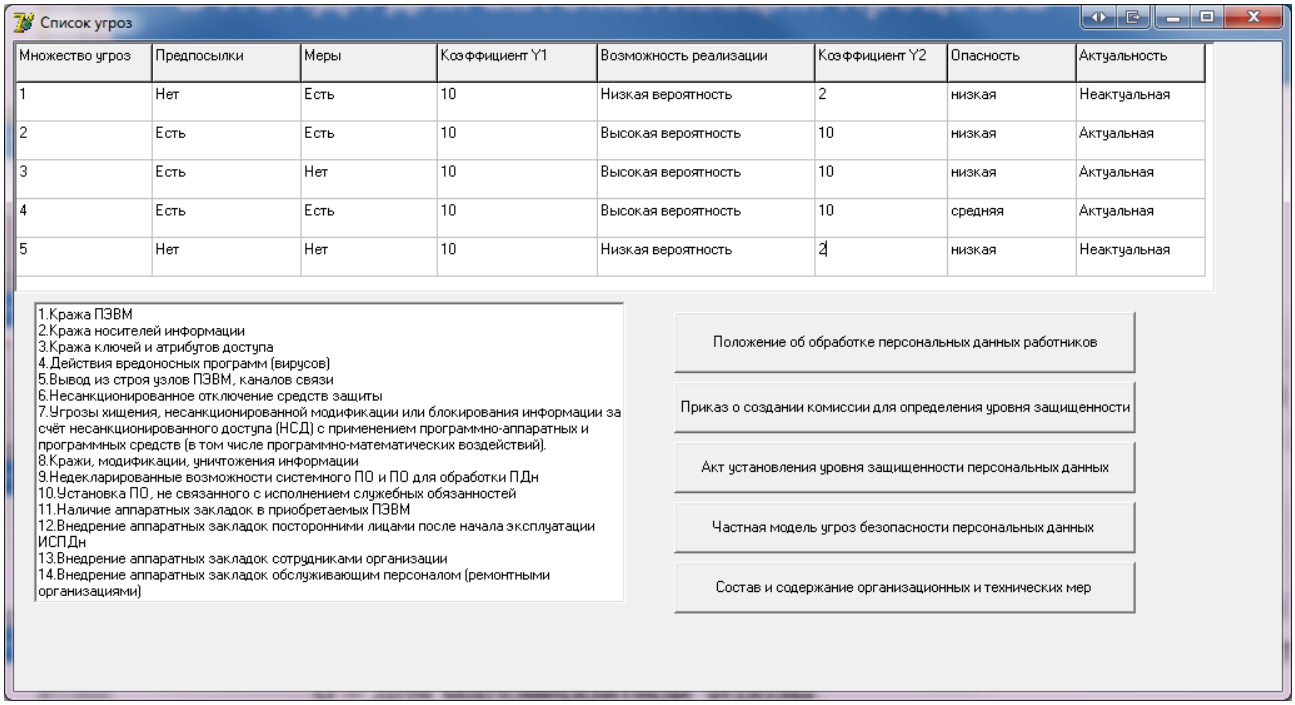


Рисунок 17 –Итоговое окно приложения

Используя разработанное программное обеспечение, оператор ИСПДн может существенно снизить время создания частной модели угроз. Автоматическая подготовка документов осуществляется в фоновом режиме. Это происходит после выбора вероятных угроз и определения опасности и расчета актуальности. Используя данные, полученные программой, документ “Частная модель угроз” собирается из заранее подготовленных файлов, содержащих информацию по той или иной угрозе. Также автоматически заполняется поля:

— наименование организации

— название ИСПДн

— информация о руководстве

— юридический адрес организации

Автоматически составленные документы уменьшаются временные затраты на заполнение и редактирование текстовых файлов.

Программа предоставлена архивом, содержащим проект приложения, с целью модернизации или исправления, исполняемым файлом, а также каталогом с шаблонами автоматически создаваемых документов. Исходный код программного обеспечения с разделением на отдельные модули(окна) представлен в приложение А. Экономическое обоснование в данном случае не является актуальным, так как полных аналогов на рынке ПО не имеется, а вся разработка программного обеспечения выполнена с целью улучшения метода построения частной модели угроз. Поэтому данный продукт будет поставляться по свободной лицензии с открытыми исходными кодами.

3.5 Вывод по главе

В данной главе были разобраны аналогичные программные комплексы на рынке информационной безопасности, выделены основные возможности каждого продукта. Затем приведена методология разработки программного обеспечения, по которой и выполнена данная выпускная квалификационная работа. В следующем пункте подробно разобран интерфейс разработанного программного комплекса с подробными комментариями. Также указаны сведения о поставке программного обеспечения.

4. Безопасность жизнедеятельности

4.1 Описание условий эксплуатации проектируемой среды

С развитием науки и техники важную роль возможность безопасного выполнения людьми своих жизненных обязанностей. Вопросам безопасности жизнедеятельности уделяется все больше внимания от года в год, так как забота о физическом и моральном состоянии человека является не только делом государственной важности, но и элементом соперничества организаций в вопросе привлечения новых кадров.В связи с этим вопросами в качестве варианта обеспечения защищенности человека была и разработана наука о безопасности жизни человека[25].

Безопасность жизнедеятельности (БЖД) - это мероприятия, нацеленные на обеспечение безопасной жизни и работы человека в окружающей среде, сохранение его самочувствия, разработку методов и средств защиты путем уменьшения воздействий вредных и опасных особенностей жизнедеятельности до минимальных значений, применение мер по снижению ущерба чрезвычайных ситуаций и стихийных бедствий.

Цель и содержание БЖД:

— нахождение и исследование факторов окружающей среды, которые представляют опасность и наносят вред здоровью человека;

— ограничение действия этих факторов до минимальных пределов или полное их исключение;

— устранение последствий после техногенных аварий и стихийных бедствий.

Круг реальных задач БЖД прежде всего зависит от выбора вариантов реализации защиты, развития и подходящем использованием средств охраны здоровья человека и окружающей среды от влияниянегативных факторов и

стихийных бедствий, а также средств, обеспечивающих комфортное состояние среды обитания.

Обеспечение возможностей для сохранения здоровья работников, безопасность условий труда, ликвидация заболевания, связанных с профессиональной сферой и травм на производстве является одной из главных забот человеческого общества. Следует обратить внимание на необходимость глобальное применения новейших форм научной организации труда, минимизации по эксплуатации неквалифицированной сотрудников, создание условий для исключения профессиональные заболевания и производственный травматизм.

Рабочее место должно быть обеспечено всеми доступными средствами защиты человека от вредоносных воздействий производства. Уровни этих факторов не должны превышать пределы, установленных санитарно-техническими, техническими и правовыми нормами. Эти правила требуют создания приемлемых условий труда на местах организации производства, при которых влияние опасных и вредных факторов на работающих либо полностью исключено, либо находится в допустимых диапазонах.

Этот раздел выпускной квалификационной работы непосредственно связан с вопросами обеспечения безопасности операторов ИСПДн и специалистов по защите информации. В нем рассмотрены следующие вопросы:

— анализ вредных и опасных факторов при работе с ПЭВМ;

— определение мер по улучшению условий труда в соответствии с правилами и нормативными документами;

4.2Анализ и выявление потенциально опасных и вредных факторов

Оператор и пользователи ИСПДниспытывают воздействию негативных факторов, как со стороны технических средств, так и из-за неправильно организованного рабочего пространства и испытывают следующие опасности:

— Влияние электромагнитного и электростатических полей на человеческие ограны и негативное воздействие на внутренние клетки;

— Излучение (инфракрасный, ультрафиолетовый и рентгеновский спектры);

— Шумовое и вибрационное воздействие на человека;

— Влияние расположения рабочего места и эргономики внешних устройств компьютера (клавиатура, «мышь») на опорно-двигательную систему и состояния мыщечной массы;

— Повышенное воздействие на зрения (условия освещения, контраст монитора);

— Повреждения, вызванные воздействием электрического тока;

— Нервно-эмоциональные нагрузки.

Влияние этих негативных факторов приводит к нарушениям центральной нервной, сердечно-сосудистой и опорно-двигательной систем и нейротрофических расстройств и патологических изменений, деформации скелета и двигательных мышц, снижения активности головного мозга, головные боли, проблемы со слухом, головокружение,раздражительность. Также возможно явное переутомление, снижение активности и внимания, быстро наступает усталость в связи постоянной рабочей активность и влиянию негативных факторов производства. Все это ведет к снижению качества и безопасности труда, работоспособности, производительности.

Долгосрочное присутствие человека в зоне комбинированного воздействия различных неблагоприятных факторов может привести к профессиональному заболеванию.

4.3Описание мероприятий, обеспечивающих безопасность

Соответствие требований к организации рабочего места, комплектующим деталям и особенностям работы, наилучшим образом снижает вредные факторы, оказывающие воздействие на пользователя.Поскольку имеется

множество вариантов вредоносных воздействий на здоровье человека, существует несколько способов, чтобы предотвратить их.

Для защиты от электромагнитных и электростатических полей, вы можете использовать экранные фильтры, специальные мониторы и другие средства личной защиты, которые прошли испытания в соответствии с сертификатом здоровья[26].

При наличии защитных фильтров, внешних или встроенных в корпус монитора, они обязательно должны быть подключены к общему заземлению

Чтобы уменьшить шанс заболеваний операторов из-за воздействия радиации во время работы на компьютере, рекомендуется использовать мониторы с минимальным уровнем излучения, разработанные по международным соглашениям MPR-II, TSO'95, TSO'99, и следить за соблюдением режимов работы и отдыха.

Для уменьшения шума в комнате с компьютером, как правило, используется способ обработки акустического пространства с использованием противостоящих поверхностей, ограждающих абсорбирующий материал с высокими коэффициентами поглощения звука (а) в диапазоне частот 63 - 8000 Гц.С этой целью, на потолке и стенах размещены перфорированные плитки с звукопоглощающим наполнителем (минеральная вата). Усиленные панели размещают либо сразу на поверхность или в корпусе, на расстоянии от него не менее 20 см. В данном случае, более эффективно применение звукопоглощающей облицовки.

Дополнительным звукопоглощением могут служить простые занавеси из плотной ткани, в гармонии с цветом стен и подвешенные в складку на расстоянии 15 – 20 см от оконного стекла. Ширина занавеси должна быть в 2 раза больше ширины окна. Снизить уровень шума возможно также за счет использования для печати лазерных принтеров с низким уровнем шума.Меры,

позволяющие устранить вредные факторы, оказывающие влияние на мышцы и суставы:

— Обеспечение свободной площади и удобной формы рабочей поверхности.

— Удобное расположение клавиатуры с возможностью изменения угла наклона плоскости.

— Соответствие формы спинки кресла форме спины работающего человека.

— Перерыв в течение 15 минут после 45 минут работы.

— Занятие специальной гимнастикой, уменьшающей напряжение в фалангах пальцев, кистях, областях плеч, шеи и спины.

— Меры предотвращения вредных воздействий на глаза:

— Наличие конструктивно удобного рабочего места

— Применение специализированных очков с линзами-фильтрами для людей, у которых уже наблюдается нарушение зрения;

— Применение специальных защитных фильтров, которые уменьшают вредное воздействие отраженных лучей от экрана.

— Экран должен обладать затемненным экраном, либо покрыт слоем материала, снижающим бликовый коэффициент.

— Монитор не должен находиться напротив отражающих поверхностей и зеркал.

— Обеспечение хорошей световой обстановки в помещении

— Одним из основных параметров экрана является размер зерна. Зерно не должно размером до 0,28 мм.

Меры безопасности, для предотвращения возможности поражения электрическим током:

— Обязательное заземление всех технических средств.

— Ограничение по подключению и ремонту средств информационной техники самим персоналом.

— Запрещение использования сломанной и неисправной аппаратуры

— Соблюдение правил техники безопасности.

Электронное оборудование, подключенное к сети переменного тока, подвергается различным негативным воздействиям со стороны питающей сети. Стандартным требованием к питающей сети является напряжение питания 220 В с допустимыми отклонениями от –15% до +10% от номинала (187-242 В) при частоте 50±1 Гц. Основные негативные факторы воздействия включают в себя следующее[27]:

— высокого напряжения –грозовые перепады, до доли секунды продолжительность, и перепады, до десятков или сотен миллисекунд. Грозовой может достигать десятков киловольт, перепады - единицы киловольт;

— радиочастотные шумы от воздействия мощных радиопередающих и иных устройств и помехи от импульсных блоков питания;

— скачок напряжения выше 110% от номинала, кратковременные (на несколько периодов сети) или длительные, связанные с техническими неполадками в сети.

— кратковременные провалы (в течение нескольких периодов), вызванные подключением мощной нагрузки, и длительные понижения уровня напряжения ниже 85% от номинального значения;

— потеря напряжения более чем на два полупериода частоты;

— отклонение частоты питающей сети от номинала 50 Гц;

— гармонические искажения питающего напряжения (отклонение формы от синусоидальной).

Воздействия питающей сети на аппаратуру может быть разным – от сбоев (импульсные помехи и провалы питающего напряжения) и самопроизвольного отключения до полного выхода из строя под действием импульсных или

длительных перенапряжений.Повреждения от сбоев питания могут быть весьма существенными – от потери данных, вовремя не сохраненных оператором, до полного вывода аппаратуры из строя[28].

Комплекс мер для защиты от воздействия сетевых возмущений

— сетевой LC-фильтр задерживает высокочастотные помехи из сети от импульсных блоков питания. Этот фильтр должен входить в конструкцию любого устройства питания, обладающим сертификатом соответствия.

— ограничитель перенапряжения – подавляет высоковольтные выбросы, как коммутационные (до 10 мкс), возникающие при переключениях мощных цепей, так и короткие – грозовые.

Энергия импульсов скачков напряжения поглощается полупроводниковым варистором. Правильно выбрав варистор, можно обезопасить технику от длительных значительных повышений напряжения сети, например, технических неполадках питающей сети[29]. В этом случае варистор должен снизить напряжение, выделяя значительную мощность, что приводит к пробою на короткое замыкание и выключает питания предохранителями от токовых скачков (если они есть и рассчитаны на соответствующий ток);

— стабилизатор напряжения (электронный или феррорезонансный) – уравнивает выходное напряжение при плавных изменениях входного. Современные варианты феррорезонансных стабилизаторов чаще всего устанавливаются в корпуса компьютерной техники. Электронные устройства на активных компонентах не получили широкого применения из-за повышенной стоимости, наравне с источника бесперебойного питания.

— источники бесперебойного питания – ИБП (UPS) –позволяют завершить работу даже после отключения питания сети. В их состав обязательно входят накопительные батареи, выпрямитель входного напряжения и инвертор, обеспечивающий нагрузку напряжением переменного тока.

Меры, ведущие к устранению нервно-эмоциональных перегрузок

— Использование удобного и усовершенствованного интерфейса. Необходимо соблюдать контрастную политику и не использовать очень яркие элементы интерфейсов, негативно воздействующие на восприятие.

— Исключение присутствия на экране неспециализированной информации, которая может отвлекать внимание и снижать работоспособность.

— Пользователям необходимо обеспечить адекватное время реакции вычислительной техники. Среднее время ответа технических средств около 5-10 секунд.

Пожарной профилактикой называют комплекс организационных и технических мер, направленных на обеспечение безопасности людей, на предотвращение возгораний, ограничения его локального распространения, а также на создание условий для непосредственного тушения возгораний[30]. Пожаром называют неконтролируемое горение во времени и пространстве, наносящее материальный ущерб и создающее угрозу жизни и здоровью людей. Опасными факторами пожара являются:

— открытое пламя и искры;

— повышение температуры воздуха и окружающей среды;

— уничтожение и повреждение зданий, сооружений.

— снижение концентрации кислорода в воздухе;

— токсичных продуктов сгорания;

— задымление помещений;

В современных ЭВМ элементы печатных плат расположены вблизи друг друга, что приводит к нагреванию этих элементов. В непосредственной близости друг от друга располагаются и соединительные провода, кабели связи. При протекании по ним электрического тока выделяется большое количество теплоты, что может привести к повышению температуры элементов до 80-100

°С. Возникает опасность потери изоляции соединительных проводов, их оголение и, как следствие, короткое замыкание, которое сопровождается дымообразованием и нагреванием соседних элементов. Последние, перегреваясь, сгорают и наносят вред техники.

Эффективным средством защиты от короткого замыкания и его причин является использование тугоплавких и негорючих материалов в изоляции приборов. Необходимо соблюдать требования пожарной безопасности, которые предусматриваются в ГОСТ 12.1.004-76 ССБТ «Пожарная безопасность. Общие требования»:

— Пожарная безопасность должна обеспечиваться системами превентивного предотвращениявозгараний и защиты от пожара. Противопожарная система состоит из мероприятий, регулируемых правилами эксплуатации технического оборудования, средств освещения, кондиционирования воздуха и вентиляции помещений.Система противопожарной защиты состоит из мероприятий, которые включают в себя использование специальных средств индивидуальной и коллективной защиты людей в случае возникновения пожара, обеспечивая надежные действия пожарной сигнализации и другие средства пожарной сигнализации и объекта организации противопожарной защиты.

— Помещения ВЦ должны соответствовать требованиям СН 512-78 и СНиП 2-2-80, которые предназначены для проектирования зданий и сооружений. Все помещения ВЦ должны быть спроектированы с соблюдением всех технических особенностей и сооружаются из кирпича, бетона, металла, стекла и отделяются от соседних комнат огнеупорными стенами. Опорные конструкции над помещениями ВЦ защищаются огнестойкой защитной краской. Перекрытия и потолки должны содержать изоляцию по всему контуру.

— В соответствии с СНиП 2-90-81 «Проектирование зданий промышленных предприятий» для помещений ВЦ устанавливается категория

безопасности «В» и системы противопожарной защиты (для твердых горючих веществ и материалов). Стены ВЦ должны быть огнеупорные с уровнем огнестойкости не менее 0.75.

— Для технологических перекрытий устанавливаются тугоплавкие плиты. Подпольное помещение должно разделяться огнеупорными перегородками на отсеки с площадью не более 250 квадратных метров. При установке электрический линий используются минераловатные плиты.

— Согласно ГОСТ 12.4.009-75 «Первичные средства тушения пожара» в ВЦ должны быть: сухой песок в железном ящике, огнетушитель, гидрант (пожарный ствол) и асбестовые одеяла. По приведенному ГОСТу пожарный кран должен находится на высоте 1.35 метров от пола в доступном для пользователей месте и оснащается рукавами диаметром 50 мм и длиной от 10 до 20 метров.

— Для указания местонахождения пожарной техники и огнетушащих средств применяются указательные знаки по ГОСТ 12.4.026-76 «Знаки указательные». Знаки размещаются на высоте 2-2.5 метров. В месте расположения гидрантов установлен указатель в виде буквы «ПГ». Огнетушители расположены на высоте не более 1,5 м от пола в кабинете с надписью, так что вы можете определить тип огнетушителя.

4.4 Вывод по главе

В данной главе были разобраны условия обеспечения безопасности жизнедеятельности оператора ЭВМ. Были составлены необходимые рекомендации для безопасной организации труда и рабочего места оператора. Также привены меры и мероприятия для предупреждения технических проишествий и аварий. Приведена спецификация пожарной и электромеханической безопасности. Составлен список необходимых требований по обеспечению благоприятнгонервно-эмоционального состояния оператора.

Заключение

В данной дипломной работы было разработано программное обеспечения для автоматизированного создания частной модели угроз в ИСПДн. В целом, данный продукт позволяет сократить временные расходы за счет автоматизации процессов. Также разработанное ПО уменьшает количество ошибок, связанных с человеческим фактором. Это происходит потому, что все данные уже внесены в программу, и нельзя пропустить или не указать важные характеристики. Одной из главных трудностей является неявная формулировка некоторых аспектов определения параметров угроз в частной модели. Это сказывается на том, что нельзя полностью исключить труд и решение оператора ИСПДн. В ходе работы были решены следующие задачи:

- Проанализирована предметная область и выбраны руководящие документы для получения необходимых сведений в ходе работы.
- Был исследован и модернизирован алгоритм создания частной модели угроз.
- Разработано программное обеспечение с целью автоматизации создания модели угроз.

Без частной модели угроз невозможно построить адекватную систему защиты информации, обеспечивающую безопасность персональных данных. Поэтому правильная и вовремя созданная частная модель угроз является одним из важнейших факторов обеспечения защищенности персональных данных. В данной работе большое внимание уделялось именно анализу и реализации алгоритма построения модели угроз, так как существующие на данный момент документы неявно предоставляют сам алгоритм и методы определения параметров угроз. Данная работа позволила существенно сократить время на создание частной модели угроз и уменьшить количество ошибок, связанных с человеческим фактором.

Список использованной литературы

1. Положение "Об обеспечении безопасности ПД при их обработке в ИСПДн", утвержденное постановлением Правительства РФ от 17 ноября 2007 г. № 781.
2. "Базовая модель угроз безопасности ПД при их обработке в ИСПДн", утвержденная ФСТЭК России 15 февраля 2008 г.
3. Малюк А.А., Пазизин С.В., Погожин Н.С. Введение в защиту информации в автоматизированных системах. М.: «Горячая Линия – Телеком» – 2001. с. 35-51, 96-105.
4. Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем. – Учебное пособие для ВУЗов.- М.: «Горячая Линия – Телеком» – 2000. – с.26–29.
5. Методика определения актуальных угроз безопасности ПД при их обработке в ИСПДн, утвержденная ФСТЭК России 14 февраля 2008 г.
6. "Об утверждении положения о методах и способах защиты информации в информационных системах персональных данных". Приказ ФСТЭК России от 05.02.2010 г. № 58 (зарегистрирован в Минюсте России 19.02.2010 г. № 16456)
7. В.Г. Миронова, А.А. Шелупанов. Предпроектное проектирование информационных систем персональных данных как этап аудита информационной безопасности // Докл. Том.гос. ун-та систем управления и радиоэлектроники.- 2010.- №2(22), Ч1.-С.257-259.
8. Доктрина информационной безопасности Российской Федерации от 09.09.2000 № ПР. 1895. 2004г. 48стр.
9. Завгородний В.И. Комплексная защита информации в компьютерных системах. М.: «Логос» – 2001. с. 16-26, 38-132
10. Лопатин, В.Н. Информационная безопасность России: Человек, общество, государство. Серия: Безопасность человека и общества. М.: 2000. - 428 с;
11. С.Н. Ивлиев, С.Д. Шибайкин. Защита персональных данных. Изд-во Мордов. ун-та, 2012. - 72 с., с.25-33.

12. Шаньгин, В.Ф. Защита компьютерной информации. Эффективные методы и средства. М.: ДМК Пресс, 2008. - 544 с.

13. Щербаков, А.Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. М.: Книжный мир, 2009. - 352 с.

14. Хубаев Г.Н. Экономика проектирования и применения банков данных: Текст лекций. – Ростов-на-Дону: РИСХМ, 1989. – 69 с.

15. Тищенко Е.Н., Степанов Д.П. Определение эффективности распределенных межсетевых экранов в зависимости от функциональной полноты // Экономические науки. – 2008. – № 41. – С. 151-156.

16. Шураков В.В. Надежность программного обеспечения систем обработки данных: Учебник. – 2-е изд., перераб. и доп. – М.: Финансы и статистика, 1987. – 272 с.

17. Тищенко Е.Н., Строкачева О.А. Модель аудита информационной безопасности систем электронной коммерции // Научная мысль Кавказа. – 2006. – № 14. – С. 134-141.

18. Тищенко Е.Н., Строкачева О.А. Оценка параметров надежности защищенной платежной системы в электронной коммерции // Вестник РГЭУ (РИНХ). – 2006. – № 22. – С. 115-122.

19. Тищенко Е.Н. Инструментальные методы защищенности распределенных экономических информационных систем Ростов-на-Дону, 2003.

20. Кармановский Н.С., Михайличенко О.В., Савков С.В. Организационно-правовое и методическое обеспечение информационной безопасности, 2012

21. Фаронов В.В. DELPHI. Программирование на языке высокого уровня. Учебник для ВУЗов. С.-П, 2010.

22. Афанасьева О.А., Дегтярев А.В., Зиновьева Е.А., Литвина Е.М., Шаталова Л.М. Информатика. Учебное пособие для студентов высших учебных заведений. М., Изд-во «Доброе слово», 2010.

23. Литвина Е.М., Шаталова Л.М. Введение в среду Delphi. Учебное пособие. – М.: Изд-во МАИ, 2004.

24. Литвина Е.М., Шаталова Л.М., Зиновьева Е.А. Разработка программных приложений в Delphi. Учебное пособие для лабораторных работ, под редакцией Дегтярева А.В., М.: Изд-во МАИ, 2006.

25. С.В.Белов, В.А.Девисилов, А.Ф.КозьяковБезопасность жизнедеятельности. Учебник для студентов средних профессиональных учебных заведений. Под общ.ред. С.В.Белова.- 6-е издание, стереотипное - М.: Высшая школа, 2008.- 423 с.

26. СанПиН 2.2.2.542-96. Гигиенические требования к видеодисплейным терминалам персональным электронно-вычислительным машинам и организация работы.

27. П.П. Кукин, Е.А. Подгорных.Безопасность жизнедеятельности. Безопасность технологических процессов и производств (Охрана труда): Учебн. пособие для вузов / – М.: Высш.шк. 1999. – 318 с.: ил.

28.. Занько Н.Г. Русак О.Н. Малаян К.Р.Безопасность жизнедеятельности. Омега-Л. 2007

29. Громов В.И. Васильев Г.А. Энциклопедия безопасности-3 (с изменениями и дополнениями). Москва 2000.

30. Маньков В.Д. Обеспечение безопасности при работе с ПЭВМ. НиТ. Москва 2005

Приложение1
Листинг главного окна

```
unitUnit1;
interface
uses
Windows, Messages, SysUtils, Variants, Classes, Graphics, Controls, Forms,
  Dialogs, StdCtrls,ComObj, ComCtrls;
type
  TForm1 = class(TForm)
    Label6: TLabel;
    Label7: TLabel;
    Label8: TLabel;
    Label9: TLabel;
    Label10: TLabel;
    Label11: TLabel;
    Label12: TLabel;
    Label13: TLabel;
    ComboBox6: TComboBox;
    ComboBox7: TComboBox;
    ComboBox8: TComboBox;
    ComboBox9: TComboBox;
    ComboBox10: TComboBox;
    ComboBox11: TComboBox;
    ComboBox12: TComboBox;
    Label14: TLabel;
    Label15: TLabel;
    Button1: TButton;
    Button2: TButton;
    RichEdit2: TRichEdit;
    RichEdit1: TRichEdit;
    RichEdit3: TRichEdit;
    RichEdit4: TRichEdit;
procedure ComboBox6Change(Sender: TObject);

procedure ComboBox7Change(Sender: TObject);
procedure ComboBox8Change(Sender: TObject);
```

```
procedure ComboBox9Change(Sender: TObject);
procedure ComboBox10Change(Sender: TObject);
procedure ComboBox11Change(Sender: TObject);
procedure ComboBox12Change(Sender: TObject);
procedure Button1Click(Sender: TObject);
procedure Button2Click(Sender: TObject);
private
{ Private declarations }
public
{ Public declarations }
end;
var
  Form1: TForm1;
  k1,k2,k3,k4,k5,k6,k7: integer;
Arr: array[1..7] of TEdit;
ByteArr: array[1..7] of integer;
i,l,m,s:integer;
  Word: variant;
  Z:string;
  W:variant;
  W1:variant;
  W2:variant;
  W3:variant;
implementation
uses Unit2, Unit3, Unit4, Unit5, Unit6, Unit7;
{$R *.dfm}
procedure TForm1.ComboBox6Change(Sender: TObject);
begin
Form3.Show;
if form1.ComboBox6.ItemIndex=0 then ByteArr[1]:=1;
if form1.ComboBox6.ItemIndex=1 then ByteArr[1]:=1;
if form1.ComboBox6.ItemIndex=2 then ByteArr[1]:=10;
if form1.ComboBox6.ItemIndex=3 then ByteArr[1]:=10;
if form1.ComboBox6.ItemIndex=4 then ByteArr[1]:=100;
end;
procedure TForm1.ComboBox7Change(Sender: TObject);
```

```
begin
if form1.ComboBox7.ItemIndex=0 then ByteArr[2]:=1;
if form1.ComboBox7.ItemIndex=1 then ByteArr[2]:=10;
if form1.ComboBox7.ItemIndex=2 then ByteArr[2]:=100;
end;
procedure TForm1.ComboBox8Change(Sender: TObject);
begin
if form1.ComboBox8.ItemIndex=0 then ByteArr[3]:=100;
if form1.ComboBox8.ItemIndex=1 then ByteArr[3]:=10;
if form1.ComboBox8.ItemIndex=2 then ByteArr[3]:=1;
end;
procedure TForm1.ComboBox9Change(Sender: TObject);
begin
if form1.ComboBox9.ItemIndex=0 then ByteArr[4]:=10;
if form1.ComboBox9.ItemIndex=1 then ByteArr[4]:=1;
if form1.ComboBox9.ItemIndex=2 then ByteArr[4]:=1;
end;
procedure TForm1.ComboBox10Change(Sender: TObject);
begin
if form1.ComboBox10.ItemIndex=0 then ByteArr[5]:=1;
if form1.ComboBox10.ItemIndex=1 then ByteArr[5]:=100;
end;
procedure TForm1.ComboBox11Change(Sender: TObject);
begin
if form1.ComboBox11.ItemIndex=0 then ByteArr[6]:=100;
if form1.ComboBox11.ItemIndex=1 then ByteArr[6]:=10;
if form1.ComboBox11.ItemIndex=2 then ByteArr[6]:=1;
end;
procedure TForm1.ComboBox12Change(Sender: TObject);
begin
if form1.ComboBox12.ItemIndex=0 then ByteArr[7]:=1;
if form1.ComboBox12.ItemIndex=1 then ByteArr[7]:=10;
if form1.ComboBox12.ItemIndex=2 then ByteArr[7]:=100;
end;
procedure TForm1.Button1Click(Sender: TObject);
var
```

```
i:integer;
begin
L:=0;
M:=0;
S:=0;
Label15.Caption:='';
Form3.Show;
for i := 1 to 7 do
begin
ifByteArr[i]=100 then
L:=L+1;
ifByteArr[i]=10 then
M:=M+1;
ifByteArr[i]=1 then
S:=S+1;
end;
Label15.Caption:= 'Низкая';
if (L>=5) and (S=0) then
Label15.Caption:='Средняя';
if (S<>0) and (L+M>=5) then
Label15.Caption:='Низкая';
end;
procedure TForm1.Button2Click(Sender: TObject);
begin

W:=CreateOleObject('Word.Application');
W.Documents.Open(FileName := 'C:\Model\1.docx');
RichEdit1.Text := W.ActiveDocument.Range.Text;
W.Quit;
W1:= CreateOleObject('Word.Application');
W1.Documents.Open(FileName := 'C:\Model\2.docx');
RichEdit2.Text := W1.ActiveDocument.Range.Text;
W1.Quit;
W2:= CreateOleObject('Word.Application');
W2.Documents.Open(FileName := 'C:\Model\3.docx');
RichEdit3.Text := W2.ActiveDocument.Range.Text;
```

```
W2.Quit;
W3:= CreateOleObject('Word.Application');
W3.Documents.Open(FileName := 'C:\Model\4.docx');
RichEdit4.Text := W3.ActiveDocument.Range.Text;
W3.Quit;
Word:=CreateOleObject('Word.Application');
Word.Documents.Open(FileName := 'C:\Model\0.docx');
Word.ActiveDocument.Range.InsertAfter(RichEdit1.Text);
Word.ActiveDocument.Range.InsertAfter(RichEdit2.Text);
Word.ActiveDocument.Range.InsertAfter(RichEdit3.Text);
Word.ActiveDocument.Range.InsertAfter(RichEdit4.Text);
Word.Visible:=Visible;
end;
end.
```

Модульитоговогоокна

```
unitUnit3;

interface

uses
  Windows, Messages, SysUtils, Variants, Classes, Graphics, Controls, Forms,
  Dialogs, Grids, StdCtrls;

type
  TForm3 = class(TForm)
    StringGrid1: TStringGrid;
    Memo1: TMemo;
    Button1: TButton;
    Button2: TButton;
    Button3: TButton;
    Button4: TButton;
    Button5: TButton;
procedureFormCreate(Sender: TObject);
private
{ Private declarations }
public
```

```
{ Public declarations }
end;
var
  Form3: TForm3;
implementation
{$R *.dfm}
procedure TForm3.FormCreate(Sender: TObject);
begin
StringGrid1.Cells[0,0]:='Множествоугроз';
StringGrid1.Cells[1,0]:='Предпосылки';
StringGrid1.Cells[2,0]:='Меры';
StringGrid1.Cells[3,0]:='Коэффициент Y1';
StringGrid1.Cells[4,0]:='Возможностьреализации';
StringGrid1.Cells[5,0]:='Коэффициент Y2';
StringGrid1.Cells[6,0]:='Опасность';
StringGrid1.Cells[7,0]:='Актуальность';
end;
end.
```

Модуль окна со сведениями об организации

```
unit Unit5;

interface

uses
  Windows, Messages, SysUtils, Variants, Classes, Graphics, Controls, Forms,
  Dialogs, StdCtrls;

type
  TForm5 = class(TForm)
    Edit1: TEdit;
    Edit2: TEdit;
    Edit3: TEdit;
    Edit4: TEdit;
    Label1: TLabel;
    Label2: TLabel;
    Label3: TLabel;
```

```
    Label4: TLabel;
    Button1: TButton;
procedure Button1Click(Sender: TObject);
private
{ Private declarations }
public
{ Public declarations }
end;
var
  Form5: TForm5;
implementation
{$R *.dfm}
procedure TForm5.Button1Click(Sender: TObject);
begin
Form5.Show;
end;
end.
```

Модуль окна определения вероятности

```
unitUnit6;

interface

uses
  Windows, Messages, SysUtils, Variants, Classes, Graphics, Controls, Forms,
  Dialogs, StdCtrls;

type
  TForm6 = class(TForm)
    Label1: TLabel;
    Label2: TLabel;
    Label3: TLabel;
    Label4: TLabel;
    Label5: TLabel;
    Label6: TLabel;
    Label7: TLabel;
    Label8: TLabel;
```

Label9: TLabel;

Label10: TLabel;

Label11: TLabel;

Label12: TLabel;

Label13: TLabel;

Label14: TLabel;

Label15: TLabel;

Label16: TLabel;

Label17: TLabel;

Label18: TLabel;

Label19: TLabel;

Label20: TLabel;

Label21: TLabel;

Label22: TLabel;

Label23: TLabel;

Label24: TLabel;

Label25: TLabel;

ComboBox1: TComboBox;

ComboBox2: TComboBox;

ComboBox4: TComboBox;

ComboBox5: TComboBox;

ComboBox6: TComboBox;

ComboBox7: TComboBox;

ComboBox8: TComboBox;

ComboBox9: TComboBox;

ComboBox10: TComboBox;

ComboBox11: TComboBox;

ComboBox12: TComboBox;

ComboBox13: TComboBox;

ComboBox14: TComboBox;

ComboBox15: TComboBox;

ComboBox16: TComboBox;

ComboBox17: TComboBox;

ComboBox18: TComboBox;

ComboBox19: TComboBox;

ComboBox20: TComboBox;

```
    ComboBox21: TComboBox;
    ComboBox3: TComboBox;
    ComboBox22: TComboBox;
    ComboBox23: TComboBox;
    ComboBox24: TComboBox;
    Button1: TButton;
private
{ Private declarations }
public
{ Public declarations }
end;
var
  Form6: TForm6;
implementation
{$R *.dfm}
end.
```

Модульокнаопределенияопасности

```
unit Unit7;

interface

uses
  Windows, Messages, SysUtils, Variants, Classes, Graphics, Controls, Forms,
  Dialogs, StdCtrls;

type
  TForm7 = class(TForm)
    Label8: TLabel;
    Label9: TLabel;
    Button1: TButton;
    Label3: TLabel;
    Label7: TLabel;
    Label6: TLabel;
    Label5: TLabel;
    Label4: TLabel;
    Label25: TLabel;
```

Label24: TLabel;

Label23: TLabel;

Label22: TLabel;

Label21: TLabel;

Label20: TLabel;

Label2: TLabel;

Label19: TLabel;

Label18: TLabel;

Label17: TLabel;

Label16: TLabel;

Label15: TLabel;

Label14: TLabel;

Label13: TLabel;

Label12: TLabel;

Label11: TLabel;

Label10: TLabel;

Label1: TLabel;

ComboBox9: TComboBox;

ComboBox8: TComboBox;

ComboBox7: TComboBox;

ComboBox6: TComboBox;

ComboBox5: TComboBox;

ComboBox4: TComboBox;

ComboBox3: TComboBox;

ComboBox24: TComboBox;

ComboBox23: TComboBox;

ComboBox22: TComboBox;

ComboBox21: TComboBox;

ComboBox20: TComboBox;

ComboBox2: TComboBox;

ComboBox19: TComboBox;

ComboBox18: TComboBox;

ComboBox17: TComboBox;

ComboBox16: TComboBox;

ComboBox15: TComboBox;

ComboBox14: TComboBox;

```
    ComboBox13: TComboBox;
    ComboBox12: TComboBox;
    ComboBox11: TComboBox;
    ComboBox10: TComboBox;
    ComboBox1: TComboBox;
private
{ Private declarations }
public
{ Public declarations }
end;
var
  Form7: TForm7;
implementation
{$R *.dfm}
end.
```

Приложение 2

Диск с электронной версией диплома, презентации и исходными файлами программы: