

Министерство образования и науки
«Вятский государственный университет»
Факультет прикладной математики и телекоммуникаций
Кафедра радиоэлектронных средств

Управление и построение системы информационной безопасности в программном комплексе Digital Security Office 2006

Комплекс лабораторных работ по дисциплине «Основы информационной
безопасности»

Методические указания к лабораторным работам:

- №1. Расчет рисков невыполнения требований стандарта ISO 17799 с помощью системы КОНДОР.
- №2. Расчет и управление информационными рисками на основе модели информационных потоков с помощью системы ГРИФ.
- №3. Расчет рисков информационной системы на основе модели угроз и уязвимостей системы ГРИФ.

Для специальности «Защищенные системы связи»

Составитель

к.т.н., доцент
Корепанов А.Г.

Компьютерная верстка

студент группы ЗС-52
Семенищев П.Л.

Киров 2011

Оглавление

1. Введение	3
2. Программный комплекс Digital Security Office 2006	4
2.1. Программа Кондор	4
2.2. Программа Гриф.....	7
2.2.1. Гриф. Модель информационных потоков	7
2.2.2. Гриф. Модель угроз и уязвимостей	18
Лабораторные работы	30
Лабораторная работа 1.....	30
Лабораторная работа 2.....	34
Лабораторная работа 3.....	48
Приложение 1 Варианты для лабораторных работ	53
Приложение 2 Средства обеспечения информационной безопасности	62
Библиографический список	66

1. Введение

Общие положения

Представленные методические указания описывают работу программного продукта Digital Security Office 2006.

Digital Security Office 2006 – программный комплекс, предназначенный для управления информационной безопасностью и построения эффективной системы управления информационной безопасностью. Digital Security Office 2006 включает в себя систему анализа и управления информационными рисками ГРИФ и систему разработки и управления политикой безопасности информационной системы КОНДОР.

Принятые сокращения

Таблица 1 – Принятые сокращения

Сокращение	Расшифровка
ИБ	Информационная безопасность
ИС	Информационная система
ИТ	Информационные технологии
ОС	Операционная система
ПО	Программное обеспечение
Ц	Целостность
К	Конфиденциальность
Д	Доступность
АРМ	Автоматизированное рабочее место
ПДн	Персональные данные
СПД	Система передачи данных
ЛВС	Локально-вычислительная сеть
АСУ	Автоматизированная система управления

2. Программный комплекс Digital Security Office 2006

2.1. Программа Кондор

КОНДОР - система разработки и управления политикой безопасности ИС компании на основе стандарта ISO 17799. Это современный и удобный инструмент для разработки всех основных положений политики ИБ компании и управления процессом внедрения этих положений на практике.

Общее описание

С помощью программы КОНДОР проводится аудит ИС компании на соответствие стандарту ISO 17799. На основе данных, полученных в результате проведения аудита, разрабатывается политика безопасности компании и система управления информационной безопасностью.

Стандарт управления информационной безопасностью ISO 17799 является стандартом верхнего уровня, описывающим безопасность ИС в целом и принципы управления процессом обеспечения ИБ. Требования стандарта ISO 17799 описывают комплексный подход к обеспечению ИБ.

Стандарт состоит из десяти разделов, содержащих требования к процессу управления ИБ.

Разделы стандарта ISO 17799:

- 1) Политика безопасности
- 2) Организационные меры
- 3) Управление ресурсами
- 4) Безопасность персонала
- 5) Физическая безопасность
- 6) Управление коммуникациями и процессами
- 7) Контроль доступа
- 8) Разработка и сопровождение систем
- 9) Непрерывность ведения бизнеса
- 10) Соответствие системы требованиям

Приступая к работе

Требования стандарта ISO 17799 предъявляются к:

- системе ИБ компании (например, нормативным документам по ИБ, выполнению проверок, связанных с ИБ, обучению пользователей по вопросам ИБ);
- ИС компании (например, безопасным настройкам ИС и корректному проведению соответствующих процедур);
- квалификации пользователей компании и специалистов служб ИТ и ИБ.

Соответственно, вопросы программы КОНДОР разделяются на вопросы к:

- специалистам службы ИБ;
- специалистам службы ИТ;
- пользователям ИС компании.

Алгоритм

Для проведения анализа рисков необходимо определить выполненные и невыполненные требования стандарта.

Методика расчета рисков невыполнения требований ISO 17799:

- 1) Каждое требование стандарта имеет определенное значение – вес требования. Вес требования – степень влияния требования на ИС компании. Определяется на основе экспертных оценок, указывается в значениях от 1 до 100 (чем больше значение эффективности, тем больше влияние данного требования). Сумма значений весов всех требований определяет максимальный риск невыполнения требований стандарта, то есть стандарт полностью не выполнен.
- 2) Риск невыполнения требований стандарта в компании определяется как отношение суммы значений весов невыполненных в компании требований к сумме значений весов всех требований стандарта. Риск невыполнения требований стандарта рассчитывается в процентах.

Риск невыполнения требований ISO 17799 показывает, насколько значимы для ИС компании невыполненные требования. Риск зависит от количества невыполненных требований и их весов.

Для снижения риска несоответствия ИС стандарту ISO 17799 необходимо выполнить максимальное количество требований. Особенно важно выполнение требований, имеющих высокие веса, то есть тех требований, которые оказывают наибольшее влияние на ИС компании.[1]

Общие принципы работы с программой

Для проведения анализа ИС компании на соответствие стандарта информационной безопасности ISO 17799 необходимо проверить, выполняются ли в компании требования стандарта.

Для этого необходимо сначала создать новый проект аудита (рисунок 1). (Проект – временной интервал, содержащий несколько периодов, в котором анализируются изменения, произошедшие в компании за истекшие периоды).

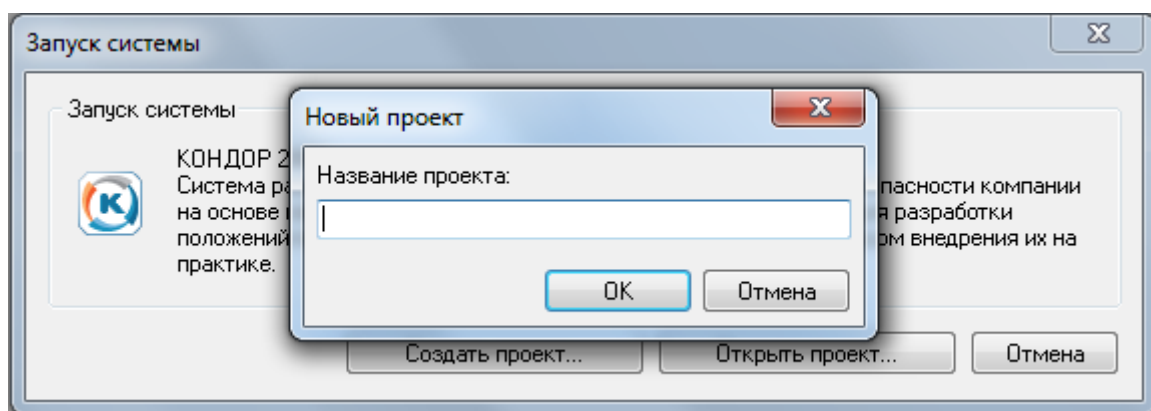


Рисунок 1 – Новый проект

В проекте нужно создать новый период аудита (рисунок 2). (Период - дата, на момент которой все введенные пользователем данные актуальны для ИС компании). При этом дата периода - это дата окончания аудита.

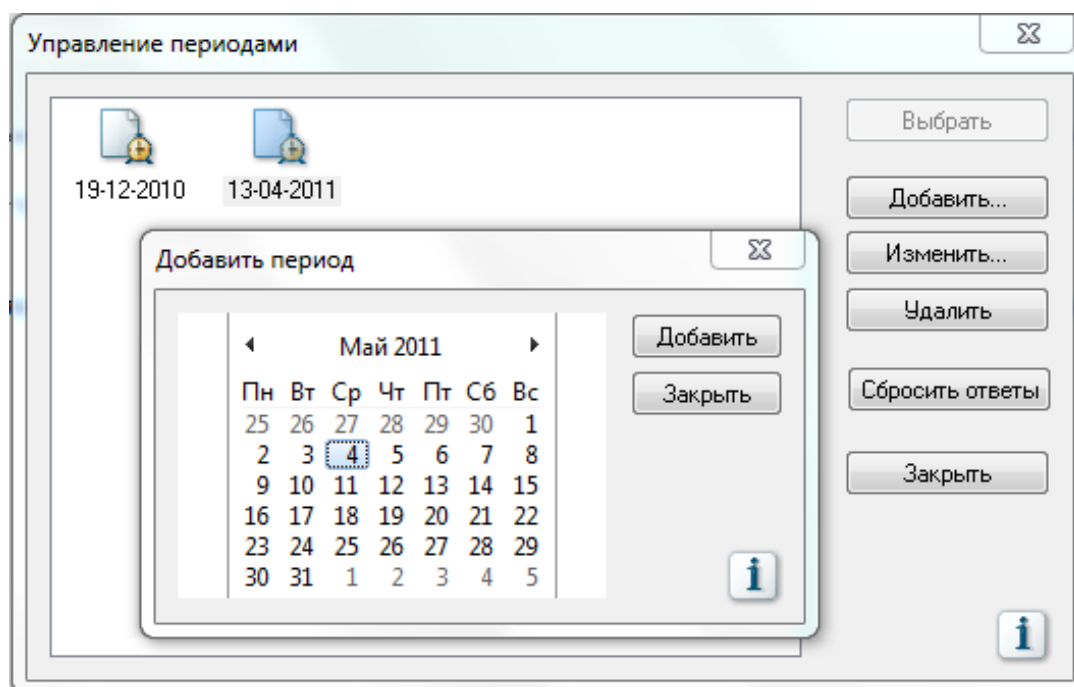


Рисунок 2 – Новый период

Далее необходимо ответить на вопросы разделов (рисунок 3). Каждый раздел соответствует разделу стандарта. Для получения наиболее верных результатов аудита необходимо ответить на все вопросы (и указать все вопросы, неприменимые к ИС).

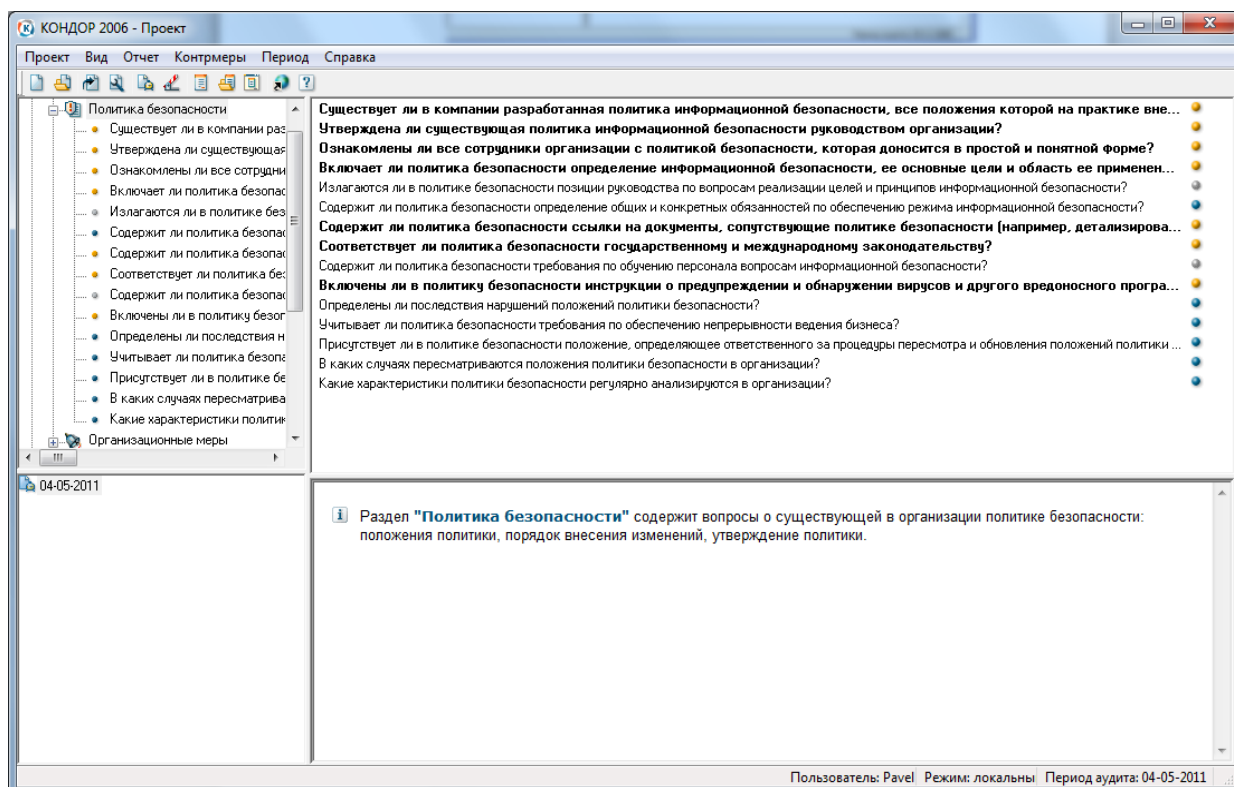


Рисунок 3 – Вопросы разделов

В результате работы алгоритма получаем:

- отчет по одному периоду;
- отчет по всему проекту (несколько периодов).

2.2. Программа Гриф

ГРИФ - инструмент для анализа защищенности ресурсов информационной системы компании и эффективного управления рисками.

2.2.1. Гриф. Модель информационных потоков

Общее описание

Анализ рисков ИБ осуществляется с помощью построения модели ИС компании. Рассматривая средства защиты ресурсов с ценной информацией, взаимосвязь ресурсов между собой, влияние прав доступа групп пользователей, организационные меры, модель исследует защищенность каждого вида информации.

В результате работы алгоритма программа представляет следующие данные:

- 1) Инвентаризация.
- 2) Значения риска для каждого ценного ресурса компании.
- 3) Перечень всех уязвимостей, которые стали причиной полученного значения риска.
- 4) Значения риска для ресурсов после задания контрмер (остаточный риск).
- 5) Эффективность контрмер.
- 6) Рекомендации экспертов.

Приступая к работе

Перед заполнением программы ГРИФ необходимо провести инвентаризацию ценных ресурсов и информации компании, то есть определить, всю ценную информацию и ресурсы, на которых она хранится.

Таблица 2 – Данные для занесения в программу

Данные, которые заносятся в программу	Сотрудник, отвечающий за предоставление данных
Виды ценной информации	Владелец информации (или начальник отдела, в котором осуществляется обработка информации)
Ущерб для каждого вида ценной информации по трем видам угроз (в деньгах или в уровнях в диапазоне от 2 до 100)	Владелец информации (или начальник отдела, в котором осуществляется обработка информации)
Бизнес-процессы, в которых обрабатывается информация	Владелец информации (или начальник отдела, в котором осуществляется обработка информации)
Ресурсы, на которых хранится ценная информация	Специалист службы ИТ
Сетевые группы, в которых находятся ресурсы системы (то есть физические связи ресурсов друг с другом)	Специалист службы ИТ
Отделы, к которым относятся ресурсы	Как правило, совпадают с

	организационной структурой компании
Группы пользователей, имеющих доступ к ценной информации	Специалист службы ИТ
Класс группы пользователей	Специалист службы ИТ
Доступ группы пользователей к информации	Специалист службы ИТ
Характеристики доступа группы пользователей к информации (вид и права)	Специалист службы ИТ
Средства защиты, установленные в ИС	Специалист службы ИТ
Расходы на ИБ	Специалист службы ИБ

Алгоритм

Основные понятия и допущения модели

- *Ресурс* – физический ресурс, на котором располагается ценная информация (сервер, рабочая станция, мобильный компьютер и так далее)
- *Сетевая группа* – группа, в которую входят физически взаимосвязанные ресурсы.
- *Отдел* - структурное подразделение компании.
- *Бизнес-процессы* - производственные процессы, в которых обрабатывается ценная информация.
- *Группа пользователей* – группа пользователей, имеющая одинаковый класс и средства защиты. Субъект, осуществляющий доступ к информации.
- *Класс группы пользователей* – особая характеристика группы, показывающая, как осуществляется доступ к информации.
- Основные классы групп пользователей:
 - Анонимные Интернет-пользователи;
 - Авторизованные Интернет-пользователи;
 - Обычные пользователи, осуществляющие локальный и удаленный доступ к информации;
 - Системные администраторы и офицеры безопасности (так называемые, суперпользователи), то есть пользователи, имеющие исключительные права;
 - Пользователи, осуществляющие доступ к информации из офиса компании через Интернет;
 - Пользователи, осуществляющие доступ к информации из офиса компании по модему;
 - Мобильные Интернет-пользователи.
- *Средства защиты рабочего места группы пользователей* – средства защиты клиентского места пользователя, то есть ресурса, с которого пользователь осуществляет доступ к информации.
- *Характеристики группы пользователей* – под характеристиками группы пользователей понимаются виды доступа группы пользователей (локальный либо удаленный доступ) и права, разрешенные группе пользователей при доступе к информации (чтение, запись или удаление).
- *Информация* – ценная информация, хранящаяся и обрабатываемая в ИС. То есть объект, к которому осуществляется доступ. Исходя из допущений данной модели, вся

информация является ценной, так как оценить риск неценной информации не представляется возможным.

- *Средства защиты* – средства защиты ресурса, на котором расположена (или обрабатывается) информация и средства защиты самой информации, то есть применяемые к конкретному виду информации, а не ко всему ресурсу.
- *Эффективность средства защиты* – количественная характеристика средства защиты, определяющая степень его влияния на ИС, то есть насколько сильно средство влияет на защищенность информации и рабочего места группы пользователей. Определяется на основе экспертных оценок.
- *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 удаленной защищенности информации на ресурсе*. Рассчитывается, когда к информации осуществляется удаленный доступ; то есть по сути это суммарный коэффициент средств защиты объекта.
- *Коэффициент локальной защищенности рабочего места группы пользователей*. Рассчитывается, когда группа пользователей осуществляет удаленный доступ к информации, то есть это суммарный коэффициент защиты субъекта или клиентского места группы пользователей. Данный коэффициент невозможно определить для групп анонимных и авторизованных Интернет-пользователей.
- *Наследование коэффициентов защищенности*. Если на ресурсе расположены несколько видов информации, причем к некоторым из них осуществляется доступ через Интернет (группами анонимных, авторизованных или мобильных Интернет-пользователей), то угрозы, исходящие от этих групп пользователей могут повлиять и на другие виды информации. Следовательно, это необходимо учесть. Если на одном из ресурсов, находящемся в сетевой группе, хранится информация, к которой осуществляют доступ указанные группы пользователей, то это учитывается аналогично для всех видов информации, хранящихся на всех ресурсах, входящих в сетевую группу. Механизм наследования будет подробно описан далее.
- *Базовое время простоя ресурса* (без применения средств защиты) – время, в течение которого доступ к информации ресурса невозможен (отказ в обслуживании). Определяется в часах в год на основе экспертных оценок без учета влияния на информацию средств защиты. Базовое время простоя зависит от групп пользователей, имеющих доступ к ресурсу: время простоя увеличивается, если к ресурсу имеют доступ Интернет-пользователи.
- *Дополнительное время простоя ресурса* – время простоя, в течение которого доступ к информации ресурса невозможен, обусловленное неадекватной работой программного или аппаратного обеспечения ресурса. Задается пользователем. Указывается в часах в год. (Исключение: время простоя не может задаваться для твердой копии).
- *Сетевое устройство* - устройство, с помощью которого осуществляется связь между ресурсами сети. Например, коммутатор, маршрутизатор, концентратор, модем, точка доступа.

- *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.
- *Максимальное критичное время простоя (T_{max})* – значение времени простоя, которое является критичным для компании. То есть ущерб, нанесенный компании при простаивании ресурса в течение критичного времени простоя, максимальный. При простаивании ресурса в течение времени, превышающего критичное, ущерб, нанесенный компании, не увеличивается.
- *Контрмера* – действие, которое необходимо выполнить для закрытия уязвимости.
- *Риск* – вероятный ущерб, который понесет организация при реализации угроз ИБ, зависящий от защищенности системы.
- *Риск после задания контрмер* – значение риска, пересчитанного с учетом задания контрмер (закрытия уязвимостей).
- *Эффективность комплекса контрмер* – оценка, насколько снизился уровень риска после задания комплекса контрмер по отношению к первоначальному уровню риска.

Введение в модель

Для того чтобы оценить риск информации, необходимо проанализировать защищенность и архитектуру построения ИС.

Владельцу ИС требуется сначала описать архитектуру своей сети:

- все ресурсы, на которых хранится ценная информация;
- сетевые группы, в которых находятся ресурсы системы (то есть физические связи ресурсов друг с другом);
- отделы, к которым относятся ресурсы;
- виды ценной информации;
- ущерб для каждого вида ценной информации по трем видам угроз;
- бизнес-процессы, в которых обрабатывается информация;
- группы пользователей, имеющих доступ к ценной информации;
- класс группы пользователей;
- доступ группы пользователей к информации;
- характеристики этого доступа (вид и права);
- средства защиты информации;
- средства защиты рабочего места группы пользователей.

Принцип работы алгоритма

Итак, пройдя первый этап (описание необходимых для модели данных), перейдем непосредственно к работе алгоритма модели.

Риск оценивается отдельно по каждой связи «группа пользователей – информация», то есть модель рассматривает взаимосвязь «субъект – объект», учитывая все их характеристики.

Риск реализации угрозы ИБ для каждого вида информации рассчитывается по трем основным угрозам: конфиденциальность, целостность и доступность. Владелец информации задает ущерб отдельно по трем угрозам; это проще и понятнее, так как оценить ущерб в целом не всегда возможно.

Рассмотрим принцип работы модели последовательно для одной связи «информация – группа пользователей» (для остальных считаем аналогично). Расчет рисков по угрозам конфиденциальность и целостность

Расчет рисков для угроз конфиденциальность и целостность¹:

- 1) Определяем вид доступа группы пользователей к информации. От этого будет зависеть количество средств защиты, так как для локального и удаленного доступа применяются разные средства защиты.
- 2) Определяем права доступа группы пользователей к информации. Это важно для целостности, так как при доступе «только чтение» целостность информации нарушить нельзя, и для доступности. Определенные права доступа влияют на средства защиты информации.
- 3) Вероятность реализации угрозы зависит от класса группы пользователей. Например, анонимные Интернет-пользователи представляют наибольшую угрозу для ценной информации компании, значит, если данная группа имеет доступ к информации, риск реализации угрозы увеличивается. Также, в зависимости от класса группы пользователей меняются их средства защиты. Например, для авторизованных и анонимных Интернет-пользователей мы не можем определить средства защиты их рабочего места.
- 4) Особым видом средства защиты является антивирусное программное обеспечение. В условиях современного функционирования компьютерных систем хранения и обработки информации вредоносное программное обеспечение представляет собой наиболее опасную и разрушительную угрозу. Зная силу влияния вирусных программ, отсутствие антивирусного программного обеспечения на ресурсе (или клиентском месте пользователя) необходимо принимать во внимание отдельно. Если на ресурсе не установлен антивирус, то вероятность реализации угроз конфиденциальности, целостности и доступности резко возрастает. Данная модель это учитывает.
- 5) Теперь у нас есть все необходимые знания, чтобы определить средства защиты информации и рабочего места группы пользователей. Просуммировав веса средств защиты, получим суммарный коэффициент. Для угрозы целостность учитываются специфические средства защиты – средства резервирования и контроля целостности информации. Если к ресурсу осуществляется локальный и удаленный доступ, то на данном этапе будут определены три коэффициента: коэффициент локальной защищенности информации на ресурсе, коэффициент удаленной защищенности информации на ресурсе и коэффициент локальной защищенности рабочего места группы пользователей. Из полученных коэффициентов выбираем минимальный. Чем меньше коэффициент защищенности, тем слабее защита, то есть важно учесть наименее защищенное (наиболее уязвимое) место в ИС.
- 6) На этом этапе вступает в силу понятие наследования коэффициентов защищенности и базовых вероятностей. Например, на ресурсе, входящем в сетевую группу, содержится информация, к которой осуществляется доступ групп пользователей (анонимных, авторизованных или мобильных) из Интернет. Для этой связи «информация – группа Интернет-пользователей» рассчитывается только коэффициент удаленной защищенности информации на ресурсе, так как оценить защищенность групп

¹ Алгоритмы расчета для угроз целостности и конфиденциальности похожи, поэтому здесь мы их объединили.

пользователей мы не можем². Теперь этот коэффициент защищенности необходимо сравнить с коэффициентами защищенности, полученными для нашей связи «информация – группа пользователей». Это очень важный момент. Таким образом, мы учитываем влияние других ресурсов системы на наш ресурс и информацию. В реальной информационной системе все ресурсы, взаимосвязанные между собой, оказывают друг на друга влияние. То есть злоумышленник, проникнув на один ресурс ИС (например, получив доступ к информации ресурса), может без труда получить доступ к ресурсам, физически связанным со взломанным. Явным преимуществом данной модели является то, что она учитывает взаимосвязи между ресурсами ИС.

- 7) Отдельно учитывается наличие криптографической защиты данных при удаленном доступе. Если пользователи могут получить удаленный доступ к ценным данным, не используя систему шифрования, это может сильно повлиять на целостность и конфиденциальность данных.
- 8) На последнем этапе перед получением итогового коэффициента защищенности связи «информация – группа пользователей» анализируем количество человек в группе пользователей и наличие у группы пользователей выхода в Интернет. Все эти параметры сказываются на защищенности информации.
- 9) Итак, пройдя по всему алгоритму, мы получили конечный, итоговый коэффициент защищенности для нашей связки «информация – группа пользователей».
- 10) Далее полученный итоговый коэффициент нужно умножить на базовую вероятность реализации угрозы ИБ. Базовая вероятность определяется на основе метода экспертных оценок. Группа экспертов, исходя из классов групп пользователей, получающих доступ к ресурсу, видов и прав их доступа к информации, рассчитывает базовую вероятность для каждой информации. Владелец ИС, при желании, может задать этот параметр самостоятельно. Перемножив базовую вероятность и итоговый коэффициент защищенности, получим итоговую вероятность реализации угрозы. Напомним, что для каждой из трех угроз ИБ мы отдельно рассчитываем вероятность реализации.
- 11) На завершающем этапе значение полученной итоговой вероятности накладываем на ущерб от реализации угрозы и получаем риск угрозы ИБ для связи «вид информации – группа пользователей».
- 12) Чтобы получить риск для вида информации (с учетом всех групп пользователей, имеющих к ней доступ), необходимо сначала просуммировать итоговые вероятности реализации угрозы по следующей формуле:

$$P_{inf} = 1 - \prod_{i=1}^n (1 - P_{ug,n}).$$

А затем полученную итоговую вероятность для информации умножаем на ущерб от реализации угрозы, получая, таким образом, риск от реализации угрозы для данной информации.

- 13) Чтобы получить риск для ресурса (с учетом всех видов информации, хранимой и обрабатываемой на ресурсе), необходимо просуммировать риски по всем видам информации.

Расчет рисков по угрозе отказ в обслуживании

² Для группы мобильных Интернет-пользователей коэффициент удаленной защиты группы пользователей не рассчитывается

Если для целостности и конфиденциальности вероятность реализации угрозы рассчитывается в процентах, то для доступности аналогом вероятности является время простоя ресурса, содержащего информацию. Однако риск по угрозе отказ в обслуживании все равно считается для связки «информация - группа пользователей», так как существует ряд параметров, которые влияют не на ресурс в целом, а на отдельный вид информации.

Итак:

- 1) На первом этапе определяем базовое время простоя для информации.
- 2) Далее необходимо рассчитать коэффициент защищенности связки «информация - группы пользователей». Для угрозы отказ в обслуживании коэффициент защищенности определяется, учитывая права доступа группы пользователей к информации и средства резервирования.
- 3) Так же, как для угроз нарушения конфиденциальности и доступности, наличие антивирусного программного обеспечения является особым средством защиты и учитывается отдельно.
- 4) Накладывая коэффициент защищенности на время простоя информации, получим время простоя информации, учитывая средства защиты информации. Оно рассчитывается в часах простоя в год.
- 5) Специфичный параметр для связки «информация – группа пользователей» - время простоя сетевого оборудования. Доступ к ресурсу может осуществляться разными группами пользователей, используя разное сетевое оборудование. Для сетевого оборудования время простоя задает владелец ИС. Время простоя сетевого оборудования суммируется со временем простоя информации, полученным в результате работы алгоритма, таким образом, мы получаем итоговое время простоя для связки «информация – группа пользователей».
- 6) Значение времени простоя для информации (T_{inf}), учитывая все группы пользователей, имеющих к ней доступ, вычисляется по следующей формуле:

$$T_{inf} = \left(1 - \prod_{i=1}^n \left(1 - \frac{T_{ug,n}}{T_{max}}\right)\right) \times T_{max}$$
 где T_{max} – максимальное критичное время простоя;
 $T_{ug,n}$ – время простоя для связки «информация – группа пользователей».
- 7) Ущерб для угрозы отказ в обслуживании задается в час. Перемножив итоговое время простоя и ущерб от реализации угрозы, получим риск реализации угрозы отказ в обслуживании для связки «информация - группа пользователей».[2]

Задание контрмер

Пользователь имеет возможность задавать контрмеры. Для расчета эффективности введенной контрмеры необходимо пройти последовательно по всему алгоритму с учетом заданной контрмеры. То есть на выходе пользователь получает значение двух рисков – риска без учета контрмеры (R_{old}) и риск с учетом заданной контрмеры (R_{new}) (или с учетом того, что уязвимость закрыта).

Эффективность введения контрмеры рассчитывается по следующей формуле (Е):

$$E = \frac{R_{old} - R_{new}}{R_{old}}$$

В результате работы алгоритма пользователь системы получает следующие данные:

- Риск реализации по трем базовым угрозам для вида информации.
- Риск реализации по трем базовым угрозам для ресурса.
- Риск реализации суммарно по всем угрозам для ресурса.
- Риск реализации по трем базовым угрозам для ИС.
- Риск реализации по всем угрозам для ИС.
- Риск реализации по всем угрозам для ИС после задания контрмер.
- Эффективность контрмеры.
- Эффективность комплекса контрмер.

Общие принципы работы с программой

Шаг 1.

На первом этапе работы с программой пользователь вносит все объекты своей ИС (рисунок 4): отделы, ресурсы (специфичными объектами данной модели являются сетевые группы, сетевые устройства, виды информации, группы пользователей, бизнес-процессы).

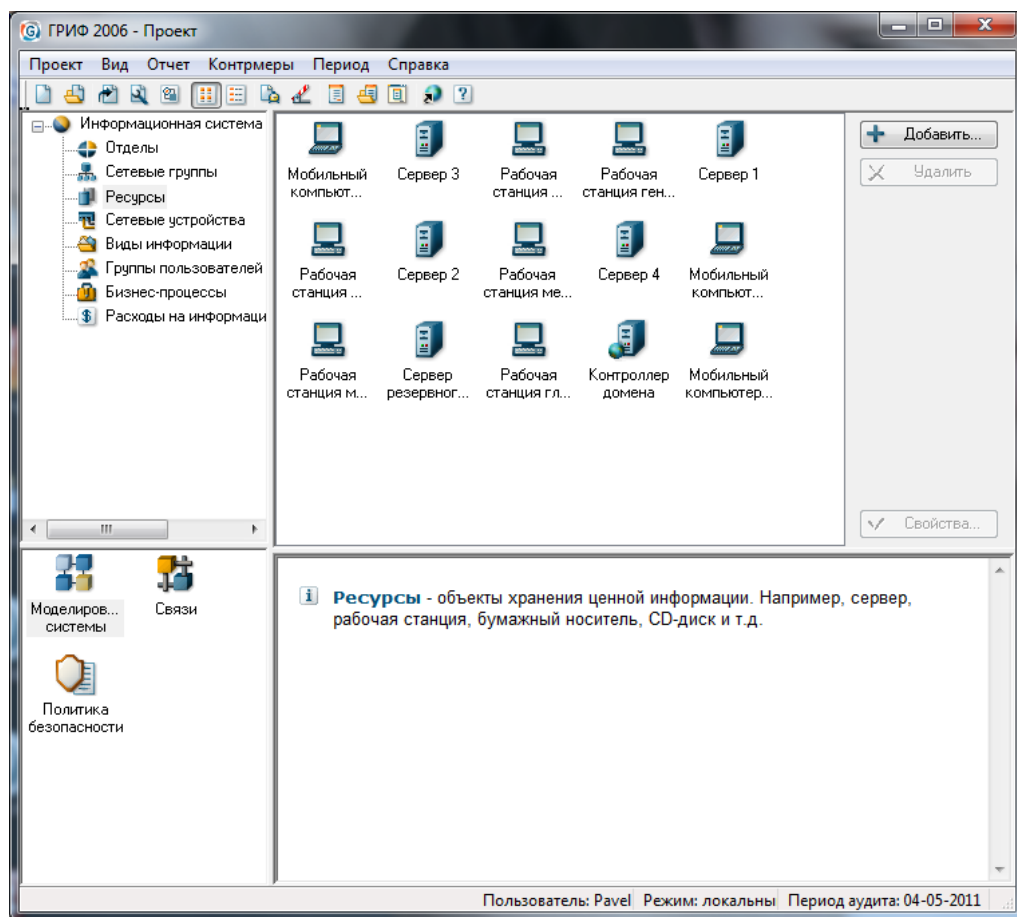


Рисунок 4 – Окно объектов ИС

Шаг 2.

Далее пользователю необходимо проставить связи, то есть определить, к каким отделам и сетевым группам относятся ресурсы, какая информация хранится на ресурсе и какие группы пользователей имеют к ней доступ. Также пользователь системы указывает средства защиты ресурса и информации. На рисунке 5 показано окно связи информации и групп пользователей.

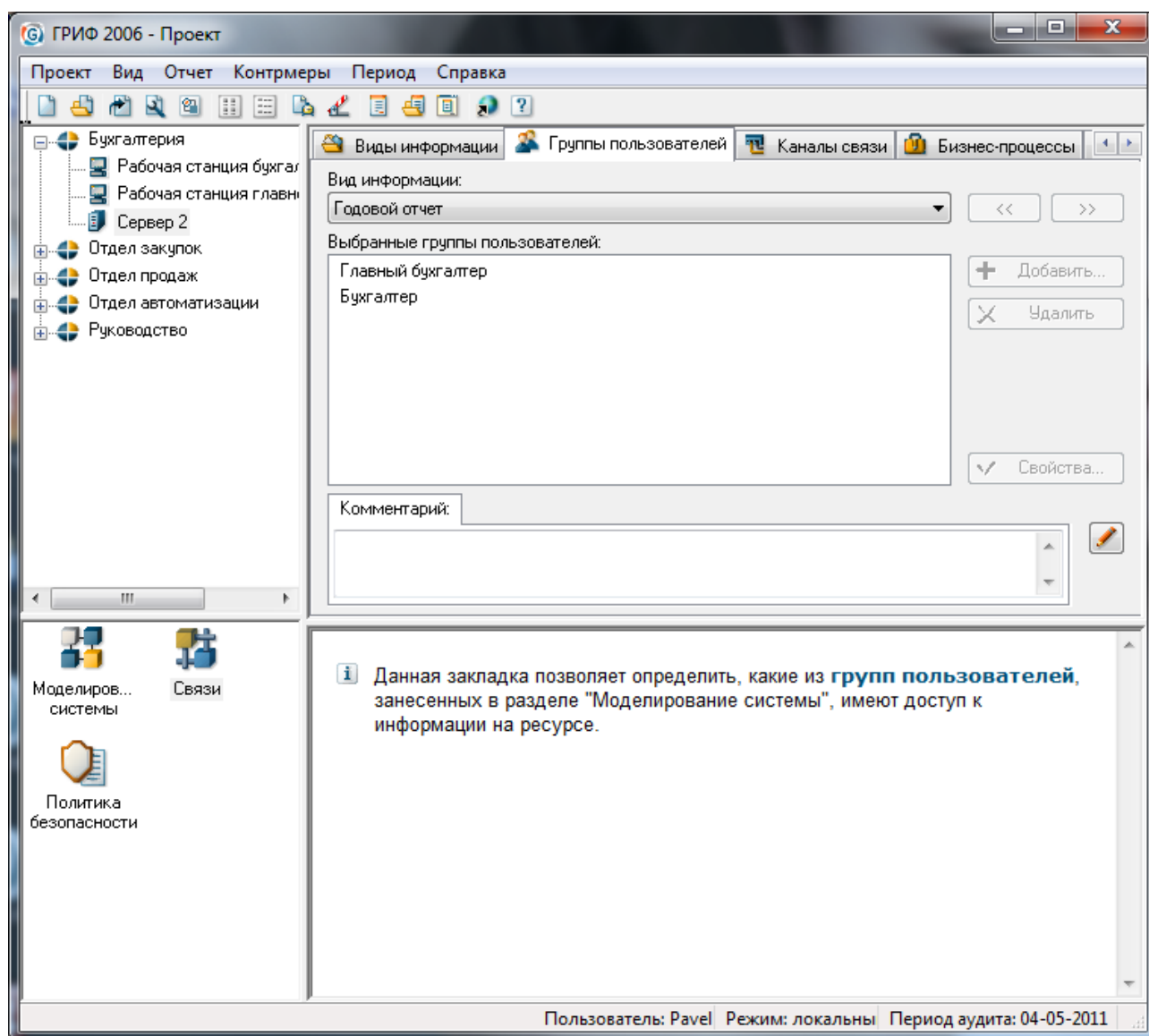


Рисунок 5 – Окно доступа групп пользователей к информации

Шаг 3.

На завершающем этапе пользователь отвечает на список вопросов по политике безопасности, реализованной в системе, изображенные на рисунке 6. Это позволяет оценить реальный уровень защищенности системы и детализировать оценки рисков.

Наличие средств информационной защиты, отмеченных на первом этапе, само по себе еще не делает систему защищенной в случае их неадекватного использования и отсутствия комплексной политики безопасности, учитывающей все аспекты защиты информации, включая вопросы организации защиты, физической безопасности, безопасности персонала, непрерывности ведения бизнеса и так далее.

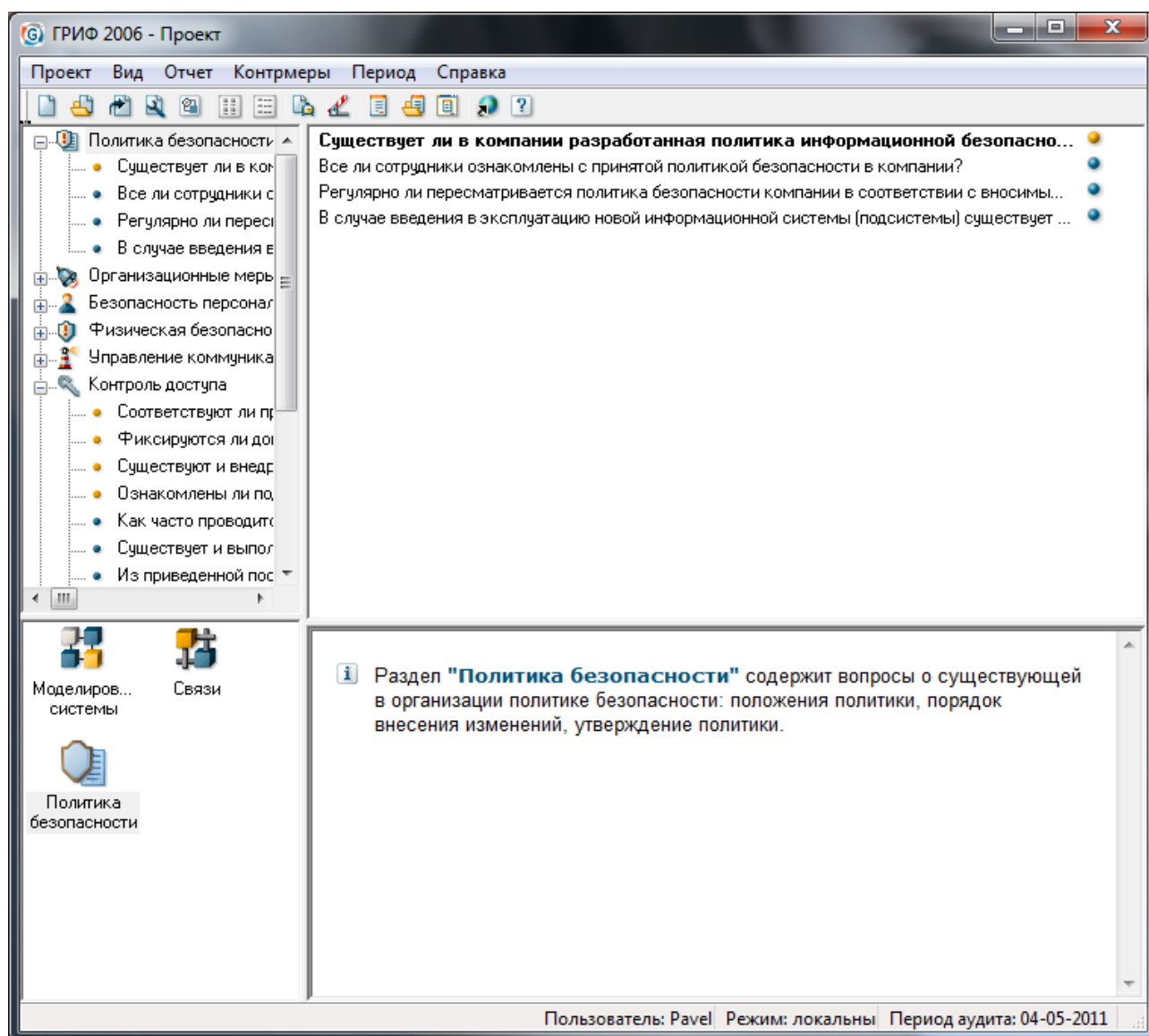


Рисунок 6 – Список вопросов по политике безопасности

В результате выполнения всех действий по данным этапам, на выходе сформирована полная модель ИС с точки зрения ИБ с учетом реального выполнения требований комплексной политики безопасности, что позволяет перейти к программному анализу введенных данных для получения комплексной оценки рисков и формирования итогового отчета.

Алгоритм системы ГРИФ анализирует построенную модель и генерирует отчет (рисунок 7), который содержит значения риска для каждого ресурса. Конфигурации отчета может быть практически любой, таким образом, позволяя пользователю создавать как краткие отчеты для руководства, так и детальные отчеты для дальнейшей работы с результатами.

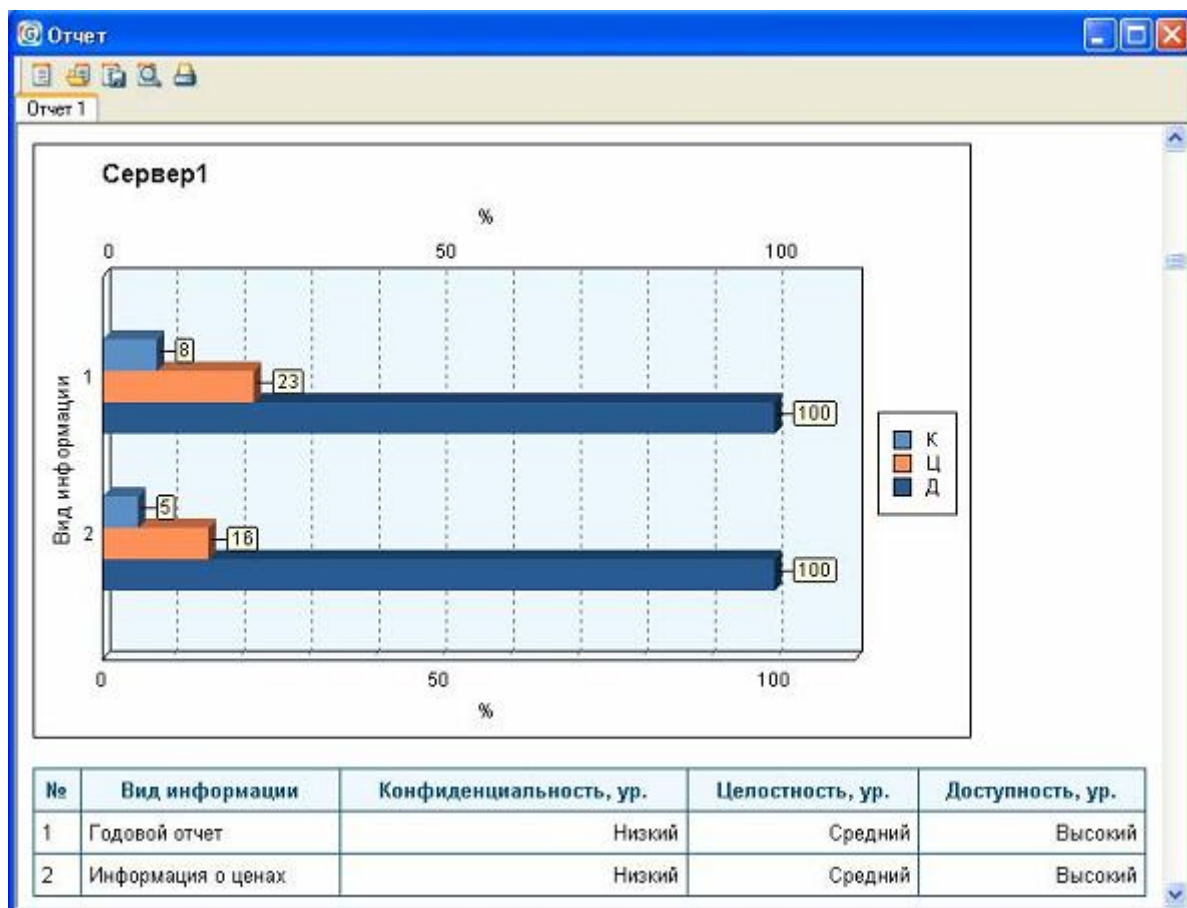


Рисунок 7 – Окно краткого отчета по одному ресурсу ИС

Система ГРИФ содержит модуль управления рисками, который позволяет проанализировать все причины того значения риска, который получается после обработки алгоритмом занесенных данных. Таким образом, зная причины, Вы будете обладать всеми данными, необходимыми для реализации контрмер и, соответственно, снижения уровня риска. Благодаря расчету эффективности каждой возможной контрмеры, а также определению значения остаточного риска, Вы сможете выбрать наиболее оптимальные контрмеры, которые позволят снизить риск до необходимого уровня с наименьшими затратами. На рисунке 8 изображено окно управления рисками.

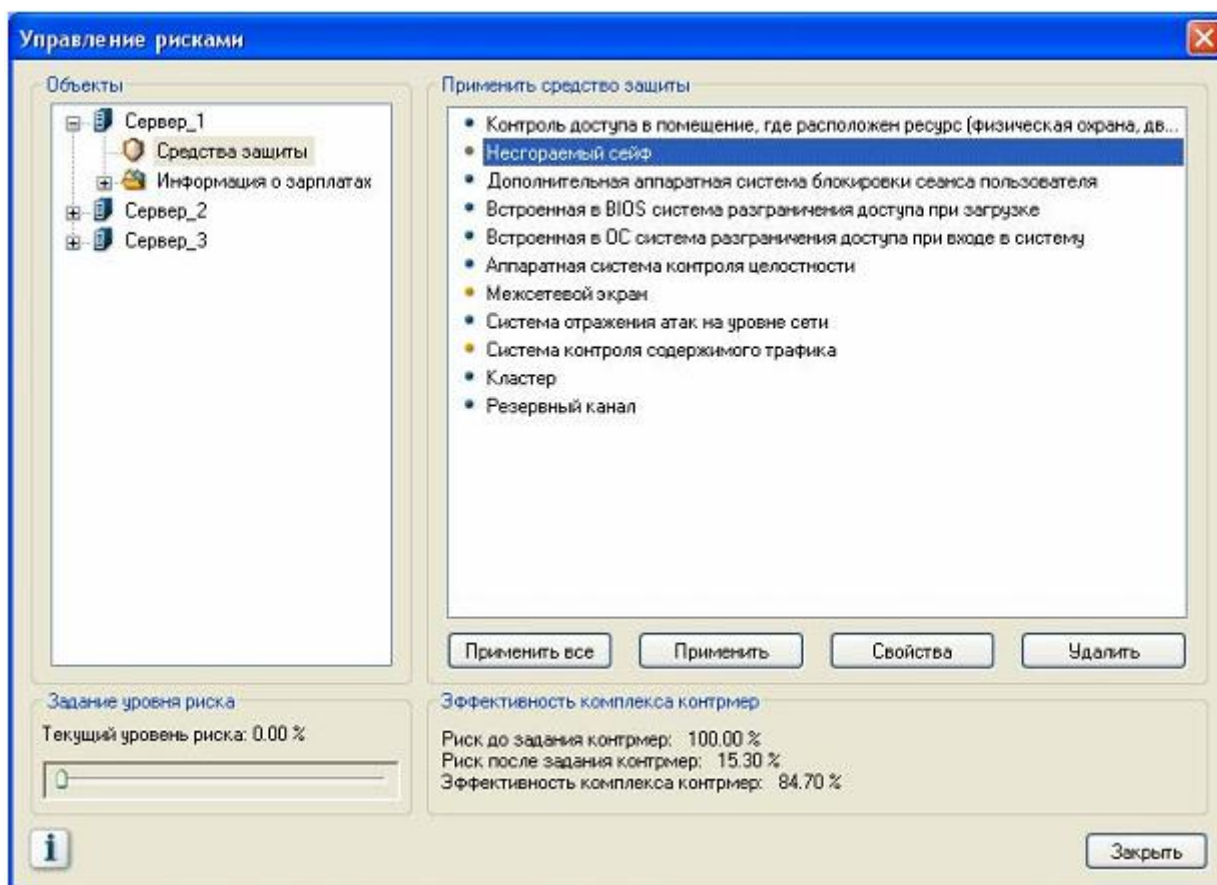


Рисунок 8 – Управление рисками

В результате работы с системой ГРИФ строится подробный отчет об уровне риска каждого ценного ресурса ИС компании, все причины риска с подробным анализом уязвимостей и оценкой экономической эффективности всех возможных контрмер.

2.2.2. Гриф. Модель угроз и уязвимостей

Назначение

Для оценки рисков ИС компании защищенность каждого ценного ресурса определяется при помощи анализа угроз, действующих на конкретный ресурс, и уязвимостей, через которые данные угрозы могут быть реализованы. Оценивая вероятность реализации актуальных для ценного ресурса угроз и степень влияния реализации угрозы на ресурсы, анализируются информационные риски ресурсов компании.

В результате работы алгоритма программа представляет следующие данные:

- 1) Инвентаризация.
- 2) Значения риска для каждого ценного ресурса компании.
- 3) Перечень всех уязвимостей, которые стали причиной полученного значения риска.
- 4) Значения риска для ресурсов после задания контрмер (остаточный риск).
- 5) Эффективность контрмер.

Приступая к работе

Перед заполнением программы ГРИФ необходимо провести инвентаризацию ценных ресурсов и информации компании, то есть определить, всю ценную информацию компании и ресурсы, на которых она хранится.

Далее владельцы информации или ответственные лица (как правило, начальники отделов, в которых ведется обработка информации) должны определить ущерб, который понесет компания при осуществлении угроз конфиденциальности, целостности и доступности данной информации. Если владелец информации затрудняется оценить ущерб информации в деньгах, программа позволяет заносить ущерб в уровнях (количество и оценку уровней владелец выбирает самостоятельно (в диапазоне от 2 до 100), но для всех видов информации в ИС компании количество и оценка уровней должны быть одинаковы).

Отметим, что в программу ГРИФ заносятся только ресурсы, на которых обрабатывается ценная информация, то есть информация, для которой можно оценить ущерб при реализации угроз.

Далее специалист службы ИТ определяет угрозы, действующие на ресурсы с ценной информацией, и уязвимости, через которые реализуются угрозы, критичность угроз и вероятность реализации угроз через указанные уязвимости.

Специалисты отдела ИБ предоставляют данные о расходах на ИБ.

Сотруднику, заполняющему программу, требуется внести следующие данные:

Таблица 3 – Данные для занесения в программу

Данные, которые заносятся в программу	Сотрудник, отвечающий за предоставление данных
Ресурсы, на которых хранится ценная информация	Специалист службы ИТ
Критичность ресурса, на котором хранится ценная информация	Владелец информации (или начальник отдела, в котором осуществляется обработка информации)
Отделы, к которым относятся ресурсы	Как правило, совпадают с организационной структурой компании
Угрозы, действующие на ресурсы	Специалист служб ИТ и ИБ
Уязвимости, через которые реализуются угрозы	Специалист служб ИТ и ИБ
Расходы на ИБ	Специалист службы ИБ

Алгоритм

Основные понятия и допущения модели

Риск – вероятный ущерб, который понесет компания при осуществлении угроз ИБ.

Базовые угрозы информационной безопасности – нарушение конфиденциальности, нарушение целостности и отказ в обслуживании.

Ресурс – любой контейнер, предназначенный для хранения информации, подверженный угрозам ИБ (сервер, рабочая станция, переносной компьютер). Свойствами ресурса являются: перечень угроз, воздействующих на него, и критичность ресурса.

Угроза – действие, которое потенциально может привести к нарушению безопасности. Свойством угрозы является перечень уязвимостей, при помощи которых может быть реализована угроза.

Уязвимость – это слабое место в ИС, которое может привести к нарушению безопасности путем реализации некоторой угрозы. Свойствами уязвимости являются: вероятность (простота) реализации угрозы через данную уязвимость и критичность реализации угрозы через данную уязвимость.

Критичность ресурса (АС)– степень значимости ресурса для ИС, то есть как сильно реализация угроз ИБ на ресурс повлияет на работу ИС. Задается в уровнях (количество уровней может быть в диапазоне от 2 до 100) или в деньгах. В зависимости от выбранного режима работы, может состоять из критичности ресурса по конфиденциальности, целостности и доступности (АСс, АСi, АСа).

Критичность реализации угрозы (ER) – степень влияния реализации угрозы на ресурс, то есть как сильно реализация угрозы повлияет на работу ресурса. Задается в процентах. Состоит из критичности реализации угрозы по конфиденциальности, целостности и доступности (ERс, ERi, ERa).

Вероятность реализации угрозы через данную уязвимость в течение года (P(V)) – степень возможности реализации угрозы через данную уязвимость в тех или иных условиях. Указывается в процентах.

Максимальное критичное время простоя (T_{max}) – значение времени простоя, которое является критичным для компании. То есть ущерб, нанесенный компании при простаивании ресурса в течение критичного времени простоя, максимальный. При простаивании ресурса в течение времени, превышающего критичное, ущерб, нанесенный компании, не увеличивается.

С точки зрения базовых угроз ИБ существует два режима работы алгоритма:

- Одна базовая угроза (суммарная).
- Три базовые угрозы.

С точки зрения единиц измерения критичности и риска ресурса существуют два режима работы алгоритма:

- В денежных единицах.
- В уровнях (процентах).

Принципы разбиения шкалы на уровни

При работе с алгоритмом используется шкала от 0 до 100%. Максимальное число уровней – 100, то есть шкалу можно разбить на 100 уровней. При разбиении шкалы на меньшее число уровней, каждый уровень занимает определенный интервал на шкале. Причем, возможно два варианта деления:

- Равномерное.

- Логарифмическое.

Например, для 5 уровней:

- Равномерное:



- 1 уровень – 20%;
- 2 уровень – 40%;
- 3 уровень – 60%;
- 4 уровень – 80%;
- 5 уровень – 100%.

- Логарифмическое.



- 1 уровень – 7%;
- 2 уровень – 18%;
- 3 уровень – 35%;
- 4 уровень – 62%;
- 5 уровень – 100%.

Расчет рисков по угрозе информационной безопасности

1. На первом этапе рассчитываем уровень угрозы по уязвимости Th на основе критичности и вероятности реализации угрозы через данную уязвимость. Уровень угрозы показывает, насколько критичным является воздействие данной угрозы на ресурс с учетом вероятности ее реализации.

1.1. Для режима с одной базовой угрозой:

$$Th = \frac{ER}{100} \times \frac{P(V)}{100}$$

где ER – критичность реализации угрозы (указывается в %);

$P(V)$ – вероятность реализации угрозы через данную уязвимость (указывается в %).

Получаем значения уровня угрозы по уязвимости в интервале от 0 до 1.

1.2. Для режима с тремя базовыми угрозами:

$$Th_c = \frac{ER_c}{100} \times \frac{P(V)_c}{100}$$

$$Th_i = \frac{ER_i}{100} \times \frac{P(V)_i}{100}$$

$$Th_a = \frac{ER_a}{100} \times \frac{P(V)_a}{100}$$

где $ER_{c,i,a}$ – критичность реализации угрозы конфиденциальность, целостность или доступность (указывается в %);

$P(V)_{c,i,a}$ – вероятность реализации угрозы конфиденциальность, целостность или доступность через данную уязвимость (указывается в %).

Получаем значения уровня угрозы по уязвимости в интервале от 0 до 1.

2. Чтобы рассчитать уровень угрозы по всем уязвимостям CTh, через которые возможна реализация данной угрозы на ресурсе, просуммируем полученные уровни угроз через конкретные уязвимости по следующей формуле:

2.1. Для режима с одной базовой угрозой:

$$CTh = 1 - \prod_{i=1}^n (1 - Th_i)$$

где Th – уровень угрозы по уязвимости.

Значения уровня угрозы по всем уязвимостям получим в интервале от 0 до 1.

2.2. Для режима с тремя базовыми угрозами:

$$CTh_c = 1 - \prod_{j=1}^n (1 - Th_{c,j})$$

$$CTh_i = 1 - \prod_{j=1}^n (1 - Th_{i,j})$$

$$CTh_a = 1 - \prod_{j=1}^n (1 - Th_{a,j})$$

где $Th_{c,i,a}$ – уровень угрозы конфиденциальность, целостность или доступность по уязвимости.

Значения уровня угрозы по всем уязвимостям получим в интервале от 0 до 1.

3. Аналогично рассчитываем общий уровень угроз по ресурсу CThR (учитывая все угрозы, действующие на ресурс):

3.1. Для режима с одной базовой угрозой:

$$CThR = 1 - \prod_{i=1}^n (1 - CTh_i)$$

где CTh – уровень угрозы по всем уязвимостям.

Значение общего уровня угрозы получим в интервале от 0 до 1.

3.2. Для режима с тремя базовыми угрозами:

$$CThR_c = 1 - \prod_{j=1}^n (1 - CTh_{c,j})$$

$$CThR_i = 1 - \prod_{j=1}^n (1 - CTh_{i,j})$$

$$CThR_a = 1 - \prod_{j=1}^n (1 - CTh_{a,j})$$

где $CTh_{c,i,a}$ - уровень угрозы конфиденциальность, целостность или доступность по всем угрозам.

Значение общего уровня угрозы получим в интервале от 0 до 1.

4. Риск по ресурсу R рассчитывается следующим образом:

4.1. Для режима с одной базовой угрозой:

$$R = CThR \times D$$

где D – критичность ресурса (задается в деньгах или уровнях);

$CThR$ – общий уровень угроз по ресурсу.

Если риск задается в уровнях, то в качестве значения критичности берем оценку уровня. Например, для трех равномерных уровней:

Таблица 4 – Оценка уровня

Название уровня	Оценка уровня, %
1	33,33
2	66,66
3	100

В случае угрозы доступность (отказ в обслуживании) критичность ресурса в год вычисляется по следующей формуле:

$$D_{a/\text{год}} = D_{a/\text{час}} \times T_{\max}$$

где $D_{a/\text{год}}$ – критичность ресурса по угрозе доступность в год;

$D_{a/\text{час}}$ - критичность ресурса по угрозе доступность в час;

T_{\max} – максимальное критичное время простоя ресурса в год.

Для остальных угроз критичность ресурса задается в год.

4.2. Для режима с тремя базовыми угрозами:

$$R_c = CThR_c \times D_c$$

$$R_i = CThR_i \times D_i$$

$$R_a = CThR_a \times D_a$$

$$R_{\Sigma} = \left(1 - \left(\left(1 - \frac{R_c}{100} \right) \times \left(1 - \frac{R_i}{100} \right) \times \left(1 - \frac{R_a}{100} \right) \right) \right) \times 100$$

$D_{c,i,a}$ – критичность ресурса по угрозе конфиденциальность, целостность или доступность. Задается в деньгах или уровнях;

$CThR_{c,i,a}$ – общий уровень угроз конфиденциальность, целостность или доступность по ресурсу;

R_{Σ} - суммарный риск по трем угрозам.

Таким образом, получим значение риска по ресурсу в уровнях (заданных пользователем) или деньгах.

5. Риск по ИС CR рассчитывается по формуле:

5.1. Для режима с одной базовой угрозой:

5.1.1. Для режима работы в деньгах:

$$CR = \sum_{i=1}^n R_i$$

где R – риск по ресурсу.

5.1.2. Для режима работы в уровнях:

$$CR = \left(1 - \prod_{i=1}^n \left(1 - \frac{R_i}{100} \right) \right) \times 100$$

где R – риск по ресурсу.

5.2. Для режима работы с тремя угрозами:

5.2.1. Для режима работы в деньгах:

$$CR_c = \sum_{j=1}^n R_{c,j}$$

$$CR_i = \sum_{j=1}^n R_{i,j}$$

$$CR_a = \sum_{j=1}^n R_{a,j}$$

$$CR_{\Sigma} = CR_c + CR_i + CR_a$$

$CR_{c,i,a}$ – риск по системе по угрозам конфиденциальность, целостность или доступность;

CR_{Σ} – риск по системе суммарно по трем видам угроз.

5.2.2. Для режима работы в уровнях:

$$CR_c = \left(1 - \prod_{j=1}^n \left(1 - \frac{R_{c,j}}{100} \right) \right) \times 100$$

$$CR_i = \left(1 - \prod_{j=1}^n \left(1 - \frac{R_{i,j}}{100} \right) \right) \times 100$$

$$CR_a = \left(1 - \prod_{j=1}^n \left(1 - \frac{R_{a,j}}{100} \right) \right) \times 100$$

$$CR_{\Sigma} = \left(1 - \left(\left(1 - \frac{CR_c}{100} \right) \times \left(1 - \frac{CR_i}{100} \right) \times \left(1 - \frac{CR_a}{100} \right) \right) \right) \times 100$$

$CR_{c,i,a}$ – риск по системе по угрозам конфиденциальность, целостность или доступность;

CR_{Σ} – риск по системе суммарно по трем видам угроз.

2.2.2.5. Общие принципы работы с программой

Шаг 1.

На первом этапе работы с продуктом пользователь вносит объекты своей ИС (рисунок 9): отделы, ресурсы (специфичными объектами для данной модели: угрозы ИС, уязвимости, через которые реализуются угрозы).

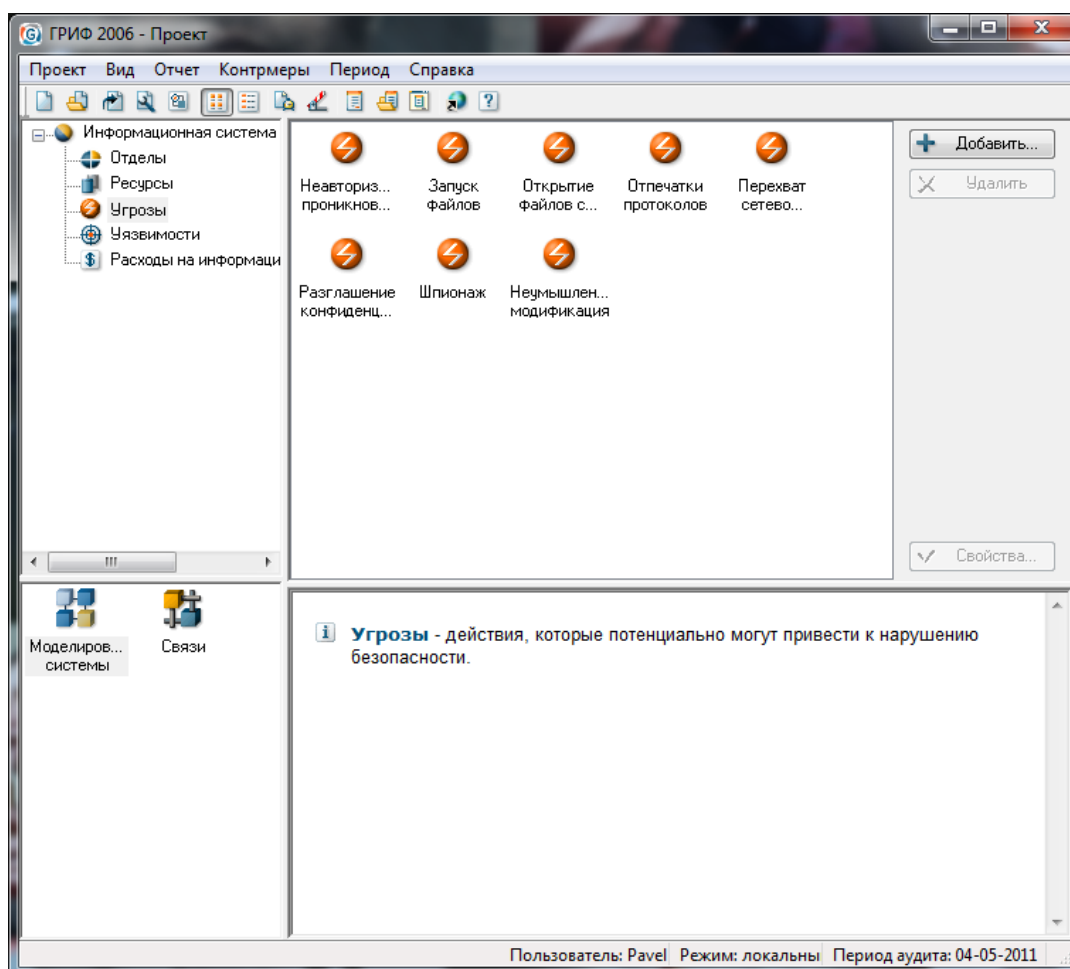


Рисунок 9 – Объекты ИС

Система ГРИФ содержит обширные встроенные каталоги угроз и уязвимостей. Используя каталоги угроз и уязвимостей, пользователь может выбрать угрозы и уязвимости, относящиеся к его ИС. Каталоги содержат около 100 угроз и 200 уязвимостей. На рисунке 10 изображено окно предопределенных угроз.

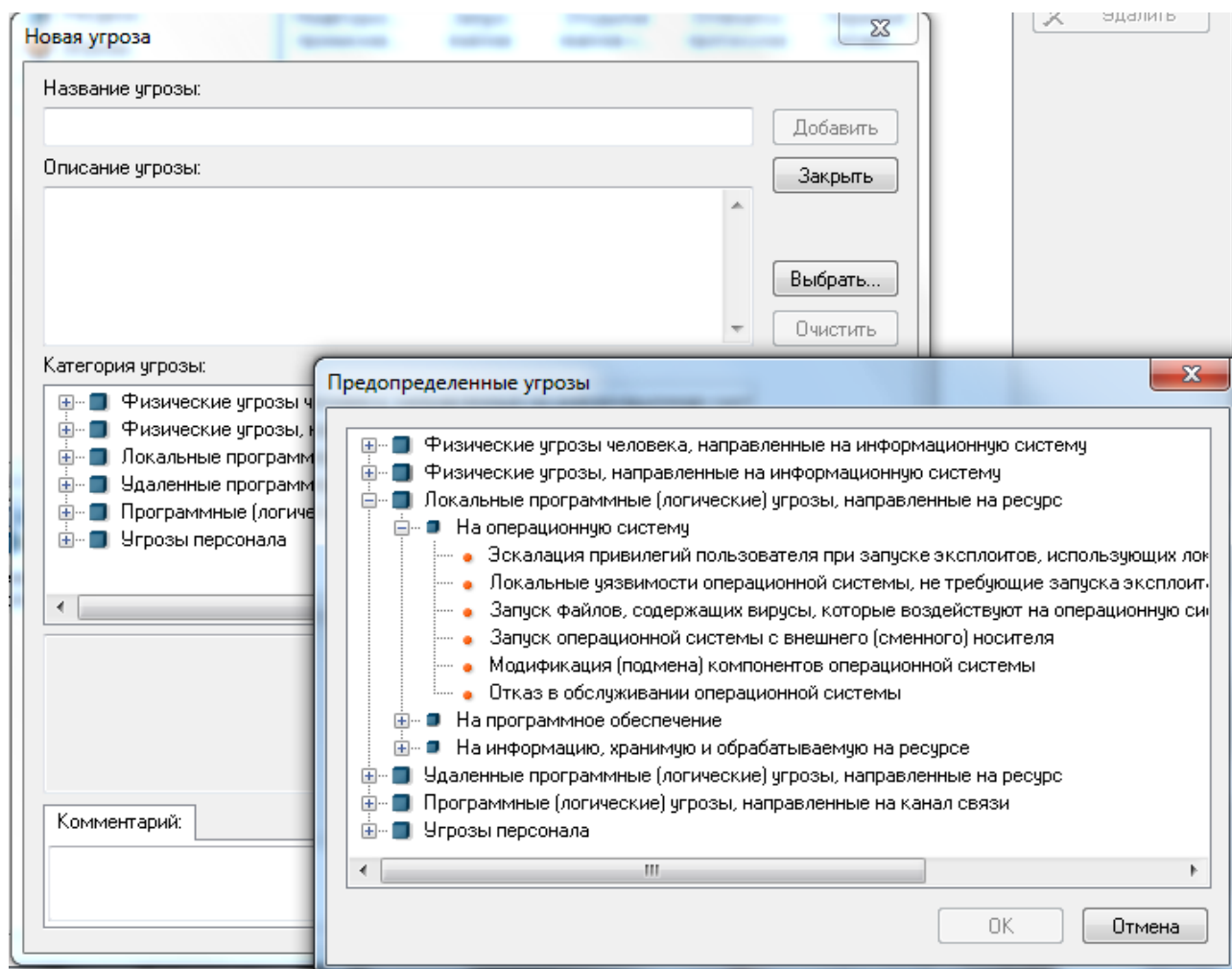


Рисунок 10 – Предопределенные угрозы

Шаг 2.

Далее пользователю необходимо проставить связи, то есть определить, к каким отделам относятся ресурсы, какие угрозы действуют на ресурс и через какие уязвимости они реализуются.

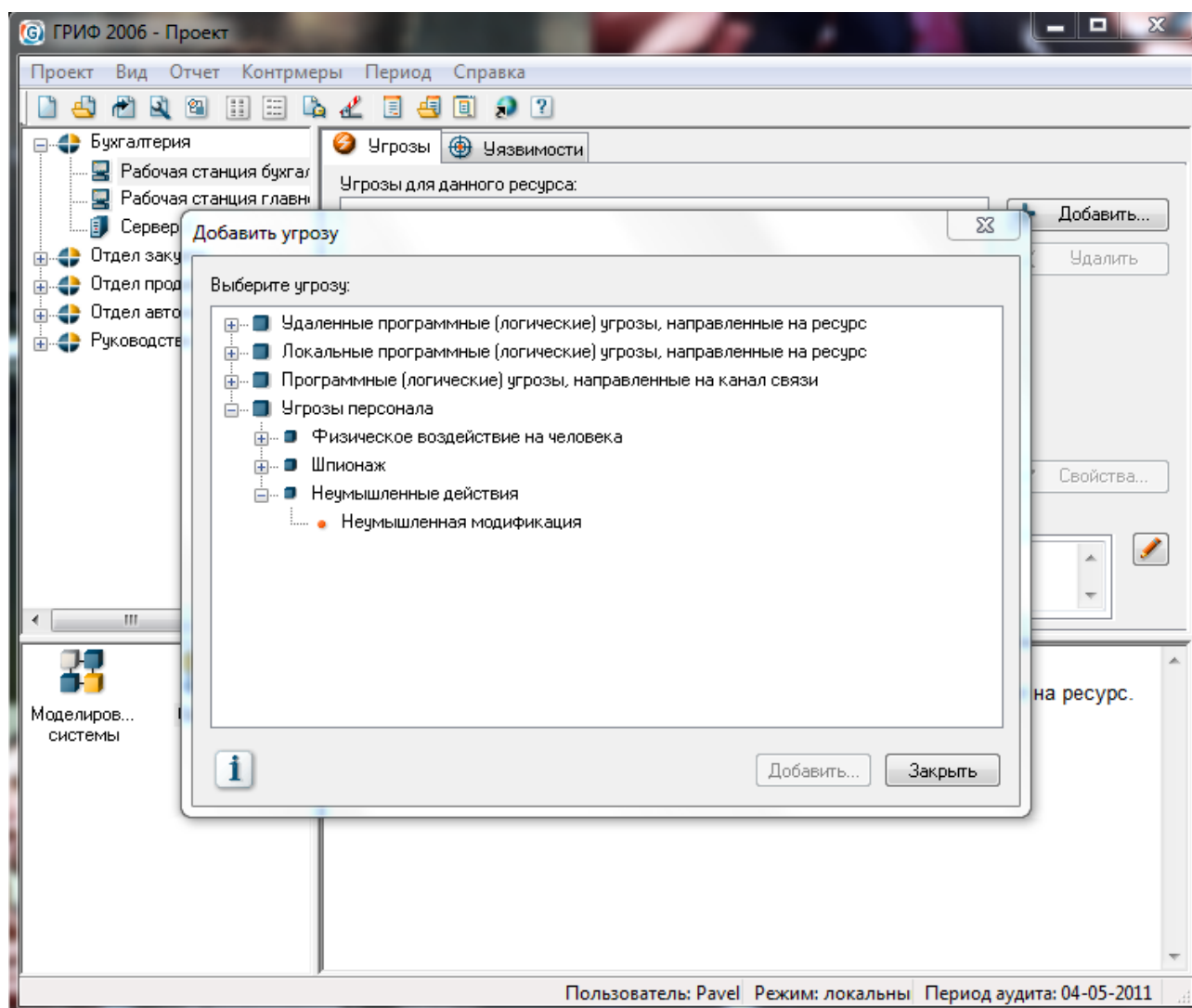


Рисунок 11 – Установка связей

Алгоритм системы ГРИФ анализирует построенную модель и генерирует отчет, который содержит значения риска для каждого ресурса. Конфигурации отчета может быть практически любой, таким образом позволяя пользователю создавать как краткие отчеты для руководства, так и детальные отчеты для дальнейшей работы с результатами.

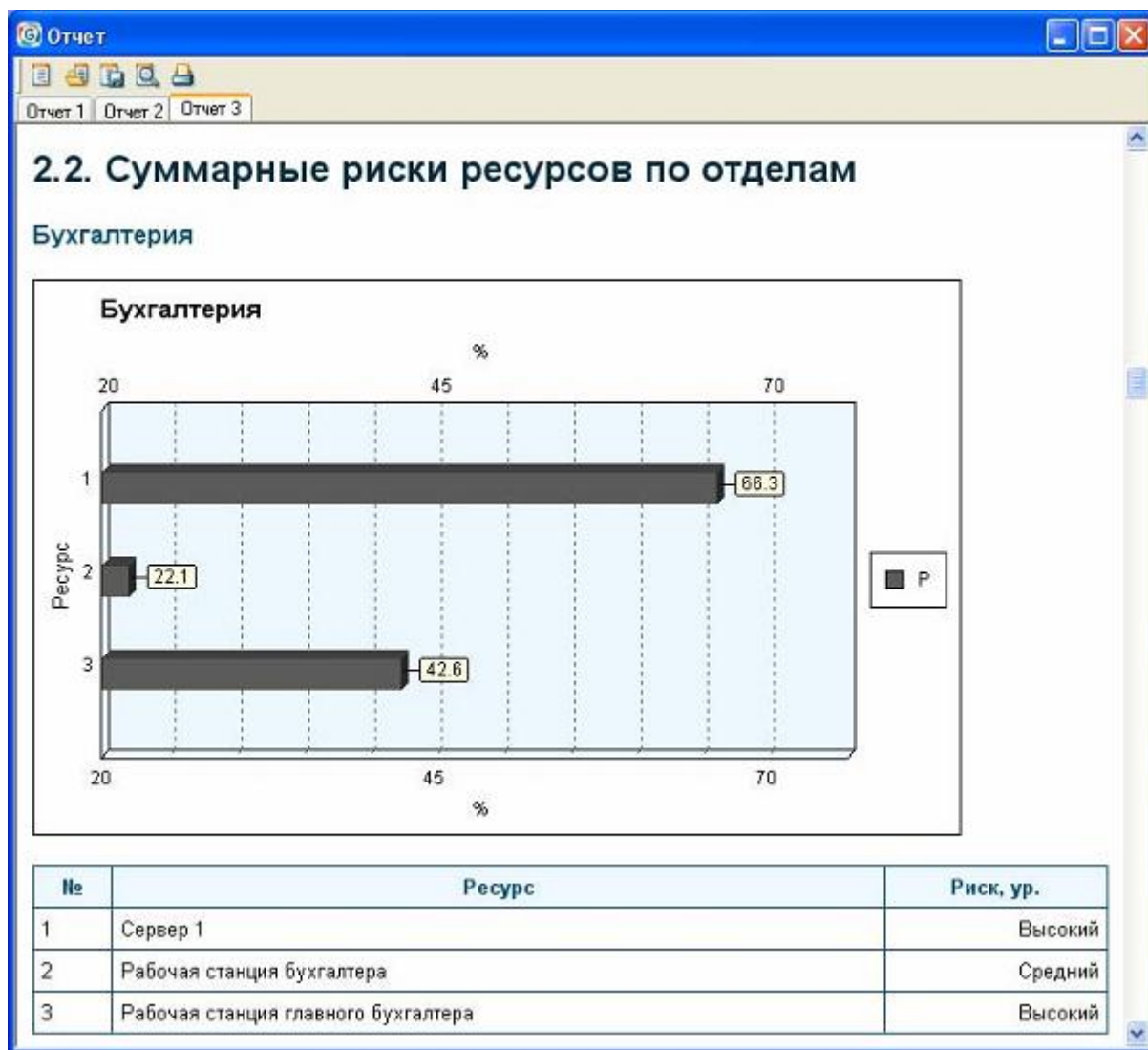


Рисунок 12 – Краткий отчет суммарных рисков ресурсов по отделу бухгалтерия

Система ГРИФ содержит модуль управления рисками, который позволяет проанализировать все причины того значения риска, который получается после обработки алгоритмом занесенных данных. Таким образом, зная причины, Вы будете обладать всеми данными, необходимыми для реализации контрмер и, соответственно, снижения уровня риска. Благодаря расчету эффективности каждой возможной контрмеры, а также определению значения остаточного риска, Вы сможете выбрать наиболее оптимальные контрмеры, которые позволят снизить риск до необходимого уровня с наименьшими затратами.

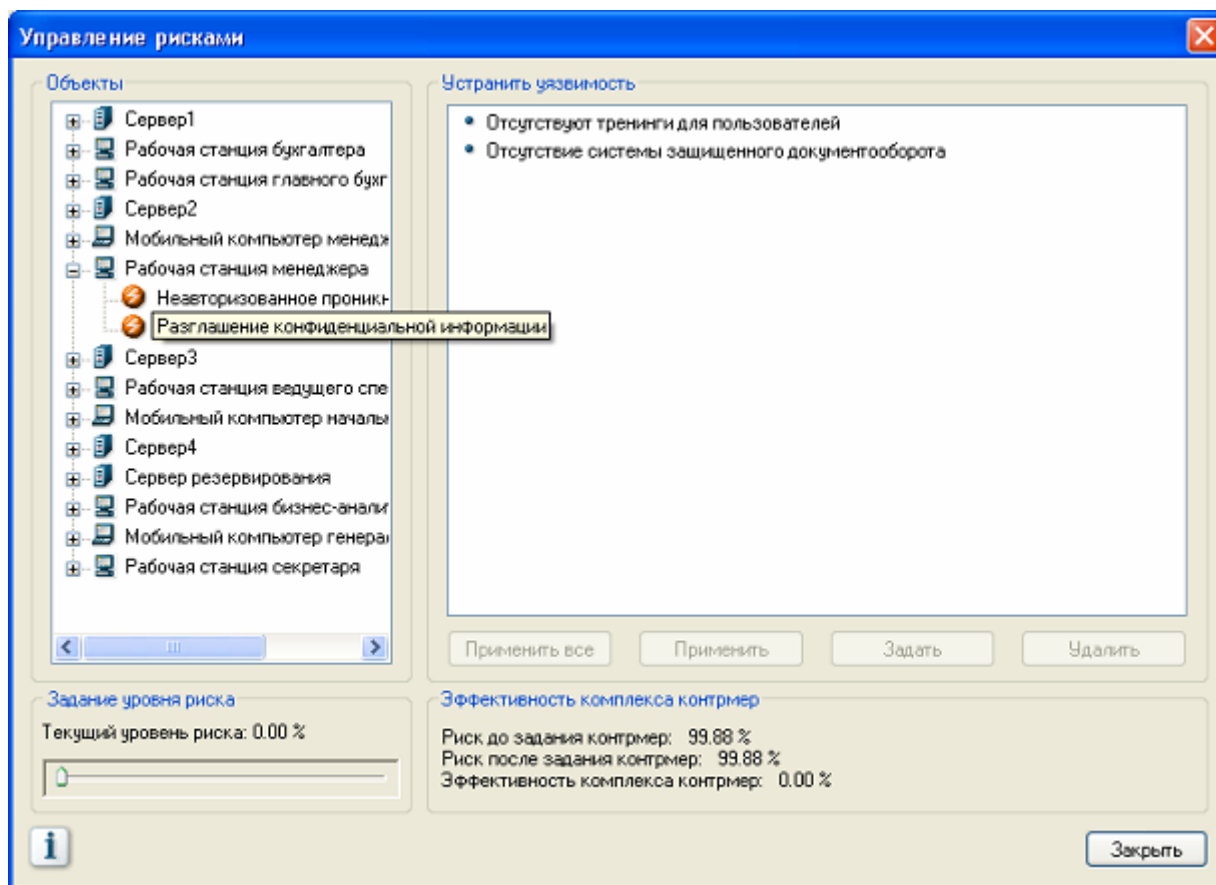


Рисунок 13 – Управление рисками

В результате работы с системой ГРИФ строится подробный отчет об уровне риска каждого ценного ресурса ИС компании, все причины риска с подробным анализом уязвимостей и оценкой экономической эффективности всех возможных контрмер.

Лабораторные работы

Лабораторная работа 1

Расчет рисков невыполнения требований стандарта ISO 17799 с помощью системы КОНДОР.

1. Цель работы

- 1.1. Теоретическое изучение функциональных возможностей системы разработки и управления политикой безопасности КОНДОР. Изучение алгоритма расчета рисков.
- 1.2. Практическое получение навыков работы с программой. Рассчитать риск невыполнения требований стандарта ISO 17799 в моделируемой ИС. Проанализировать полученные результаты. Смоделировать изменения, которые следует ввести в ИС для снижения риска до приемлемого уровня. Проанализировать изменения.

2. Подготовка к работе

Получить у преподавателя свой вариант на выполнение всех лабораторных работ. Согласно варианту в Приложении А к лабораторным работам найти описание моделируемой ИС и необходимые данные для выполнения работы

3. Задание

- 3.1. Ознакомиться с примером ручного расчета риска невыполнения требований стандарта ISO 17799.
- 3.2. Вручную рассчитать риск невыполнения требований стандарта ISO 17799 для раздела, согласно варианту.
- 3.3. Смоделировать ИС в программе КОНДОР.
- 3.4. Создание отчета.
- 3.5. Тестирование

4. Методика выполнения работы

К пункту 3.1

Таблица 5 – Требования и выполнения их в ИС компании, значения веса требований:

№	Требование стандарта ISO 17799	Вес	Выполнение
1	В ИС должна существовать политика безопасности	90	Выполнено
2	Политика безопасности должна утверждаться руководством организации	90	Выполнено
3	Политика безопасности должна доноситься до всех сотрудников в простой и понятной форме	70	Выполнено
4	Политика безопасности должна включать в себя	—	—
	1 Определение ИБ, ее основные цели и область ее применения, а также ее значение как механизма, позволяющего коллективно использовать информацию	70	Выполнено
	2 Позицию руководства по вопросам реализации целей и принципов ИБ	70	Выполнено

	3	Определение общих и конкретных обязанностей по обеспечению режима ИБ	90	Не выполнено
	4	Ссылки на документы, сопутствующие политике безопасности, например детализированные принципы безопасности и процедуры для специфичных ИС или правила для пользователей	70	Выполнено
5	Политика безопасности должна удовлетворять определенным требованиям		–	–
	1	Соответствовать государственному и международному законодательству	50	Не выполнено
	2	Содержать положения по обучению персонала вопросам безопасности	100	Не выполнено
	3	Включать инструкции предупреждения и обнаружения вредоносного программного обеспечения	90	Не выполнено
	4	Должны быть определены последствия нарушений положений политики безопасности	90	Выполнено
	5	Учитывать требования непрерывности ведения бизнеса	70	Не выполнено
6	Должен быть определен сотрудник, ответственный за процедуры пересмотра и обновления положений политики безопасности		90	Выполнено
7	Пересмотр положений политики безопасности обязательно должен проводиться в результате следующих случаев:		–	–
	1	Серьезных инцидентов в области ИБ	70	Выполнено
	2	Обнаружения новых уязвимостей	70	Выполнено
	3	Изменений в организационной или технической инфраструктуре организации	45	Выполнено
8	Регулярному пересмотру подлежат следующие характеристики политики безопасности:		–	–
	1	Эффективность политики безопасности, характеризуемая количеством и степенью влияния фиксируемых инцидентов в области ИБ	70	Не выполнено
	2	Стоимость и степень влияния контрмер на эффективность деятельности организации	70	Не выполнено
	3	Результаты технологических изменений	70	Выполнено

1) Максимальный риск невыполнения требований ISO 17799 равен сумме значений весов всех требований раздела:

$$R_{max} = 1435$$

- 2) Риск невыполнения требований ISO 17799 в компании равен отношению суммы значений весов невыполненных требований к сумме значений весов всех требований раздела стандарта.

$$R = \frac{540}{1435} \cdot 100\% = 37,7\%$$

Вывод: риск невыполнения требований ISO 17799 в компании составляет 37,7%, то есть данный раздел в компании выполнен больше чем на половину.

К пункту 3.2

- 1) Изменить весовые коэффициенты раздела, указанного в задании в соответствии с типом моделируемой системы. Проставить статус выполнения.
- 2) Рассчитать максимальный риск R_{\max} невыполнения требований.
- 3) Рассчитать сумму значений весов невыполненных требований.
- 4) Найти риск невыполнения требований R раздела ISO 17799.

К пункту 3.3

1. Открыть программу КОНДОР. Нажать кнопку «Создать проект...», если проект уже создан, то откройте его, нажав на кнопку «Открыть проект...»

Примечание: Проект создается один раз на все лабораторные работы.

2. Создание проекта:
 - 2.1. Введите название нового проекта.
3. Свойства проекта:
 - 3.1. На вкладке Проект перейдите в Свойства проекта/Идентификация. Введите название объекта, ответственного за выполнение работы пользователя и его должность.
 - 3.2. В текущем окне на вкладке Весовые коэффициенты измените весовые коэффициенты тех требований стандарта ISO 17799, которые, на Ваш взгляд, специфичны для моделируемой ИС.
4. Моделирование ИС:
 - 4.1. Ответьте на вопросы разделов стандарта ISO 17799. Укажите вопросы, которые неприменимы к моделируемой ИС (то есть вопросы, относящиеся к бизнес-процессам, которых не существует в компании).
 - 4.2. Введите затраты на обеспечение ИБ в компании. Стоимость некоторых средств обеспечения безопасности приведена в Приложении Б.
5. Отчет:
 - 5.1. Создайте отчет (Отчет/Создать отчет).
 - 5.2. Выберите структуру отчета и необходимые пункты
 - 5.3. Проанализируйте данные отчета.
6. Управление рисками:
 - 6.1. В разделе управление рисками (Контрмеры/Управление рисками) Задайте текущий уровень риска по отделам из отчета №1 и контрмеры к требованиям стандарта ISO 17799. Для этого внесите изменения в ИС, которые повлекут за собой выполнение требований стандарта ISO 17799 и уменьшение риска невыполнения требований. Введите стоимость внедрения контрмеры и возможное снижение затрат на ИБ (Приложение Б).

7. Отчет:

7.1. Создайте повторный отчет.

7.2. Проанализируйте, изменился ли риск при задании контрмер.

7.3. На сколько эффективны были введенные контрмеры и оправдываются ли затраты на них.

К пункту 3.4

Отчет по лабораторной работе должен содержать:

- данные и результаты ручного расчета;
- обоснование выбора весовых коэффициентов и статуса выполнения по разделам стандарта ISO 17799;
- экранные формы процесса выполнения работы;
- краткий первичный отчет программы и его анализ;
- задание контрмер их стоимость и обоснование выбора с конечным анализом второго отчета;
- выводы.

К пункту 3.5

Контрольные вопросы:

- 1) Что показывает риск невыполнения требований стандарта ISO 17799 и как его определить?
- 2) Какие действия необходимо выполнить для проведения анализа ИС на соответствие стандарту?
- 3) Что означает понятие «период аудита»?
- 4) Что показывает эффективность комплекса контрмер?
- 5) Какие виды отчетов доступны в программе КОНДОР?

Тестирование по лабораторной работе проходить на сайте <http://des.fpmt.vyatsu.ru/> в разделе «Основы информационной безопасности»

Лабораторная работа 2

Расчет и управление информационными рисками на основе модели информационных потоков с помощью системы ГРИФ.

1. Цель работы

- 1.1. Теоретическое изучение функциональных возможностей системы анализа защищенности ресурсов ГРИФ (Модель информационных потоков). Изучение алгоритма расчета рисков.
- 1.2. Практическое получение навыков работы с программой в режиме Модель информационных потоков. Расчет риска информационной системы на основе модели информационных потоков. Построение модели информационных потоков исследуемой ИС. Проанализировать полученные результаты и внести необходимые контрмеры в модель системы для снижения риска. Сделать выводы по результатам моделирования и управления рисками.

2. Подготовка к работе

Согласно варианту в Приложении А к лабораторным работам найти необходимые данные для своей ИС.

3. Задание

- 3.1. Ознакомиться с примером ручного расчета рисков информационной системы на основе модели информационных потоков.
- 3.2. Смоделировать ИС в программе ГРИФ Модель информационных потоков.
- 3.3. Написать отчет по проделанной работе.
- 3.4. Пройти тестирование.

4. Методика выполнения работы

К пункту 3.1

Пример расчета рисков информационной системы на основе модели информационных потоков

Исходные данные

Например, ИС компании состоит из двух ресурсов: сервера³ и рабочей станции, которые находятся в одной сетевой группе, то есть физически связаны между собой. На сервере хранятся виды информации: бухгалтерский отчет и база клиентов компании. На рабочей станции расположена база данных наименований товаров компании с описанием.

К серверу локальный доступ имеет группа пользователей (к первой информации – бухгалтерский отчет):

- главный бухгалтер.

К серверу удаленный доступ имеют группы пользователей (ко второй информации – база клиентов компании):

- бухгалтер (с рабочей станции);
- финансовый директор (через глобальную сеть Интернет).

³ При этом сервером в данном примере будем считать компьютер, на котором несколько папок открыты для удаленного доступа.

К рабочей станции локальный доступ имеет группа пользователей (к базе данных наименований товаров компании с описанием):

- бухгалтер.

По правилам работы модели бухгалтер при удаленном доступе к серверу является группой обычных пользователей, а финансовый директор – группой авторизованных пользователей. При чем, бухгалтер имеет удаленный доступ к серверу через коммутатор.

Средства защиты:

Таблица 6 – Средства защиты сервера:

Средство защиты	Вес средства защиты
Средства физической защиты	
Контроль доступа в помещение, где расположен ресурс (физическая охрана, дверь с замком, специальный пропускной режим в помещение)	25
Средства локальной защиты	
Отсутствие дисководов и USB портов	10
Средства корпоративной сетевой защиты	
Межсетевой экран	10
Обманная система	2
Система антивирусной защиты на сервере	10
Средства резервирования и контроля целостности	
Аппаратная система контроля целостности	20

Таблица 7 – Средства защиты первой информации (бухгалтерский отчет):

Средство защиты	Вес средства защиты
Средства локальной защиты	
Средства криптографической защиты (криптозащита данных на ПК)	20
Средства резервирования и контроля целостности	
Резервное копирование	10
Программная система контроля целостности	10

Средства защиты второй информации (база клиентов компании):

Средств защиты информации нет.

Таблица 8 – Средства защиты рабочей станции:

Средство защиты	Вес средства защиты
Средства физической защиты	

Контроль доступа в помещение, где расположен ресурс (дверь с замком, видео наблюдение)	10
Средства локальной защиты	
Средства антивирусной защиты (антивирусный монитор)	10
Отсутствие дисководов и USB портов	10
Средства персональной сетевой защиты	
Персональный межсетевой экран	3
Система криптозащиты электронной почты	10

Таблица 9 – Средства защиты информации (база данных наименований товаров компании с их описанием):

Средство защиты	Вес средства защиты
Средства резервирования и контроля целостности	
Резервное копирование	10
Программная система контроля целостности	10

Средства защиты клиентского места группы пользователей:

Таблица 10 – Средства защиты клиентского места бухгалтера (группа обычных пользователей):

Средство защиты	Вес средства защиты
Средства физической защиты	
Контроль доступа в помещение, где расположен ресурс (дверь с замком, видео наблюдение)	10
Средства локальной защиты	
Средства антивирусной защиты (антивирусный монитор)	10
Отсутствие дисководов и USB портов	10
Средства персональной сетевой защиты	
Персональный межсетевой экран	3
Система криптозащиты электронной почты	10

Таблица 11 – Средства защиты клиентского места главного бухгалтера (группа обычных пользователей):

Средство защиты	Вес средства защиты
Средства физической защиты	

Контроль доступа в помещение, где расположен ресурс (дверь с замком, видео наблюдение)	10
Средства локальной защиты	
Средства антивирусной защиты (антивирусный монитор)	10
Отсутствие дисководов и USB портов	10
Средства персональной сетевой защиты	
Персональный межсетевой экран	3
Система криптозащиты электронной почты	10

Средства защиты клиентского места финансового директора (группа авторизованных Интернет-пользователей):

Средства защиты клиентского места групп авторизованных Интернет-пользователей невозможно оценить, так как неизвестно, откуда будут осуществлять доступ пользователи этой группы.

Таблица 12 – Вид и права доступа групп пользователей к информации, наличие соединения через VPN, количество человек в группе:

	Вид доступа	Права доступа	Наличие VPN-соединения	Количество человек в группе
Главный бухгалтер / бухгалтерский отчет	локальный	чтение, запись, удаление	нет	1
Бухгалтер / база клиентов Компании	удаленный	чтение	есть	1
Финансовый директор / база клиентов Компании	удаленный	чтение, запись	есть	1
Бухгалтер / база данных наименований товаров Компании	локальный	чтение, запись, удаление	нет	1

Таблица 13 – Наличие у группы пользователей выхода в Интернет:

	Доступ в Интернет
Главный бухгалтер	Есть
Бухгалтер	Нет
Финансовый директор	Не анализируется ⁴

⁴ Доступ в Интернет групп пользователей, осуществляющих доступ к информации через Интернет, по понятным причинам не анализируется

Таблица 14 – Ущерб компании от реализации угроз ИБ:

	Конфиденциальность (у.е. в год)	Целостность (у.е. в год)	Доступность (у.е. в час)
Бухгалтерский отчет	100 у.е.	100 у.е.	1 у.е.
База клиентов Компании	100 у.е.	100 у.е.	1 у.е.
База данных наименований товаров Компании	100 у.е.	100 у.е.	1 у.е.

Наследование:

Так как сервер и рабочая станция компании находятся в одной сетевой группе, то есть физически соединены между собой, необходимо распространить наименьший, коэффициент защиты и наибольшую базовую вероятность группы Интернет-пользователей на все информации на всех ресурсах, входящих в сетевую группу.

Пример расчета рисков по угрозе конфиденциальность

1) Коэффициенты защищенности:

При локальном доступе к информации на ресурсе необходимо найти коэффициент локальной защищенности информации на ресурсе, который состоит из суммы весов средств физической и локальной защиты.

При удаленном доступе рассчитываем коэффициенты локальной защищенности рабочего места группы пользователей, имеющей доступ к информации, (сумма весов средств физической, локальной и персональной сетевой защиты) и удаленной защищенности информации на ресурсе (сумма весов средств корпоративной сетевой защиты). В дальнейших расчетах участвует наименьший коэффициент.

При локальном и удаленном доступе находим все три коэффициента, из которых также выбираем наименьший.

Расчет рисков по угрозе конфиденциальность:

Таблица 15 – Коэффициенты защищенности:

	Коэффициент локальной защищенности информации	Коэффициент удаленной защищенности информации	Коэффициент локальной защищенности рабочего места группы пользователей	Наименьший коэффициент
Главный бухгалтер / бухгалтерский отчет	55	-	-	55
Бухгалтер / база клиентов Компании	-	22	43	22

Финансовый директор / база клиентов Компании	-	22	-	22
Бухгалтер / база данных наименований товаров Компании	30	-	-	30

2) Учет наличия доступа при помощи VPN:

При локальном доступе наличие VPN не анализируется. При удаленном доступе, при использовании VPN, к наименьшему коэффициенту защищенности прибавляется вес VPN шлюза (20). Если при удаленном доступе VPN-соединение не используется для групп Интернет-пользователей, итоговый коэффициент защищенности умножается на 4, для групп обычных пользователей (не Интернет-пользователей) – остается неизменным.

Таблица 16 – Учет VPN соединения

	Наименьший коэффициент	Вес VPN-соединения	Результирующий коэффициент
Главный бухгалтер / бухгалтерский отчет	55	-	55
Бухгалтер / база клиентов Компании	22	20	42
Финансовый директор / база клиентов Компании	22	20	42
Бухгалтер / база данных наименований товаров Компании	30	-	30

3) Учет количества человек в группе и наличия у группы пользователей доступа в Интернет.

Таблица 17 – Учет количества человек

	Результирующий коэффициент	Количество человек в группе пользователей	Наличие у группы пользователей доступа в Интернет	Итоговый коэффициент
Главный бухгалтер / бухгалтерский отчет	55	1	2	0,036

Бухгалтер / база клиентов Компании	42	1	1	0,024
Финансовый директор / база клиентов Компании	42	1	-	0,024
Бухгалтер / база данных наименований товаров Компании	30	1	1	0,033

Если к информации имеет доступ группа пользователей, превышающая 50 человек, то это соответственно увеличивает итоговый коэффициент.

Если группа пользователей имеет доступ в Интернет, то это увеличивает итоговый коэффициент в 2 раза.

Пример расчета итогового коэффициента: $K = \frac{1 \cdot 2}{55} = 0.036$

4) Итоговая вероятность:

Чтобы получить итоговую вероятность, необходимо определить базовую вероятность и умножить ее на итоговый коэффициент.

Таблица 18 – Итоговая вероятность

	Базовая вероятность	Итоговая базовая вероятность	Итоговый коэффициент	Промежуточная вероятность	Итоговая вероятность
Главный бухгалтер / бухгалтерский отчет	0,35	0,7	0,036	0,0252	0,0252
Бухгалтер / база клиентов Компании	0,35	0,7	0,024	0,0168	0,0331
Финансовый директор / база клиентов Компании	0,7	0,7	0,024	0,0168	
Бухгалтер / база данных наименований товаров Компании	0,35	0,7	0,033	0,0231	0,0231

Так как к информации на ресурсе, находящейся в сетевой группе, имеют доступ группа Интернет-пользователей, их базовая вероятность распространяется на все информации.

Итоговая вероятность для второй информации, к которой имеют доступ несколько групп пользователей, рассчитываем по формуле:

$$P_{inf} = 1 - \prod_{i=1}^n (1 - P_{ug,n}).$$

5) Риск по угрозе конфиденциальность

Таблица 19 – Риск конфиденциальности

	Итоговая вероятность	Ущерб от реализации угрозы	Риск
Бухгалтерский отчет	0,0252	100	2,52
База клиентов Компании	0,0331	100	3,31
База данных наименований товаров Компании	0,0231	100	2,31

Пример расчета рисков по угрозе целостность

- 1) Первый пункт вычисляется аналогично расчету по угрозе конфиденциальность.
- 2) Учет средств резервирования и контроля целостности

Таблица 20 – Учет средств резервирования и контроля целостности

	Наименьший коэффициент	Вес VPN- соединения	Веса средств резервирования и контроля целостности	Результирующий коэффициент
Главный бухгалтер / бухгалтерский отчет	55	-	40	95
Бухгалтер / база клиентов Компании	22	20	20	62
Финансовый директор / база клиентов Компании	22	20	20	62
Бухгалтер / база данных наименований товаров Компании	30	-	20	50

3) Учет наличия резервного копирования, количества человек в группе пользователей и наличия у группы пользователей доступа в Интернет:

Таблица 21 – Подсчет итогового коэффициента

	Результирующий коэффициент	Наличие резервного копирования	Количество человек в группе пользователей	Наличие у группы пользователей доступа в Интернет	Итоговый коэффициент
Главный бухгалтер / бухгалтерский отчет	95	1	1	2	0,021
Бухгалтер / база клиентов Компании	62	1	1	1	0,016
Финансовый директор / база клиентов Компании	62	4	1	-	0,065
Бухгалтер / база данных наименований товаров Компании	50	1	1	1	0,02

Наличие резервного копирования учитывается следующим образом: если у информации на ресурсе осуществляется резервное копирование, то вес резервного копирования (10) прибавляется к коэффициенту защищенности. Если у информации на ресурсе резервное копирование не осуществляется, и группе пользователей, имеющей доступ к информации, разрешены запись или удаление, то итоговый коэффициент увеличивается в 4 раза.

4) Аналогично расчету по угрозе конфиденциальность получим итоговую вероятность:

Таблица 22 – Итоговая вероятность

	Базовая вероятность	Итоговая базовая вероятность	Итоговый коэффициент	Промежуточная вероятность	Итоговая вероятность
Главный бухгалтер / бухгалтерский отчет	0,25	0,7	0,021	0,0147	0,0147
Бухгалтер /	0,1	0,7	0,016	0,0112	0,05619

база клиентов Компании					
Финансовый директор / база клиентов Компании	0,7	0,7	0,065	0,0455	
Бухгалтер / база данных наименований товаров Компании	0,25	0,7	0,02	0,014	0,014

5) Риск по угрозе целостность

Таблица 23 – Риск целостности

	Итоговая вероятность	Ущерб от реализации угрозы	Риск
Бухгалтерский отчет	0,0147	100	1,47
База клиентов Компании	0,05619	100	5,61
База данных наименований товаров Компании	0,014	100	1,4

Пример расчета рисков по угрозе отказ в обслуживании

Расчет рисков по угрозе доступность

1) Расчет коэффициента защищенности по угрозе доступность

При расчете рисков по угрозе доступность анализируются средства резервирования: кластер, резервное копирование и резервный канал. Влияние резервного канала учитывается в том случае, если группа обычных пользователей (не Интернет-пользователей) имеет только удаленный доступ к информации на ресурсе.

Таблица 24 – Учет резервного копирования и резервного канала

	Кластер		Резервное копирование		Резервный канал	
	Есть	нет	есть	нет	есть	Нет
Запись и Удаление	20	Const	4	Увеличивается в 5 раз	5	Const
Удаление	20	Const	4	Увеличивается в 4 раз	5	Const
Запись	20	Const	4	Увеличивается в 4 раз	5	Const
Чтение	40	Const	4	Увеличивается в 2 раз	5	Const

Таблица 25 – Расчет итогового коэффициента

	Коэффициент защищенности	Наличие у группы пользователей доступа в Интернет	Итоговый коэффициент
Главный бухгалтер / бухгалтерский отчет	0,25	2	0,5
Бухгалтер / база клиентов Компании	2	1	2
Финансовый директор / база клиентов Компании	4	-	4
Бухгалтер / база данных наименований товаров Компании	0,25	1	0,25

2) Расчет итогового времени простоя

Таблица 26 – Расчет времени простоя

	Базовое время простоя	Итоговое базовое время простоя	Время простоя сетевого оборудования	Итоговый коэффициент	Промежуточное время простоя	Итоговое время простоя
Главный бухгалтер / бухгалтерский отчет	40	70	-	0,5	35	35
Бухгалтер / база клиентов Компании	40	70	10	2	140	280
Финансовый директор / база клиентов Компании	70	70	-	4	280	
Бухгалтер / база данных наименований товаров Компании	40	40	-	0,25	10	10

При расчете рисков по угрозе доступность базовые времена простоя наследуются только в пределах ресурса.

Время простоя сетевого оборудования добавляется к итоговому времени простоя.

Если итоговое время простоя превышает максимально критичное (280 часов в год по базовым настройкам), оно приравнивается к максимально критичному времени простоя.

Для второй информации на сервере, к которой имеют доступ несколько групп пользователей, итоговое время простоя рассчитывается по следующей формуле:

$$T_{inf} = \left(1 - \prod_{i=1}^n \left(1 - \frac{T_{ug,n}}{T_{max}}\right)\right) \times T_{max}$$

3) Расчет рисков

Таблица 27 – Расчет рисков по угрозе отказ в обслуживании

	Итоговое время простоя	Ущерб от реализации угрозы	Риск
Бухгалтерский отчет	35	1	35
База клиентов Компании	280	1	280
База данных наименований товаров Компании	10	1	10

К пункту 3.2

1. Открыть программу ГРИФ. Выбрать алгоритм «Анализ модели информационных потоков». Открыть ранее созданный проект, нажав кнопку «Открыть проект...», либо создайте новый проект, если его еще нет.
2. Открытие проекта:
 - 2.1. Выберите название проекта.
3. Свойства проекта:
 - 3.1. На вкладке Проект перейдите в Свойства проекта/Идентификация. Введите название объекта, ответственного за выполнение работы пользователя и его должность.
 - 3.2. На вкладке Уровни выберите уровни. Измените значения эффективности средств защиты, которые специфичны для моделируемой ИС, на вкладке Средства защиты.
4. Раздел «Моделирование системы»:
 - 4.1. Занесите отделы компании.
 - 4.2. Укажите сетевые группы компании, соответствующие отделам компании, то есть все ресурсы отдела входят в одну сетевую группу.
 - 4.3. Занесите ресурсы компании, укажите к какому отделу и сетевой группе относятся ресурсы согласно исходным данным.
 - 4.4. Занесите сетевое оборудование, с помощью которого пользователи получают доступ к информации.
 - 4.5. Занесите сведения о группах пользователей, согласно исходным данным.
 - 4.6. Укажите виды информации, которая хранится и обрабатывается на ресурсах ИС (следует указать не менее 7 видов информации, например, бухгалтерский отчет, сведения о поставщиках, сведения о зарплатах и так далее).
 - 4.7. Укажите бизнес-процессы, в которых обрабатывается информация.
 - 4.8. Введите расходы на ИБ из Приложения Б.
5. Раздел «Связи»
 - 5.1. Для каждого ресурса в ИС укажите, какая информация хранится или обрабатывается на нем.
 - 5.2. Укажите, какие пользователи имеют доступ к хранимой или обрабатываемой на ресурсе информации и вид доступа пользователей (следует учесть, что группы

обычных пользователей (пользователи, менеджеры, топ-менеджеры) могут иметь локальный доступ только к одной рабочей станции или к одному мобильному компьютеру).

- 5.3. Укажите, используя, какие каналы связи каждая группа пользователей осуществляет доступ к информации, хранимой или обрабатываемой на ресурсе.
- 5.4. Укажите, в каких бизнес-процессах обрабатывается информация.
- 5.5. Укажите средства защиты для каждого ресурса. Значение эффективности средств защиты можно посмотреть в «Свойствах проекта».
- 5.6. Укажите средства защиты информации, хранимой или обрабатываемой на ресурсе.
6. Раздел «Политика Безопасности»
 - 6.1. Ответьте на вопросы, учитывающие организационные меры обеспечения ИБ, то есть аспекты, которые невозможно отобразить при построении модели ИС. Укажите вопросы, которые неприменимы к моделируемой ИС, (то есть вопросы, относящиеся к бизнес-процессам, которых не существует в компании).
7. Отчет:
 - 7.1. Создайте отчет (Отчет/ создать отчет).
 - 7.2. Выберите структуру отчета и необходимые пункты.
 - 7.3. Проанализируйте результаты.
8. Управление рисками:
 - 8.1. Смоделируйте установку дополнительных средств защиты в моделируемой ИС.
 - 8.2. Запретите некоторым группам пользователей доступ к видам информации.
 - 8.3. Для каждого вида информации смоделируйте установку дополнительных средств защиты информации.
 - 8.4. Обратите внимание на эффективность комплекса контрмер и на снижение риска после задания контрмер.
9. Отчет:
 - 9.1. Создайте повторный отчет.
 - 9.2. Проанализируйте, изменился ли риск при задании контрмер.
10. Управление рисками
 - 10.1. Исходя из полученных результатов, внедрите в модель ИС некоторые самые значимые изменения ИС.
11. Отчет
 - 11.1. Создайте отчет.
 - 11.2. Проанализируйте риски в ИС.

К пункту 3.3

Отчет по лабораторной работе должен содержать:

- данные и результаты ручного расчета;
- обоснование выбора эффективности специфичных средств защиты;
- экранные формы процесса выполнения работы;
- краткие отчеты программы до и после введения контрмер;
- анализ рисков в ИС по отчетам;
- выводы.

К пункту 3.4

Контрольные вопросы:

- 1) Сформулируйте определение «информационная система».
- 2) Какие категории средств защиты выделяются в системе ГРИФ?
- 3) Дайте определение «контрмера».
- 4) Каким образом учитывается понятие наследования?
- 5) Перечислите шаги проведения анализа информационных рисков.

Тестирование по лабораторной работе проходить на сайте <http://des.fpmt.vyatsu.ru/> в разделе «Основы информационной безопасности»

Лабораторная работа 3

Расчет рисков информационной системы на основе модели угроз и уязвимостей системы ГРИФ.

1. Цель работы

- 1.1. Изучение функциональных возможностей системы анализа защищенности ресурсов ГРИФ (Модель угроз и уязвимостей). Изучение двух вариантов работы алгоритма расчета рисков.
- 1.2. Практическое получение навыков работы с программой в режиме Модель угроз и уязвимостей. Расчет риска информационной системы на основе модели угроз и уязвимостей. Построение модели угроз и уязвимостей исследуемой ИС. Анализ и вынесение рекомендаций по модификации ИС с целью уменьшения угроз.

2. Подготовка к работе

Согласно варианту в Приложении А к лабораторным работам найти необходимые данные для своей ИС.

3. Задание

- 3.1. Ознакомиться с примером ручного расчета рисков информационной системы на основе модели угроз и уязвимостей.
- 3.2. Смоделировать ИС в программе ГРИФ Модель угроз и уязвимостей.
- 3.3. Написать отчет по проделанной работе.
- 3.4. Пройти тестирование.

4. Методика выполнения работы

К пункту 3.1

Пример расчета рисков информационной системы на основе модели угроз и уязвимостей

Рассмотрим расчет рисков для одного ресурса ИБ, так как для остальных риск рассчитывается аналогично.

Таблица 28 – Исходные данные

Ресурс	Угрозы	Уязвимости
Сервер (критичность ресурса 100 у.е.)	Угроза 1 Неавторизованное проникновение нарушителя внутрь охраняемого периметра (одного из периметров)	Уязвимость 1 Отсутствие регламента доступа в помещения с ресурсами, содержащими ценную информацию
		Уязвимость 2 Отсутствие системы наблюдения (видеонаблюдение, сенсоры и т.д.) за объектом (или существующая система наблюдения охватывает не все важные объекты)

	Угроза 2	Уязвимость 1
	Неавторизованная модификация информации в системе электронной почты, хранящейся на ресурсе	Отсутствие авторизации для внесения изменений в систему электронной почты
		Уязвимость 2
		Отсутствие регламента работы с системой криптографической защиты электронной корреспонденции
	Угроза 3	Уязвимость 1
	Разглашение конфиденциальной информации сотрудниками компании	Отсутствие соглашений о конфиденциальности
		Уязвимость 2
		Распределение атрибутов безопасности (ключи доступа, шифрования) между несколькими доверенными сотрудниками

Таблица 29 – Значение вероятности и критичности для связки угроза – уязвимость

Угроза/Уязвимость	Вероятность реализации угрозы через данную уязвимость в течение года $P(V)$, %	Критичность реализации угрозы ER, %
Угроза 1/Уязвимость 1	50	60
Угроза 1/Уязвимость 2	20	60
Угроза 2/Уязвимость 1	60	40
Угроза 2/Уязвимость 2	10	40
Угроза 3/Уязвимость 1	10	80
Угроза 3/Уязвимость 2	80	80

Решение

Таблица 30 – Уровень угрозы

Угроза/Уязвимость	Уровень угрозы Th $Th = \frac{ER}{100} \times \frac{P(V)}{100}$	Уровень угрозы по всем уязвимостям, через которые реализуется данная угроза CTh $CTh = 1 - \prod_{i=1}^n (1 - Th_i)$
Угроза 1/Уязвимость 1	0,3	0,384
Угроза 1/Уязвимость 2	0,12	
Угроза 2/Уязвимость 1	0,24	0,270

Угроза 2/Уязвимость 2	0,04	0,669
Угроза 3/Уязвимость 1	0,08	
Угроза 3/Уязвимость 2	0,64	

Таблица 31 – Общий уровень угроз, действующих на ресурс

Угроза/Уязвимость	Уровень угрозы по всем уязвимостям, через которые реализуется данная угроза $CTh = 1 - \prod_{i=1}^n (1 - Th_i)$	Общий уровень угроз по ресурс CThR $CThR = 1 - \prod_{i=1}^n (1 - CTh_i)$
Угроза 1/Уязвимость 1	0,384	0,8511
Угроза 1/Уязвимость 2		
Угроза 2/Уязвимость 1	0,270	
Угроза 2/Уязвимость 2		
Угроза 3/Уязвимость 1	0,669	
Угроза 3/Уязвимость 2		

Критичность ресурса (ущерб, который понесет компания от потери ресурса) – 100 у.е.

Таблица 32 – Риск ресурса в денежных единицах

Угроза/Уязвимость	Общий уровень угроз по ресурсу CThR $CThR = 1 - \prod_{i=1}^n (1 - CTh_i)$	Риск ресурса R, у.е. $R = CThR \times D$
Угроза 1/Уязвимость 1	0,8511	85,11
Угроза 1/Уязвимость 2		
Угроза 2/Уязвимость 1		
Угроза 2/Уязвимость 2		
Угроза 3/Уязвимость 1		
Угроза 3/Уязвимость 2		

Таким образом, получим риск ресурса, рассчитанный по модели угроз и уязвимостей.

Риск ресурса в уровнях (процентах)

Критичность ресурса D – 4 уровень (по 5-уровневой шкале).

Шкала:



1 уровень – 20%;

- 2 уровень – 40%;
- 3 уровень – 60%;
- 4 уровень – 80%;
- 5 уровень – 100%.

D = 80%.

Таблица 33 – Расчет риска ресурса по модели угроз и уязвимостей

Угроза/Уязвимость	Общий уровень угроз по ресурсу CThR $CThR = 1 - \prod_{i=1}^n (1 - CTh_i)$	Риск ресурса R, у.е. $R = CThR \times D$
Угроза 1/Уязвимость 1	0,8511	0.8511×80=68,088 68,088%=4 уровень
Угроза 1/Уязвимость 2		
Угроза 2/Уязвимость 1		
Угроза 2/Уязвимость 2		
Угроза 3/Уязвимость 1		
Угроза 3/Уязвимость 2		

К пункту 3.2

1. Открыть программу ГРИФ. Выбрать алгоритм «Анализ модели угроз и уязвимостей». Открыть ранее созданный проект, нажав кнопку «Открыть проект...», либо создайте новый проект, если его еще нет.
2. Открытие проекта:
 - 2.1. Выберите название проекта.
3. Свойства проекта
 - 3.1. На вкладке Проект перейдите в Свойства проекта/Идентификация. Введите название объекта, ответственного за выполнение работы пользователя и его должность.
 - 3.2. Выберите уровни, оценку критичности и единицы измерения по своему усмотрению.
4. Раздел «Моделирование системы»:
 - 4.1. Занесите отделы компании.
 - 4.2. Занесите ресурсы компании, укажите, к каким отделам они относятся, в свойствах ресурса укажите критичность ресурса.
 - 4.3. Выберите из списка predetermined угрозы, действующие на информационную систему (не менее 10 угроз).
 - 4.4. Самостоятельно введите уязвимости (не выбирая из списка predetermined уязвимостей), укажите угрозы, которые реализуют введенные уязвимости.
 - 4.5. Введите расходы на ИБ (Приложение Б).
5. Раздел «Связи»:
 - 5.1. Укажите, какие угрозы действуют на каждый ресурс и уязвимости, через которые реализуются угрозы, так, чтобы в расчетах участвовали все введенные угрозы и уязвимости.
 - 5.2. Укажите вероятность угрозы через данную уязвимость.

- 5.3. Укажите критичность реализации угрозы.
6. Отчет:
- 6.1. Создайте отчет (Отчет/Создать отчет).
 - 6.2. Выберите структуру отчета и необходимые пункты.
 - 6.3. Проанализируйте данные отчета.
7. Управление рисками:
- 7.1. Задайте контрмеры к угрозам (Контрмеры/Управление рисками). Для этого устраните некоторые уязвимости, введите стоимость внедрения контрмеры и возможное снижение затрат на ИБ.
8. Отчет:
- 8.1. Создайте повторный отчет.
 - 8.2. Проанализируйте, изменился ли риск при задании контрмер.
 - 8.3. При необходимости, проделайте процедуру управления рисками еще раз.

К пункту 3.3

Отчет по лабораторной работе должен содержать:

- данные и результаты ручного расчета;
- обоснование выбора уязвимостей и угроз в ИС;
- экранные формы процесса выполнения работы;
- краткие отчеты программы до и после управления рисками;
- анализ рисков в ИС по отчетам;
- выводы.

К пункту 3.4

Контрольные вопросы:

- 1) Дайте определение риска ИБ.
- 2) Дайте определение угрозы ИБ.
- 3) Напишите и поясните формулу для расчета уровня угрозы по уязвимости T_h для режима с одной базовой угрозой.
- 4) Сформулируйте основную задачу инженерно-технических средств защиты.
- 5) Как вы понимаете принцип «четырех глаз» и как на практике можно его реализовать.

Тестирование по лабораторной работе проходить на сайте <http://des.fpmt.vyatsu.ru/> в разделе «Основы информационной безопасности»

Приложение А
Варианты для лабораторных работ

Таблица 34 - Варианты моделей информационных систем и дополнительные данные

№ варианта	Название модели	Дополнительные данные к лабораторной работе №1
1	Учебно-методический центр	Раздел «Контроль доступа»
2	Оптово-розничная торговля	Раздел «Физическая безопасность»
3	Подразделение государственного учреждения	Раздел «Организационные меры»
4	Строительная фирма	Раздел «Управление коммуникациями и процессами»

Описание моделей:

ИС «Учебно-методический центр»

1. Условия расположения основных составляющих ИС
 - 1.1. ИС расположена на 1 этаже 2 этажного здания.
 - 1.2. Вход в помещение осуществляется по пропускам через вахтера.
 - 1.3. Охрану помещения осуществляет охранное предприятие.
 - 1.4. Кабинеты, в которых расположена ИС, оборудованы охранно-пожарной сигнализацией.
 - 1.5. Двери оборудованы замками.
 - 1.6. Окна помещения оборудованы жалюзи.
2. Топология ИС и конфигурация её отдельных компонентов.
 - 2.1. Центральный узел обработки данных
Сервер с базой данных 1С Бухгалтерия на ОС Microsoft Windows Server 2003 R2. Антивирус Касперского 6.0 для Windows Workstation. В ИС используется один центральный узел обработки данных, который расположен в отдельном кабинете.
 - 2.2. Автоматизированные рабочие места (АРМ) персонала.
Осуществляют ввод и обработку данных в ИС. ОС Microsoft Windows XP Professional SP2 и средство антивирусной защиты Антивирус Касперского 6.0 для Windows Workstation. Используется 8 АРМ персонала установленных в отдельном кабинете.
 - 2.3. Автоматизированные рабочие места (АРМ) учеников.
Осуществляют ввод данных в ИС. ОС Microsoft Windows XP Professional SP2 и средство антивирусной защиты Антивирус Касперского 6.0 для Windows Workstation. Тридцать АРМ учеников установлены в трех отдельных кабинетах.
3. Перечень обрабатываемых данных:
 - данные о сотрудниках;
 - данные об учащихся;
 - бухгалтерия;
 - данные учебного процесса;
 - данные администрирования сети.
4. Связи между основными компонентами ИС.
 - 4.1. Физические связи.

Структура информационного взаимодействия в ИС реализована на основе собственной одноранговой локальной Сети передачи данных. За пределы контролируемой зоны локально-вычислительная сеть не выходит. Имеет одноточечное подключение к сетям связи общего пользования и сетям международного информационного обмена через сеть провайдера, и имеет следующие физические связи:

- оборудование ИС подключено при помощи ADSL модема к сегменту сети провайдера;
- в каждом кабинете АРМ объединены в сеть через концентраторы;
- все АРМ объединены в сеть и имеют выход в интернет через активное сетевое оборудование производства Cisco.

4.2. Технологические связи.

В процессе обработки данных в ИС используются следующие технологии:

- данные хранятся на центральном узле обработки данных в специально предназначенной для этого СУБД (1С Бухгалтерия);
- ПО, обеспечивающее передачу персональных данных от конечного периферийного оборудования до СУБД, работает по протоколу TCP/IP.

4.3. Функциональные связи.

Введенные на АРМ сотрудников данные пересылаются непосредственно на центральный узел обработки данных и загружаются оттуда.

5. Режим и степень участия пользователей в обработке данных.

Обработка данных во всех компонентах ИС осуществляется в многопользовательском режиме. Для ограничения доступа к информационной системе, на автоматизированных рабочих местах активирована функция входа в систему по паролю средствами операционной системы Windows XP.

5.1. Пользователи, участвующие в обработке данных.

- Администратор сети (1 человек) осуществляет настройку сетевых устройств и сервисов, входящих в ИС, отвечает за настройку и бесперебойную работу сетевого оборудования. Администратор сети вправе проводить техническое обслуживание и настройку АРМ сотрудников, осуществлять контроль за антивирусной защитой. Администратор занимается обслуживанием и настройкой средств защиты информации в ИС, осуществляет разграничение доступа в защищенную инфраструктуру ИС, развертывание и настройку СЗИ в рамках ИС, а так же имеет полный доступ к данным администрирования сети.
- Директор (1 человек) не имеет полномочий вносить модификации в настройки какого-либо оборудования, но способен вводить и удалять записи из 1С Бухгалтерия в рамках базы данных о работниках и учащихся.
- Бухгалтер (1 человек) не имеет полномочий вносить модификации в настройки какого-либо оборудования, но способен вводить и удалять записи из БД 1С Бухгалтерия в рамках данных бухгалтерии, а так же имеет право чтения данных о работниках и учащихся.
- Преподаватель (5 человек) не имеет полномочий вносить модификации в настройки какого-либо оборудования, но способен вводить и удалять записи из БД 1С в рамках данных учебного процесса, а так же чтение данных об учащихся.
- Ученик (50 человек) не имеет полномочий вносить модификации в настройки какого-либо оборудования, но способен читать записи БД 1С Бухгалтерия в рамках данных учебного процесса. Так же учащийся имеет право авторизованного доступа к данным учебного процесса удаленно через интернет.

6. Прочие данные о системе.

- 6.1. Для восстановления операционной системы и средств защиты, входящей в ее состав используются лицензионные дистрибутивные программы MS Windows и MS Office.
- 6.2. Резервное копирование информации с рабочих мест производится системным администратором на съемные дисковые накопители информации.
- 6.3. Все работы с автоматизированной системой, в том числе обновление программного обеспечения, антивирусных баз, ремонт, модернизация АС проводятся администратором сети и отражаются в журнале учета работ с автоматизированной системой.

ИС «Оптово-розничная торговля»

1. Условия расположения основных составляющих ИС
 - 1.1. ИС расположена на 1 этаже 2 этажного здания.
 - 1.2. Вход в помещение осуществляется по электронным пропускам через турникет и вахтера.
 - 1.3. Охрану помещения осуществляет охранное предприятие.
 - 1.4. Кабинеты, в которых расположена ИС, оборудованы охранно-пожарной сигнализацией.
 - 1.5. Двери оборудованы замками.
 - 1.6. Окна помещения оборудованы жалюзи.
 - 1.7. Удаленный одноэтажный склад находится в промышленной зоне города.
 - 1.8. Ворота склада оборудованы замком.
 - 1.9. Охрану периметра складской зоны осуществляет охранное предприятие.
2. Топология ИС и конфигурация её отдельных компонентов.
 - 2.1. Центральный узел обработки данных
Сервер с базой данных 1С Бухгалтерия на ОС Microsoft Windows Server 2008. Антивирус Kaspersky Enterprise Space Security. В ИС используется один центральный узел обработки данных, который расположен в кабинете отдела технического обеспечения.
 - 2.2. Автоматизированные рабочие места (АРМ) персонала.
Осуществляют ввод и обработку данных в ИС. ОС Microsoft Windows Seven и средство антивирусной защиты Kaspersky Enterprise Space Security. Используется 9 АРМ персонала установленных в кабинетах отдела технического обеспечения, руководства, отдела закупок и продаж и на складе.
 - 2.3. Мобильный компьютер администратора сети.
Осуществляет ввод и обработку данных в ИС. ОС Microsoft Windows Seven и средство антивирусной защиты Kaspersky Enterprise Space Security. Используется один мобильный компьютер, имеющий доступ к сети через зашифрованное wi-fi соединение из любой точки здания.
3. Перечень обрабатываемых данных:
 - зарплатные начисления;
 - документы товарооборота;
 - данные о сотрудниках;
 - данные о клиентах;
 - коммерческая тайна о стратегии развития предприятия;
 - данные о товарах;
 - данные администрирования сети;
 - документация на пожарно-охранную сигнализацию.
4. Связи между основными компонентами ИС.
 - 4.1. Физические связи.

Структура информационного взаимодействия в ИС реализована на основе собственной одноранговой локальной Сети передачи данных. Имеет одноточечное подключение к сетям связи общего пользования и сетям международного информационного обмена через сеть провайдера, и имеет следующие физические связи:

- удаленный АРМ менеджера по продажам 2 на складе подключен сети internet через оператора сотовой связи;
- оборудование ИС подключено при помощи ADSL модема к сегменту сети провайдера;
- все АРМ и мобильный компьютер головного офиса объединены в сеть и имеют выход в интернет через активное сетевое оборудование маршрутизатор производства D-Link.

4.2. Технологические связи.

В процессе обработки данных в ИС используются следующие технологии:

- удаленный АРМ менеджера по продажам на складе подключен к локальной СПД по технологии Intranet VPN через сеть internet провайдера;
- данные хранятся на центральном узле обработки данных в специально предназначенной для этого СУБД;
- ПО, обеспечивающее передачу персональных данных от конечного периферийного оборудования до СУБД, работает по протоколу TCP/IP.

4.3. Функциональные связи.

Введенные на АРМ сотрудников данные пересылаются непосредственно на центральный узел обработки данных и загружаются оттуда.

5. Режим и степень участия пользователей в обработке данных.

Обработка данных во всех компонентах ИС осуществляется в многопользовательском режиме. Для ограничения доступа к информационной системе, на автоматизированных рабочих местах и мобильном компьютере активирована функция входа в систему по паролю средствами операционной системы Windows Seven.

5.1. Пользователи, участвующие в обработке данных.

- Администратор сети (1 человек) осуществляет настройку сетевых устройств и сервисов, входящих в ИС, отвечает за настройку и бесперебойную работу сетевого оборудования. Администратор сети вправе проводить техническое обслуживание и настройку АРМ сотрудников, осуществлять контроль за антивирусной защитой. Администратор занимается обслуживанием и настройкой средств защиты информации в ИС, осуществляет разграничение доступа в защищенную инфраструктуру ИС, развертывание и настройку СЗИ в рамках ИС, а так же имеет полный доступ к данным администрирования сети.
- Начальник отдела технического обеспечения (1 человек) осуществляет контроль работоспособности систем пожарно-охранной сигнализации, инженерно-технических средств защиты, отвечает за проведение мероприятий по обучению сотрудников информационной и физической безопасности предприятия. Имеет доступ к документации на пожарно-охранную сигнализацию.
- Директор (1 человек) не имеет полномочий вносить модификации в настройки какого-либо оборудования, но способен вводить и удалять записи из БД в рамках базы данных о работниках и стратегии развития предприятия, данных о клиентах.
- Бухгалтер (1 человек) не имеет полномочий вносить модификации в настройки какого-либо оборудования, но способен вводить и удалять записи из БД в рамках данных зарплатных начислений, документации товарооборота, а так же имеет право чтения данных о работниках.

- Два начальника отделов закупок и продаж, менеджер по закупкам и два менеджера по продажам (5 человек) не имеют полномочий вносить модификации в настройки какого-либо оборудования, но способен вводить и удалять записи из БД в рамках данных документов товарооборота, данных о клиентах, данных о товарах.
6. Прочие данные о системе.
- 6.1. Для восстановления операционной системы и средств защиты, входящей в ее состав используются лицензионные дистрибутивные программы MS Windows.
- 6.2. Резервное копирование информации с рабочих мест производится автоматически в конце рабочего дня средствами программы Acronis Backup & Recovery.
- 6.3. Все работы с автоматизированной системой, в том числе обновление программного обеспечения, антивирусных баз, ремонт, модернизация АС проводятся администратором сети и отражаются в журнале учета работ с автоматизированной системой.

ИС «Подразделение государственного учреждения»

1. Условия расположения основных составляющих ИС
- 1.1. ИС расположена на 1 и 2 этажах 2 этажного здания.
- 1.2. Здание обнесено забором, оборудованным периметральными средствами обнаружения проникновения и закрывающимися воротами.
- 1.3. Вход в помещение осуществляется по электронным пропускам через турникет и вахтера.
- 1.4. Охрану помещения осуществляет охранное предприятие.
- 1.5. Кабинеты, в которых расположена ИС, оборудованы охранно-пожарной сигнализацией.
- 1.6. Двери оборудованы электронными замками.
- 1.7. Окна помещения оборудованы жалюзи.
- 1.8. Окна первого этажа оборудованы решетками с защитой от спиливания.
2. Топология ИС и конфигурация её отдельных компонентов.
- 2.1. Центральный узел хранения данных
Осуществляет хранение данных. ОС Microsoft Server 2003 R2 и средство антивирусной защиты Norton Internet Security 2011. Сервер расположен в кабинете службы безопасности.
- 2.2. Автоматизированные рабочие места (АРМ).
Осуществляют ввод и обработку данных в ИС. ОС Microsoft Windows XP Professional SP2 и средство антивирусной защиты Norton Internet Security 2011. Используется 2 АРМ в кабинете начальника подразделения (начальник, секретарь), 6 АРМ в кабинете привилегированных сотрудников (5 сотрудников, секретарь), 4 АРМ в кабинете специалистов по работе с населением (3 сотрудника, секретарь), 2 АРМ в кабинете службы безопасности (администратор сети, офицер безопасности подразделения). Корпусы всех АРМ опечатаны, возможность подключения внешних носителей информации имеет только администратор сети.
3. Перечень обрабатываемых данных:
- персональные данные сотрудников;
 - персональные данные клиентов;
 - документы служебного пользования;
 - документы секретного характера;
 - данные администрирования сети;
 - данные сетевой безопасности;
 - документация пожарно-охранной сигнализации.
4. Связи между основными компонентами ИС.

4.1. Физические связи.

Структура информационного взаимодействия в ИС реализована на основе собственной одноранговой локальной Сети передачи данных. За пределы контролируемой зоны локально-вычислительная сеть не выходит. Имеет подключение к ЛВС головного офиса. Имеет подключение к сетям связи общего пользования и сетям международного информационного обмена через ЛВС головного офиса, и имеет следующие физические связи:

- все АРМ объединены в сеть и имеют выход в интернет через активное сетевое оборудование маршрутизатор производства Cisco;
- маршрутизатор данной ЛВС подключен к маршрутизатору ЛВС головного офиса через оптоволоконный кабель.

4.2. Технологические связи.

В процессе обработки данных в ИС используются следующие технологии:

- ПО, обеспечивающее передачу данных по сети, работает по протоколу TCP/IP;
- для защиты передаваемых данных используется протокол IPsec.

4.3. Функциональные связи.

Введенные на АРМ сотрудников данные пересылаются непосредственно на центральный узел обработки данных и загружаются оттуда.

5. Режим и степень участия пользователей в обработке данных.

Обработка данных во всех компонентах ИС осуществляется в однопользовательском режиме. Для ограничения доступа к информационной системе, на автоматизированных рабочих местах активирована функция входа в систему по паролю средствами операционной системы Windows XP. Аутентификация пользователя на сервере для возможности обмена данными реализована средствами программного обеспечения Secret Disk Server NG.

5.1. Пользователи, участвующие в обработке данных.

- Администратор сети (1 человек) осуществляет настройку сетевых устройств и сервисов, входящих в ИС, отвечает за настройку и бесперебойную работу сетевого оборудования. Администратор сети вправе проводить техническое обслуживание и настройку АРМ сотрудников, осуществлять контроль за антивирусной защитой. Имеет полный доступ к данным администрирования сети.
- Офицер безопасности (1 человек) занимается обслуживанием и настройкой средств защиты информации в ИС, осуществляет разграничение доступа в защищенную инфраструктуру ИС, развертывание и настройку СЗИ в рамках ИС, а так же имеет полный доступ к данным сетевой безопасности и документации пожарно-охранной сигнализации.
- Начальник подразделения (1 человек) не имеет полномочий вносить модификации в настройки какого-либо оборудования. Имеет полный доступ к данным о сотрудниках, клиентах, документам служебного пользования, секретного характера.
- Привилегированный сотрудник (5 человек) не имеет полномочий вносить модификации в настройки какого-либо оборудования. Имеет полный доступ к данным клиентов, документам для служебного пользования, способен читать данные секретного характера.
- Специалист (3 человека) не имеет полномочий вносить модификации в настройки какого-либо оборудования, но имеет полный доступ к данным о клиентах и документам служебного пользования.

- Секретарь (3 человека) не имеет полномочий вносить модификации в настройки какого-либо оборудования, но способен читать данные о клиентах и документы служебного пользования.
6. Прочие данные о системе.
- 6.1. Для резервного копирования данных на съемные дисковые накопители информации в конце рабочей смены и восстановления операционной системы и средств защиты, входящей в ее состав используются лицензионные дистрибутивные программы Acronis Backup & Recovery.
- 6.2. Все работы с автоматизированной системой, в том числе обновление программного обеспечения, антивирусных баз, ремонт, модернизация АС проводятся администратором сети и отражаются в журнале учета работ с автоматизированной системой.

ИС «Строительная фирма»

1. Условия расположения основных составляющих ИС
- 1.1. ИС расположена на 2 этаже многоэтажного здания.
- 1.2. Вход в здание в рабочее время свободный.
- 1.3. Вход в офис осуществляется по электронным пропускам.
- 1.4. Охрану помещения осуществляет охранный предприятие.
- 1.5. Кабинеты, в которых расположена ИС, оборудованы охранно-пожарной сигнализацией.
- 1.6. Двери оборудованы замками.
2. Топология ИС и конфигурация её отдельных компонентов.
- 2.1. Узел хранения данных
- Сервер хранения данных на ОС Microsoft Windows Server 2008. Антивирус Kaspersky Enterprise Space Security. В ИС используется два узла хранения данных, которые располагаются в кабинете администрации и рабочем кабинете.
- 2.2. Автоматизированные рабочие места (АРМ) персонала.
- Осуществляют ввод и обработку данных в ИС. ОС Microsoft Windows Seven и средство антивирусной защиты Kaspersky Enterprise Space Security. Используется 11 АРМ персонала установленных в кабинете администрации (директор, бухгалтер, менеджер по работе с клиентами, менеджер по работе с подрядными организациями) и кабинете отдела разработок (3 дизайнера, 3 проектировщика, специалист АСУ).
- 2.3. Мобильный компьютер администратора сети.
- Осуществляет ввод и обработку данных в ИС. ОС Microsoft Windows Seven и средство антивирусной защиты Kaspersky Enterprise Space Security. Используется два мобильных компьютера, используемых менеджерами по работе с клиентами и по работе с подрядными организациями при выездах на объекты.
3. Перечень обрабатываемых данных:
- ПДн персонала;
 - ПДн клиентов;
 - данные о подрядных организациях;
 - данные администрирования сети;
 - бухгалтерия предприятия;
 - дизайнерские разработки;
 - проектные разработки;
 - данные об объектах;
 - коммерческая тайна о стратегии развития предприятия.

4. Связи между основными компонентами ИС.

4.1. Физические связи.

Структура информационного взаимодействия в ИС реализована на основе собственной одноранговой локальной Сети передачи данных. Имеет одноточечное подключение к сетям связи общего пользования и сетям международного информационного обмена через сеть провайдера, и имеет следующие физические связи:

- оборудование ИС подключено при помощи ADSL модема к сегменту сети провайдера;
- все АРМ объединены в сеть и имеют выход в интернет через активное сетевое оборудование маршрутизатор производства D-Link;
- два мобильных компьютера подключены к сети internet через оператора сотовой связи.

4.2. Технологические связи.

В процессе обработки данных в ИС используются следующие технологии:

- мобильные компьютеры подключаются к локальной СПД по технологии Intranet VPN через сеть internet провайдера;
- дизайнеры и проектировщики могут подключаться к локальной СПД из дома по технологии Intranet VPN через сеть internet провайдера;
- данные хранятся на серверах хранения данных в специально предназначенной для этого БД;
- ПО, обеспечивающее передачу персональных данных от конечного периферийного оборудования до СУБД, работает по протоколу TCP/IP.

4.3. Функциональные связи.

Данные с серверов могут быть загружены на АРМ сотрудников и мобильные компьютеры и после всех операций загружаются на сервер.

5. Режим и степень участия пользователей в обработке данных.

Для ограничения доступа к информационной системе, на автоматизированных рабочих местах и мобильном компьютере активирована функция входа в систему по паролю средствами операционной системы Windows Seven.

5.1. Пользователи, участвующие в обработке данных.

- Специалист АСУ (1 человек) осуществляет настройку сетевых устройств и сервисов, входящих в ИС, отвечает за настройку и бесперебойную работу сетевого оборудования. Администратор сети вправе проводить техническое обслуживание и настройку АРМ сотрудников, осуществлять контроль за антивирусной защитой. Администратор занимается обслуживанием и настройкой средств защиты информации в ИС, осуществляет разграничение доступа в защищенную инфраструктуру ИС, развертывание и настройку СЗИ в рамках ИС, а так же имеет полный доступ к данным администрирования сети.
- Директор (1 человек) не имеет полномочий вносить модификации в настройки какого-либо оборудования. Имеет полный доступ ко всем данным кроме администрирования сети и к бухгалтерии только чтение.
- Бухгалтер (1 человек) не имеет полномочий вносить модификации в настройки какого-либо оборудования. Имеет полный доступ к бухгалтерии и чтению ПДн персонала.
- Дизайнер (3 человека) не имеет полномочий вносить модификации в настройки какого-либо оборудования. Имеет полный доступ к дизайнерским разработкам и чтению данных об объектах.

- Проектировщик (3 человека) не имеет полномочий вносить модификации в настройки какого-либо оборудования. Имеет полный доступ к проектным разработкам и чтению данных об объектах.
- Менеджер по работе с клиентами (1 человек) не имеет полномочий вносить модификации в настройки какого-либо оборудования. Имеет полный доступ к данным о клиентах и чтению данных об объектах, дизайнерских и проектных разработках.
- Менеджер по работе с подрядными организациями (1 человек) не имеет полномочий вносить модификации в настройки какого-либо оборудования. Имеет полный доступ к данным о подрядных организациях и чтению данных об объектах, дизайнерских и проектных разработках.

6. Прочие данные о системе.

- 6.1. Для восстановления операционной системы и средств защиты, входящей в ее состав используются лицензионные дистрибутивные программы MS Windows.
- 6.2. Резервное копирование информации с рабочих мест производится автоматически в конце рабочего дня средствами программы Acronis Backup & Recovery.

Приложение Б

Средства обеспечения информационной безопасности

Таблица 35 – Стоимость некоторых средств обеспечения информационной безопасности.

Название	Описание	Цена
ПО		
Лицензия на использование Secret Disk 4. Базовый комплект.	Система защиты конфиденциальной информации и персональных данных шифрованием, хранящихся и обрабатываемых на персональном компьютере, с возможностью защиты системного раздела и двухфакторной аутентификацией пользователя до загрузки ОС.	4 720
Лицензия на использование Secret Disk Server NG для файлового сервера на N пользователей (одновременных подключений). Базовый комплект.	Система защиты корпоративной конфиденциальной информации (баз данных, файловых архивов, бизнес-приложений и их данных) шифрованием, хранящейся и обрабатываемой на серверах.	N = 5 18 000
		N = 10 35 000
		N = 25 45 000
		N = 50 60 000
Лицензия на использование Secret Disk Server NG для сервера приложений. Базовый комплект.	Поставка включает USB-ключ eToken PRO/32K с лицензией на использование Secret Disk Server NG для сервера приложений, USB-ключ eToken PRO/32 с лицензией администратора Secret Disk Server NG, дистрибутив продукта, комплект документации, устройство "красная кнопка" для подачи сигнала "тревога", удлинительный USB-кабель с присоской.	38 000
Kaspersky Enterprise Space Security	<p>Антивирус, монитор, Firewall, антиспам, криптозащита почты, обнаружение атак</p> <p>Защищает: рабочие станции, смартфоны, файловые и почтовые серверы</p> <p>Решение для защиты рабочих станций, смартфонов и серверов совместной работы от всех видов современных интернет-угроз; удаляет вирусы из потока электронной почты, обеспечивает сохранность информации и безопасный доступ пользователей к сетевым ресурсам.</p> <p>Произвольное количество рабочих станций, смартфонов и почтовых ящиков</p>	23 100
Norton Internet Security 2011	Защита от вирусов, защита от программ-шпионов, защита от фишинга, защита от спама, защита от руткитов, защита от ботов, защита идентификационных данных, интеллектуальный брандмауэр, схема сети и мониторинг, импульсные обновления, эвристическая защита SONAR 3	N = 1 1 590
		N = 5 4 490
Dallas Lock 7.5	<p>Запрет загрузки компьютера посторонними лицам.</p> <p>Двухфакторная авторизация по паролю и аппаратным идентификаторам (USB eToken, Touch Memory) до загрузки ОС.</p> <p>Разграничение прав пользователей на доступ к локальным и сетевым ресурсам.</p> <p>Контроль работы пользователей со сменными накопителями.</p> <p>Мандатный и дискреционный принципы разграничения прав.</p>	12 500

	Организация замкнутой программной среды. Аудит действий пользователей. Контроль целостности ресурсов компьютера. Очистка остаточной информации. Возможность автоматической печати штампов (меток конфиденциальности) на всех распечатываемых документах. Защита содержимого дисков путем прозрачного преобразования.	
Acronis® Backup & Recovery	Решение для локального аварийного восстановления и защиты серверов под управлением Windows.	27 000
Аппаратные средства		
Wi-Fi точка доступа, маршрутизатор D-Link DIR-320	Маршрутизатор с межсетевым экраном	1600
Маршрутизатор D-link DFL-210	Ethernet router с VPN каналами	9 700
Коммутатор HP ProCurve Switch 2510-24	24 x Ethernet Switch	12 200
Концентратор HUB ACORP HU8D	8 портовый hub	470
ZyXEL P660RT3 EE	ADSL модем	1 000
Инженерно-технические средства и прочие средства защиты		
Бедж	Идентификатор персонала	10*N
ГШ-1000М	Генератор радишума, предназначен для защиты от утечки информации по каналам ПЭМИН, 0,1-1000 МГц	7 930
Соната-Р2	Устройство защиты объектов информатизации от утечки информации за счет ПЭМИ, 1-2000 МГц; сети электропитания и заземления 0,1 – 1000 МГц	12 980
Фаза-1-10	Фильтр сетевой для предотвращения утечки информации от ПЭВМ и других технических средств передачи информации по цепям электропитания напряжение 100-240В, 50-60 Гц. Нагрузочная способность до 200 ВА. Количество подключаемых потребителей – 3	12 000
Соната-РК1	Устройство комбинированной защиты объектов информатизации от утечки информации за счет ПЭМИН, 0,01-1000 МГц	14 986
Гном-3М	Широкополосный генератор шума для защиты от утечки информации по каналам ПЭМИН и цепям первичного электропитания, 0,01 - 1000 МГц	18 460
Барон-S1	Комплекс виброакустической защиты	33 500
Корунд	Защита ТЛФ линий	826
УБМ-1	Устройство блокирования несанкционированного включения микрофонов цифрового телефонного аппарата	3 900
Грот	Телефонный скремблер	10 000
Огнестойкий сейф VALBERG	Огнеупорный сейф. Электронный кодовый замок + ключ	6 290
Генератор SDMO Pacific T 6 KM	Резервный дизель генератор	275 173
Охрана		
Турникет «КРОНБЕРК»	Контроль посетителей периметра (фото, время, по аутентификатору)	32 500
Дверь	Дверь с замком	От 2 000
INTEGRA 24 P	Плата INTEGRA 24. 4 зоны, расширение до 24, 8 программируемых выходов (2 по 1А и 2 по 50mA), 1 раздел, 4	2 952

	подраздела, 16 системных таймеров, 16 паролей пользователя, 4 телефонных номера для оповещения, 16 голосовых (1 СА-64SM) и 16 пейджерных сообщений, память на 899 событий, трансформатор, отсек для АКБ 7.0 А/ч	
INTEGRA 32 P	Плата INTEGRA 32. 8 зон, расширение до 32, 8 программируемых выходов (2 по 1А и 6 по 50mA), 4 раздела, 16 подразделов, 32 системных таймеров, 64 паролей пользователя, 8 телефонных номера для оповещения, 16 голосовых (1 СА-64SM) и 32 пейджерных сообщений, память на 899 событий, трансформатор, отсек для АКБ 7.0 А/ч	3 327
INTEGRA 64 P	Плата INTEGRA 64. 16 зон, расширение до 64, 16 программируемых выходов (4 по 2А и 12 по 50mA), 8 разделов, 32 подраздела, 64 системных таймеров, 192 паролей пользователя, 16 телефонных номера для оповещения, 16 голосовых (1 СА-64SM) и 64 пейджерных сообщений, память на 6143 события, трансформатор, отсек для АКБ 7-17.0 А/ч	4 956
INTEGRA 128 P	Плата INTEGRA 128. 16 зон, расширение до 128, 16 программируемых выходов (4 по 2А и 12 по 50mA), 8 разделов, 32 подраздела, 64 системных таймеров, 240 паролей пользователя, 16 телефонных номера для оповещения, 32 голосовых (2 СА-64SM) и 64 пейджерных сообщений, память на 22527 событий, трансформатор, отсек для АКБ 7-17.0 А/ч	5 328
INTEGRA 128 WRL	Приемно-контрольный прибор INTEGRA 128 WRL с беспроводным интерфейсом ABAX и GSM/GPRS коммунитором, 2 антенны ANT-S, в корпусе OPU-3 без трансформатора	14 490
CA-64 PTSA	Модуль светодиодной индикации состояния 64 зон и 32 подразделов, RS-232	5 511
CA-64 E	Блок расширения, 8 зон	1 176
GPRS-T1	Модуль для передачи сигналов мониторинга полученных от ПКП в форматах ContactID, по каналам GPRS/SMS	4 401
AQUA PLUS	цифровой микропроцессорный инфракрасный датчик, сдвоенный пироэлемент, отличается высокой чувствительностью и устойчивостью к помехам	363
COBALT PRO	совмещенный датчик - счетверенный пироэлемент и микроволновый сенсор, антимаскинг	531
INDIGO	цифровой извещатель разбития стекла (нормального, армированного и многослойного), двухканальный (низкая частота - звук удара, высокая частота - звук разбитого стекла)	477
VD-1	Вибрационный извещатель с магнитоконтактным датчиком	1 293
ACTIVA-7	Активный ИК-барьер (7-лучевой), дальность до 20 м (до 10 м вне помещений), кронштейн для параллельной или перпендикулярной установки на стену, оптическая и звуковая сигнализация, облегчающая установку устройства	11 565
K-1	датчик магнитоконтактный накладной, пластмассовый корпус, поверхностный монтаж - самоклеящаяся лента или шурупы, длина 24,2мм, ширина 7,2мм, белый	126
PNK-1	Тревожная кнопка с механической памятью	252
SPW-220	Сирена внутренняя 120 дБ, 12VDC, светодиодный проблесковый маяк	681
SP-500	Внешняя сирена 115 дБ, проблесковый маяк - лампа накаливания 5Вт/12В, звук 120mA, маяк 130mA, -35°C...+60°C, 300x190x86мм	1 065
Проект	Проект охранной сигнализации	от 10 000
Обслуживание	Обслуживание охранной сигнализации	от 2 600 /мес.
Видеонаблюдение		

Миниатюрная видеокамера	Миниатюрная видеокамера - цилиндрическая. Устанавливается внутри помещений. Средние размеры: d=20 мм; L=50мм	1 350
Купольная видеокамера	Купольная видеокамера. Устанавливается в помещениях на поверхности потолка. Благодаря элегантному дизайну отлично вписывается в любой интерьер. Средние размеры: d=80 мм; h=80мм	1 800
Уличная видеокамера	Уличная видеокамера. Поставляется в корпусе с подогревом, встроенным несъемным объективом и кронштейном. Обычно более экономичное решение, чем стандартная корпусная камера в термокожухе, но качество изображения тоже ниже. Средние размеры: d=40 мм; L=100мм	2 900
Видеорегистратор	Законченное устройство видеорегистратора со встроенным жестким диском	4 канала - от 9 900 8 каналов - от 15 980 16 каналов - от 26 450
ББП-20	Блок бесперебойного питания	2 030
Пуско-наладка	Установка и наладка системы видеонаблюдения	От 10 000

Библиографический список

1. Алгоритм расчета рисков невыполнения требований стандарта ISO 17799 [Электронный ресурс]. – СПб.: Режим доступа: <http://dsec.ru/products/kondor/fulldesc/algorithm/>, свободный. – Загл. с экрана.
2. Куканова, Н. Методика оценки риска ГРИФ 2006 из состава Digital Security Office [Электронный ресурс]. – СПб. Режим доступа: http://dsec.ru/about/articles/grif_ar_methods/, свободный. – Загл. с экрана.