ФЕДЕРАЛЬНОЕ АГЕНТСТВО ВОЗДУШНОГО ТРАНСПОРТА
(РОСАВИАЦИЯ)

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ
УНИВЕРСИТЕТ ГРАЖДАНСКОЙ АВИАЦИИ» (МГТУ ГА)

Кафедра основ радиотехники и защиты информации

С.П. Матыюк

МЕНЕДЖМЕНТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Учебно-методическое пособие
по выполнению лабораторных работ № 1–4

для студентов IV курса
специальности 10.05.02
очной формы обучения

Москва
ИД Академии Жуковского
2021

УДК 004.056
ББК 001.8
М34

Рецензент:
Петров В.И. – канд. техн. наук, доцент

Матыюк С.П.
М34 Менеджмент информационной безопасности [Текст] : учебно-методическое пособие по выполнению лабораторных работ № 1–4 / С.П. Матыюк. – М.: ИД Академии Жуковского, 2021. – 28 с.

Данное учебно-методическое пособие издается в соответствии с рабочей программой учебной дисциплины Б1.В.ОД.10 «Менеджмент информационной безопасности» по учебному плану специальности 10.05.02 для студентов IV курса очной формы обучения.

Рассмотрено и одобрено на заседаниях кафедры 26.02.2021 г. и методического совета 23.03.2021 г.

УДК 004.056
ББК 001.8

В авторской редакции

Подписано в печать 13.09.2021 г.
Формат 60х84/16 Печ. л. 1,75 Усл. печ. л. 1,63
Заказ № 792/0616-УМП07 Тираж 40 экз.

Московский государственный технический университет ГА
125993, Москва, Кронштадтский бульвар, д. 20

Издательский дом Академии имени Н. Е. Жуковского
125167, Москва, 8-го Марта 4-я ул., д. 6А
Тел.: (495) 973-45-68
E-mail: zakaz@itsbook.ru

ЛАБОРАТОРНАЯ РАБОТА № 1

Разработка корпоративной политики информационной безопасности

1. Цель работы – получение студентами навыков в работе с нормативными документами, регламентирующими создание корпоративной политики предприятия.

2. Краткие теоретические сведения

По своему назначению корпоративная политика информационной безопасности (ПолИБ) является каркасом, объединяющим все остальные документы, регламентирующие обеспечение и управление ИБ в организации. В нее *рекомендуется включать следующие положения:*

- Определение ИБ в терминах деятельности данной организации, области действия политики, целей, задач и принципов ОИБ организации;
- Изложение намерения ОИБ, направленного на достижение указанных целей и на реализацию принципов ОИБ;
- Общие сведения об активах, подлежащих защите, их классификацию;
- Модели угроз и нарушителей (внутреннего и внешнего) ИБ, на противодействие которым ориентирована корпоративная ПолИБ;
- Высокоуровневое изложение правил и требований по организации информационной безопасности (ОИБ), представляющих особую важность для организации (например, обеспечение соответствия законодательным актам, нормативным документам РФ в области ОИБ и нормативным актам организации; требования к управлению ИБ; требования по предотвращению и обнаружению компьютерных вирусов и другого вредоносного программного обеспечения (ПО); требования по управлению непрерывности бизнеса (УНБ);
- Санкции и последствия нарушений корпоративной ПолИБ;
- Определение общих ролей и обязанностей, связанных с ОИБ, включая информирование об инцидентах ИБ;
- Перечень частных ПолИБ, развивающих и детализирующих положения корпоративной Пол ИБ, а также указание подразделений организации, ответственных за их соблюдение и/или реализацию;
- Положения по контролю реализации корпоративной ПолИБ организации.
- Ответственность за реализацию и поддержку документа;
- Условия пересмотра (выпуска новой редакции) документа;

К разработке и согласованию корпоративной ПолИБ рекомендуется привлекать представителей следующих служб организации, связанных с ее информационной сферой: руководство организации; профильные подразделения; служба информатизации; служба безопасности (ИБ).

Корпоративная ПолИБ обязательно утверждается руководителем организации (например, председателем, генеральным директором, президентом) и в ее названии указывается название организации, которой она принадлежит. Она может быть представлена как комплектом документов, так и единым обобщающим документом.

3. Краткое описание используемого оборудования

Процессор Intel(R) Atom(TM) CPU D525 @ 1.80 GHz, ОЗУ 2.00 Гб.

4. Порядок выполнения работы

4.1 Основные разделы ПолИБ

Корпоративная ПолИБ как политика верхнего уровня должна включать в себя следующие разделы:

Цель (назначение). Корпоративная ПолИБ обычно содержит утверждение, поясняющее, зачем она была разработана. Всегда полезно явно указать цель или причины ее написания. Например, если организация предоставляет услуги по поддержке больших баз данных (БД), тогда ее основными целями могут быть снижение числа ошибок, потери и искажения данных, а также быстрота восстановления после нештатных ситуаций. Для организации, обрабатывающей персональные данные, первостепенной задачей может быть усиленная защита от несанкционированного раскрытия информации о клиентах. Поэтому типовыми являются следующие цели:

- обеспечение устойчивого функционирования организации за счет предотвращения реализации угроз ИБ ее активам, защита законных интересов владельца информации от противоправных посягательств, обеспечении нормальной производственной деятельности всех подразделений организации;
- обеспечение уровня ИБ в конкретных функциональных областях, соответствующего нормативным документам организации и рассчитанного на основе риск-ориентированного подхода (с учетом результатов оценки рисков ИБ);
- выработка планов восстановления после критических ситуаций и ОНБ организации и другие;
- достижение экономической целесообразности в выборе защитных мер;
- реализация подотчетности анализа регистрационной информации и всех действий пользователей с информационными ресурсами и т. п.

Задачами ОИБ являются все действия, которые необходимо выполнить для достижения поставленных целей. В частности, необходимо решать такие задачи, как анализ и управление рисками ИБ, расследование инцидентов ИБ, разработка и внедрение планов ОНБ, повышение квалификации и осведомленности сотрудников в области ИБ и т. д.

Область действия. Перед изложением самой ПолИБ определяется область ее действия с помощью ограничений и условий в понятных всем терминах, которые вводятся в явном виде. Надо уточнить, где, как, когда, кем и к чему

применяется данная ПолИБ. Если, например, говорить о ПолИБ при подключении организации к Интернету, то может понадобиться уточнение, какие соединения, через которые ведется работа с Интернетом (напрямую или опосредованно), охватывает эта политика. ПолИБ также может определять, учитываются ли другие аспекты работы в Интернете, такие как соединение с Интернетом с домашнего компьютера.

ПолИБ точно определяет, какие активы организации она затрагивает персонал, информацию, ПО и АО, устройства, технологии и т. п. Например, защищаемые в рамках ПолИБ активы организации можно описать так: «Положения настоящей ПолИБ распространяются на все виды информации, хранящиеся или передающиеся в организации. В том числе на информацию, зафиксированную на материальных носителях или передающуюся в устной или визуальной форме». Но во многих случаях корпоративная ПолИБ имеет отношение ко всем системам и всем сотрудникам организации без исключения.

Основные положения ПолИБ. В явной форме описывается позиция организации (то есть решение ее руководства) по данному вопросу. Позиция может быть сформулирована как в наиболее общем виде как набор целей, которые преследует организация в данном аспекте, так и конкретизирована.

В ПолИБ требуется кратко описать все процессы и процедуры системы управления (СУИБ). В частности, выделяются такие процедуры, как контроль доступа к активам организации, внесение изменений в ее ИС, взаимодействие с третьими лицами, повышение квалификации сотрудников в области ИБ, расследование инцидентов ИБ, аудит ИБ. В описании каждой процедуры необходимо четко определить цели и задачи процедуры, основные правила ее выполнения, регулярность или сроки выполнения.

Перечисляются конкретные меры, реализующие ПолИБ в организации, дается обоснование выбора именно такого перечня мер и указывается, какие угрозы ИБ для активов наиболее эффективно предотвращаются данными защитными мерами.

С целью формализации процесса управления ИБ в соответствии с ПолИБ требуется создание организационной структуры, которую также требуется описать.

Необходимо предусмотреть период пересмотра ПолИБ, что может быть изложено, например, следующим образом: «Положения Политики ИБ требуют регулярного пересмотра и корректировки не реже одного раза в полгода.

Внеплановый пересмотр Политики ИБ проводится в случаях:

- существенных изменений в национальной законодательной базе в области ИБ;
- внесения существенных изменений в интранет организации;
- возникновения инцидентов ИБ.

При внесении изменений в положения Политики ИБ организации учитываются:

- результаты анализа функционирования СУИБ со стороны руководства организации;

- результаты аудита ИБ (внешнего и внутреннего);

- рекомендации независимых экспертов по ИБ.

Ответственность (роли и обязанности). В этом разделе ПолИБ точно устанавливается, кто и за что отвечает. Указывается, на кого конкретно возлагается ответственность за соблюдение ПолИБ (например, менеджеров, владельцев активов, пользователей, администраторов систем и т. д.). Если для использования ПО сотрудникам требуется разрешение руководства, должно быть известно, у кого и как его можно получить.

Для ПолИБ уместно описание (с краткой детализацией) нарушений, которые неприемлемы, и последствий такого поведения. Могут быть явно перечислены наказания, применяемые к нарушителям ПолИБ (предварительно их нужно согласовывать с соответствующими должностными лицами и отделами и законодательными актами).

За нарушение ПолИБ должны быть предусмотрены конкретные дисциплинарные, административные взыскания и материальная ответственность. Но при этом нельзя забывать, что нарушения ПолИБ бывают и непреднамеренными со стороны сотрудников - они могут быть связаны, например, с отсутствием соответствующих знаний.

Устанавливаются как организационные, так и технические меры реагирования на нарушение ПолИБ. Эти меры предусматривают оповещение об инциденте ИБ, соответствующую реакцию, процедуры восстановления, сбор доказательств, проведение расследования и привлечение нарушителя к ответственности. Система мер по реагированию на инциденты ИБ должна быть скоординирована между ИТ-департаментом, службой безопасности и службой персонала.

Также полезно поставить задачу конкретному подразделению организации следить за соблюдением ПолИБ. Кроме этого, приводится информация о должностных лицах, ответственных за реализацию ПолИБ, и четко устанавливаются их обязанности в отношении разработки и внедрения различных аспектов ПолИБ, а также в случае нарушения политики. Обязанность за общее управление ИБ возлагается на руководство организации. Ответственность сторонних пользователей обязательно оговаривается в соответствующих договорах. Отдельно описывается ответственность за контроль соблюдения ПолИБ.

Соблюдение ПолИБ. Это выражается в соблюдении двух видов соответствий:

1. Общее соответствие, обеспечивающее выполнение требований по разработке ПолИБ и определению ответственности, возложенной на различные организационные структуры поддержания ИБ. Часто на отдел надзора возлагается ответственность за контроль за соблюдением такого соответствия, в

том числе, насколько хорошо организация реализует приоритеты руководства, установленные в ПолИБ.

2. Использование только установленных наказаний и дисциплинарных мер. Поскольку ПолИБ - это высокоуровневый документ, то конкретные меры наказания за различные нарушения, как правило, не детализированы в корпоративной ПолИБ. Поэтому политика может разрешить создание соответствующих структур, которые будут заниматься нарушениями и реализацией конкретных дисциплинарных мер.

Ответственные (консультанты) по вопросам ИБ и справочная информация. Для любой ПолИБ нужны консультанты, с кем можно связаться в случае необходимости и получить квалифицированную помощь, разъяснения и дополнительную информацию по вопросам ОИБ. Можно назначить сотрудника, занимающего конкретную должность консультанта. Например, по некоторым вопросам консультантом может быть один из менеджеров, по другим - начальник отдела, сотрудник технического отдела, системный администратор или сотрудник службы ИБ. Они должны уметь разъяснять положения ПолИБ и правила работы с конкретной системой. В их обязанности входит ознакомление всех новых служащих организации с ПолИБ при поступлении на работу и сообщение об изменениях в политике по мере их внесения. Также должно вестись обучение всех сотрудников основным вопросам ОИБ, а администратор и сотрудники отдела ИБ организации должны регулярно проходить переподготовку с целью повышения квалификации в специализирующихся в этих вопросах учебных заведениях.

4.2 Задание к работе

Разработать корпоративную ПолИБ для следующих организаций:

1. Страховая компания;
2. Авиакомпания;
3. Телекоммуникационная компания.

При написании документа учитывать следующее:

Современные общепризнанные стандарты, описывающими общее содержание комплексной ПолИБ организации (в контексте данного учебного пособия — корпоративной ПолИБ) являются ISO/IEC 27002:2005 и ГОСТ Р ИСО/МЭК 17799-2005. В этих документах отмечается, что ПолИБ как неотъемлемая часть общей политики организации включает, как минимум, следующее:

1. определение ИБ, ее общих целей и области действия, а также раскрытие значимости безопасности как инструмента, обеспечивающего возможность совместного использования информации;
2. изложение целей и принципов ИБ, сформулированных руководством, и соответствующих бизнес-стратегии и целям организации, включая вопросы оценки и управления рисками ИБ;
3. краткое изложение и разъяснение наиболее существенных для организации политик, принципов, правил и требований, например: соответствие

законодательным требованиям и договорным обязательствам; требования в отношении обучения вопросам ИБ; предотвращение появления и обнаружение вирусов и другого вредоносного ПО; УНБ; последствия нарушений и ответственность за нарушения ПолИБ;

4. определение общих и конкретных обязанностей сотрудников в Рамках управления ИБ, включая информирование об инцидентах ИБ;

5. ссылки на документы, дополняющие ПолИБ, например, более детальные политики и процедуры безопасности для конкретных ИС, а также правила безопасности, которым должны следовать пользователи.

5. Содержание отчета

5.1 Корпоративная политика информационной безопасности;

5.2 Анализ документа и выводы.

6. Литература

6.1. ISO/IEC 27002:2005;

6.2. ГОСТ Р ИСО/МЭК 17799-2005.

ЛАБОРАТОРНАЯ РАБОТА № 2

Разработка частной политики информационной безопасности

1. Цель работы – получение студентами навыков разработки частной политики информационной безопасности.

2. Краткие теоретические сведения

Содержания частных ПолИБ по перечню разделов не отличаются от таковых для корпоративной ПолИБ. Все их положения ни в коем случае не должны вступать в противоречия с корпоративной ПолИБ и формируются на основании принципов, требований и задач, определенных в корпоративной ПолИБ, с учетом:

- детализации, уточнения и дополнительной классификации активов и угроз ИБ;
- определения владельцев защищаемых активов;
- оценки рисков ИБ и возможных последствий реализаций угроз ИБ в границах области действия регламентируемой политикой области, системы, технологии, подразделения и т. п.

Не рекомендуется повторение одинаковых правил в различных частных политиках. Включение в частную ПолИБ правила, содержащегося в другой существующей политике, целесообразно осуществлять посредством соответствующей ссылки.

Частные ПолИБ определяют следующее:

- цели и задачи ОИБ, на обеспечение которых направлена частная ПолИБ;
- область действия, определение объектов защиты, уязвимостей, угроз ИБ и оценка рисков ИБ, связанных с объектами защиты;
- сведения о виде деятельности, на ОИБ которой направленно действие положений частной ПолИБ, совокупности банковских технологий, применяемых в рамках выполнение данного вида деятельности, и основных технологических процессов, реализующих указанные технологии;
- определение субъектов (ролей), на которых распространяется действие политики (как структурных подразделений организации, так и отдельных исполнителей);
- содержательную часть (требования и правила);
- обязанности по ОИБ в рамках области действия частной ПолИБ, описание функций субъектов (ролей) над управляемыми объектами в рамках регламентируемых технологических процессов;
- состав ссылочных документов (документы, ознакомление с которыми обязательно для адекватного понимания текста политики);
- положения по контролю реализации политики;
- ответственность за реализацию и поддержку политики;
- условия пересмотра политики.

3. Краткое описание используемого оборудования

Процессор Intel(R) Atom(TM) CPU D525 @ 1.80 GHz, ОЗУ 2.00 Гб.

4. Порядок выполнения работы

4.1 Виды частных политик ИБ

Обобщая лучшие мировые практики написания частных ПолИБ, более подробно рассмотрим *ПолИБ по конкретному вопросу (проблеме, области)*. Также как и корпоративная, данная ПолИБ обычно распространяется на организацию в целом.

Описание вопроса. Чтобы сформулировать такую ПолИБ, сначала необходимо описать проблему с учетом принятой терминологии, её особенностей и условий успешного разрешения. Кроме того, часто бывает полезно указать цели или обоснование политики, которые могут быть полезны при ее реализации. Например, организации нужно разработать политику использования «неофициального» ПО, под которым понимается любое ПО, не одобренное официально, не переданное, не администрируемое и не находящееся в собственности организации. Кроме того, должны быть оговорены некоторые условия, например, для ПО, находящегося в собственности сотрудников, но одобренного для использования в их работе, и для ПО бизнес-партнеров организации.

Описание позиции организации. Четко излагается позиция организации (т. е. решение руководства) по данному вопросу. Продолжая предыдущий пример, это будет означать заявление, когда использование неофициального ПО

запрещено - во всех или отдельных случаях, есть ли дополнительные руководящие указания по его возможному утверждению и использованию, возможны ли некоторые исключения из правил, когда, как и на какой основе их получить.

Применимость. Здесь уточняется, где, как, когда, к кому и какая конкретно политика применяется. Например, это может означать, что упомянутая политика использования неофициального ПО предназначена для применения только в основном офисе организации его сотрудниками и не применима к сотрудникам офисов, расположенных в других регионах. Кроме того, необходимо уточнение применения политики к сотрудникам, работающим в нескольких офисах и/или на дому.

Роли и ответственность. Например, если политика позволяет после соответствующего согласования использовать в работе неофициальное ПО, находящееся в собственности работников, то должно быть указано, как и где официально получить такое разрешение. Также необходимо уточнить, кто будет нести ответственность за обеспечение того, чтобы только рекомендованное ПО используется на компьютерах организации и, возможно, осуществлять мониторинг компьютеров с целью обнаружения неофициального ПО.

Вопросы соответствия. Для некоторых типов политики может быть целесообразно описать, с некоторыми деталями, неприемлемые нарушения и последствий такого поведения. Наказания могут быть сформулированы вполне конкретно и должны быть согласованы с кадровой политикой организации, соответствующими должностными лицами и ведомствами и, возможно, общественными организациями (например, профсоюзами). Желательно, чтобы какое-либо подразделение организации осуществляло контроль за таким соответствием.

Контактные лица и дополнительная информация. Конкретные фамилии в данном разделе не указываются, а пишутся только должности лиц, к которым следует обращаться за дополнительной информацией и разъяснениями.

В поддержку рассмотренной политики обычно создаются руководства и описываются процедуры. Для рассмотренного примера может быть создано руководство по проверке дисков и других мобильных устройств, приносимых сотрудниками из дома или привозимых из командировки в другой офис.

ПолИБ для конкретной системы особенно важна для использования и обеспечения ИБ этой системы. В разных подразделениях организации могут использоваться различные системы (например, информационные), поэтому данная политика чаще всего имеет более узкую направленность, чем корпоративная. Она обязательно должна учитывать позицию тех, кто с этими системами непосредственно работает.

Разработать последовательную ПолИБ для конкретной системы можно, только выводя правила из целей ОИБ в поддержку основного назначения самой системы. Поэтому для такой ПолИБ полезно рассмотреть двухуровневую модель: цели ОИБ и функциональные правила ОИБ, которые тесно

взаимосвязаны и часто трудно различимы с технической точки зрения их осуществления.

Цели ОИБ системы. Процесс их определения начинается с анализа потребности в обеспечение конфиденциальности, целостности и доступности для достижения основных целей использования системы. Но только такой формулировки не достаточно - цели должны быть указаны более конкретно. Они должны быть достижимы на практике и согласованы с целями других политик организации. Цели формулируются в виде ряда утверждений в отношении защищаемых ресурсов, с которыми работает система. Они должны учитывать допустимые в организации затраты на их достижение, а также функциональные, технические и другие ограничения.

Роли по ОИБ системы. Детализируются и формализуются правила назначения ответственности за ОИБ, правила использования системы и последствия их несоблюдения. Выделяются правила функционирования системы. Например, определяется санкционированное и несанкционированное изменение ее настроек, кто (по должности, рабочему положению и т. п.) может вносить санкционированные изменения (например, модифицировать, уничтожать и т. д.), в какие типы данных и при каких условиях. Степень детализации этих положений может быть различна. Чем более точно установлены правила, тем проще выявить, когда и кем они были нарушены, и автоматизировать обнаружение таких событий. Это создает определенные вычислительные сложности, поэтому при установлении, например, прав доступа лучше всего пользоваться принципом разумной достаточности.

Любые обоснованные отклонения от соблюдения корпоративной ПодИБ или общей практики при работе с рассматриваемой системой должны бггь оговорены.

Реализация политики. Описываются все аспекты ОИБ системы, включая организационные, технические и другие. Ограничение физического доступа в помещения, контроль логического доступа, системы обнаружения вторжений (СОВ), защита компьютеров от загрузки с дискет, контроль за работой ПО, регулярный внутренний аудит - лишь некоторые из средств, которые могут участвовать в реализации политики на практике.

4.2 Задания к работе

Разработать частные ПолИБ учитывая корпоративную ПолИБ для следующих организаций:

1. Страховая компания:
- ПолИБ работы с конфиденциальной информацией;
- ПолИБ антивирусной защиты.
2. Авиакомпания:
- ПолИБ аудита ИБ;
- ПолИБ веб-сервера компании.
3. Телекоммуникационная компания:

- ПолИБ оценки рисков ИБ;
- ПолИБ виртуальных частных сетей.

5. Содержание отчета

5.1.Корпоративная политика информационной безопасности;
5.2.Анализ документа и выводы.

6. Литература

5.1. ISO/IEC 27002:2005;
5.2. ГОСТ Р ИСО/МЭК 17799-2005.

ЛАБОРАТОРНАЯ РАБОТА № 3

Инструментальное средство управления рисками КОНДОР

1. Цель работы – Изучить возможности инструментальных средств управления рисками КОНДОР. Отработать навыки с программными средствами построенных с помощью SSADM.

2. Краткие теоретические сведения

Для управления рисками ИБ и проведения их оценки разработаны разнообразные методы, начиная от простых подходов, основанных на анкетах с вопросами и ответами, и заканчивая методами, использующими структурный анализ. Существует множество различных методов оценки рисков ИБ. Некоторые из них основаны на достаточно простых табличных подходах и не предполагают применения специализированного ПО, другие, наоборот, его используют.

В табличных методах можно наглядно отразить связь факторов негативного воздействия на активы организации и значении вероятностей реализации угроз ИБ с учетом используемых ими уязвимостей. Применение каких-либо инструментальных средств не является обязательным, однако позволяет уменьшить трудоемкость процессов оценки рисков ИБ и выбора защитных мер. Так, завершив в первый раз процесс оценки рисков ИБ, необходимо сохранить и документировать результаты этого процесса (активы и оценки их ценности, требования ИБ и уровни рисков ИБ, а также идентифицированные элементы управления рисками ИБ), например, в БД. Средства программной поддержки могут значительно облегчить эту работу, а также все будущие действия по повторной переоценке.

В организации рекомендуется сначала внедрить политику управления

рисками ИБ и методологию оценки рисков ИБ и провести первоначальную высокоуровневую оценку рисков вручную, а затем перейти к выбору инструментов, которые бы соответствовали выбранному подходу и облегчали выполнение основных операций по оценке рисков ИБ. Положительный эффект от использования таких инструментов может быть значительно выше при детальной оценке рисков ИБ, предполагающей рассмотрение большого количества рисков, так как в этом случае аналитическая работа существенно усложняется.

Основными преимуществами использования ПО оценки рисков ИБ являются:

- автоматизация алгоритма процесса оценки рисков ИБ;
- унификация методологии оценки рисков ИБ, обеспечивающая воспроизводимость результатов;
- интеграция с другими системами управления организации, со средствами контроля соответствия и с системами защиты информации;
- поддержание в актуальном состоянии реестров активов, уязвимостей, угроз ИБ и требований ИБ;
- автоматическое формирование планов обработки рисков ИБ и деклараций о применимости;
- документирование процессов и жизненного цикла СУИБ.

Что должно обеспечивать средство для оценки рисков ИБ? Приводимый ниже список позволяет получить некоторое представление о критериях, которые следует учесть при выборе конкретного решения:

- средство должно, по меньшей мере, содержать модули сбора данных, анализа, вывода результатов;
- должны охватываться все компоненты риска ИБ и взаимосвязь между ними;
- метод, на основе которого работает и функционирует выбранное средство, должен отражать политику организации и общий подход к оценке рисков ИБ;
- если в процессе управления требуется выполнить сравнение альтернативных вариантов и выбрать адекватные, надежные и экономически эффективные элементы управления рисками ИБ, то важнейшей частью этого процесса является эффективное предоставление результатов, поэтому данное средство должно обеспечивать предоставление отчетов с результатами в понятном и четком виде;
- возможность вести архив информации, полученной на этапе сбора

данных, и архив аналитических данных которые могут пригодиться при проведении последующих оценок рисков ИБ или запросов;

- должна быть доступна документация, описывающая данное средство, поскольку она играет важную роль в его эффективном использовании;

выбранное средство должно быть совместимо с программным и аппаратным обеспечением, используемым в организации;

- автоматизированные средства, как правило, эффективны и свободны от ошибок, но некоторые из них могут иметь сложные процессы установки или использования, поэтому может возникнуть необходимость рассмотреть доступность программ обучения и поддержки;

- эффективное применение данного средства частично зависит от того, насколько хорошо пользователь понимает этот продукт, а также от корректной установки и конфигурации используемого средства, поэтому большое значение может иметь наличие руководства по установке и использованию и сопровождение в виде обучения и постоянной поддержки.

В настоящее время на рынке есть около двух десятков программных продуктов для оценки рисков ИБ: от простейших, ориентированных на базовый уровень ИБ, до сложных и дорогостоящих, позволяющих реализовать полный вариант оценки рисков ИБ и выбрать комплекс защитных мер требуемой эффективности.

Они представляют собой инструментарий для выполнения следующих операции:

- построения модели ИС с позиции ИБ;
- оценки ценности активов;
- составления списка угроз ИБ и уязвимостей, оценки их характеристик;
- выбора защитных мер и анализа их эффективности;
- анализа вариантов построения защиты;
- документирования (генерация отчетов).

3. Краткое описание используемого оборудования

Процессор Intel(R) Atom(TM) CPU D525 @ 1.80 GHz, ОЗУ 2.00 Гб.

4. Порядок выполнения работы

КОНДОР – мощная система разработки и управления политикой безопасности информационной системы компании на основе стандарта ISO 17799. КОНДОР 2006 - это инструмент для разработки всех основных положений политики информационной безопасности компании и управления процессом внедрения этих положений на практике.

Система КОНДОР:

- Определяет все слабые места в политике безопасности информационной системы.

- Анализирует риск невыполнения каждого положения политики безопасности и ранжирует их по степени критичности, что дает возможность определить приоритет планируемых действий.

- Позволяет эффективно управлять рисками, возникающими в связи с невыполнением положений политики безопасности.

Основные понятия и допущения модели

Контрмера - действие, которое необходимо выполнить для закрытия уязвимости.

Риск до задания контрмер - вероятный ущерб, который понесет организация при реализации угроз информационной безопасности, зависящий от защищенности системы.

Риск после задания контрмер - значение риска, пересчитанного с учетом задания контрмер (закрытия уязвимостей).

Эффективность комплекса контрмер - оценка, показывающая, на сколько снизился уровень риска после задания комплекса контрмер по отношению к первоначальному уровню риска.

4.1 Подготовка к выполнению лабораторной работы

Для выполнения лабораторной работы вам понадобится предварительно установленная среда виртуализации с операционной системой Windows XP

4.1.1*Запуск в локальном режиме работы*

Для запуска в локальном режиме запустите и закройте ПО «КОНДОР 2006», после запуска на панели задач в правой части появиться иконка «DS Office Агент» (рис.1.). Нажмите правой кнопкой мыши на неё и выберете пункт «Переключиться в локальный режим», соглашаемся со всеми всплывающими окнами. Теперь снова можно запустить ПО «КОНДОР 2006» и пройти регистрацию.

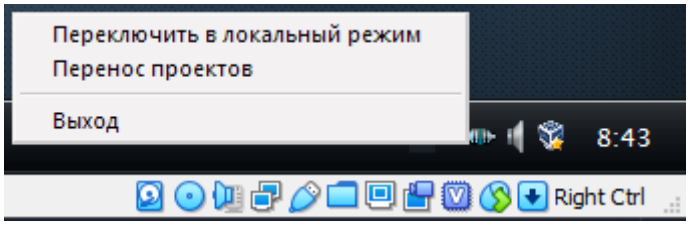

Рис. 1

4.1.2 Запуск в серверном режиме работы

Для работы в сетевом режиме вам понадобиться запустить DS Office Сервер, для этого перейдите в Пуск>Все программы>Digital Security Office 2006 Сервер> Digital Security Office Управление Сервером. На панели задач справа появиться иконка «DS Office Управление сервером» кликаем правой кнопкой

мыши по нему > Администрирование > Вводим пароль который вводили при установке сервера > перейдите во в кладку «Управление пользователями», и создайте несколько пользователей с правами администратора(Желательно на одного человека две записи) (рис. 2).

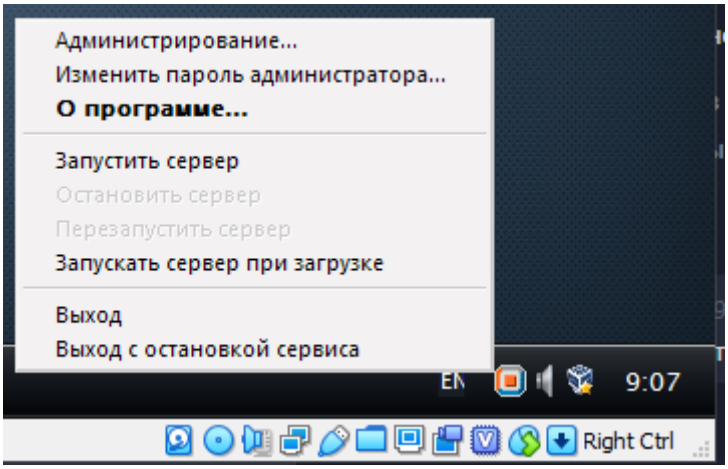

Рис. 2

Запустите «КОНДОР 2006» и ведите данные пользователя и IP адрес сервера.

4.1.3 Построение модели ИС с позиции ИБ

Для построения модели ИБ необходимо ответить на все вопросы всех частей ИС, после чего заполнить информацию о расходах на Информационную безопасность.

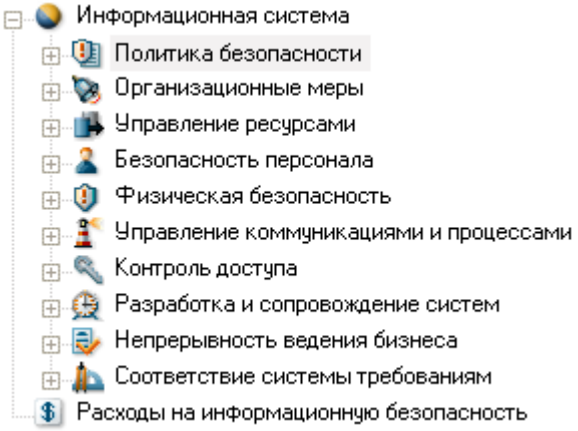

Рис. 3

Для ответа на вопросы выберите вопрос и нажмите «Изменить».

Проанализируйте полученный отчёт, и сделайте выводы.

Задайте необходимые контрмеры

Для того чтобы задать контрмеры перейдите (Контрмеры->Управление рисками).

Для задания контрмеры выполните следующие шаги:

1. Выберите раздел и невыполненное требование, для которого необходимо задать контрмеру.

Для удобства можете воспользоваться Заданием уровня риска.

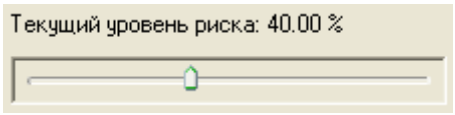

Рис. 4

Данный параметр является фильтром требований по уровням риска. Он позволяет отображать на рабочем поле только те положения, невыполнение которых повлечет больший риск, чем тот, который приемлем для Вас.

2. Нажмите кнопку «Задать».

3. В окне "Новая контрмера" введите необходимые данные

Введите название контрмеры для отчета (не более 64 символов).

Укажите стоимость внедрения контрмеры.

Укажите возможное снижение затрат на информационную безопасность.

Примечания

- После применения контрмеры в поле "Изменение затрат после внедрения контрмер" (раздел "Расходы на информационную безопасность") отобразится значение, равное разности стоимости внедрения контрмеры и возможного снижения затрат на информационную безопасность.

- При применении следующей контрмеры значение "Изменение затрат после внедрения контрмер" суммируется с предыдущим значением.

4. При необходимости введите полное описание контрмеры.

Примечание

Введенное описание в отчете не выводится.

5. Нажмите кнопку «Задать».

Примечание

В отчет выводятся только те контрмеры, которые заданы, но не применены.

6. Создайте отчёт, после того как вы ввели контрмеры и проанализируйте его.

Это можно сделать, выбрав сверху вкладку (Отчёт / Создать отчёт)

7. Примените все заданные контрмеры.

Для того чтобы применить контрмеры перейдите (Контрмеры / Применить контрмеры).

8. Создайте второй отчёт.

9. Сравните два отчёта и сделайте выводы.

5. Содержание отчета

5.1 Цель работы;
5.2 Сгенерированный отчёт до применения контрмер;
5.3 Анализ сгенерированного отчёта;
5.4 Сгенерированный отчёт после применения контрмер;
5.5 Анализ и сравнение двух сгенерированных отчётов.

6. Литература

6.1. Основы управления информационной безопасностью. Учебное пособие для вузов. А.П. Курило, Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. - М.: Горячая линия - Телеком, 2014.

6.2. Управление рисками информационной безопасности. Учебное пособие для вузов. Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. - М.: Горячая линия - Телеком, 2014.

ЛАБОРАТОРНАЯ РАБОТА № 4

Инструментальное средство управления рисками ГРИФ

1. Цель работы – Изучить программу ГРИФ, построить модель информационной системы организации, на основе которой проанализировать риск и защищенность ресурсов.

2. Краткие теоретические сведения

ГРИФ - комплексная система анализа и управления рисками информационной системы компании. ГРИФ 2006 дает Вам полную картину защищенности информационных ресурсов в Вашей системе и позволяет выбрать оптимальную стратегию защиты информации Вашей компании.

Система ГРИФ:

- Анализирует уровень защищенности всех ценных ресурсов компании;
- Оценивает возможный ущерб, который понесет компания в результате реализации угроз информационной безопасности;
- Позволяет эффективно управлять рисками при помощи выбора контрмер, наиболее оптимальных по соотношению цена/качество.

Система ГРИФ 2006 предоставляет возможность проводить анализ рисков Вашей информационной системы при помощи анализа модели информационных потоков или модели угроз и уязвимостей в зависимости от того, какие исходные данные есть в Вашем распоряжении, а также от того, какие данные Вас интересуют на выходе.

При работе с моделью информационных потоков, в систему вносится полная информация обо всех ресурсах с ценной информацией, о пользователях, имеющих доступ к этим ресурсам, о видах и правах доступа. Заносятся данные

обо всех средствах защиты каждого ресурса, сетевые взаимосвязи ресурсов, а также характеристики политики безопасности компании. В результате получается полная модель информационной системы.

Работа с моделью анализа угроз и уязвимостей подразумевает определение уязвимостей каждого ресурса с ценной информацией и подключение соответствующих угроз, которые могут быть реализованы через данные уязвимости. В результате получается полная картина того, какие слабые места есть в Вашей информационной системе и тот ущерб, который может быть нанесен.

2.1. Основные понятия и допущения модели

Бизнес-процессы - это производственные процессы, в которых обрабатывается ценная информация.

Веб-сервер - ресурс, не содержащий ценную информацию, к которому возможен неконтролируемый доступ анонимных пользователей из Интернет.

Группа пользователей - это группа пользователей, имеющая одинаковый класс и средства защиты. Субъект, осуществляющий доступ к информации.

Время простоя сетевого устройства - время, в течение которого доступ, осуществляемый с помощью сетевого устройства, к информации ресурса невозможен из-за отказа в обслуживании сетевого устройства.

Дополнительное время простоя ресурса - дополнительное к базовому время простоя, в течение которого доступ к информации ресурса невозможен. Обусловлено неадекватной работой программного или аппаратного обеспечения ресурса. Указывается в часах в год.

Доступ осуществляется при помощи VPN - доступ к информации осуществляется с помощью защищенного криптографическими средствами соединения.

Информационная система - это организационно упорядоченная совокупность документов (массивов документов) и информационных технологий, в том числе с использованием средств вычислительной техники и связи, реализующих информационные процессы.

Информация -_ ценная информация, хранящаяся и обрабатываемая в информационной системе. Т.е. объект, к которому осуществляется доступ. Исходя из допущений данной модели, вся информация является ценной, т.к. оценить риск неценной информации не представляется возможным.

Класс группы пользователей - это особая характеристика группы, показывающая, как осуществляется доступ к информации.

Основные классы групп пользователей:

- Авторизованные пользователи из Интернет - пользователи, осуществляющие авторизованный доступ к ресурсам организации из Интернет.
- Анонимные пользователи из Интернет - пользователи, осуществляющие неавторизованный доступ к открытым ресурсам организации из Интернет.
- Менеджеры - руководители среднего звена, имеющие удаленный и/или локальный доступ к ресурсам из офиса организации.

- Мобильные пользователи - сотрудники организации, осуществляющие авторизованный доступ к ресурсам организации по телекоммуникационным каналам (например, находясь в командировке).
- Офицеры безопасности - пользователи, имеющие исключительные привилегии при доступе к ресурсам организации и администрировании информационной системы организации (специалисты, отвечающие за обеспечение информационной безопасности системы).
- Пользователи - обычные сотрудники, имеющие удаленный и/или локальный доступ к ресурсам из офиса организации.
- Системные администраторы - пользователи, имеющие исключительные привилегии при доступе к ресурсам организации и администрировании информационной системы организации (специалисты, отвечающие за конфигурирование и настройку информационной системы).
- Сотрудники, осуществляющие доступ через Интернет - сотрудники организации, осуществляющие доступ к ресурсам компании через Интернет из офиса (филиала) организации.
- Сотрудники, осуществляющие доступ через модем - сотрудники организации, осуществляющие доступ к ресурсам компании по модемному соединению из офиса организации.
- Топ-менеджеры - руководители высшего звена, имеющие удаленный и/или локальный доступ к ресурсам из офиса организации.

Коммутатор - концентратор, который может одновременно устанавливать соединения между несколькими парами портов и реализует виртуальные соединения между сетевыми сегментами.

Контрмера - это действие, которое необходимо выполнить для закрытия уязвимости

Концентратор - многопортовое устройство, используемое для усиления сигналов при передаче данных.

Коэффициент локальной защищенности информации на ресурсе - _рассчитывается, если к информации осуществляется только локальный доступ. В этом случае клиентское место группы пользователей и ресурс, на котором хранится информация, совпадают, поэтому защищенность группы пользователей отдельно оценивать не нужно.

Коэффициент локальной защищенности рабочего места группы пользователей -_рассчитывается, когда группа пользователей осуществляет удаленный доступ к информации; это сумма значений эффективности средств защиты субъекта или клиентского места группы пользователей. Данный коэффициент невозможно определить для групп анонимных и авторизованных Интернет-пользователей.

Коэффициент удаленной защищенности информации на ресурсе -_ рассчитывается, когда к информации осуществляется удаленный доступ; это сумма значений эффективности средств защиты объекта.

Критичность ресурса - степень значимости ресурса для информационной системы, т.е. как сильно реализация угроз информационной безопасности на ресурс повлияет на работу информационной системы.

Локальный доступ - доступ к ресурсу, который осуществляется без использования каналов связи. Примечание: к ресурсам "Рабочая станция", "Мобильный компьютер" и "Твердая копия" возможен только локальный доступ.

Маршрутизатор - устройство, обеспечивающее трафик между локальными сетями, имеющими разные сетевые адреса.

Мобильный компьютер - ресурс, содержащий ценную информацию, к которому возможен только локальный доступ. Пользователь имеет возможность выносить мобильный компьютер за пределы офиса организации.

Моделирование системы - раздел, в котором заносятся данные обо всех объектах существующей информационной системы (отделы, сетевые группы, ресурсы, сетевые устройства, виды информации, группы пользователей, бизнес-процессы).

Модем - внешнее или внутреннее устройство, подключаемое к компьютеру для передачи и приема сигналов по телекоммуникационным линиям.

Отдел - это структурное подразделение организации.

Политика безопасности - раздел, в котором приведены вопросы, учитывающие организационные меры обеспечения информационной безопасности, т.е. аспекты, которые невозможно отобразить при построении модели информационной системы.

Права доступа - права пользователей при доступе к информации.

- чтение - право на чтение.
- запись - право на запись (модификацию).
- удаление - право на удаление.

Рабочая станция - ресурс, содержащий ценную информацию, к которому возможен только локальный доступ.

Расходы на информационную безопасность - это затраты организации на обеспечение информационной безопасности, включающие затраты на приобретение систем защиты информации и управление ими, стоимость обучения персонала.

Ресурс - это физический ресурс, на котором располагается ценная информация (сервер, рабочая станция, мобильный компьютер и т.д.).

Риск - это вероятный ущерб, который понесет организация при реализации угроз информационной безопасности, зависящий от защищенности системы.

Риск после задания контрмер - это значение риска, пересчитанного с учетом задания контрмер (закрытия уязвимостей).

Связи - раздел, в котором определяются связи между объектами, занесенными в разделе "Моделирование системы".

Сервер - ресурс, содержащий ценную информацию, к которому возможен удаленный доступ.

Сетевая группа - это группа, в которую входят физически взаимосвязанные ресурсы.

Твердая копия - носитель, содержащий ценную информацию (CD, дискета, кассета, жесткий диск, бумажные документы и т.д.)

Точка доступа - коммутатор беспроводной связи.

Угроза - действие, которое потенциально может привести к нарушению безопасности.

Удаленный доступ - доступ к ресурсу, который осуществляется с использованием каналов связи (локальная сеть организации, телекоммуникационные сети и т.д.).

Ущерб по угрозе Доступность - ущерб, который понесет организация при блокировании доступа к ценной информации (за один час).

Ущерб по угрозе Конфиденциальность - ущерб, который понесет организация в случае несанкционированного раскрытия или перехвата ценной информации.

Ущерб по угрозе Целостность - ущерб, который понесет организация при уничтожении или изменении ценной информации.

Уязвимость - слабое место в информационной системе, наличие которого может привести к нарушению безопасности путем реализации некоторой угрозы (отсутствие средства защиты ресурса, информации или рабочего места группы пользователей, а также доступ группы пользователей к информации).

Эффективность комплекса контрмер - это оценка, насколько снизился уровень риска после задания комплекса контрмер по отношению к первоначальному уровню риска.

3. Краткое описание используемого оборудования

Процессор Intel(R) Atom(TM) CPU D525 @ 1.80 GHz, ОЗУ 2.00 Гб**.**

4. Порядок выполнения работы

4.1. Запустить программу ГРИФ. На экране появится окно, в которое необходимо ввести имя пользователя и пароль.

4.2. В появившемся окне алгоритм "Анализ модели информационных потоков" и нажать «Открыть проект». Если же у вас нету готовых проектов КОНДОР, то создайте проект, нажав «Создать проект».

4.3. Для построения модели информационной системы организации, на основе которой будут анализироваться риск и защищенность ресурсов, необходимо сначала занести данные о системе. Для этого необходимо в рабочем меню выбрать: Проекта-Свойства проекта и в закладке «Идентификация» ввести данные о системе. Пример показан на (рис. 1).

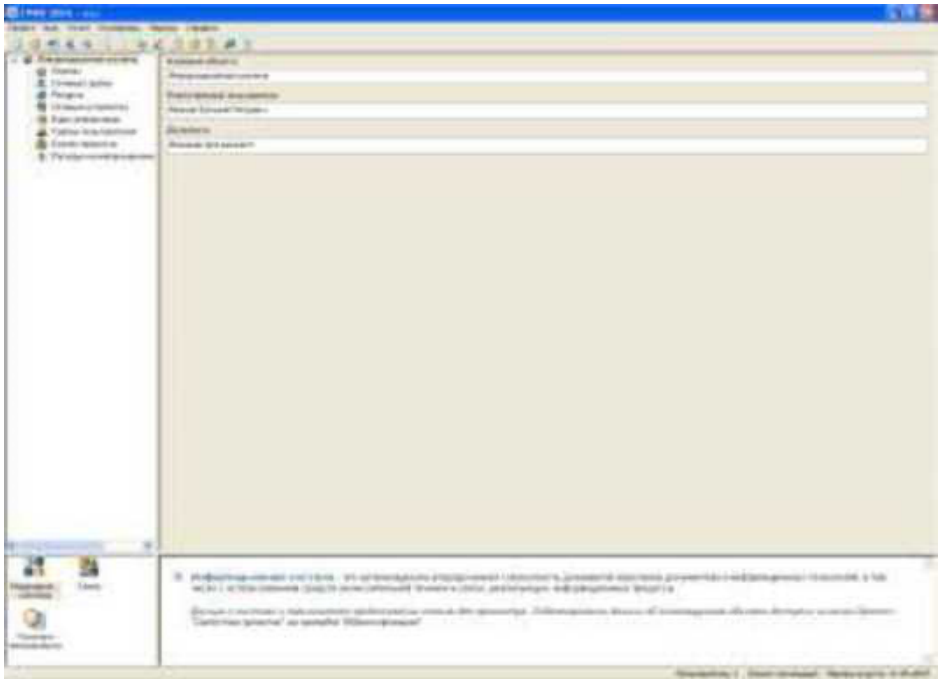

Рис. 1

4.4. В раздел «Моделирование системы» занести данные обо всех объектах существующей информационной системы (отделы, сетевые группы, ресурсы, сетевые устройства, виды информации, группы пользователей, бизнес-процессы).

4.4.1 Открыть элемент информационной системы «Отделы» и согласно вашему варианту ввести название отдела.

Для создания нового отдела выполните следующие шаги:

- Нажать кнопку «Добавить».
- Ввести название нового отдела.
- При необходимости ввести комментарий.
- Нажать кнопку «Добавить» или клавишу «Enter». Созданный отдел появится на рабочем поле.
- Для закрытия окна нажать кнопку «Закрыть» или клавишу «Esc».

4.4.2 Сетевые группы записываются аналогично пункту 4.1.

4.4.3 Для создания нового ресурса выполните следующие шаги:

- Нажать кнопку «Добавить».
- Ввести название нового ресурса.
- Указать тип ресурса.
- Укажите параметр "Дополнительное время простоя".
- В раскрывающемся списке "Укажите сетевую группу" выберите ту сетевую группу, к которой принадлежит добавляемый ресурс. Данный раскрывающийся список - перечень сетевых групп, добавленных в информационную систему. Ресурс может не принадлежать ни к одной сетевой группе.

- В раскрывающемся списке "Укажите отдел" выберите тот отдел, к которому принадлежит добавляемый ресурс. Данный раскрывающийся список - перечень отделов, добавленных в информационную систему. Ресурс может не принадлежать ни к одному отделу.

- При необходимости введите комментарий.

- Нажмите кнопку «Добавить» или клавишу «Enter». Созданный ресурс появится на рабочем поле.

- Для закрытия окна нажмите кнопку «Закрыть» или клавишу «Esc».

4.4.4 Для создания нового сетевого устройства выполнить следующие шаги:

- Нажать кнопку «Добавить».

- Ввести название сетевого устройства.

- Указать тип сетевого устройства:

- Указать параметр "Время простоя".

- При необходимости ввести комментарий.

- Нажать кнопку «Добавить» или клавишу «Enter». Созданное сетевое устройство появится на рабочем поле.

- Для закрытия окна нажать кнопку «Закрыть» или клавишу «Esc».

4.4.5 Для создания нового вида информации выполнить следующие шаги:

- Нажать кнопку «Добавить».

- Ввести название нового вида информации.

- При необходимости ввести комментарий.

- Нажать кнопку «Добавить» или клавишу «Enter». Созданный вид информации появится на рабочем поле.

- Для закрытия окна нажмите кнопку «Закрыть» или клавишу «Esc».

4.4.6 Для создания новой группы пользователей выполнить следующие шаги:

- Нажать кнопку «Добавить».

- Ввести название группы пользователей.

- Указать класс группы пользователей.

- Указать параметр "Число пользователей в группе", произвольно.

- Указать параметр "Данной группе разрешен доступ в Интернет".

- Параметр "Данной группе разрешен доступ в Интернет" означает, что группа пользователей имеет доступ к ресурсам, расположенным в сети Интернет, однако, доступ к ресурсам организации данная группа пользователей получает напрямую, не используя сеть Интернет.

- Указать, какие средства используются для защиты рабочего места пользователя, по усмотрению.

- При необходимости ввести комментарий.

- Нажать кнопку «Добавить» или клавишу «Enter». Созданная группа пользователей появится на рабочем поле.

4.4.7 Для закрытия окна нажмите кнопку «Закрыть» или клавишу «Esc».

4.4.8 Для создания нового бизнес-процесса выполнить следующие шаги:

- Нажать кнопку «Добавить».

- Ввести название нового бизнес-процесса.

- При необходимости ввести комментарий.

- Нажать кнопку «Добавить» или клавишу {Enter}. Созданный бизнес-процесс появится на рабочем поле.

- Для закрытия окна нажать кнопку «Закрыть» или клавишу «Esc».

4.4.9 Для того, что бы задать расходы необходимо:

- Открыть элемент информационной системы «Расходы на информационную безопасность».

- Нажать на кнопку 0 . В появившемся окне задать расходы.

- Ввести значение расходов, по своему усмотрению.

- Нажать кнопку OK или клавишу «Enter».

- Для закрытия окна нажать кнопку Отмена или клавишу «Esc».

4.5. В разделе «Связи» определяются связи между объектами, занесенными в разделе "Моделирование системы".

4.5.1 Для добавления вида информации выполнить следующие шаги:

- Нажать кнопку «Добавить».

- В раскрывающемся списке выбрать вид информации.

- Указать ущерб по угрозам.

- Нажать кнопку «Добавить» или клавишу «Enter». Выбранный вид информации появится на рабочем поле.

- Для закрытия окна нажать кнопку «Закрыть» или клавишу «Esc».

4.5.2 Для добавления группы пользователей выполнить следующие шаги:

- Нажать кнопку «Добавить».

- В раскрывающемся списке выбрать группу пользователей.

- Указать параметр "Вид доступа".

- Указать параметр "Права доступа".

- Для удаленного доступа к ресурсу "Сервер" указать параметр "Доступ осуществляется при помощи VPN".

- Нажать кнопку «Добавить» или клавишу «Enter». Выбранная группа пользователей появится на рабочем поле.

- Для закрытия окна нажать кнопку «Закрыть» или клавишу «Esc».

4.5.3 Для выбора сетевых устройств, через которые группа пользователей осуществляет доступ к ресурсу "Сервер", выполнить следующие шаги:

- Отметить используемые сетевые устройства. Данный список - перечень сетевых устройств, добавленных в разделе "Моделирование системы".

- Нажать кнопку OK или клавишу «Enter».

- Для закрытия окна без сохранения изменений нажать нопку «Отмена» или клавишу «Esc».

4.5.4 Следующая закладка «Бизнес-процессы» позволяет выбрать бизнес-процессы, в которых хранится и обрабатывается ценная информация.

- Отметить те бизнес-процессы, которые используются для данного вида информации.

- Нажать кнопку OK или клавишу «Enter».

- Для закрытия окна без сохранения изменений нажать кнопку Отмена или клавишу {Esc}.

4.5.5 Для выбора средств защиты ресурса выполнить следующие шаги:

- Отметить используемые средства защиты.

- Нажать кнопку OK или клавишу «Enter».

- Для закрытия окна нажать кнопку Отмена или клавишу «Esc».

4.5.6 Для выбора средств защиты указанного вида информации выполнить следующие шаги:

- Отметить используемые средства защиты.

- Нажать кнопку OK или клавишу «Enter».

- Для закрытия окна нажать кнопку Отмена или клавишу «Esc».

4.6. Политика безопасности - раздел, в котором приведены вопросы, учитывающие организационные меры обеспечения информационной безопасности. В правой части окна находится рабочее поле. Сначала необходимо выбрать раздел, тогда на рабочем поле отобразится перечень вопросов по данному разделу. Далее необходимо выбрать вопрос и нажать кнопку «Изменить». Для ответа на вопрос выполнить следующие шаги:

- Отметить ответ на данный вопрос.

- Нажать на кнопку «Принять».

- После принятия ответа программа перейдет к следующему не отвеченному вопросу

4.7. Политика безопасности - раздел, в котором приведены вопросы, учитывающие организационные меры обеспечения информационной безопасности. В правой части окна находится рабочее поле. Сначала необходимо выбрать раздел, тогда на рабочем поле отобразится перечень вопросов по данному разделу. Далее необходимо выбрать вопрос и нажать кнопку «Изменить». Для ответа на вопрос выполнить следующие шаги:

- Отметить ответ на данный вопрос.

- Нажать на кнопку «Принять».

- После принятия ответа программа перейдет к следующему не отвеченному вопросу (рис. 2).

4.8. Далее необходимо ввести контрмеры. Для этого необходимо выбрать пункт меню Контрмеры Управление рисками и для каждого объекта задать контрмеры (рис. 3).

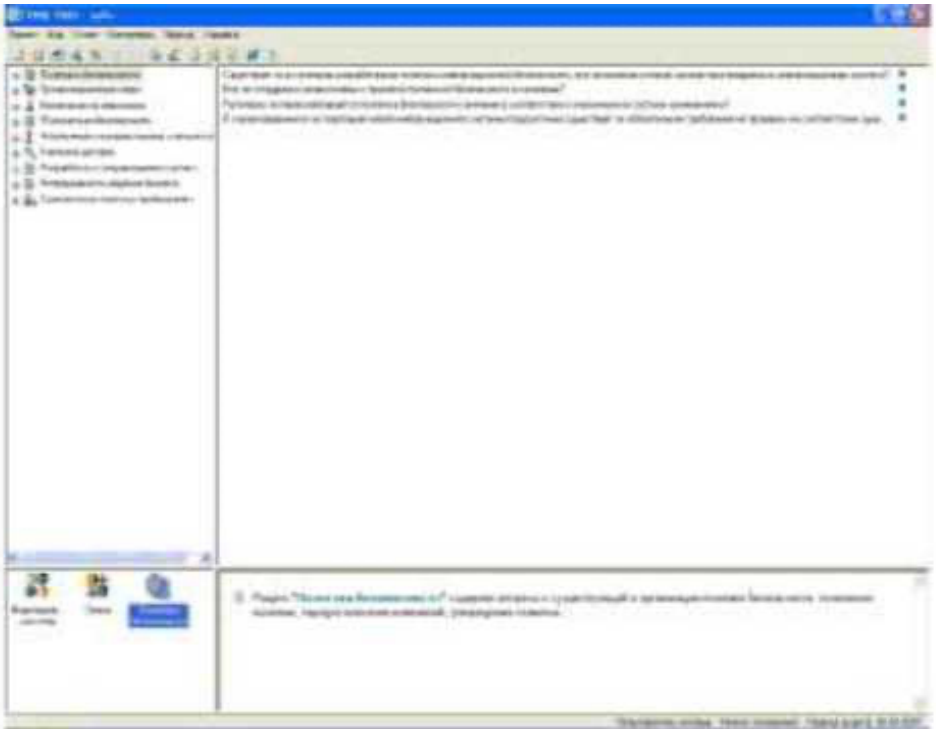

Рис.2

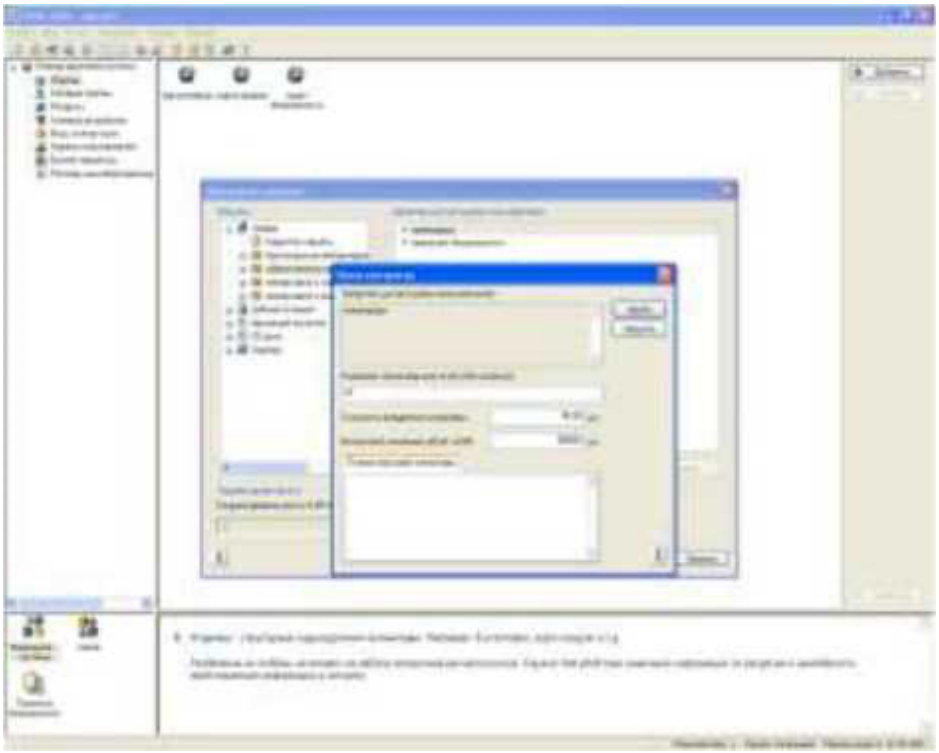

Рис. 3

4.9. После задания контрмер нужно создать отчет. Для настройки параметров и создания отчета выполнить следующие шаги:

- Выбрать пункт меню Отчета Создать отчет;
- Выбрать состав отчета;
- Выбрать форму отчета;
- Нажать кнопку ОК или клавишу «Enter».

Далее необходимо применить все контрмеры и повторить действия пункта. Должно получиться 2 отчета. Необходимо их сравнить.

5. Содержание отчета

5.1. Цель работы;
5.2. Сгенерированный отчёт до применения контрмер;
5.3. Анализ сгенерированного отчёта;
5.4. Сгенерированный отчёт после применения контрмер;
5.5. Анализ и сравнение двух сгенерированных отчётов.

6. Литература

6.1. Основы управления информационной безопасностью. Учебное пособие для вузов. А.П. Курило, Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. - М.: Горячая линия - Телеком, 2014.

6.2. Управление рисками информационной безопасности. Учебное пособие для вузов. Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. - М.: Горячая линия - Телеком, 2014.